

Figure 1

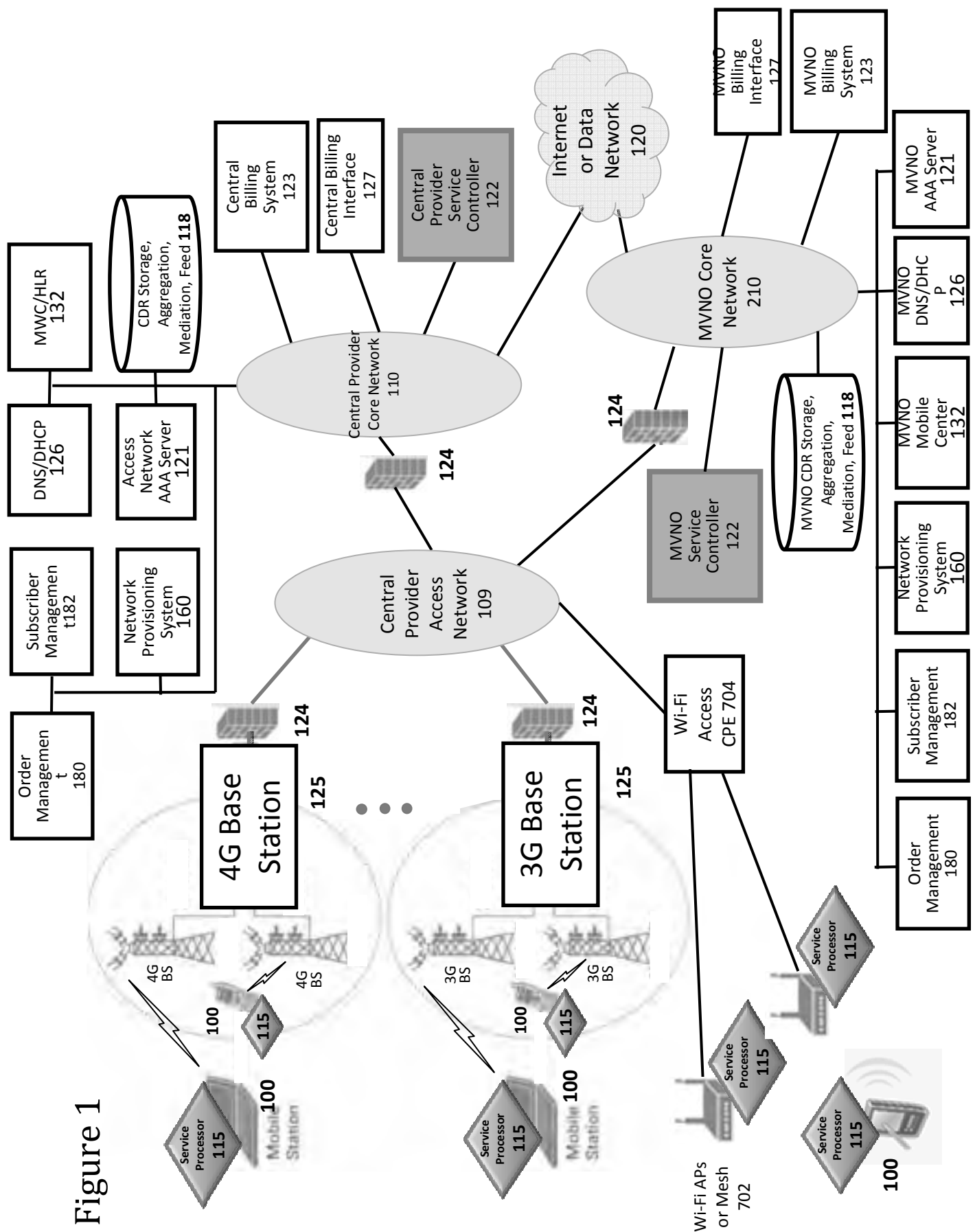


Figure 2

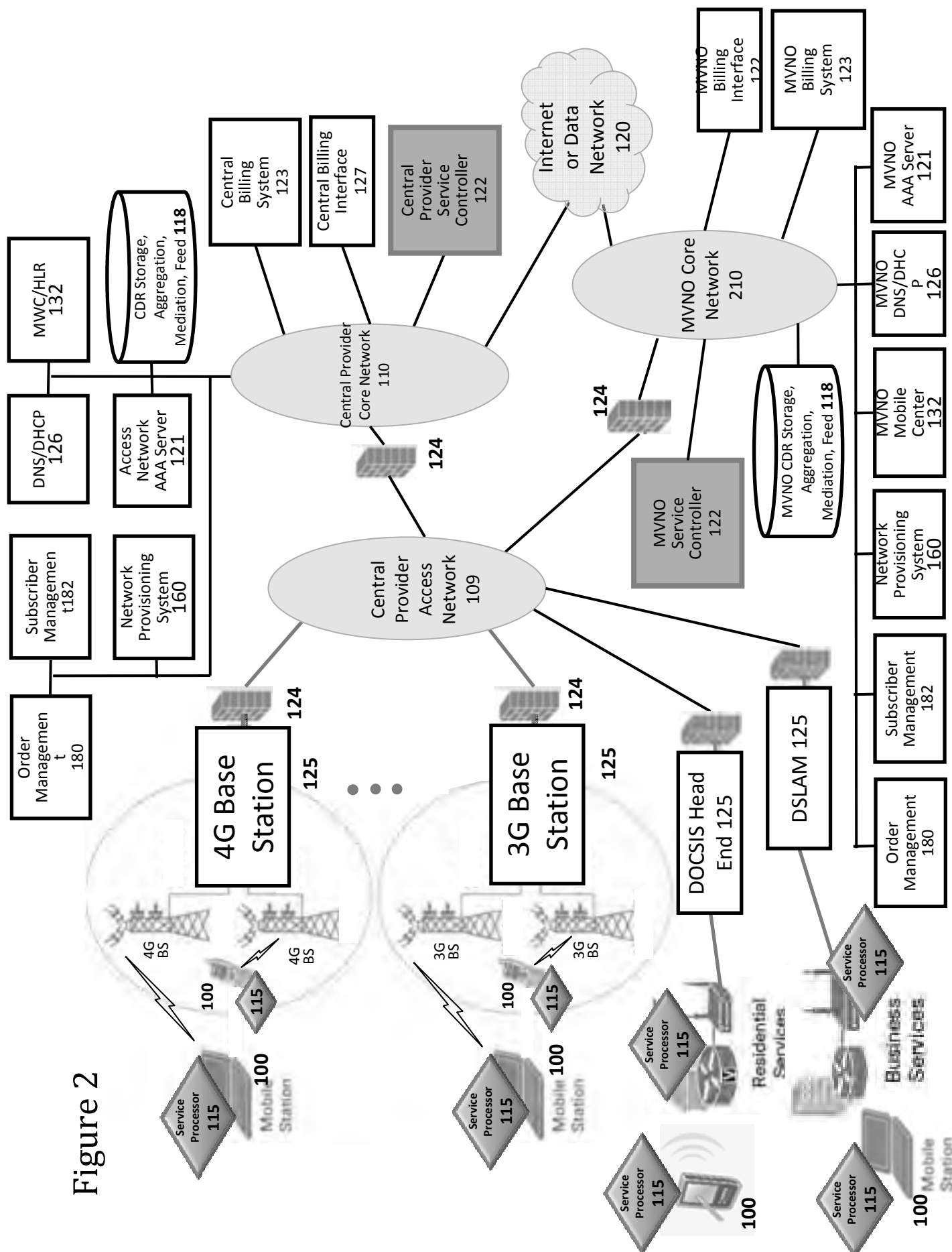


Figure 3

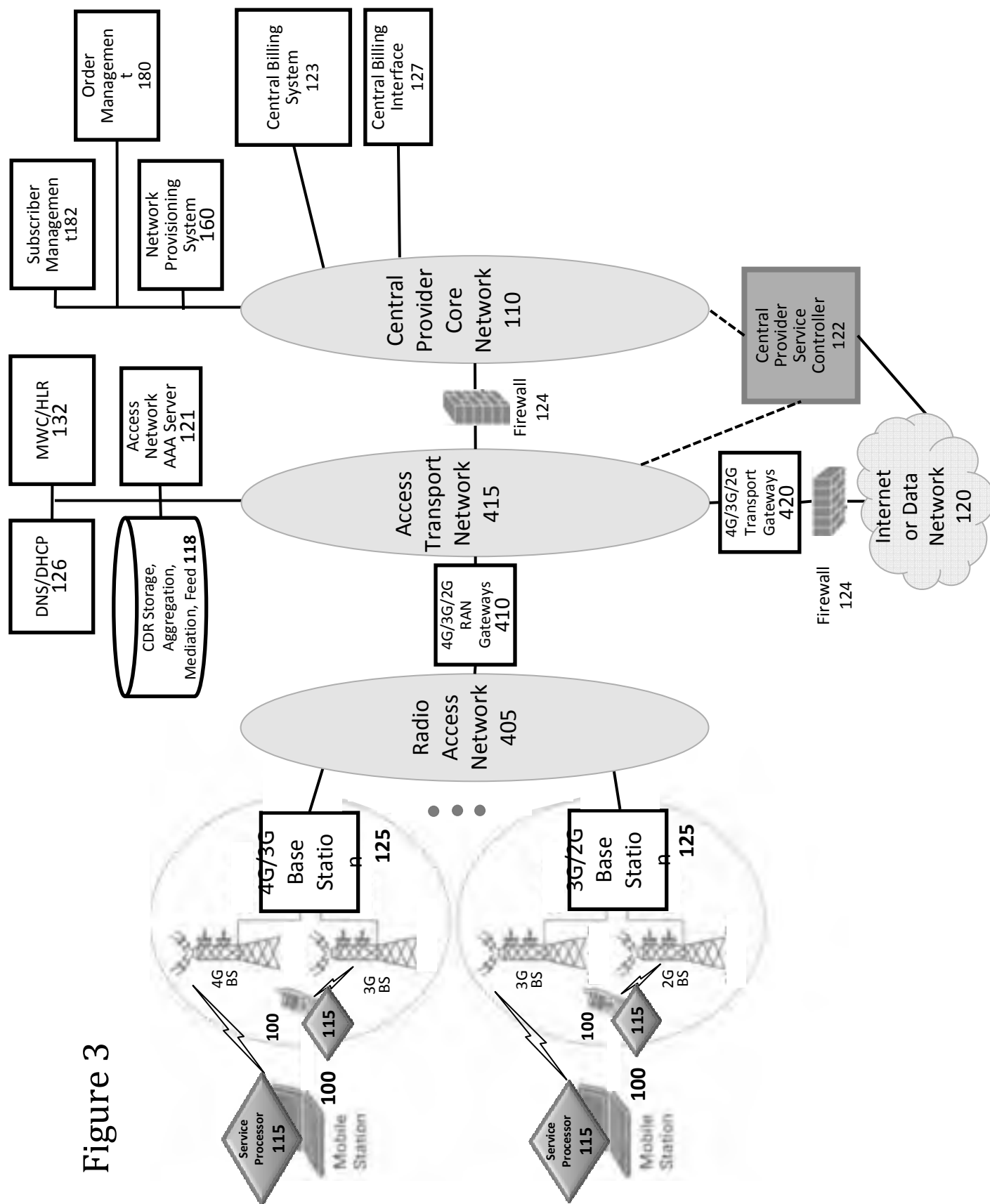


Figure 4

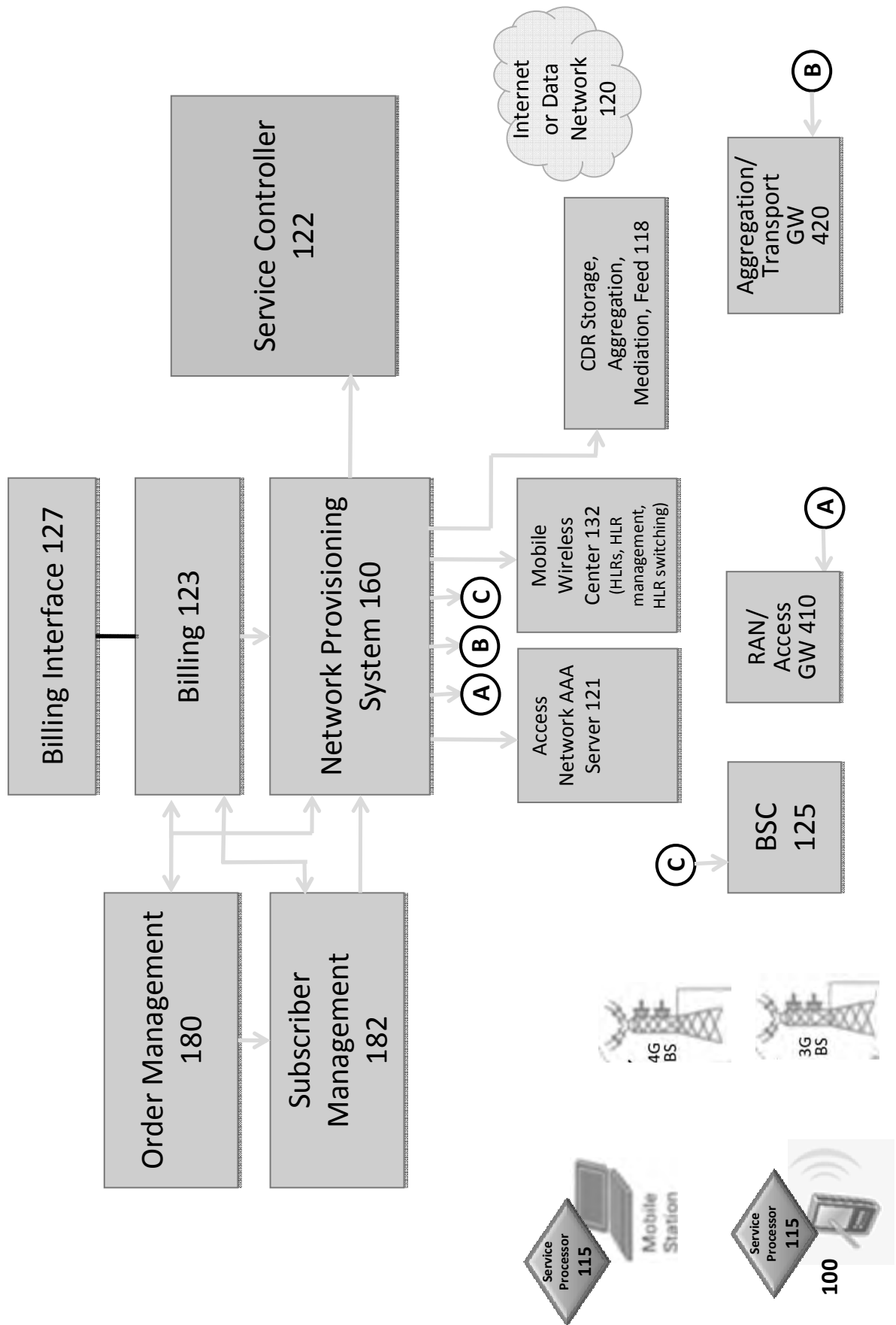


Figure 5

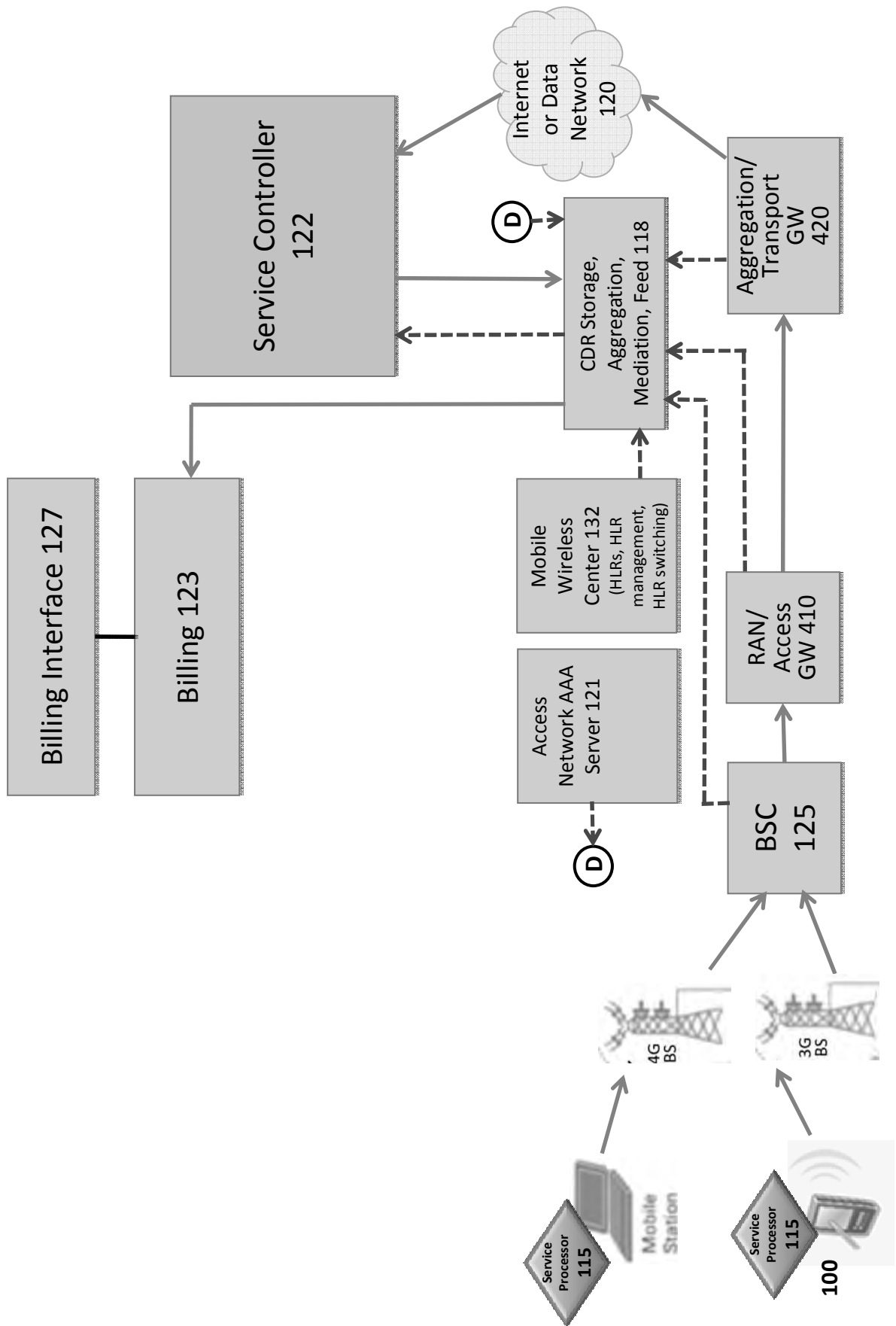


Figure 6

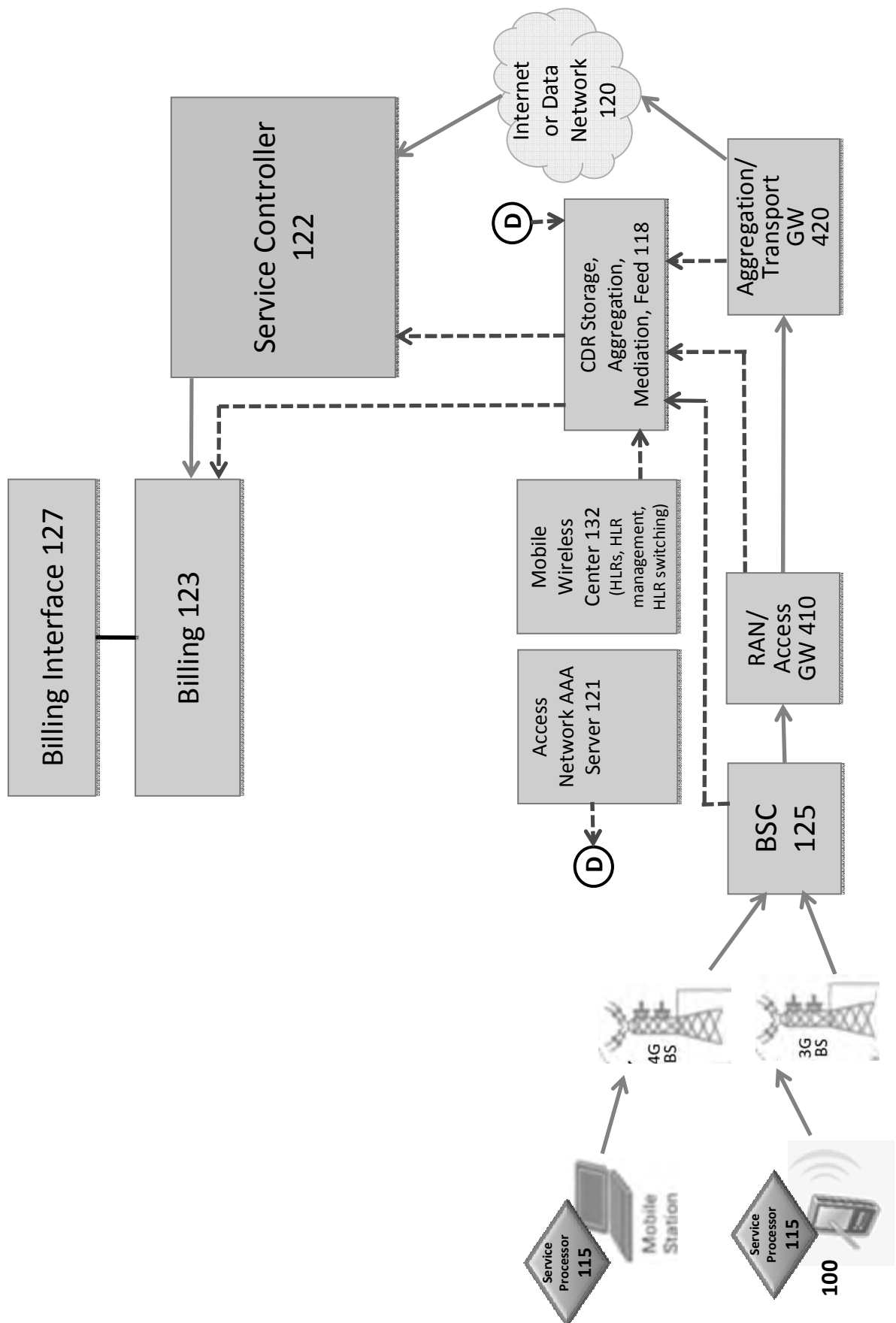


Figure 7

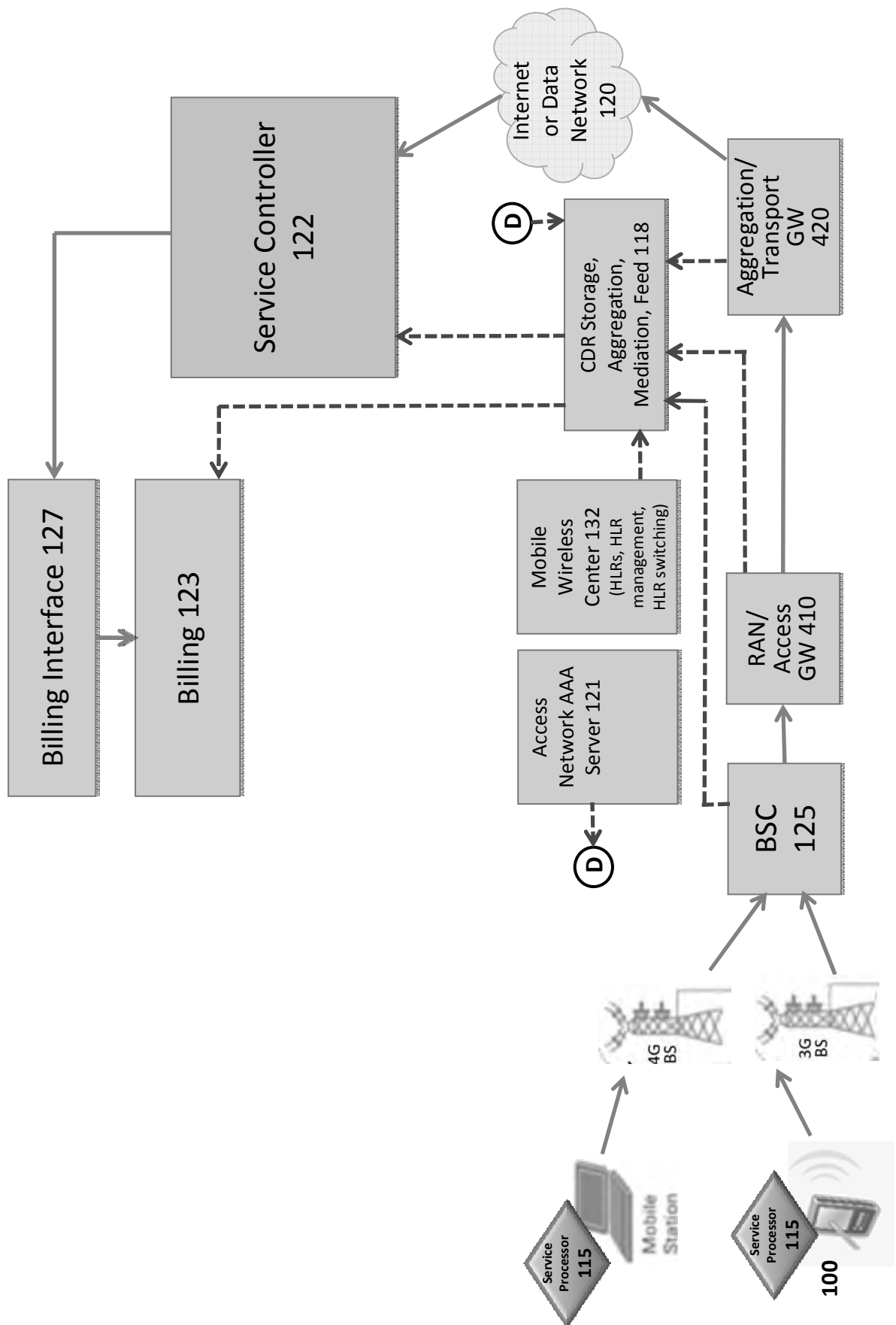
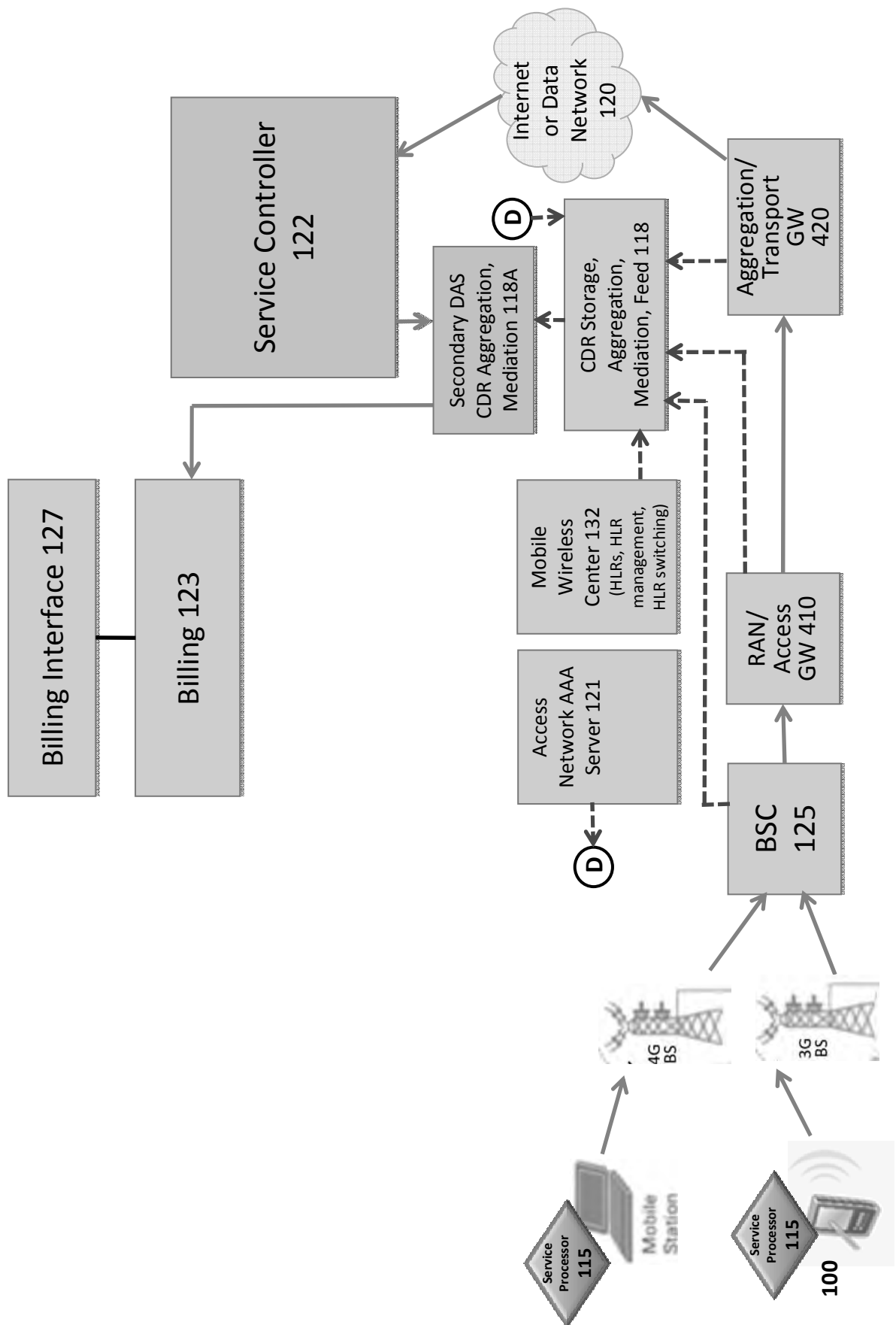


Figure 8



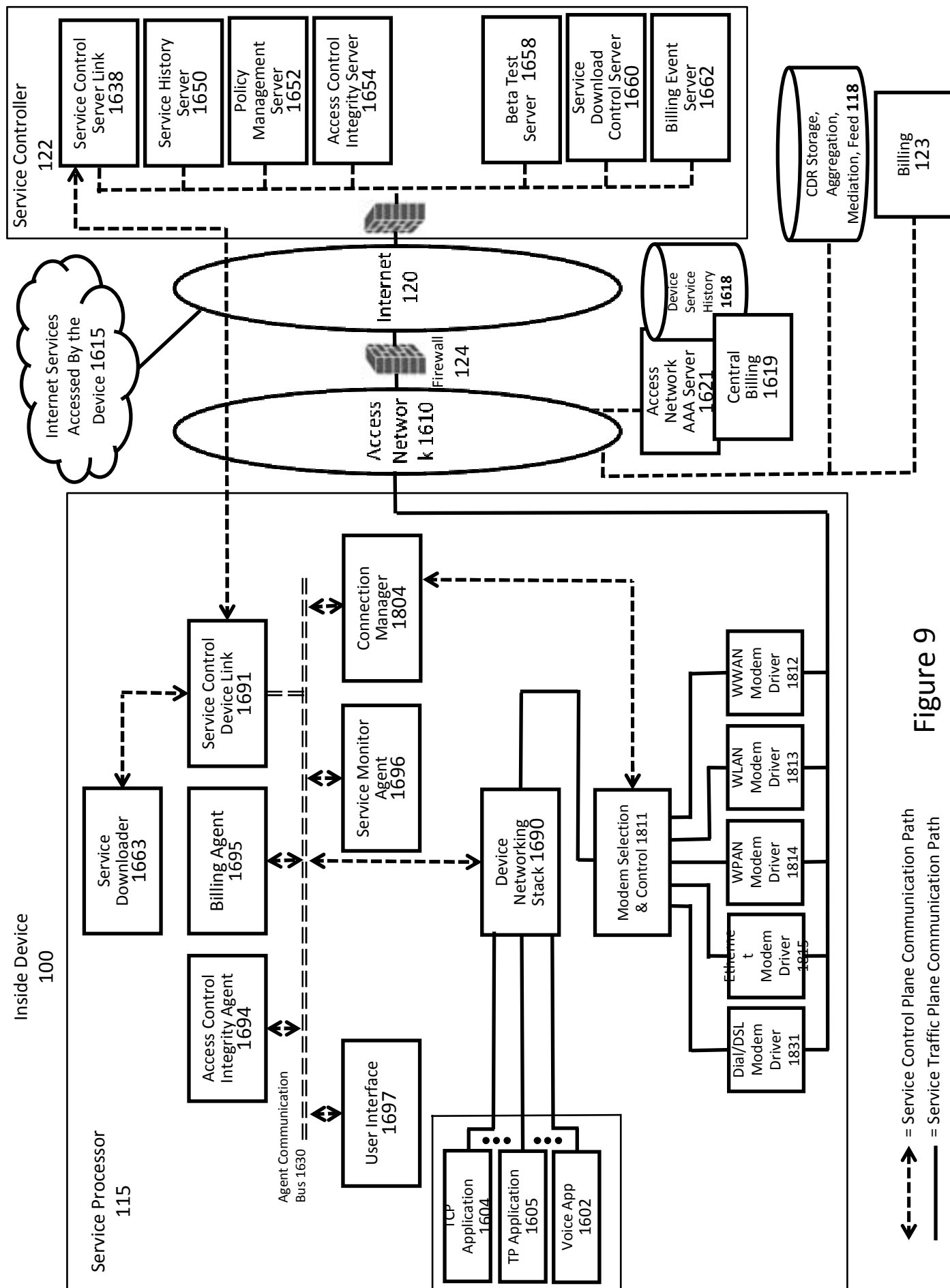


Figure 9

Service Processor 115 Embodiment	Partial Summary of Embodiment Functions
Service Control Device Link 1691	Device side control plane link for connecting Service Processor 415 to Service Controller. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Agent 1694	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected. In some embodiments, verifies configuration of other agents or performs challenge-response sequence testing. In some embodiments, monitors software loading activity, protected memory access or communication with Service Processor agents to detect unauthorized changes to Service Processor software or configuration.
Service Monitor Agent 1696	Records and reports device service usage. In some embodiments, assists in communicating application tagging of traffic flows through the networking stack policy implementation. In some embodiments, maintains a history and provides reports or summary reports of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection.
Billing Agent 1695	Detects and reports billing events. In some embodiments interacts with the User Interface Agent 497 to provide the user with service plan options, accept service plan selections, provide notification on service usage levels, provide options on service usage control policy, accept choices on service usage policy, provide transaction options or accept transaction choices. In some embodiments, interacts with Transaction Servers 134 to conduct ecommerce transactions with central billing.
User Interface 1697	Provide service interface to users.
Service Downloader 1663	Provides a download function to install or update service software elements on the device.
Connection Manager 1804	Provides a control and supervision function for one or more modem drivers or modems that connect to an access network.
Modem Selection and Control 1811	Selects the access network connection.
Modem Drivers 1831, 1815, 1814, 1813, 1812	Converts data traffic into modem bus traffic for one or more modems.
Modems 2141, 2125, 2124, 2123, 2122	Connects the device to one or more networks.

Figure 10

Service Controller 122 Element	Partial Summary of Embodiment Functions
Service Control Server Link 1638	Network side control plane link for connecting Service Controller 122 and Service Processor 115 device agents. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Server 1654	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected.
Service History Server 1650	Collects and records service usage reports from the Access Network AAA Server 1621 and the Service Monitor Agent 1696. In some embodiments, maintains a history of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection. In some embodiments, this activity summary is further analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.
Central Provider Billing System 123	Provides mediation function for central provider billing events. Accepts service plan changes. In some embodiments, provides updates on device service usage, service plan limits or service policies.
Billing Event Server 1662	In some embodiments, collects billing events, provides service plan information to the Service Processor 115, provides service usage updates to the Service Processor 115, serves as interface between device and central Provider Billing System 123, or provides trusted third party function for certain ecommerce billing transactions.
Service Download Control Server 1660	Provides a download function to install or update service software elements on the device.

Figure 11

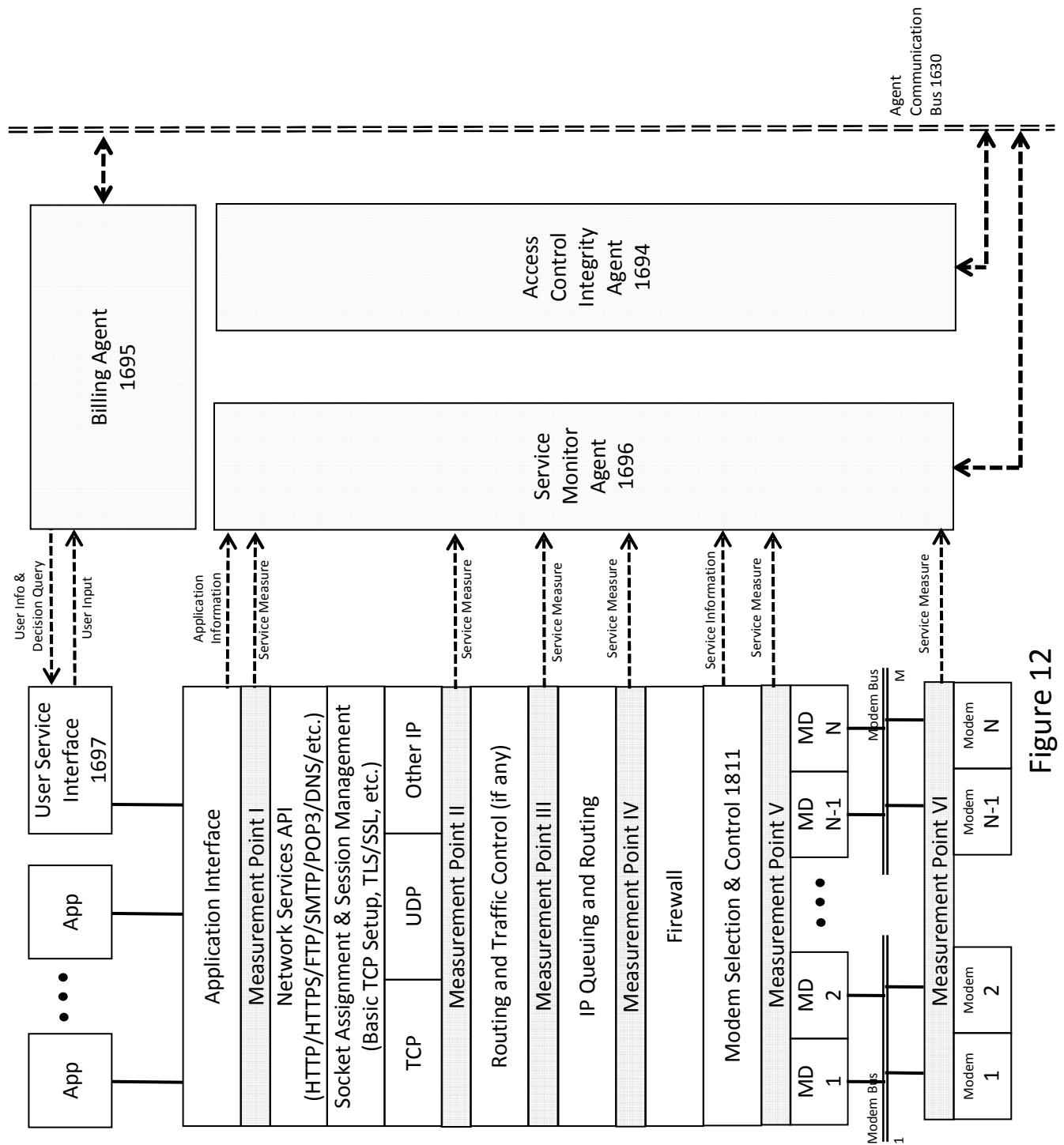
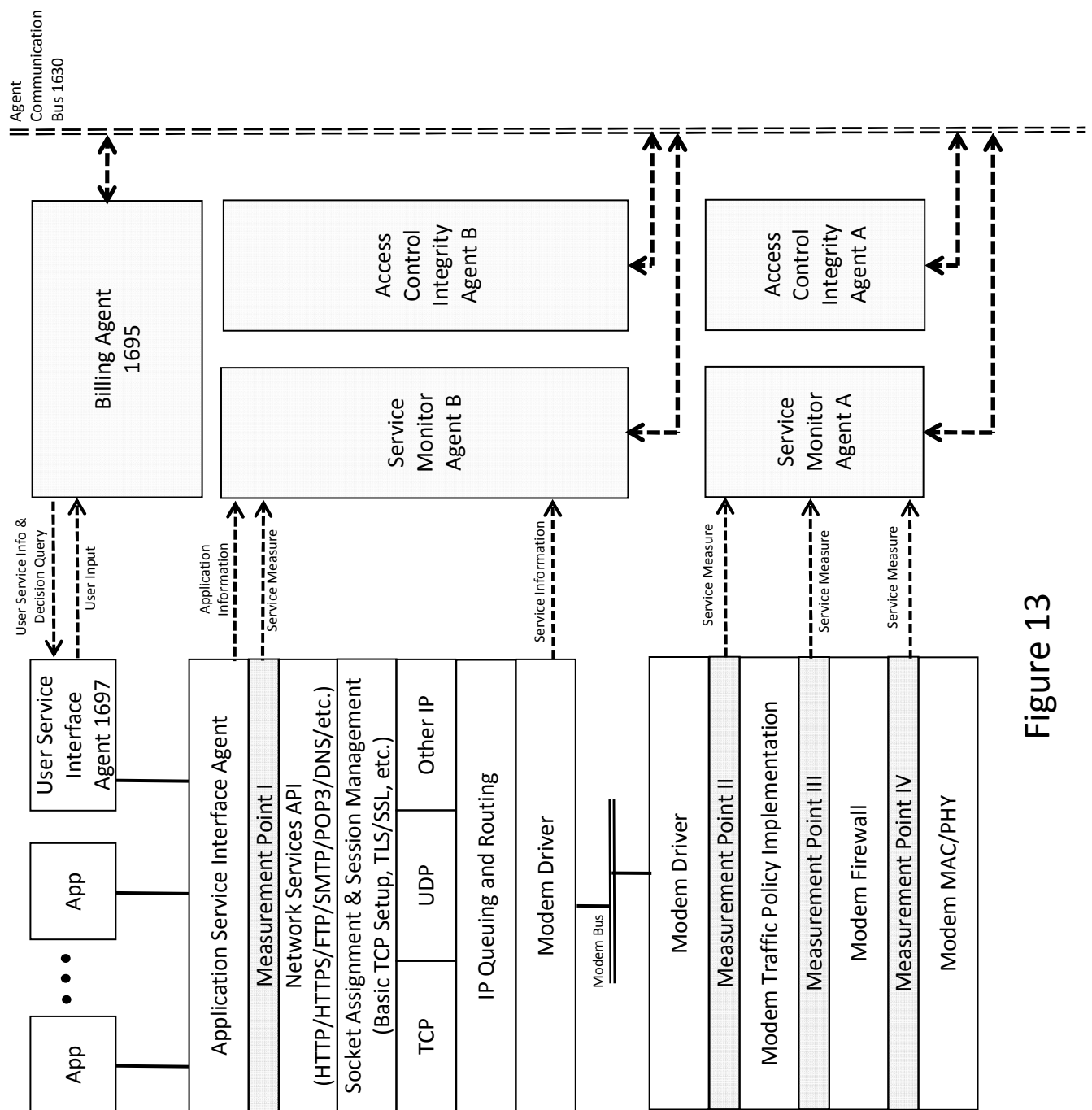


Figure 12



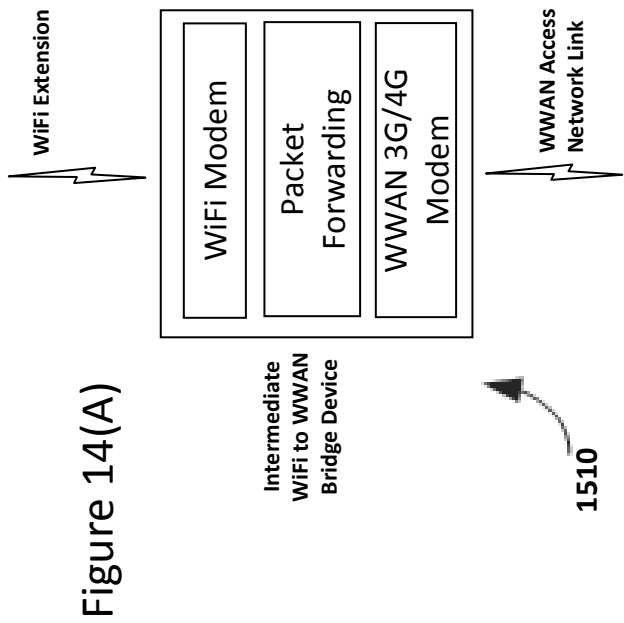
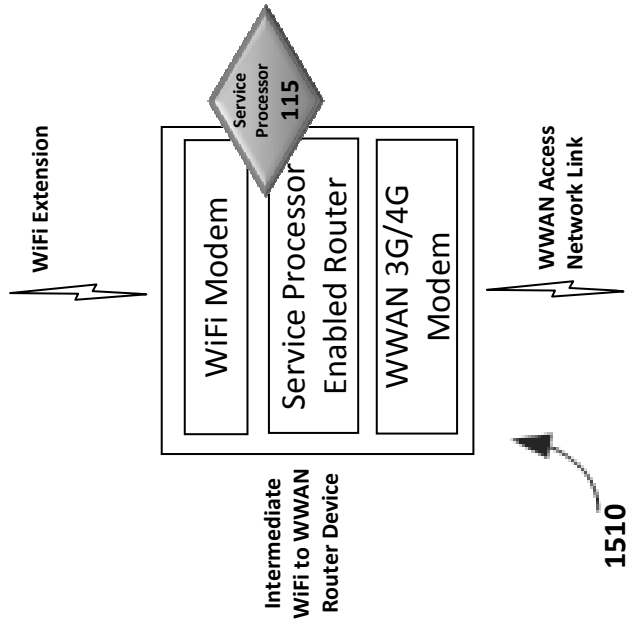
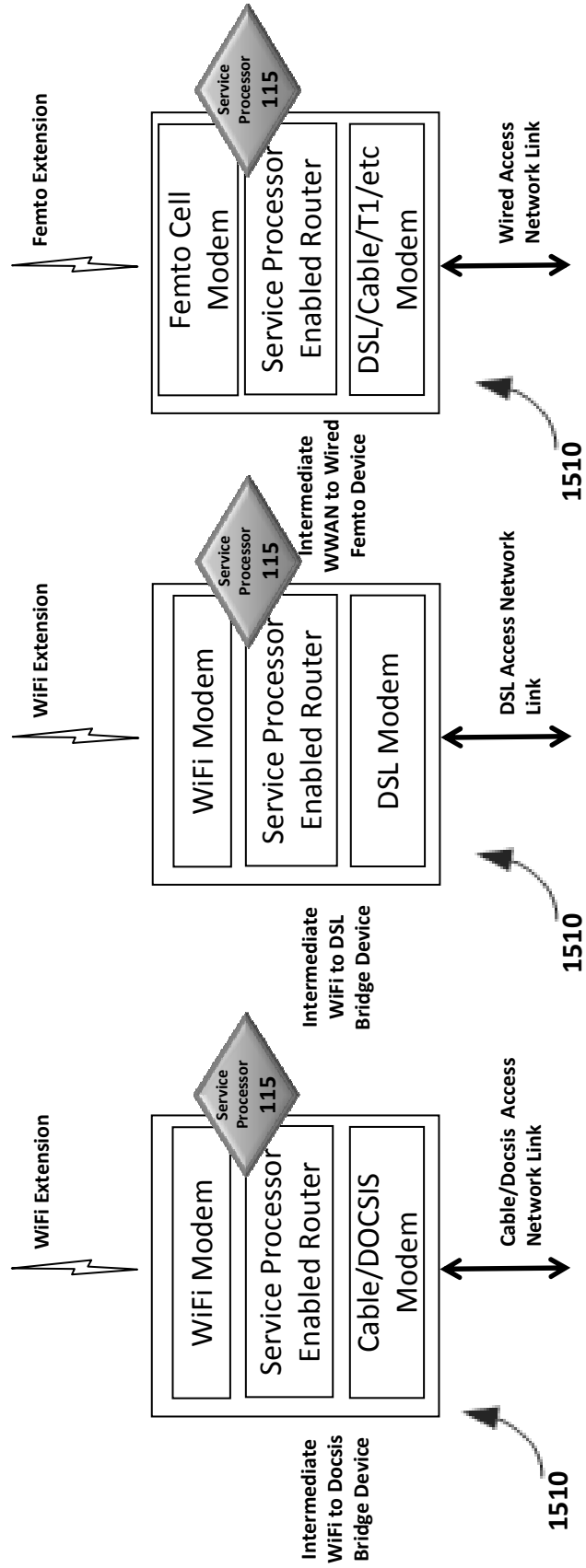


Figure 14



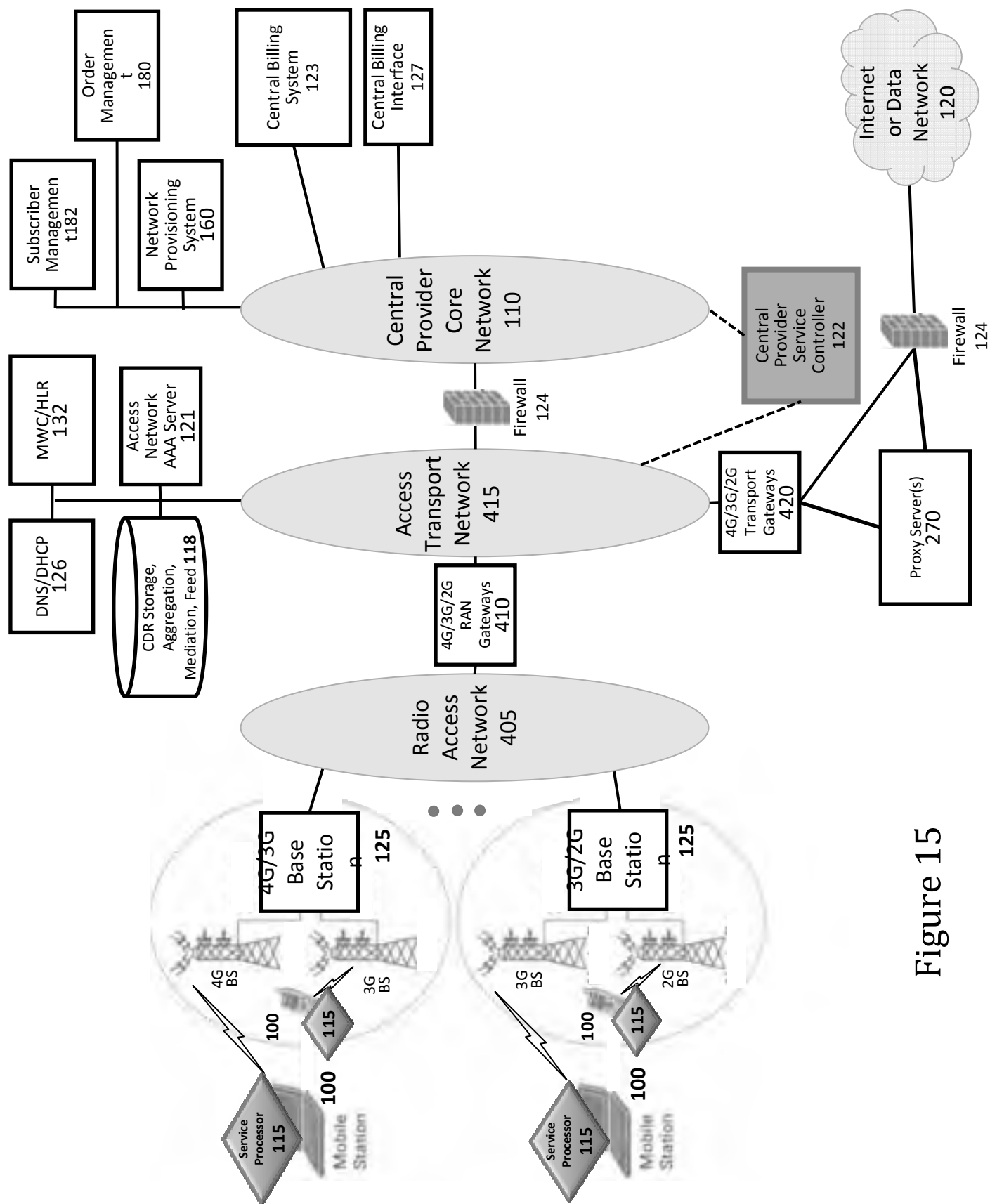


Figure 15

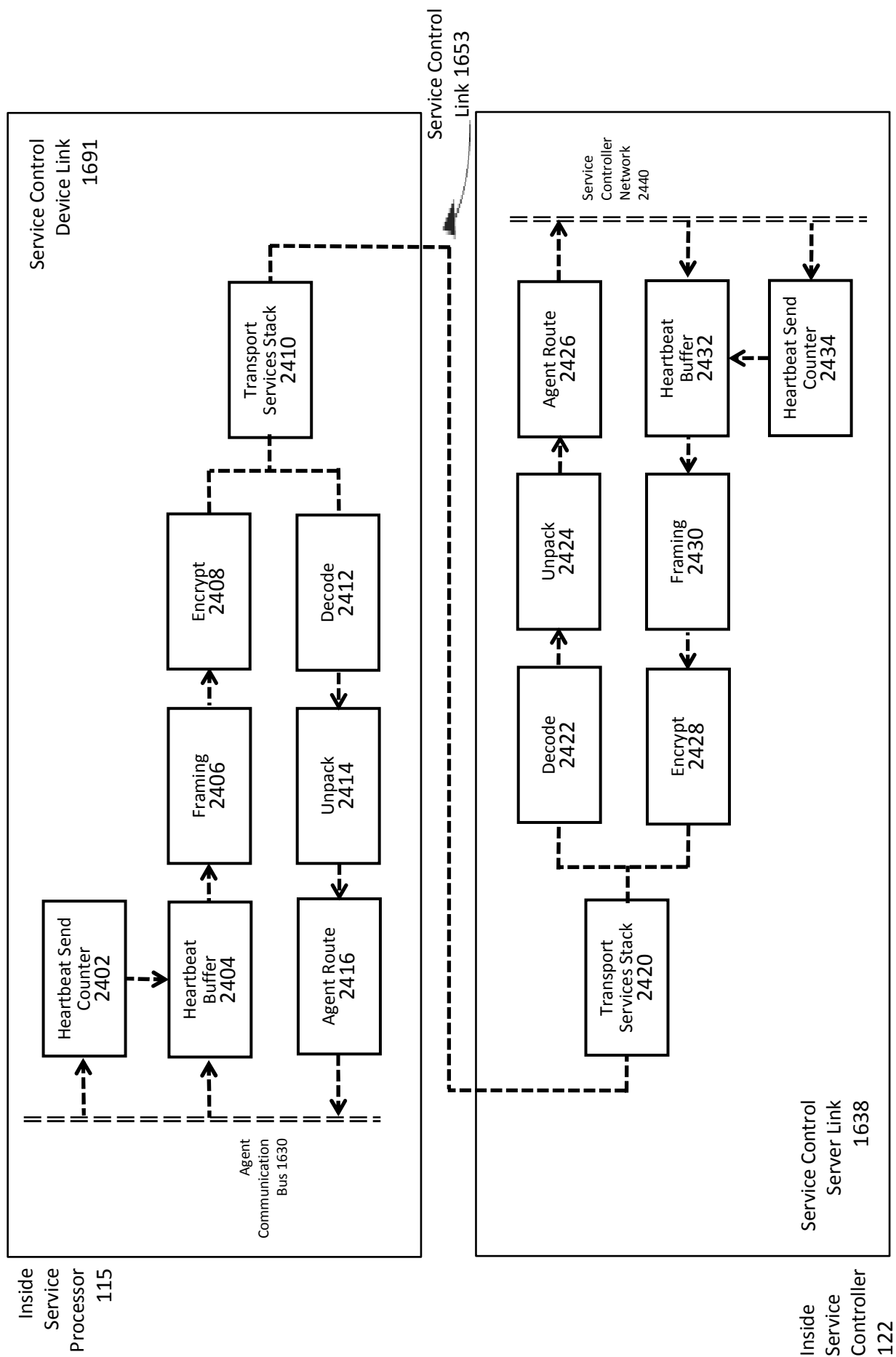


Figure 16

Service Processor Framing Sequence # 2504	Time Stamp 2506	Agent Function #1 ID 2508	Agent Function #1 Message Length 2510	Agent Function #1 Message 2512	...	Agent Function #N ID 2514	Agent Function #N Message Length 2516	Agent Function #N Message 2518
---	--------------------	------------------------------------	---	---	-----	------------------------------------	---	---

Service Processor Communication Frame 2502

Service Controller Framing Sequence # 2524	Time Stamp 2526	Agent Function #1 ID 2528	Agent Function #1 Message Length 2530	Agent Function #1 Message 2532	...	Agent Function #N ID 2534	Agent Function #N Message Length 2536	Agent Function #N Message 2538
--	--------------------	------------------------------------	---	---	-----	------------------------------------	---	---

Service Controller Communication Frame 2522

Figure 17

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Access control integrity report	Contains the latest results of the Access Control Integrity agents Service Processor system checks and reports any error events.	Not necessary to report in every heartbeat if there are no errors. Can report only on error, set a minimum frequency or respond to Service Controller polling.
Service monitor report	Reports filtered summary of Service Monitor Agent measurements. Summary reduces control traffic and filters out unauthorized private information.	Every heartbeat. Some embodiments link this to amount of data usage in the data path to keep overhead low. Report immediately upon polling from Service Controller.
Billing event report	Reports any billing activity since the last heartbeat. Billing events may include service usage events, transaction events, bill by account records, bill by account offset reports, or any other event that results in a billing event report.	Send upon billing event. Report immediately upon polling from Service Controller.
Service Processor settings report	Reports service policy settings for all Service Processor agents.	Not necessary to send every heartbeat. Some embodiments link this to amount of data usage to reduce overhead. Can report every N heartbeats. Report immediately upon polling from Service Controller.
Customer resource management report	Reports filtered summary of Service Monitor Agent measurements or filtered summary of other device or user activity such as service preferences, advertisement behavior and location. Summary reduces control traffic and filters out unauthorized private information.	Not necessary to send every heartbeat. Some embodiments link this to amount of data usage to reduce overhead. Can report every N heartbeats. Report immediately upon polling from Service Controller.
Responses to Service Processor agent queries	Sends agent responses to challenge-response queries from the Service Controller.	Report immediately upon polling from Service Controller.
Location tracking service update	Reports filtered summary of location tracking information. Summary reduces control traffic and filters out unauthorized private information.	Not necessary to send every heartbeat. Some embodiments call for a minimum time based transmission frequency.
Service usage based transmission frequency	Lowers overhead by buffering and reserving heartbeat communications from agents and server's until a certain amount of data has been transmitted or received in the network, or a certain amount of service has been consumed. When the parameters are chosen properly, this can result in the network control plane traffic overhead being a small percentage of data path traffic or result in the control plane traffic cost being a small percentage of the service usage cost.	Ranges depending on settings. For example, if there are 5 agents messages that typically need to be communicated, and each message is less than 100 bytes, and Service Processor heartbeat framing plus network overhead would result in a packet size of less than 1,000 bytes, and the heartbeat packet is transmitted when 10,000,000 bytes have been communicated over the data path, then the overhead loss due to one heartbeat packet in each direction is less than 0.02%.
Constant frequency transmissions	Since the device may be off line for long periods of time where the Service Control Processor needs to verify service control integrity, in some embodiments it can be advantageous to transmit heartbeat packets at a minimum rate regardless of data traffic activity. This is accomplished by setting a timer that sends queued heartbeat packets on a regular schedule.	Ranges depending on settings and applications.
Service Controller polled transmissions	In some embodiments, the Service Controller may poll the Service Processor for a heartbeat transmission at which time the Service Processor will frame and transmit all queued heartbeat messages.	Ranges depending on applications. In some embodiments this is used as an on demand function while in others it is used as a way to set heartbeat transmission timing functions in the Service Controller.
Service Processor polled transmissions	In some embodiments, the Service Processor polls the Service Controller for a heartbeat transmission at which time the Service Controller will frame and transmit all queued heartbeat messages.	Ranges depending on applications. In some embodiments this is used as an on demand function while in others it is used as a way to set heartbeat transmission timing functions in the Service Processor.

Figure 18A

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Agent self-check reports	Agent reports results of various agent self-diagnosis procedures to ensure that the agent is properly configured, operating properly, properly implementing service control policy or has not been tampered with. [provide examples which are extensions of typical software security self diagnosis reporting]	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Environment reports	One or more agents scan the storage or execution environment for one or more of the agents to identify potential threats to the integrity of the service implementation or agent integrity and makes a report. In one example embodiment, a scan is done to determine if unauthorized software or hardware is executing in a secure agent environment. In another embodiment, a scan is done to determine the software that has been loaded into a portion of the device operating environment, memory or storage, and the software list is referenced against a known threat list. In another example embodiment, the list of entities that accessed one or more agents is scanned to determine if an unauthorized access to an agent has occurred. In another embodiment a scan is performed to determine if unauthorized access to secure execution environment, memory or storage has occurred. In another example embodiment, the network access pattern for the device is logged and analyzed to determine if there is an access pattern that is known to be associated with a threat to service or agent control integrity. In another example embodiment, the internal device software, memory or peripheral access pattern is logged and analyzed to determine if there is an access pattern that is known to be associated with a threat to service or agent control integrity.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
User notification response reports	Billing agent, UI agent or another agent logs user notification events and the response of the user to the notification event. In some embodiments these events may be cross-referenced to the notification policy that should be in force on the device and the device service usage to ensure that the proper notification sequences are being adhered to. In other embodiments, the user notification responses are logged and used to document user choices to notification events, billing event decisions, service control decisions or service cost control decisions. In some embodiments, the user may be asked to provide a password, biometric signature, hardware key or other mechanism to positively identify that the user is in possession of the device or to verify that the service is operating properly or is implemented properly. In some embodiments, the user may be asked to acknowledge a service coverage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service coverage acknowledgement.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device, for example when there has been a user notification sequence action with the user. In some embodiments, the report is generated when there is a verification error of some kind that is identified.

Figure 18B

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
User warning response reports	Billing agent, UI agent or another agent logs user warning events and the response of the user to warning event. In some embodiments the user response is used to determine if the user is in positive control of the device. In some embodiments the response is used to confirm that the user acknowledges a billing overage or other service cost event. In some embodiments, the user may be asked to provide a password, biometric signature, hardware key or other mechanism to positively identify that the user is in possession of the device or to verify that the service is operating properly or is implemented properly.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device, for example when there has been a warning sequence action with the user. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Agent communication log reports	Reports entities that established or attempted to establish communication with the agents. In one embodiment, reports a list of entities and the number of times the entity communicated or attempted to communicate with the agent. In another embodiment, reports an error flag when unauthorized entities attempt to establish communication with an agent.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Service usage synchronization data	IPDR or other data that is used to synchronize the device service usage counters. In some embodiments the data is time stamped so that the service usage at a point in time may be reconciled between the local device usage count and the network based usage count, and then the local device usage count since the point in time may be used to estimate the present real-time usage count. In some embodiments, the service usage data from the device is used by the network as the actual service usage or billing data base for the device. In other embodiments, a bill by account function is included in the service usage synchronization data so that the service usage may be billed to different accounts other than a single or main user account.	Service usage synchronization is continuous with each heartbeat in some embodiments. In other embodiments service usage synchronization is based on a push from the Service Controller or other network function that sends the IPDR information to the device. In other embodiments, the device requests a synchronization data transmission.
Service cost synchronization data	Information to reconcile a service cost estimate on the local device with a service cost count from a network based function. Similar to the service usage count, in some embodiments the service cost information is time stamped so that service cost at a point in time may be reconciled between the device and the network based function, and then a local measure of service cost may be used to estimate the present real-time service cost. In some embodiments the local service cost is determined by taking recorded billing events and looking up the cumulative cost of one or more billing events using a service usage to cost look up data base stored locally on the device or available from a network function. In some embodiments, service cost estimation is done entirely in the network and the result is pushed out to the device UI. In other embodiments service cost estimation is done in the device based on local usage estimates and a local usage to cost lookup table.	Service cost synchronization is continuous with each heartbeat in some embodiments. In other embodiments service cost synchronization is based on a push from the Service Controller or other network function that sends the IPDR information to the device. In other embodiments, the device requests a synchronization data transmission.

Figure 18C

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Available network information and roaming information	Device receives available network or available roaming service provider information from a network function. The available network or roaming service information may include the potential network service or roaming service a device or user may choose to select, or the network service or roaming service the user has already selected. In some embodiments this information includes service cost information to aid the device or the user in determining the potential or actual costs of service usage while using the available network or roaming network. In some embodiments the service cost information is used to help the user in selecting the available network provider or roaming service provider. In some embodiments the available network cost information or roaming cost information is combined with a measure of expected or possible service usage to estimate how much a typical usage scenario may cost. In some embodiments, the available network information or roaming information is used to help the user estimate the present available network or roaming service charges for services used to date. In some embodiments service usage is recorded and sent to a network function that estimates the current service cost. In other embodiments the service cost is estimated locally on the device based on a service usage estimate and a service usage to cost look up function. In other embodiments, the service cost is derived by querying the available network or roaming network billing system.	In some embodiments available network information or roaming information is requested by the device. In other embodiments, the information is periodically updated by the Service Controller or other network function that contains the information.
System messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display a system messages or screen that is generated by a network function or server to the end user and possibly report user inputs to the UI message or screen. Examples include, etc.	System messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments, some system messages are generated in response to user input or requests. In other embodiments, system messages are generated on a regular time table or in accordance with a certain amount of service usage.
UI screen messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display user interface message or screen that is generated by a network function or server to the end user and possibly report user inputs to the UI message or screen. Examples include service usage UI, service choice UI, upgrade UI, transaction UI, marketing UI, billing UI, user identify confirmation UI, user service warning UI, user potential service tamper response request UI, etc.	UI screen messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments, some user UI messages are generated in response to user input or requests. In other embodiments, UI messages are generated on a regular time table or in accordance with a certain amount of service usage.
Local agent check-in history	Logs and reports agent check-ins or self-reports that are made to a local agent integrity verification function.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.

Figure 18D

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Software install report	Logs and reports one or more aspects of software installs that have occurred on the device.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified. In some embodiments, the report is generated when new SW is installed.
Test billing event	In some embodiments the Service Controller or other network function may send or cause a test billing event wherein the device triggers a local billing sequence for the purpose of verifying that the billing sequence is properly logged, conducted and reported. The billing sequence can be related to a service usage event or sequence, a transaction event or sequence, or any other event or sequence that should result in a billing event.	In some embodiments, the test billing event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.
Test service event	In some embodiments the service Controller or other network function may send or cause a service usage event wherein the device triggers a local service usage event or sequence for the purpose of verifying that the service usage event or sequence is properly logged and reported.	In some embodiments, the test service usage event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.

Figure 18E

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify service usage measure in network is consistent with expected service behavior	Network service usage measure is in conflict with expected service usage. Examples: traffic usage outside limits, address access outside limits, data rate outside limits, traffic shaping rules not being followed.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify service usage measure at device is consistent with expected service behavior	Device service usage measure is in conflict with expected service usage. Examples: traffic usage too high, address access outside limits, email accessed against policy.	Same as above.
Verify service usage measure in network is consistent with service usage measure at device	Device service usage measure varies significantly from network service usage measure	Same as above.
Verify service usage measure at one point in device is consistent with service usage measure at a second point in device	Service usage measure at one point in device stack that is inconsistent with another point indicates error or potential parasitic usage	Same as above. In some embodiments, the differences in service measures on the device may be used to evaluate the nature of the service usage policy implementation problem.
Verify that service policies in effect are as intended	Service policy setting queries result in settings that are different than intended	In some embodiments, reset service policies and see if error persist. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 19A

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify presence of Service Processor agents	Agent does not respond to agent communication or query-response	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify configuration of Service Processor agents	Agent configuration audit or configuration self-check fails.	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify billing events are reported or are reported properly	Billing Agent query reveals logged billing events that have not been reported.	In some embodiments, perform a billing event test to determine if the billing event reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 19B

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify network reported service usage measure are consistent with reported device billing data.	Billing agent is not properly reporting billing events for service usage, transactions, bill by account, or other billing event functions.	<p>In some embodiments, perform a service usage test to determine if the service usage reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify device reported service usage measure are consistent with reported device billing data.	Billing agent reports are inconsistent with service usage reports.	<p>In some embodiments, perform a billing event test to determine if the billing event reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, perform a service usage test to determine if the service usage reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>

Figure 19C

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Send test billing event through device and verify it is reported.	Test billing event is nor properly reported by the device.	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify device reports billing events reported from transaction servers.	Transaction server receipts do not correspond with billing events from device.	In some embodiments, perform checks to determine of transaction server receipts are valid. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify activation tracking system presence, configuration or operation	Activation tracking service is not present, is not providing scheduled network activity reporting, or is exhibiting erroneous reports.	In some embodiments the response is to place the device ID, on a list of devices suspected of having activation tracking functions that have been tampered with for the purpose of central provider billing reconciliation. In some embodiments, install a new copy of the activation tracking service agent software either from a locally stored device copy or a network download. In some embodiments where authorization exists to manage device software and some aspects of service tracking, run further checks on device service integrity such as agent query-response. In some embodiments where authorization exists to manage a device access service connection, send error message to device UI, suspend device or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Verify device standing or service plan standing	No service plan on record or device not authorized	In some embodiments, if device is not yet activated with a service plan, provide UI with activation sequence. In some embodiments, if device is not authorized for service on one of the networks controlled by the Service Controller, send the UI an error message instructing the user how to proceed. In some embodiments, configure the Service Processor for the ambient service intended for that device. In some embodiments, download the appropriate Service Processor agent software that is appropriate for that device.

Figure 19D

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify proper operation of Service Processor agents	Check input to output relationship on Policy Implementation agent, Firewall agent. Check billing event reports to verify events are being recorded. Check application and traffic inspection tagging system correctly tagging traffic. Verify Service Processor heartbeat reports proper agent integrity self-checks, cross-checks and query/response sequences with Service Controller.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Service Processor heartbeat response reports	One or more of the heartbeat reports indicate an error in operation, configuration, or tamper and error prevention system. Heartbeat function not functioning properly but device is still indicating service usage on the network.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Test service event	Service usage reporting system does not properly report test service usage event	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing test event to determine if the device is properly reporting billing events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 19E

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Load a fresh version of Service Processor software and perform integrity reports	After fresh load of Access Control Integrity Agent, agent discovers one or more of the other agents are corrupted.	Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify Service Processor code configuration with agent self diagnosis checks	One or more of the agents indicates an error after running a self-check.	Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify that device uses service only after being authorized	Device gains access to the network and does not check in with the Access Control Integrity Server and service measures indicate device is on the network.	In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 19F

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify user standing	User does not respond with proper response to UI query such as request for ID., password or biometric input. This process may be part of handling a suspected error.	In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis. In some embodiments, the user may be asked to acknowledge a service coverage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service coverage acknowledgement.
Agent communications log	Unauthorized communications with one or more agents is detected	In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 19G

Service Policy Implementation Tamper or Error Protection Technique	Example Error Trigger Criteria	Example Error Responses
Detect or block device networking activity that is potentially harmful for the operation of Service Processor.	Network activity is observed in service monitor reports that fit known patterns that indicated harmful software may be present on device.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized Service Processor software from being loaded.	Access Control Integrity Agent discovers software that is on a known malicious list.	Same as above.
Detect or block unauthorized access of protected Service Processor software or hardware memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized communication with Service Processor software or hardware.	Unauthorized communication is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure loader with signed SW installed into protected memory	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure encrypted communication between Service Processor agents.	Secure communication link is in error or unauthorized access is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh agents with communication links that are in error or entire Service Processor. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure encrypted communication between Service Processor and Service Controller.	Service Processor communication is lost.	Send error message to device UI (if possible), suspend device, place on SPAN, place on watch list, place on further action list or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Execution of Service Processor software within secure memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.

Figure 20A

Service Policy Implementation Tamper or Error Protection Technique	Example Error Trigger Criteria	Example Error Responses
Storage of service processor software in secure memory	Secure memory violation or Service Processor stored in non-secure memory	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detection or removal of software thought to be harmful to Service Processor operation.	Unauthorized software is detected.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Recording and reporting of software loading signatures, software activity signatures or network activity signatures for later identification of threat sequences.	Unauthorized software or malicious network activity is detected	Same as above.
Implement critical Service Processor software as a self-refreshing program that resists corruption by running self-audit and reinstall processes such as placing audit function in inaccessible memory or OS functions or bios.	Re-installation function alerts that re-installation has been required. Continued re-installations or failure to re-install alert increases severity of warnings.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Encrypted agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code encryption	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Obfuscated agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code obfuscation	Same as above.
Unique agent identification numbers and signatures	Agent is discovered to have an incorrect ID. or fails signature	Same as above.
Secure agent communication bus	Agent communication bus monitoring discovers unauthorized communication or other unauthorized access to one or more agents is discovered	Same as above.
Agent level message encryption	Agent is found to be communicating without the required level of agent communication encryption	Same as above.

Figure 20B

Service Policy Implementation Tamper or Error Protection Technique	Example Error Trigger Criteria	Example Error Responses
Service control link message level encryption	Unauthorized communication traffic is discovered on service control link	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Service control link transport layer encryption	Unauthorized communication traffic is discovered on service control link	Same as above.
Agent communication access permissions	Unauthorized communication is discovered with one or more agents	Same as above.
Agent communication log	Unauthorized communication is discovered with one or more agents	Same as above.
Encrypted agent code for downloads	Agent download is found to have incorrect or absent encryption or signature	Same as above.
Secure downloader memory	Unauthorized access to or storage in secure downloader memory is discovered	Same as above.

Figure 20C

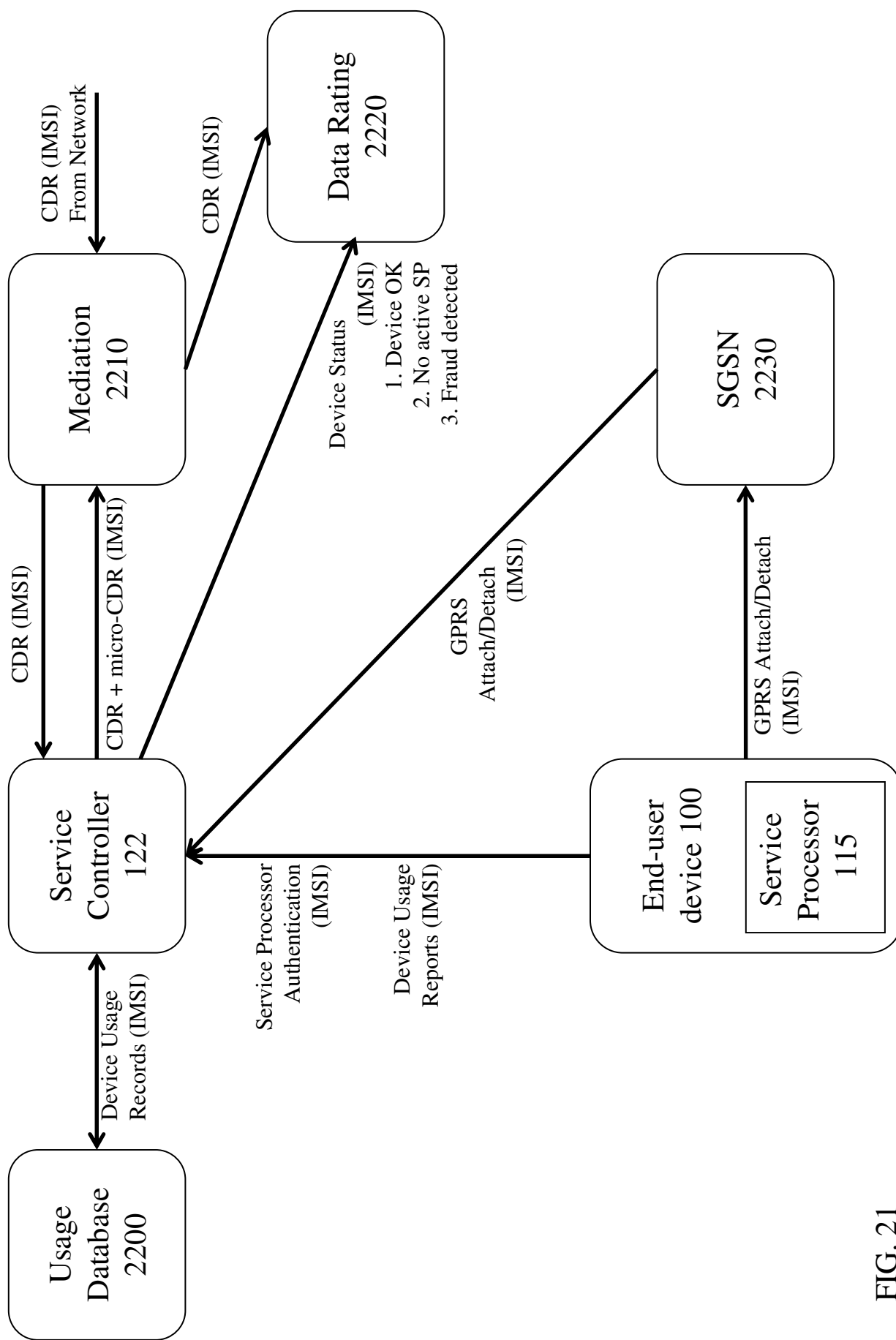


FIG. 21

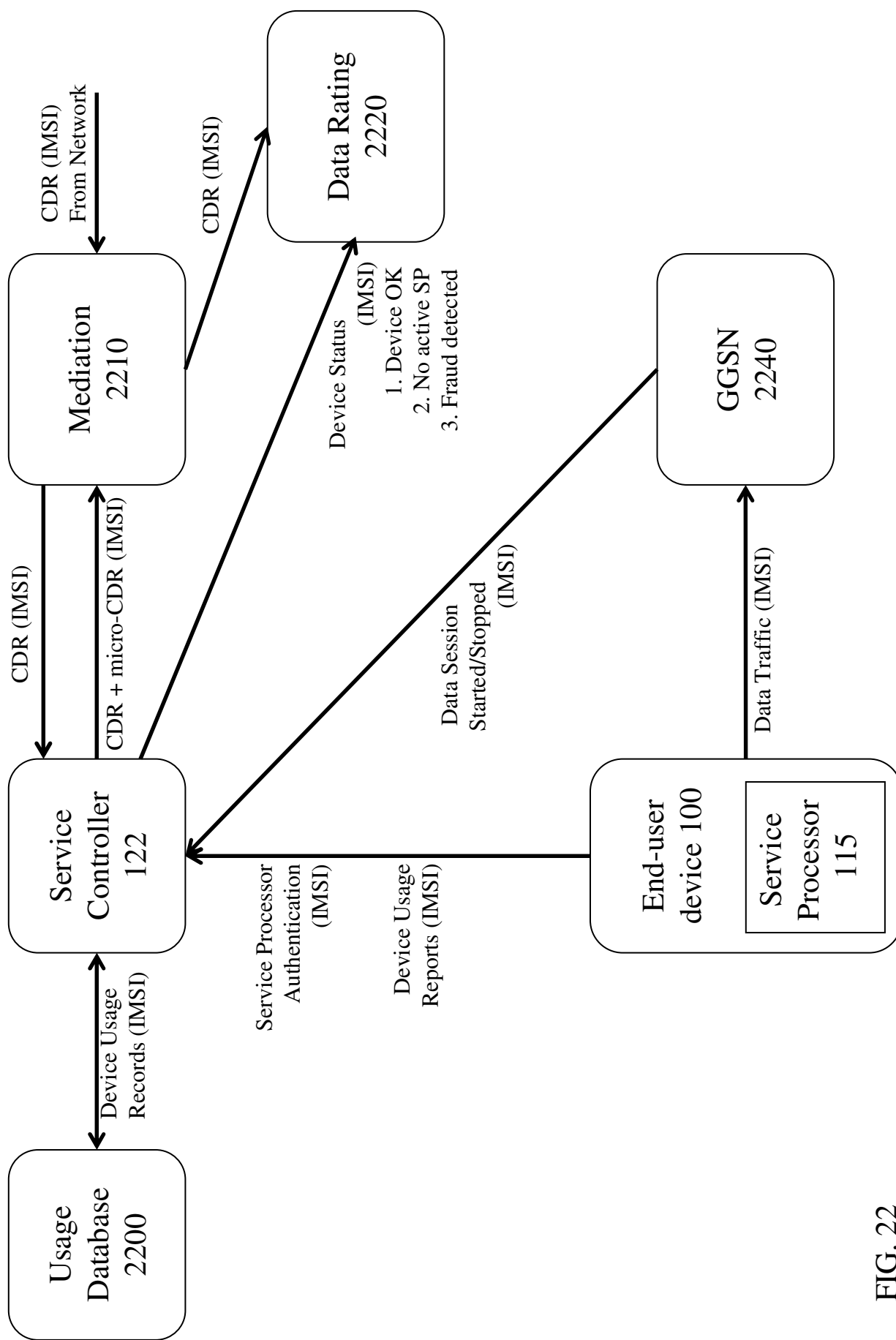


FIG. 22

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**UTILITY
PATENT APPLICATION
TRANSMITTAL**

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.

26WV-160511 [RALEP034]

First Inventor

Gregory G. Raleigh, et al.

Title

Adapting Network Policies Based on
Device Service Processor Configuration

Express Mail Label No.

N/A - EFS Filing

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☐ **Fee Transmittal Form** (e.g., PTO/SB/17)
2. ☒ **Applicant claims small entity status.**
See 37 CFR 1.27.
3. ☒ **Specification** [Total Pages 103]
Both the claims and abstract must start on a new page
(For information on the preferred arrangement, see MPEP 608.01(a))
4. ☒ **Drawing(s)** (35 U.S.C. 113) [Total Sheets 34]
5. **Oath or Declaration** [Total Sheets]
a. ☐ Newly executed (original or copy)
b. ☐ A copy from a prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 18 completed)
i. ☐ **DELETION OF INVENTOR(S)**
Signed statement attached deleting inventor(s)
name in the prior application, see 37 CFR
1.63(d)(2) and 1.33(b).
6. ☐ **Application Data Sheet.** See 37 CFR 1.76
7. ☐ **CD-ROM or CD-R** in duplicate, large table or
Computer Program (Appendix)
☐ Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
(if applicable, items a. - c. are required)
a. ☐ Computer Readable Form (CRF)
b. **Specification Sequence Listing on:**
i. ☐ CD-ROM or CD-R (2 copies); or
ii. ☐ Paper
c. ☐ Statements verifying identity of above copies

ADDRESS TO:

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450**ACCOMPANYING APPLICATION PARTS**

9. ☐ **Assignment Papers** (cover sheet & document(s))
Name of Assignee _____
10. ☐ **37 CFR 3.73(b) Statement** ☐ **Power of Attorney**
(when there is an assignee)
11. ☐ **English Translation Document** (if applicable)
12. ☐ **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
☐ Copies of citations attached
13. ☐ **Preliminary Amendment**
14. ☐ **Return Receipt Postcard** (MPEP 503)
(Should be specifically itemized)
15. ☐ **Certified Copy of Priority Document(s)**
(if foreign priority is claimed)
16. ☐ **Nonpublication Request** under 35 U.S.C. 122(b)(2)(B)(i).
Applicant must attach form PTO/SB/35 or equivalent.
17. ☒ **Other:** General Authorization to Petition for
Extensions of Time (1 pg.)

18. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:

☐ Continuation ☐ Divisional ☒ Continuation-in-part (CIP) of prior application No.: See specification

Prior application information: Examiner _____ Art Unit: _____

19. CORRESPONDENCE ADDRESS☒ The address associated with Customer Number 69849 OR ☐ Correspondence address below

Name

Address

City

State

Zip Code

Country

Telephone

Email

Signature

Date September 20, 2011Name
(Print/Type)Marc A. SockolRegistration No.
(Attorney/Agent) 40,823

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

American LegalNet, Inc.
www.FormsWorkflow.com

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:

Examiner: Not Yet Assigned

Gregory G. Raleigh, et al.

Art Unit: Not Yet Assigned

Serial No: Not Yet Assigned

Filed: Herewith

For: Adapting Network Policies Based on
Device Service Processor Configuration

Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

GENERAL AUTHORIZATION TO PETITION FOR EXTENSIONS OF TIME

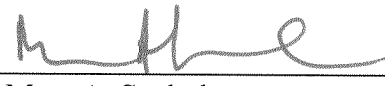
Dear Sir:

With reference to the subject application, and pursuant to 37 C.F.R. § 1.136, Applicants hereby authorize and request the Commissioner to treat any correspondence requiring a petition for extension of time as containing such a request therefor for the appropriate length of time. This general authorization is effective during the pendency of this application, including any divisional or continuing application therefrom.

Where no check is received by the Commissioner, you are hereby authorized to charge payment of the requisite petition fees, or charge any additional fee required under 37 C.F.R. § 1.17, or credit any overpayment of same, to Deposit Account No. **50-4561**.

Respectfully submitted,

Date: September 20, 2011

By: 

Marc A. Sockol
Reg. No. 40,823
Customer Number 69849
Sheppard Mullin Richter & Hampton LLP
390 Lytton Avenue
Palo Alto, CA 94301-1432

**CONTINUATION-IN-PART APPLICATION FOR
UNITED STATES PATENT
IN THE NAME**

of

- Gregory G. Raleigh -

- James Lavine -

For

**- ADAPTING NETWORK POLICIES BASED ON DEVICE
SERVICE PROCESSOR CONFIGURATION -**

DOCKET NO. 26WV-160511 [RALEP034]

Please direct communications to:

**Sheppard, Mullin, Richter & Hampton LLP
390 Lytton Avenue
Palo Alto, California 94301-1432
(650) 815-2600**

ADAPTING NETWORK POLICIES BASED ON DEVICE

SERVICE PROCESSOR CONFIGURATION

CROSS REFERENCE TO OTHER APPLICATIONS

[0001] This application is a continuation-in-part of and incorporates by reference the following published U.S. pending nonprovisional patent applications: U.S. publication No. 2010/0188975, filed March 2, 2009, entitled “Verifiable Device Assisted Service Policy Implementation,” U.S. publication No. 2010/0192170, filed March 2, 2009, entitled “Device Assisted Service Profile Management with User Preference, Adaptive Policy, Network Neutrality, and User Privacy,” U.S. publication No. 2010/0191612, filed March 2, 2009, entitled “Verifiable Device Assisted Service Usage Monitoring with Reporting, Synchronization, and Notification,” U.S. publication No. 2010/0191576, filed March 2, 2009, entitled “Verifiable Device Assisted Service Usage Billing with Integrated Accounting, Mediation Accounting, and Multi-Account,” U.S. publication No. 2010/0188991, filed March 2, 2009, entitled “Network Based Service Policy Implementation with Network Neutrality and User Privacy,” U.S. publication No. 2010/0188990, filed March 2, 2009, entitled “Network Based Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy,” U.S. publication No. 2010/0192212, filed March 2, 2009, entitled “Automated Device Provisioning and Activation,” U.S. publication No. 2010/0191604, filed March 2, 2009, entitled “Device Assisted Ambient Services,” U.S. publication No. 2010/0191575, filed March 2, 2009, entitled “Network Based Ambient Services,” U.S. publication No. 2010/0188993, filed March 2, 2009, entitled “Network Tools for Analysis, Design, Testing, and Production of Services,” U.S. publication No. 2010/0190470, filed March 2, 2009, entitled “Roaming Services Network and Overlay Networks,” U.S. publication No. 2010/0192120, filed March 2, 2009, entitled “Open Development System for Access Service Providers,” U.S. publication No. 2010/0192207, filed March 2, 2009, entitled “Virtual Service Provider Systems,” U.S. application serial No. 12/380,757, filed March 2, 2009, and entitled “Service Activation Tracking System,” U.S. publication No. 2010/0191613, filed March 2, 2009, entitled “Open Transaction Central Billing

System,” U.S. publication No. 2010/0188995, filed March 2, 2009, entitled “Verifiable and Accurate Service Usage Monitoring for Intermediate Networking Devices,” U.S. publication No. 2010/0188994, filed March 2, 2009, entitled “Verifiable Service Billing for Intermediate Networking Devices,” U.S. publication No. 2010/0191846, filed March 2, 2009, entitled “Verifiable Service Policy Implementation for Intermediate Networking Devices,” U.S. publication No. 2010/0188992, filed March 2, 2009, entitled “Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy for Intermediate Networking Devices,” U.S. publication No. 2010/0191847, filed March 2, 2009, entitled “Simplified Service Network Architecture,” U.S. publication No. 2010/0197266, filed January 27, 2010, entitled “Device Assisted CDR Creation, Aggregation, Mediation, and Billing,” U.S. publication No. 2010/0198698, filed January 27, 2010, entitled “Adaptive Ambient Services,” U.S. publication No. 2010/0199325, filed January 27, 2010, entitled “Security Techniques for Device Assisted Services,” U.S. publication No. 2010/0197267, filed January 27, 2010, entitled “Device Group Partitions and Settlement Platform,” U.S. publication No. 2010/0198939, filed January 27, 2010, entitled “Device Assisted Services Install,” U.S. publication No. 2010/0195503, filed January 27, 2010, entitled “Quality of Service for Device Assisted Services,” U.S. publication No. 2010/0197268, filed January 28, 2010, entitled “Enhanced Roaming Services and Converged Carrier Networks with Device Assisted Services and a Proxy,” and U.S. application serial No. 13/134,005, filed May 25, 2011, and entitled “System and Method for Wireless Network Offloading,” U.S. application serial No. 13/134,028, filed May 25, 2011, and entitled “Device-Assisted Services for Protecting Network Capacity,” and U.S. application serial No. 13/229,580, filed September 9, 2011, and entitled “Wireless Network Service Interfaces.”

[0002] This application claims priority to and incorporates by reference the following U.S. pending provisional patent applications: U.S. provisional application serial No. 61/381,159, filed September 9, 2010, entitled “Device Assisted Services for Protecting Network Capacity,” U.S. provisional application serial No. 61/381,162, filed September 9, 2010, entitled “Service Controller Interfaces and Workflows,” U.S. provisional application serial No. 61/384,456, filed September 20, 2010, entitled “Securing Service Processor with Sponsored SIMs,” U.S. provisional application serial No. 61/389,547, filed October 4, 2010, entitled “User Notifications for Device Assisted Services,” U.S. provisional application serial No. 61/385,020, filed

September 21, 2010, entitled “Service Usage Reconciliation System Overview,” U.S. provisional application serial No. 61/387,243, filed September 28, 2010, entitled “Enterprise and Consumer Billing Allocation for Wireless Communication Device Service Usage Activities,” U.S. provisional application serial No. 61/387,247, filed September 28, 2010, entitled “Secured Device Data Records,” U.S. provisional application serial No. 61/407,358, filed October 27, 2010, entitled “Service Controller and Service Processor Architecture,” U.S. provisional application serial No. 61/418,507, filed December 1, 2010, entitled “Application Service Provider Interface System,” U.S. provisional application serial No. 61/418,509, filed December 1, 2010, entitled “Service Usage Reporting Reconciliation and Fraud Detection for Device Assisted Services,” U.S. provisional application serial No. 61/420,727, filed December 7, 2010, entitled “Secure Device Data Records,” U.S. provisional application serial No. 61/422,565, filed December 13, 2010, entitled “Service Design Center for Device Assisted Services,” U.S. provisional application serial No. 61/422,572, filed December 13, 2010, entitled “System Interfaces and Workflows for Device Assisted Services,” U.S. provisional application serial No. 61/422,574, filed December 13, 2010, entitled “Security and Fraud Detection for Device Assisted Services,” U.S. provisional application serial No. 61/435,564, filed January 24, 2011, entitled “Framework for Device Assisted Services,” and U.S. provisional application serial No. 61/472,606, filed April 6, 2011, entitled “Managing Service User Discovery and Service Launch Object Placement on a Device.”

[0003] Further, this application incorporates by reference the following U.S. provisional patent applications: U.S. provisional application serial No. 61/206,354, filed January 28, 2009, entitled “Services Policy Communication System and Method,” U.S. provisional application serial No. 61/206,944, filed February 4, 2009, entitled “Services Policy Communication System and Method,” U.S. provisional application serial No. 61/207,393, filed February 10, 2009, entitled “Services Policy Communication System and Method,” U.S. provisional application serial No. 61/207,739, filed February 13, 2009, entitled “Services Policy Communication System and Method,” U.S. provisional application serial No. 61/270,353, filed July 6, 2009, entitled “Device Assisted CDR Creation, Aggregation, Mediation and Billing,” U.S. provisional application serial No. 61/275,208, filed August 25, 2009, entitled “Adaptive Ambient Services,” U.S. provisional application serial No. 61/237,753, filed August 28, 2009, entitled “Adaptive Ambient Services,” U.S. provisional application serial No. 61/252,151, filed October 15, 2009, entitled “Security

Techniques for Device Assisted Services,” U.S. provisional application serial No. 61/252,153, filed October 15, 2009, entitled “Device Group Partitions and Settlement Platform,” U.S. provisional application serial No. 61/264,120, filed November 24, 2009, entitled “Device Assisted Services Install,” U.S. provisional application serial No. 61/264,126, filed November 24, 2009, entitled “Device Assisted Services Activity Map,” and U.S. provisional application serial No. 61/348,022, filed May 25, 2010, entitled “Device Assisted Services for Protecting Network Capacity.”

BACKGROUND OF THE INVENTION

[0004] With the advent of mass market digital communications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access), LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access), and Wi-Fi (Wireless Fidelity) wireless networks increasingly becoming user capacity constrained. Although wireless network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

[0005] Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user, wire line user service consumption habits are trending toward very high bandwidth applications that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Various embodiments are disclosed in the following detailed description and the accompanying drawings.

[0007] **Figure 1** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

[0008] **Figure 2** illustrates another wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

[0009] **Figure 3** illustrates another wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

[0010] **Figure 4** illustrates provisioning of a wireless network for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

[0011] **Figure 5** illustrates a network architecture for providing device assisted CDRs in accordance with some embodiments.

[0012] **Figure 6** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments.

[0013] **Figure 7** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments.

[0014] **Figure 8** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments.

[0015] **Figure 9** is a functional diagram illustrating a device based service processor and a service controller in accordance with some embodiments.

[0016] **Figure 10** provides a table summarizing various service processor functional elements in accordance with some embodiments.

[0017] **Figure 11** provides a table summarizing various service controller functional elements in accordance with some embodiments.

[0018] **Figure 12** illustrates a device stack providing various service usage measurement from various points in the networking stack for a service monitor agent, a billing agent, and an access control integrity agent to assist in verifying the service usage measures and billing reports in accordance with some embodiments.

[0019] **Figure 13** illustrates an embodiment similar to Figure 12 in which some of the service processor is implemented on the modem and some of the service processor is implemented on the device application processor in accordance with some embodiments.

[0020] **Figure 14** illustrates various embodiments of intermediate networking devices that include a service processor for the purpose of verifiable service usage measurement, reporting, and billing reports in accordance with some embodiments.

[0021] **Figure 15** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including a proxy server in accordance with some embodiments.

[0022] **Figure 16** is a functional diagram illustrating the service control device link of the service processor and the service control service link of the service controller in accordance with some embodiments.

[0023] **Figure 17** is a functional diagram illustrating framing structure of a service processor communication frame and a service controller communication frame in accordance with some embodiments.

[0024] **Figures 18A through 18E** provide tables summarizing various service processor heartbeat functions and parameters in accordance with some embodiments.

[0025] **Figures 19A through 19G** provide tables summarizing various device based service policy implementation verification techniques in accordance with some embodiments.

[0026] Figures 20A through 20C provide tables summarizing various techniques for protecting the device based service policy from compromise in accordance with some embodiments.

[0027] Figure 21 illustrates an example embodiment of a process to start or stop a data session with SGSN notification.

[0028] Figure 22 illustrates an example embodiment of a process to start or stop a data session with GGSN notification.

DETAILED DESCRIPTION

[0029] The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term ‘processor’ refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

[0030] A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

[0031] There are many new types of digital devices where it is becoming desirable, for example, to connect these devices to wireless networks including wireless wide area networks (WWAN, such as 3G and 4G) and/or wireless local area (WLAN) networks. These devices include, for example, consumer electronics devices, business user devices, and machine to machine devices that benefit from flexible wide area data connections and the Internet. Example devices include netbooks, notebooks, mobile Internet devices, personal navigation (e.g., GPS

enabled) devices, music and multimedia players, eReaders, industrial telemetry, automotive emergency response and diagnostics, 2-way home and industrial power metering and control, vending machines, parking meters, and many other devices. For example, it is highly advantageous to offer service usage and service billing plans for such devices that are more optimal for each type of device and each type of desired user experience. To accomplish this, more sophisticated service usage measuring and service usage billing systems are needed as compared to the conventional network based techniques in existence today. By providing more flexibility in service measurement and billing, more advantageous and cost effective service plans can be created for, for example, the new WWAN connected devices cited above for all three markets (e.g., consumer, business and machine to machine) that still maintain the necessary profit margins for the WWAN carriers to be successful with these various service businesses.

[0032] Accordingly, various embodiments disclosed herein provide for a new and flexible augmentation or replacement for existing carrier network service usage measurement, service usage accounting, and service usage billing systems and techniques.

[0033] A charging data record (CDR) is a term that as used herein defines a formatted measure of device service usage information, typically generated by one or more network functions that supervise, monitor, and/or control network access for the device. CDRs typically form the basis for recording device network service usage, and often form the basis for billing for such usage. Various embodiments are provided herein for device assisted CDR creation, mediation, and billing. There are many limitations to the capabilities of service usage recording, aggregation and/or billing when CDRs are generated exclusively by network based functions or equipment. Accordingly, by either augmenting network based service usage measures with device based service usage measures, or by replacing network based service usage measures with device based service usage measures, it is possible to create a CDR generation, aggregation, mediation and/or billing solution that has superior or more desirable capabilities/features. While in theory, many of the service usage measures that can be evaluated on a device can also be evaluated in the network data path using various network equipment technologies including but not limited to deep packet inspection (DPI), there are many examples where measuring service usage at the device is either more desirable or more practical, or in some cases it is the only way to obtain the desired measure. Such examples include but are not limited to the following:

- Application layer service usage measures (e.g., traffic usage categorized by application or by combinations of application, destination, and/or content type);
- Usage measures that do not involve user traffic but instead involve network overhead traffic (e.g., basic connection maintenance traffic, signaling traffic, network logon/AAA/authentication/monitoring traffic, service software update traffic);
- Usage that is associated with services that are charged to another entity other than the end user (e.g., basic network connection service offer traffic, traffic associated with providing network access to or downloading service marketing information, traffic associated with advertiser sponsored services, traffic associated with content provider sponsored services, 911 service traffic);
- Usage measures involving encrypted traffic (e.g., traffic that is run over encrypted networking protocols or between secure end points);
- Implementing service usage measure collection and/or service usage billing across multiple networks that may have different and in some cases incompatible, inaccessible (to the CDR system of record) or incomplete service usage measurement capabilities;
- Service usage measurement and/or service usage billing capabilities that are not supported by the present network gateways, routers, MWC/HLRs, AAA, CDR aggregation, CDR mediation, billing and/or provisioning systems;
- New service usage measures and/or new service usage billing capabilities that are desirable to implement in a manner that does not require major changes or upgrades to the existing network gateways, routers, MWC/HLRs, AAA, CDR aggregation, CDR mediation, billing and/or provisioning systems;
- New service usage measures and/or new service usage billing capabilities that are desirable to implement in a manner that allows for rapid definition and implementation of new service measures and/or billing plans;
- New service usage measures and/or new service usage billing capabilities that are desirable to implement in a manner that may be implemented in a manner that enables multiple device group definitions in which each device group gets a customized programmable definition for service usage collection, accounting and/or billing;
- Multi device billing;
- Multi user billing;

- Intermediate device billing with single user and multi user with and without multi device;
- Content downloads from a specific source to a specific application with the content being of a specific type or even identified down to a particular content ID; and/or
- Various other single event transactions used for billing purposes.

For these and other reasons, it is desirable to provide a system/process that utilizes device assisted service usage measures that provides either an enhancement of existing network based service usage CDR system capabilities and techniques and/or a replacement for network based CDR system capabilities and techniques.

[0034] In some embodiments, techniques, such as a system and/or process, that utilize device assisted service usage measures include one or more of the following: (1) receiving a service usage measure from a device in communication with a wireless network, (2) verifying or protecting the validity of the service usage measure, (3) generating a CDR based on the service usage measure (e.g., device assisted CDR), (4) aggregating CDRs, and (5) mediating the CDR with network CDRs. In some embodiments, the techniques also include providing a design and provisioning of devices/network equipment to recognize the CDRs. In some embodiments, the techniques also include provisioning to recognize that the device belongs to a Device Assisted Services (DAS) device group and that corresponding CDRs should be accepted and mediated. In some embodiments, the device assisted CDRs are also generated using formats, network communications protocols, network device authentication and/or provisioning to allow device assisted CDRs into the network CDR system, encryption, and/or signatures as required by the network (e.g., to comply with network generated CDR requirements or based on any other network and/or service provider requirements and/or standards).

[0035] In some embodiments, mediation rules include multi device, multi user, single user devices, and/or intermediate networking devices that can be single user or multi user, as described herein.

[0036] In some embodiments, a device assisted CDR generator collects device based service usage measures that are used as the basis for, or as an enhancement (e.g., as a supplement or in addition) to, one or more (e.g., network generated) CDRs that provide one or more networking functions with properly formatted service usage reports that the network function(s) accepts as

being transmitted from an authorized source, read, and utilized for helping to determine the service usage of a device or group of devices. In some embodiments, the network functions that the device assisted CDR generator shares CDRs with typically include one or more of the following: service usage/CDR aggregation and/or mediation servers, gateways, routers, communication nodes, Mobile Wireless Centers (MWCs, including HLRs), databases, AAA systems, billing interfaces, and billing systems. For example, the process of CDR creation in the CDR generator typically includes either using one or more device based measures of service usage, or one or more device based measures of service usage in combination with one or more network based measures of service usage, possibly processing one or more of such service usage measures according to a set of CDR creation, CDR aggregation, and/or CDR mediation rules to arrive at a final device usage measure that is, for example, then formatted with the proper syntax, framed, possibly encrypted and/or signed, and encapsulated in a communication protocol or packet suitable for sharing with network functions. In some embodiments, the CDR generator resides in the device. In some embodiments, the CDR generator resides in a network server function that receives the device assisted service usage measures, along with possibly network based usage measures, and then creates a CDR (e.g., in the service controller 122).

[0037] In some embodiments, the device assisted CDR generator can reside in the service processor (e.g., service processor 115), for example, in the service usage history or billing server functions. In some embodiments, the device assisted CDR generator resides in the device itself, for example, within the service processor functions, such as the billing agent or the service monitor agent.

[0038] There are several factors that are considered in the various embodiments in order to create a useful, reliable, and secure device assisted CDR system, including, for example, but not limited to:

- Identification of each device based service usage measure with one or more usage transaction codes;
- Verification of the device based usage measure(s);
- Secure communication of the device based usage measures to the network;

- Efficient (e.g., low bandwidth) communication of the device based service usage measure;
- Coordination/comparison/aggregation of the device based service usage measure with network based service usage measure(s);
- Formatting the device based service usage measure into a CDR that can be properly communicated to the network functions and/or equipment that process service usage information;
- Causing the network based functions and/or equipment used for CDR collection, aggregation, mediation and/or billing to recognize, authorize, and accept communications and CDRs from the device assisted CDR generator, reading and properly implementing the correct network session context for the CDR so that the CDR is properly associated with the correct device /user/session;
- Implementing the CDR aggregation rules that determine how to collect and aggregate the device assisted CDRs as they are reported through the network CDR system hierarchy;
- Implementing the mediation rules that determine how the various device based service usage transaction code measures are combined and mediated with the other device based service usage transaction code measures to result in consistent service usage information for each of the transaction code categories maintained in the network;
- Implementing the mediation rules that determine how the device assisted CDRs are combined and mediated with network based CDRs to result in consistent service usage information for each of the transaction code categories maintained in the network;
- Implementing mediation rules to reconcile the variances between network based CDR usage measures and device assisted CDR usage measures;
- Classification of one or more device groups, with each group having the capability to uniquely define the service usage collection, accounting, and/or billing rules;
- Collecting CDRs generated on networks other than the home network so that service usage may be measured, accounted for, and/or billed for across multiple networks;
- Multi device billing;
- Multi user billing; and/or
- Intermediate device billing with single user and multi user with and without multi device.

[0039] In some embodiments, verification of the relative accuracy of the device assisted service usage measure is provided. Given that, for example, the service usage measure is often being generated on an end user device or a device that is readily physically accessed by the general public or other non-secure personnel from a network management viewpoint, in some embodiments, the device agents used in one or more of the service processor 115 agents are protected from hacking, spoofing, and/or other misuse. Various techniques are provided herein for protecting the integrity of the agents used for generating the device assisted service usage measures.

[0040] In some embodiments, the service usage measures are verified by network based cross checks using various techniques. For example, network based cross checks can provide valuable verification techniques, because, for example, it is generally not possible or at least very difficult to defeat well designed network based cross checks using various techniques, such as those described herein, even if, for example, the measures used to protect the device agents are defeated or if no device protection measures are employed. In some embodiments, network based cross checks used to verify the device assisted service usage measures include comparing network based service usage measures (e.g. CDRs generated by service usage measurement apparatus in the network equipment, such as the BTS/BSCs 125, RAN Gateways 410, Transport Gateways 420, Mobile Wireless Center/HLRs 132, AAA 121, Service Usage History/CDR Aggregation, Mediation, Feed 118, or other network equipment), sending secure query/response command sequences to the service processor 115 agent(s) involved in device assisted CDR service usage measurement or CDR creation, sending test service usage event sequences to the device and verifying that the device properly reported the service usage, and using various other techniques, such as those described herein with respect to various embodiments.

[0041] In some embodiments, one or more of the following actions are taken if the device based service usage measure is found to be in error or inaccurate: bill the user for usage overage or an out of policy device, suspend the device, quarantine the device, SPAN the device, and/or report the device to a network administration function or person.

[0042] In some embodiments, the CDR syntax used to format the device assisted service usage information into a CDR and/or network communication protocols for transmitting CDRs are

determined by industry standards (e.g., various versions of 3GPP TS 32.215 format and 3GPP2 TSG-X X.S0011 or TIA-835 format). In some embodiments, for a given network implementation the network designers will specify modifications of the standard syntax, formats and/or network communication/transmission protocols. In some embodiments, for a given network implementation the network designers will specify syntax, formats, and/or network communication/transmission protocols that are entirely different than the standards.

[0043] In some embodiments, within the syntax and formatting for the CDR the device assisted service usage is typically categorized by a transaction code. For example, the transaction code can be similar or identical to the codes in use by network equipment used to generate CDRs, or given that the device is capable of generating a much richer set of service usage measures, the transaction codes can be a superset of the codes used by network equipment used to generate CDRs (e.g., examples of the usage activities that can be labeled as transaction codes that are more readily supported by device assisted CDR systems as compared to purely network based CDR systems are provided herein).

[0044] In some embodiments, the device sends an identifier for a usage activity tag, an intermediate server determines how to aggregate into CDR transaction codes and which CDR transaction code to use.

[0045] In some embodiments, the device service processor 115 compartmentalizes usage by pre-assigned device activity transaction codes (e.g., these can be sub-transactions within the main account, transactions within a given bill-by-account transaction or sub-transactions within a bill-by-account transaction). The device implements bill-by-account rules to send different usage reports for each bill-by-account function. In some embodiments, the service controller 122 programs the device to instruct it on how to compartmentalize these bill-by-account service usage activities so that they can be mapped to a transaction code.

[0046] In some embodiments, the device reports less compartmentalized service usage information and the service controller 122 does the mapping of service usage activities to CDR transaction codes, including in some cases bill-by-account codes.

[0047] In some embodiments, the CDR sent to 118 or other network equipment, for example, can include various types of transaction codes including but not limited to a raw device usage CDR, a bill-by-account (e.g., a sub-activity transaction code) CDR, a billing offset CDR, and/or a billing credit CDR. For example, the decision logic (also referred to as business rules or CDR aggregation and mediation rules) that determines how these various types of CDR transaction codes are to be aggregated and mediated by the core network and the billing system can be located in the network equipment (e.g., a network element, such as service usage 118), in the service controller 122, and/or in the billing system 123.

[0048] In some embodiments, the device assisted CDR generator uses the device assisted service usage measures to generate a CDR that includes service usage information, service usage transaction code(s), and, in some embodiments, network information context. In some embodiments, the service usage information, transaction code, and/or network information context is formatted into communication framing, syntax, encryption/signature, security and/or networking protocols that are compatible with the formatting used by conventional networking equipment to generate CDRs. For example, this allows networking equipment used for CDR collection, recording, aggregation, mediation, and/or conversion to billing records to properly accept, read, and interpret the CDRs that are generated with the assistance of device based service usage measurement. In some embodiments, the device assisted service measures are provided to an intermediate network server referred to as a service controller (e.g., service controller 122). In some embodiments, the service controller uses a CDR feed aggregator for a wireless network to collect device generated usage information for one or more devices on the wireless network; and provides the device generated usage information in a syntax (e.g., charging data record (CDR)), and a communication protocol (e.g., 3GPP or 3GPP2, or other communication protocol(s)) that can be used by the wireless network to augment or replace network generated usage information for the one or more devices on the wireless network.

[0049] In some embodiments, mediation rules include multi device, multi user, single user devices, intermediate networking devices that can be single user or multi user. For example, the device assisted CDRs can be formatted by the device assisted CDR generator to include a transaction code for one user account, even though the CDRs originate from multiple devices that all belong to the same user. This is an example for a multi-user device assisted CDR billing

solution. In another example for a multi-user device assisted CDR billing solution, device assisted CDRs from multiple devices and multiple users can all be billed to the same account (e.g., a family plan or a corporate account), but the bill-by-account CDR transaction records can be maintained through the billing system so that sub-account visibility is provided so that the person or entity responsible for the main account can obtain visibility about which users and/or devices are creating most of the service usage billing. For example, this type of multi-user, multi-device device assisted CDR billing solution can also be used to track types of service usage and/or bill for types of service usage that are either impossible or at least very difficult to account and/or bill for with purely network based CDR systems. In some embodiments, bill-by-account CDR transaction records can be used to provide sponsored transaction services, account for network chatter, provide service selection interfaces, and other services for multi-user or multi-device service plans.

[0050] In addition to conventional single user devices (e.g., cell phones, smart phones, netbooks/notebooks, mobile internet devices, personal navigation devices, music players, electronic eReaders, and other single user devices) device assisted service usage measurement and CDRs are also useful for other types of network capable devices and/or networking devices, such as intermediate networking devices (e.g., 3G/4G WWAN to WLAN bridges/routers/gateways, femto cells, DOCSIS modems, DSL modems, remote access/backup routers, and other intermediate network devices). For example, in such devices, particularly with a secure manner to verify that the device assisted service usage measures are relatively accurate and/or the device service processor 115 software is not compromised or hacked, many new service provider service delivery and billing models can be supported and implemented using the techniques described herein. For example, in a WiFi to WWAN bridge or router device multiple user devices can be supported with the same intermediate networking device in a manner that is consistent and compatible with the central provider's CDR aggregation and/or billing system by sending device assisted CDRs as described herein that have a service usage and/or billing code referenced to the end user and/or the particular intermediate device.

[0051] In some embodiments, the device assisted CDRs generated for the intermediate networking device are associated with a particular end user in which there can be several or many end users using the intermediate networking device for networking access, and in some

embodiments, with each end user being required to enter a unique log-in to the intermediate networking device. For example, in this way, all devices that connect using WiFi to the intermediate networking device to get WWAN access generate CDRs can either get billed to a particular end user who is responsible for the master account for that device, or the CDRs can get billed in a secure manner, with verified relative usage measurement accuracy to multiple end users from the same intermediate networking device. In another example, an end user can have one account that allows access to a number of intermediate networking devices, and each intermediate networking device can generate consistent device assisted CDRs with transaction codes for that end user regardless of which intermediate networking device the end user logs in on.

[0052] In some embodiments, some of the services provided by the intermediate networking device are billed to a specific end user device assisted CDR transaction code, while other bill-by-account services are billed to other transaction code accounts, such as sponsored partner transaction service accounts, network chatter accounts, sponsored advertiser accounts, and/or service sign up accounts. For example, in this manner, various embodiments are provided in which intermediate networking devices (e.g., a WWAN to WiFi router/bridge) can sold to one user but can service and be used to bill other users (e.g., and this can be covered in the first purchasing user's service terms perhaps in exchange for a discount), or such intermediate networking devices can be located wherever access is desired without concern that the device will be hacked into so that services can be acquired without charge.

[0053] In some embodiments, various types of service usage transactions are billed for on the intermediate networking device, to any of one or more users, in which the information required to bill for such services is not available to the central provider or MVNO network equipment, just as is the case with, for example, conventional single user devices. In view of the various embodiments and techniques described herein, those skilled in the art will appreciate that similar service models are equally applicable not just to WWAN to WiFi intermediate networking devices, but also to the Femto Cell, remote access router, DOCSIS, DSL and other intermediate WWAN to WiFi networking devices.

[0054] **Figure 1** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments. As shown, Figure 1 includes a 4G/3G/2G wireless network operated by, for example, a central provider. As shown, various wireless devices 100 are in communication with base stations 125 for wireless network communication with the wireless network, and other devices 100 are in communication with Wi-Fi Access Points (APs) or Mesh 702 for wireless communication to Wi-Fi Access CPE 704 in communication with central provider access network 109. In some embodiments, each of the wireless devices 100 includes a service processor 115 (as shown), and each service processor connects through a secure control plane link to a service controller 122. In some embodiments, the network based service usage information (e.g., CDRs) is obtained from one or more network elements. As shown, an MVNO core network 210 also includes a CDR storage, aggregation, mediation, feed 118, a MVNO billing interface 122, and a MVNO billing system 123 (and other network elements as shown in Figure 1).

[0055] As shown in Figure 1, a CDR storage, aggregation, mediation, feed 118 (e.g., service usage 118, including a billing aggregation data store and rules engine) is a functional descriptor for, in some embodiments, a device/network level service usage information collection, aggregation, mediation, and reporting function located in one or more of the networking equipment components attached to one or more of the sub-networks shown in Figure 1 (e.g., central provider access network 109 and/or central provider core network 110), which is in communication with the service controller 122, and a central billing interface 127. As shown in Figure 1, service usage 118 is shown as a function in communication with the central provider core network 110. In some embodiments, the CDR storage, aggregation, mediation, feed 118 function is located elsewhere in the network or partially located in elsewhere or integrated with as part of other network elements. In some embodiments, CDR storage, aggregation, mediation, feed 118 functionality is located or partially located in the AAA server 121 and/or the mobile wireless center/Home Location Register(HLR) 132 (as shown, in communication with a DNS/DHCP server 126). In some embodiments, service usage 118 functionality is located or partially located in the base station, base station controller and/or base station aggregator, collectively referred to as base station 125 in Figure 1. In some embodiments, CDR storage, aggregation, mediation, feed 118 functionality is located or partially located in a networking component in the central provider access network 109, a networking component in the core

network 110, the central billing system 123, the central billing interface 127, and/or in another network component or function. This discussion on the possible locations for the network based and device based service usage information collection, aggregation, mediation, and reporting function (e.g., CDR storage, aggregation, mediation, feed 118) can be easily generalized as described herein and as shown in the other figures described herein by one of ordinary skill in the art. Also as shown in Figure 1, the service controller 122 is in communication with the central billing interface 123 (also sometimes referred to as the external billing management interface or billing communication interface) 127, which is in communication with the central billing system 123. As shown, an order management 180 and subscriber management 182 are also in communication with the central provider core network 110 for facilitating order and subscriber management of services for the devices 100 in accordance with some embodiments.

[0056] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) provides a device/network level service usage information collection, aggregation, mediation, and reporting function. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) collects device generated usage information for one or more devices on the wireless network (e.g., devices 100); and provides the device generated usage information in a syntax and a communication protocol that can be used by the wireless network to augment or replace network generated usage information for the one or more devices on the wireless network. In some embodiments, the syntax is a charging data record (CDR), and the communication protocol is selected from one or more of the following: 3GPP, 3GPP2, or other communication protocols. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) includes a service usage data store (e.g., a billing aggregator) and a rules engine for aggregating the collected device generated usage information. In some embodiments, the syntax is a charging data record (CDR), and the network device is a CDR feed aggregator, and the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) also aggregates CDRs for the one or more devices on the wireless network; applies a set of rules to the aggregated CDRs using a rules engine (e.g., bill by account, transactional billing, and/or any other billing or other rules for service usage information collection, aggregation, mediation, and reporting), and communicates a new set of CDRs for the

one or more devices on the wireless network to a billing interface or a billing system (e.g., providing a CDR with a billing offset by account/service). In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates a new set of CDRs for the one or more devices on the wireless network to a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates with a service controller to collect the device generated usage information for the one or more devices on the wireless network. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates with a service controller, in which the service controller is in communication with a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates the device generated usage information to a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed (and/or other network elements or combinations of network elements) communicates with a transport gateway and/or a Radio Access Network (RAN) gateway to collect the network generated usage information for the one or more devices on the wireless network. In some embodiments, the service controller 122 communicates the device generated service usage information to the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements).

[0057] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs rules for performing a bill by account aggregation and mediation function. In some embodiments, the service controller 122 in communication with the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device generated usage information. In some embodiments, a rules engine device in communication with the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device generated usage information.

[0058] In some embodiments, the rules engine is included in (e.g., integrated with/part of) the CDR storage, aggregation, mediation, feed 118. In some embodiments, the rules engine and associated functions, as described herein, is a separate function/device. In some embodiments, the service controller 122 performs some or all of these rules engine based functions, as described herein, and communicates with the central billing interface 127. In some embodiments, the service controller 122 performs some or all of these rules engine based functions, as described herein, and communicates with the central billing system 123.

[0059] In some embodiments, duplicate CDRs are sent from the network equipment to the billing system 123 that is used for generating service billing. In some embodiments, duplicate CDRs are filtered to send only those CDRs/records for devices controlled by the service controller and/or service processor (e.g., the managed devices). For example, this approach can provide for the same level of reporting, lower level of reporting, and/or higher level of reporting as compared to the reporting required by the central billing system 123.

[0060] In some embodiments, a bill-by-account billing offset is provided. For example, bill-by-account billing offset information can be informed to the central billing system 123 by providing a CDR aggregator feed that aggregates the device based service usage data feed to provide a new set of CDRs for the managed devices to the central billing interface 127 and/or the central billing system 123. In some embodiments, transaction billing is provided using similar techniques. For example, transaction billing log information can be provided to the central billing interface 127 and/or the central billing system 123.

[0061] In some embodiments, the rules engine (e.g., performed by the service usage 118 or another network element, as described herein) provides a bill-by-account billing offset. For example, device generated usage information (e.g., charging data records (CDRs)) includes a transaction type field (e.g., indicating a type of service for the associated service usage information). The rules engine can apply a rule or a set of rules based on the identified service associated with the device generated usage information to determine a bill-by-account billing offset (e.g., a new CDR can be generated to provide the determined bill-by-account billing offset). In some examples, the determined bill-by-account billing offset can be provided as a credit to the user's service usage account (e.g., a new CDR can be generated with a negative

offset for the user's service usage account, such as for network chatter service usage, or transactional service usage, or for any other purposes based on one or more rules performed by the rules engine).

[0062] As another example, for a transactional service, a first new CDR can be generated with a negative offset for the user's service usage account for that transactional service related usage, and a second new CDR can be generated with a positive service usage value to charge that same service usage to the transactional service provider (e.g., Amazon, eBay, or another transactional service provider). In some embodiments, the service controller 122 generates these two new CDRs, and the service usage 118 stores, aggregates, and communicates these two new CDRs to the central billing interface 127. In some embodiments, the service controller 122 generates these two new CDRs, and the service usage 118 stores, aggregates, and communicates these two new CDRs to the central billing interface 127, in which the central billing interface 127 applies rules (e.g., performs the rules engine for determining the bill-by-account billing offset).

[0063] In some embodiments, the service controller 122 sends the device generated CDRs to the rules engine (e.g., service usage 118), and the rules engine applies one or more rules, such as those described herein and/or any other billing/service usage related rules as would be apparent to one of ordinary skill in the art. In some embodiments, the service controller 122 generates CDRs similar to other network elements, and the rules (e.g., bill-by-account) are performed in the central billing interface 127. For example, for the service controller 122 to generate CDRs similar to other network elements, in some embodiments, the service controller 122 is provisioned on the wireless network and behaves substantially similar to other CDR generators on the network) as would be apparent to one of ordinary skill in the art.

[0064] In some embodiments, the service controller 122 is provisioned as a new type of networking function that is recognized as a valid and secure source for CDRs by the other necessary elements in the network (e.g., the Service Usage History/ CDR Aggregation and Mediation Server 118). In some embodiments, in which the network apparatus typically only recognize CDRs from certain types of networking equipment (e.g., RAN Gateway 410 or Transport Gateway 420 (as shown in Figure 3)), then the Service Controller 122 can provide authentication credentials to the other networking equipment that indicate it is one of the

approved types of equipment (e.g., for purposes of generating/providing CDRs). In some embodiments, the link between the Service Controller 122 and the necessary CDR aggregation and mediation equipment is secured, authenticated, encrypted and/or signed.

[0065] In some embodiments, the CDR storage, aggregation, mediation, feed 118 discards the network based service usage information (e.g., network based CDRs) received from one or more network elements. In these embodiments, the service controller 122 can provide the device based service usage information (e.g., device based CDRs) to the CDR storage, aggregation, mediation, feed 118 (e.g., the CDR storage, aggregation, mediation, feed 118 can just provide a store, aggregate, and communication function(s)), and the device based service usage information is provided to the central billing interface 127 or the central billing system 123.

[0066] In some embodiments, the device based CDRs and/or new CDRs generated based on execution of a rules engine as described herein is provided only for devices that are managed and/or based on device group, service plan, or any other criteria, categorization, and/or grouping.

[0067] **Figure 2** illustrates another wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments. As shown in Figure 2, some devices 100 are in communication with DOCSIS Head End 125 and some devices 100 are in communication with DSLAM 125, which are in communication with the central provider access network 109.

[0068] **Figure 3** illustrates another wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

Referring now to the 4G/3G/2G access network as shown in Figure 3, the 4G/3G and 3G/2G base stations/nodes 125 are in communication with a 4G/3G/2G Radio Access Network (RAN) gateway 410 via a radio access network 405, which are in communication with a 4G/3G/2G transport gateway 420 via an access transport network 415. The central provider core network 110 is in network communication with the access transport network 415 (e.g., via a dedicated/leased line, and as shown, via a firewall 124). The Internet 120 is available via a firewall 124 and the transport gateway(s) 420, as shown. Also, as shown, a network apparatus provisioning system 160, order management 180, and subscriber management 182 are in communication with the central provider core network 110. As shown, a AAA server 121, a

mobile wireless center/Home Location Register(HLR) 132, a DNS/DHCP 126, and CDR storage, aggregation, mediation, feed 118 are also in communication with the access transport network 415. The central billing system 123 and the central billing interface 127 are shown in communication with the central provider core network 110.

[0069] As shown, Figure 3 includes a 4G/3G/2G wireless network operated by, for example, a central provider. In some embodiments, each of the wireless devices 100 includes a service processor 115 (as shown), and each service processor connects through a secure control plane link to a service controller 122. In some embodiments, the network based service usage information (e.g., network generated CDRs) is obtained from Radio Access Network (RAN) gateway(s) 410 and/or transport gateway(s) 420. In some embodiments, device based service usage information (e.g., device assisted CDRs) are generated by the service processor 115 and/or service controller 122 for some or all of the wireless devices 100 using similar techniques as described herein, and in some embodiments, such device based service usage information (e.g., device assisted CDRs) is sent to the CDR storage, aggregation, mediation, feed 118 (e.g., the CDR storage, aggregation, mediation, feed 118 can just provide a store, aggregate, and communication function(s)), and/or to the central billing interface 127 or the central billing system 123, as similarly described herein with respect to various embodiments.

[0070] **Figure 4** illustrates provisioning of a wireless network for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments. As shown in Figure 4, the provisioning of various network equipment is provided as shown to recognize each other as an authorized source of CDRs (e.g., this can be done manually or in an automated manner). For example, order management 180, subscriber management, billing interface 127, billing system 123, network provisioning system 160, service controller 122, access network AAA server 121, mobile wireless center 132, and CDR storage, aggregation, mediation feed 118 communicate with each other for such provisioning, which can be implemented using various techniques. In some embodiments, the various network elements are provisioned to recognize device assisted CDRs being generated by the service controller 122, which, for example, can be provided to the billing interface 127 and/or the billing system 123. In some embodiments, network generated CDRs are provided by RAN/Access gateway 410,

aggregation/transport gateway 425, and/or base station controller 125. In some embodiments, other network elements generate/receive/store device assisted CDRs.

[0071] In some embodiments, provisioning of various network equipment is provided to recognize a given device as belonging to a device group that supports a service usage and/or billing plan that relies upon and/or utilizes device assisted CDRs.

[0072] In some embodiments, the CDR formats, transaction codes, and CDR transmission destinations are programmed for each device that generates CDRs, including the service controller 122 (e.g., in some embodiments, the service controller 122 is the intermediary for CDRs) and/or service processor 115 (e.g., in some embodiments, the device sends CDRs to network CDR aggregation or billing interface 127/billing system 123 with no intermediate server function).

[0073] **Figure 5** illustrates a network architecture for providing device assisted CDRs in accordance with some embodiments. As shown, network generated CDRs are sent from various network elements to the CDR storage, aggregation, mediation, feed 118 and the service controller 122, as shown in dashed lines with arrows in Figure 5. In some embodiments, the network generated CDRs are used for verification of device assisted service (DAS) usage and/or billing information. In some embodiments, the network generated CDRs are provided to the service controller 122, and the service controller 122 implements aggregation and/or mediation rules to examine and, in some cases, aggregate and/or mediate network generated/based CDRs with device assisted/based CDRs.

[0074] In some embodiments, device assisted CDRs are sent from the service controller 122 to CDR storage, aggregation, mediation, feed 118 and communicated to the billing system 123, as shown in solid lines with arrows in Figure 5. In some embodiments, CDR storage, aggregation, mediation, feed 118 uses DAS service usage CDRs to augment network generated/based CDRs with bill-by-account transaction codes (e.g., as similarly described herein). In some embodiments, CDR storage, aggregation, mediation, feed 118 implements aggregation and/or mediation rules to account for DAS CDR usage amount in a new bill-by-account transaction code and removes the same service usage amount from the bulk device account transaction code. In some embodiments, a first DAS CDR is sent for the new bill by account transaction code, and

a second DAS CDR is sent to be used as a correction (credit) to the main device usage account transaction code, and CDR storage, aggregation, mediation, feed 118 implements the rules to perform this mediation. In some embodiments, a first DAS CDR is used for a given bill-by-account transaction code, and a second DAS CDR is used as the main device account transaction code, in which the service controller 122 (or device) has already implemented the mediation rules so that CDR storage, aggregation, mediation, feed 118 simply passes such DAS CDRs to billing after aggregating them.

[0075] **Figure 6** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments. Figure 6 also shows the communication of device assisted CDRs and network generated CDRs using solid and dashed lines with arrows, respectively. As shown, in some embodiments, CDR storage, aggregation, mediation, feed 118 sends network based CDRs to service controller 122 for various purposes, such as those previously described herein.

[0076] In some embodiments, service controller 122 sends DAS CDRs to billing for various uses by the billing system 123. In some embodiments, the billing system 123 uses DAS service usage CDRs to augment network based CDRs with bill-by-account transaction codes. In some embodiments, the billing system 123 implements aggregation and/or mediation rules to account for DAS CDR usage amount in a new bill-by-account transaction code and removes the same service usage amount from the bulk device account transaction code. In some embodiments, a first DAS CDR is sent for the new bill by account transaction code, and a second DAS CDR is sent to be used as a correction (credit) to the main device usage account transaction code, and the billing system 123 implements the rules to perform this mediation. In some embodiments, a first DAS CDR is used for a given bill-by-account transaction code, and a second is used as the main device account transaction code, in which the service controller 122 (or device) has already implemented the mediation rules so that the billing system 123 simply passes such DAS CDRs after aggregating them.

[0077] **Figure 7** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments. Figure 7 also shows the communication of device assisted CDRs and network generated CDRs using solid and dashed lines with arrows, respectively.

Figure 7 is similar to Figure 6, except as shown in Figure 7, service usage information is passed through the billing interface 127 instead of the billing CDR aggregation interface. For example, the service usage detailed bill-by-account information and offset (credit) information can be formatted as a CDR or can be formatted in a higher level syntax as required by the billing interface 127.

[0078] Figure 8 illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments. Figure 8 also shows the communication of device assisted CDRs and network generated CDRs using solid and dashed lines with arrows, respectively. In some embodiments, as shown in Figure 8, the central provider need not modify the existing CDR storage, aggregation, mediation, feed 118, so the additional aggregation and mediation rules discussed above with respect to Figure 5 are implemented as a new layer of rules in a new network function, shown as secondary DAS CDR aggregation mediation 118A, that is located between the billing system and the CDR storage, aggregation, mediation, feed 118. For example, this new network function (e.g., secondary DAS CDR aggregation mediation 118A) can reside in the network (as shown) or in the service processor 115, in the service controller 122, or elsewhere in the network or on the device.

[0079] Figure 9 is a functional diagram illustrating a device based service processor 115 and a service controller 122 in accordance with some embodiments. For example, this provides relatively full featured device based service processor implementation and service controller implementation. As shown, this corresponds to a networking configuration in which the service controller 122 is connected to the Internet 120 and not directly to the access network 1610. As shown, a data plane (e.g., service traffic plane) communication path is shown in solid line connections and control plane (e.g., service control plane) communication path is shown in dashed line connections. As will be apparent, the division in functionality between one device agent and another is based on, for example, design choices, networking environments, devices and/or services/applications, and various different combinations can be used in various different implementations. For example, the functional lines can be re-drawn in any way that the product designers see fit. As shown, this includes certain divisions and functional breakouts for device agents as an illustrative implementation, although other, potentially more complex, embodiments can include different divisions and functional breakouts for device agent functionality

specifications, for example, in order to manage development specification and testing complexity and workflow. In addition, the placement of the agents that operate, interact with or monitor the data path can be moved or re-ordered in various embodiments. For example, the functional elements shown in Figure 9 are described below with respect to Figures 10 and 11.

[0080] As shown in Figure 9, service processor 115 includes a service control device link 1691. For example, as device based service control techniques involving supervision across a network become more sophisticated, it becomes increasingly important to have an efficient and flexible control plane communication link between the device agents and the network elements communicating with, controlling, monitoring, or verifying service policy. In some embodiments, the service control device link 1691 provides the device side of a system for transmission and reception of service agent to/from network element functions. In some embodiments, the traffic efficiency of this link is enhanced by buffering and framing multiple agent messages in the transmissions. In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security or encryption are used to make the link robust to discovery, eavesdropping or compromise. In some embodiments, the service control device link 1691 also provides the communications link and heartbeat timing for the agent heartbeat function. As discussed below, various embodiments disclosed herein for the service control device link 1691 provide an efficient and secure solution for transmitting and receiving service policy implementation, control, monitoring and verification information with other network elements.

[0081] As shown in Figure 9, the service controller 122 includes a service control server link 1638. In some embodiments, device based service control techniques involving supervision across a network (e.g., on the control plane) are more sophisticated, and for such it is increasingly important to have an efficient and flexible control plane communication link between the device agents (e.g., of the service processor 115) and the network elements (e.g., of the service controller 122) communicating with, controlling, monitoring, or verifying service policy. For example, the communication link between the service control server link 1638 of service controller 122 and the service control device link 1691 of the service processor 115 can provide an efficient and flexible control plane communication link, a service control link 1653 as

shown in Figure 9, and, in some embodiments, this control plane communication link provides for a secure (e.g., encrypted) communications link for providing secure, bidirectional communications between the service processor 115 and the service controller 122. In some embodiments, the service control server link 1638 provides the network side of a system for transmission and reception of service agent to/from network element functions. In some embodiments, the traffic efficiency of this link is enhanced by buffering and framing multiple agent messages in the transmissions (e.g., thereby reducing network chatter). In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency and/or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security and/or encryption are used to secure the link against potential discovery, eavesdropping or compromise of communications on the link. In some embodiments, the service control server link 1638 also provides the communications link and heartbeat timing for the agent heartbeat function.

[0082] In some embodiments, the service control server link 1638 provides for securing, signing, encrypting and/or otherwise protecting the communications before sending such communications over the service control link 1653. For example, the service control server link 1638 can send to the transport layer or directly to the link layer for transmission. In another example, the service control server link 1638 further secures the communications with transport layer encryption, such as TCP TLS SSH version 1 or 2 or another secure transport layer protocol. As another example, the service control server link 1638 can encrypt at the link layer, such as using IPSEC, various possible VPN services, other forms of IP layer encryption and/or another link layer encryption technique.

[0083] As shown in Figure 9, the service controller 122 includes an access control integrity server 1654. In some embodiments, the access control integrity server 1654 collects device information on service policy, service usage, agent configuration and/or agent behavior. For example, the access control integrity server 1654 can cross check this information to identify integrity breaches in the service policy implementation and control system. In another example, the access control integrity server 1654 can initiate action when a service policy violation or a system integrity breach is suspected.

[0084] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) acts on access control integrity agent 1694 reports and error conditions. Many of the access control integrity agent 1654 checks can be accomplished by the server. For example, the access control integrity agent 1654 checks include one or more of the following: service usage measure against usage range consistent with policies (e.g., usage measure from the network and/or from the device); configuration of agents; operation of the agents; and/or dynamic agent download.

[0085] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy implementations by comparing various service usage measures (e.g., based on network monitored information, such as by using IPDRs or CDRs, and/or local service usage monitoring information) against expected service usage behavior given the policies that are intended to be in place. For example, device service policy implementations can include measuring total data passed, data passed in a period of time, IP addresses, data per IP address, and/or other measures such as location, downloads, email accessed, URLs, and comparing such measures expected service usage behavior given the policies that are intended to be in place.

[0086] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy, and the verification error conditions that can indicate a mismatch in service measure and service policy include one or more of the following: unauthorized network access (e.g., access beyond ambient service policy limits); unauthorized network speed (e.g., average speed beyond service policy limit); network data amount does not match policy limit (e.g., device not stop at limit without re-up/revising service policy); unauthorized network address; unauthorized service usage (e.g., VOIP, email, and/or web browsing); unauthorized application usage (e.g., email, VOIP, email, and/or web); service usage rate too high for plan, and policy controller not controlling/throttling it down; and/or any other mismatch in service measure and service policy. Accordingly, in some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) provides a policy/service control integrity service to continually (e.g., periodically and/or based on trigger events) verify that the service control of the device has not been compromised and/or is not behaving out of policy.

[0087] As shown in Figure 9, service controller 122 includes a service history server 1650. In some embodiments, the service history server 1650 collects and records service usage or service activity reports from the Access Network AAA Server 1621 and the Service Monitor Agent 1696. For example, although service usage history from the network elements can in certain embodiments be less detailed than service history from the device, the service history from the network can provide a valuable source for verification of device service policy implementation, because, for example, it is extremely difficult for a device error or compromise event on the device to compromise the network based equipment and software. For example, service history reports from the device can include various service tracking information, as similarly described above. In some embodiments, the service history server 1650 provides the service history on request to other servers and/or one or more agents. In some embodiments, the service history server 1650 provides the service usage history to the device service history 1618. In some embodiments, for purposes of facilitating the activation tracking service functions (described below), the service history server 1650 maintains a history of which networks the device has connected to. For example, this network activity summary can include a summary of the networks accessed, activity versus time per connection, and/or traffic versus time per connection. As another example, this activity summary can further be analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.

[0088] As shown in Figure 9, service controller 122 includes a policy management server 1652. In some embodiments, the policy management server 1652 transmits policies to the service processor 115 via the service control link 1653. In some embodiments, the policy management server 1652 manages policy settings on the device (e.g., various policy settings as described herein with respect to various embodiments) in accordance with a device service profile. In some embodiments, the policy management server 1652 sets instantaneous policies on policy implementation agents (e.g., policy implementation agent 1690). For example, the policy management server 1652 can issue policy settings, monitor service usage and, if necessary, modify policy settings. For example, in the case of a user who prefers for the network to manage their service usage costs, or in the case of any adaptive policy management needs, the policy management server 1652 can maintain a relatively high frequency of communication with the device to collect traffic and/or service measures and issue new policy settings. In this example,

device monitored service measures and any user service policy preference changes are reported, periodically and/or based on various triggers/events/requests, to the policy management server 1652. In this example, user privacy settings generally require secure communication with the network (e.g., a secure service control link 1653), such as with the policy management server 1652, to ensure that various aspects of user privacy are properly maintained during such configuration requests/policy settings transmitted over the network. For example, information can be compartmentalized to service policy management and not communicated to other databases used for CRM for maintaining user privacy.

[0089] In some embodiments, the policy management server 1652 provides adaptive policy management on the device. For example, the policy management server 1652 can issue policy settings and objectives and rely on the device based policy management (e.g., service processor 115) for some or all of the policy adaptation. This approach can require less interaction with the device thereby reducing network chatter on service control link 1653 for purposes of device policy management (e.g., network chatter is reduced relative to various server/network based policy management approaches described above). This approach can also provide robust user privacy embodiments by allowing the user to configure the device policy for user privacy preferences/settings so that, for example, sensitive information (e.g., geo-location data, website history) is not communicated to the network without the user's approval. In some embodiments, the policy management server 1652 adjusts service policy based on time of day. In some embodiments, the policy management server 1652 receives, requests or otherwise obtains a measure of network availability and adjusts traffic shaping policy and/or other policy settings based on available network capacity.

[0090] As shown in Figure 9, service controller 122 includes a network traffic analysis server 1656. In some embodiments, the network traffic analysis server 1656 collects/receives service usage history for devices and/or groups of devices and analyzes the service usage. In some embodiments, the network traffic analysis server 1656 presents service usage statistics in various formats to identify improvements in network service quality and/or service profitability. In other embodiments, the network traffic analysis server 1656 estimates the service quality and/or service usage for the network under variable settings on potential service policy. In other embodiments, the network traffic analysis server 1656 identifies actual or potential service

behaviors by one or more devices that are causing problems for overall network service quality or service cost.

[0091] As shown in Figure 9, service controller 122 includes a beta test server 1658. In some embodiments, the beta test server 1658 publishes candidate service plan policy settings to one or more devices. In some embodiments, the beta test server 1658 provides summary reports of network service usage or user feedback information for one or more candidate service plan policy settings. In some embodiments, the beta test server 1658 provides a mechanism to compare the beta test results for different candidate service plan policy settings or select the optimum candidates for further policy settings optimization.

[0092] As shown in Figure 9, service controller 122 includes a service download control server 1660. In some embodiments, the service download control server 1660 provides a download function to install and/or update service software elements (e.g., the service processor 115 and/or agents/components of the service processor 115) on the device, as described herein.

[0093] As shown in Figure 9 service controller 122 includes a billing event server 1662. In some embodiments, the billing event server 1662 collects billing events, provides service plan information to the service processor 115, provides service usage updates to the service processor 115, serves as interface between device and central billing server 1619, and/or provides trusted third party function for certain ecommerce billing transactions.

[0094] As shown in Figure 9, the Access Network AAA server 1621 is in network communication with the access network 1610. In some embodiments, the Access Network AAA server 1621 provides the necessary access network AAA services (e.g., access control and authorization functions for the device access layer) to allow the devices onto the central provider access network and the service provider network. In some embodiments, another layer of access control is required for the device to gain access to other networks, such as the Internet, a corporate network and/or a machine to machine network. This additional layer of access control can be implemented, for example, by the service processor 115 on the device. In some embodiments, the Access Network AAA server 1621 also provides the ability to suspend service for a device and resume service for a device based on communications received from the service controller 122. In some embodiments, the Access Network AAA server 1621 also provides the

ability to direct routing for device traffic to a quarantine network or to restrict or limit network access when a device quarantine condition is invoked. In some embodiments, the Access Network AAA server 1621 also records and reports device network service usage (e.g., device network service usage can be reported to device service history 1618).

[0095] As shown in Figure 9, the device service history 1618 is in network communication with the access network 1610. In some embodiments, the device service history 1618 provides service usage data records used for various purposes in various embodiments. In some embodiments, the device service history 1618 is used to assist in verifying service policy implementation. In some embodiments, the device service history 1618 is used to verify service monitoring. In some embodiments, the device service history 1618 is used to verify billing records and/or billing policy implementation. In some embodiments, the device service history 1618 is used to synchronize and/or verify the local service usage counter.

[0096] As shown in Figure 9, the central provider billing server 1619 is in network communication with the access network 1610. In some embodiments, the central provider billing server 1619 provides a mediation function for central provider billing events. For example, the central provider billing server 1619 can accept service plan changes. In some embodiments, the central provider billing server 1619 provides updates on device service usage, service plan limits and/or service policies. In some embodiments, the central provider billing server 1619 collects billing events, formulates bills, bills service users, provides certain billing event data and service plan information to the service controller 122 and/or device 100.

[0097] As shown in Figure 9, in some embodiments, modem selection and control 1811 selects the access network connection and is in communication with the modem firewall 1655, and modem drivers 1831, 1815, 1814, 1813, 1812 convert data traffic into modem bus traffic for one or more modems and are in communication with the modem selection and control 1811. In some embodiments, different profiles are selected based on the selected network connection (e.g., different service profiles/policies for WWAN, WLAN, WPAN, Ethernet and/or DSL network connections), which is also referred to herein as multimode profile setting. For example, service profile settings can be based on the actual access network (e.g., home DSL/cable or work network) behind the Wi-Fi not the fact that it is Wi-Fi (or any other network, such as DSL/cable,

satellite, or T-1), which is viewed as different than accessing a Wi-Fi network at the coffee shop. For example, in a Wi-Fi hotspot situation in which there are a significant number of users on a DSL or T-1 backhaul, the service controller can sit in a service provider cloud or an MVNO cloud, the service controls can be provided by a VSP capability offered by the service provider or the service controller can be owned by the hotspot service provider that uses the service controller on their own without any association with an access network service provider. For example, the service processors can be controlled by the service controller to divide up the available bandwidth at the hotspot according to QoS or user sharing rules (e.g., with some users having higher differentiated priority (potentially for higher service payments) than other users). As another example, ambient services (as similarly described herein) can be provided for the hotspot for verified service processors.

[0098] In some embodiments, the service processor 115 and service controller 122 are capable of assigning multiple service profiles associated with multiple service plans that the user chooses individually or in combination as a package. For example, a device 100 starts with ambient services that include free transaction services wherein the user pays for transactions or events rather than the basic service (e.g., a news service, eReader, PND service, pay as you go session Internet) in which each service is supported with a bill by account capability to correctly account for any subsidized partner billing to provide the transaction services (e.g., Barnes and Noble may pay for the eReader service and offer a revenue share to the service provider for any book or magazine transactions purchased from the device 100). In some embodiments, the bill by account service can also track the transactions and, in some embodiments, advertisements for the purpose of revenue sharing, all using the service monitoring capabilities disclosed herein. After initiating services with the free ambient service discussed above, the user may later choose a post-pay monthly Internet, email and SMS service. In this case, the service controller 122 would obtain from the billing system 123 in the case of network based billing (or in some embodiments the service controller 122 billing event server 1622 in the case of device based billing) the billing plan code for the new Internet, email and SMS service. In some embodiments, this code is cross referenced in a database (e.g., the policy management server 1652) to find the appropriate service profile for the new service in combination with the initial ambient service. The new superset service profile is then applied so that the user maintains free access to the ambient services, and the billing partners continue to subsidize those services, the user also gets access to

Internet services and may choose the service control profile (e.g., from one of the embodiments disclosed herein). The superset profile is the profile that provides the combined capabilities of two or more service profiles when the profiles are applied to the same device 100 service processor. In some embodiments, the device 100 (service processor 115) can determine the superset profile rather than the service controller 122 when more than one “stackable” service is selected by the user or otherwise applied to the device. The flexibility of the service processor 115 and service controller 122 embodiments described herein allow for a large variety of service profiles to be defined and applied individually or as a superset to achieve the desired device 100 service features.

[0099] As shown in Figure 9, an agent communication bus 1630 represents a functional description for providing communication for the various service processor 115 agents and functions. In some embodiments, as represented in the functional diagram illustrated in Figure 9, the architecture of the bus is generally multipoint to multipoint so that any agent can communicate with any other agent, the service controller or in some cases other components of the device, such user interface 1697 and/or modem components. As described below, the architecture can also be point to point for certain agents or communication transactions, or point to multipoint within the agent framework so that all agent communication can be concentrated, or secured, or controlled, or restricted, or logged or reported. In some embodiments, the agent communication bus is secured, signed, encrypted, hidden, partitioned and/or otherwise protected from unauthorized monitoring or usage. In some embodiments, an application interface agent (not shown) is used to literally tag or virtually tag application layer traffic so that the policy implementation agent(s) 1690 has the necessary information to implement selected traffic shaping solutions. In some embodiments, an application interface agent (not shown) is in communication with various applications, including a TCP application 1604, an IP application 1605, and a voice application 1602.

[00100] In some embodiments, device assisted services (DAS) techniques for providing an activity map for classifying or categorizing service usage activities to associate various monitored activities (e.g., by URL, by network domain, by website, by network traffic type, by application or application type, and/or any other service usage activity categorization/classification) with associated IP addresses are provided. In some embodiments, a

policy control agent (not shown), service monitor agent 1696, or another agent or function (or combinations thereof) of the service processor 115 provides a DAS activity map. In some embodiments, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor provides an activity map for classifying or categorizing service usage activities to associate various monitored activities (e.g., by Uniform Resource Locator (URL), by network domain, by website, by network traffic type, by application or application type, and/or any other service usage activity classification/categorization) with associated IP addresses. In some embodiments, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor determines the associated IP addresses for monitored service usage activities using various techniques to snoop the DNS request(s) (e.g., by performing such snooping techniques on the device 100 the associated IP addresses can be determined without the need for a network request for a reverse DNS lookup). In some embodiments, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor records and reports IP addresses or includes a DNS lookup function to report IP addresses or IP addresses and associated URLs for monitored service usage activities. For example, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor can determine the associated IP addresses for monitored service usage activities using various techniques to perform a DNS lookup function (e.g., using a local DNS cache on the monitored device 100). In some embodiments, one or more of these techniques are used to dynamically build and maintain a DAS activity map that maps, for example, URLs to IP addresses, applications to IP addresses, content types to IP addresses, and/or any other categorization/classification to IP addresses as applicable. In some embodiments, the DAS activity map is used for various DAS traffic control and/or throttling techniques as described herein with respect to various embodiments. In some embodiments, the DAS activity map is used to provide the user various UI related information and notification techniques related to service usage as described herein with respect to various embodiments. In some embodiments, the DAS activity map is used to provide service usage monitoring, prediction/estimation of future service usage, service usage billing (e.g., bill by account and/or any other service usage/billing categorization techniques), DAS techniques for ambient services usage monitoring, DAS techniques for generating micro-CDRs (e.g., also referred to as service usage partition,

service usage recording partition, service charging bucket, device generated CDRs, such as in the case where the device and not a network component are generating the usage records, ambient usage records, specialized service usage records, or other terms to indicate a service usage data record generated to provide a more refined or detailed breakdown of service usage for the device), and/or any of the various other DAS related techniques as described herein with respect to various embodiments.

[00101] In some embodiments, all or a portion of the service processor 115 functions disclosed herein are implemented in software. In some embodiments, all or a portion of the service processor 115 functions are implemented in hardware. In some embodiments, all or substantially all of the service processor 115 functionality (as discussed herein) is implemented and stored in software that can be performed on (e.g., executed by) various components in device 100. In some embodiments, it is advantageous to store or implement certain portions or all of service processor 115 in protected or secure memory so that other undesired programs (and/or unauthorized users) have difficulty accessing the functions or software in service processor 115. In some embodiments, service processor 115, at least in part, is implemented in and/or stored on secure non-volatile memory (e.g., non volatile memory can be secure non-volatile memory) that is not accessible without pass keys and/or other security mechanisms. In some embodiments, the ability to load at least a portion of service processor 115 software into protected non-volatile memory also requires a secure key and/or signature and/or requires that the service processor 115 software components being loaded into non-volatile memory are also securely encrypted and appropriately signed by an authority that is trusted by a secure software downloader function, such as service downloader 1663 as shown in Figure 16. In some embodiments, a secure software download embodiment also uses a secure non-volatile memory. Those of ordinary skill in the art will also appreciate that all memory can be on-chip, off-chip, on-board and/or off-board.

[00102] **Figure 10** provides a table summarizing various service processor 115 functional elements in accordance with some embodiments. Many of these agents are similarly described above, and the table shown in Figure 10 is not intended to be an exhaustive summary of these agents, nor an exhaustive description of all functions that the agents perform or are described herein, but rather Figure 10 is provided as a summary aid in understanding the basic functions of

each agent in accordance with some embodiments and how the agents interact with one another, with the service controller server elements, and/or with other network functions in certain embodiments to form a reliable device based service delivery solution and/or platform.

[00103] Figure 11 provides a table summarizing various service controller 122 functional elements in accordance with some embodiments. Many of these agents/elements are similarly described above, and the table shown in Figure 11 is not intended to be an exhaustive summary of these server elements, nor an exhaustive description of all functions that the elements perform or are described herein, but rather Figure 11 is provided as a summary aid in understanding the basic functions of each element in accordance with some embodiments and how the elements interact with one another, certain network elements, and/or the service processor agents in certain embodiments to form a reliable device based service delivery solution and/or platform.

[00104] Figure 12 illustrates a device stack providing various service usage measurement from various points in the networking stack for a service monitor agent, a billing agent, and an access control integrity agent to assist in verifying the service usage measures and billing reports in accordance with some embodiments. As shown in Figure 12, several service agents take part in data path operations to achieve various data path improvements, and, for example, several other service agents can manage the policy settings for the data path service, implement billing for the data path service, manage one or more modem selection and settings for access network connection, interface with the user and/or provide service policy implementation verification. Additionally, in some embodiments, several agents perform functions to assist in verifying that the service control or monitoring policies intended to be in place are properly implemented, the service control or monitoring policies are being properly adhered to, that the service processor or one or more service agents are operating properly, to prevent unintended errors in policy implementation or control, and/or to prevent tampering with the service policies or control. As shown, the service measurement points labeled I through VI represent various service measurement points for service monitor agent 1696 and/or other agents to perform various service monitoring activities. Each of these measurement points can have a useful purpose in various embodiments described herein. For example, each of the traffic measurement points that is employed in a given design can be used by a monitoring agent to track application layer traffic through the communication stack to assist policy implementation functions, such as the policy

implementation agent 1690, or in some embodiments the modem firewall agent 1655 or the application interface agent, in making a determination regarding the traffic parameters or type once the traffic is farther down in the communication stack where it is sometimes difficult or impossible to make a complete determination of traffic parameters. The particular locations for the measurement points provided in these figures are intended as instructional examples, and other measurement points can be used for different embodiments, as will be apparent to one of ordinary skill in the art in view of the embodiments described herein. Generally, in some embodiments, one or more measurement points within the device can be used to assist in service control verification and/or device or service troubleshooting.

[00105] In some embodiments, the service monitor agent and/or other agents implement virtual traffic tagging by tracking or tracing packet flows through the various communication stack formatting, processing and encryption steps, and providing the virtual tag information to the various agents that monitor, control, shape, throttle or otherwise observe, manipulate or modify the traffic. This tagging approach is referred to herein as virtual tagging, because there is not a literal data flow, traffic flow or packet tag that is attached to flows or packets, and the book-keeping to tag the packet is done through tracking or tracing the flow or packet through the stack instead. In some embodiments, the application interface and/or other agents identify a traffic flow, associate it with a service usage activity and cause a literal tag to be attached to the traffic or packets associated with the activity. This tagging approach is referred to herein as literal tagging. There are various advantages with both the virtual tagging and the literal tagging approaches. For example, it can be preferable in some embodiments to reduce the inter-agent communication required to track or trace a packet through the stack processing by assigning a literal tag so that each flow or packet has its own activity association embedded in the data. As another example, it can be preferable in some embodiments to re-use portions of standard communication stack software or components, enhancing the verifiable traffic control or service control capabilities of the standard stack by inserting additional processing steps associated with the various service agents and monitoring points rather than re-writing the entire stack to correctly process literal tagging information, and in such cases, a virtual tagging scheme may be desired. As yet another example, some standard communication stacks provide for unused, unspecified or otherwise available bit fields in a packet frame or flow, and these unused, unspecified or otherwise available bit fields can be used to literally tag traffic without the need to

re-write all of the standard communication stack software, with only the portions of the stack that are added to enhance the verifiable traffic control or service control capabilities of the standard stack needing to decode and use the literal tagging information encapsulated in the available bit fields. In the case of literal tagging, in some embodiments, the tags are removed prior to passing the packets or flows to the network or to the applications utilizing the stack. In some embodiments, the manner in which the virtual or literal tagging is implemented can be developed into a communication standard specification so that various device or service product developers can independently develop the communication stack and/or service processor hardware and/or software in a manner that is compatible with the service controller specifications and the products of other device or service product developers.

[00106] It will be appreciated that although the implementation/use of any or all of the measurement points illustrated in Figure 12 is not required to have an effective implementation, such as was similarly shown with respect to various embodiments described herein, various embodiments can benefit from these and/or similar measurement points. It will also be appreciated that the exact measurement points can be moved to different locations in the traffic processing stack, just as the various embodiments described herein can have the agents affecting policy implementation moved to different points in the traffic processing stack while still maintaining effective operation. In some embodiments, one or more measurement points are provided deeper in the modem stack where, for example, it is more difficult to circumvent and can be more difficult to access for tampering purposes if the modem is designed with the proper software and/or hardware security to protect the integrity of the modem stack and measurement point(s).

[00107] Referring to Figure 12, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Example measurement point VI resides within or just above the modem driver layer. For example, the modem driver performs modem bus communications, data protocol translations, modem control and configuration to interface the networking stack traffic to the modem. As shown, measurement point VI is common to all modem drivers and modems, and it is advantageous for certain embodiments to differentiate the traffic or service activity taking place

through one modem from that of one or more of the other modems. In some embodiments, measurement point VI, or another measurement point, is located over, within or below one or more of the individual modem drivers. The respective modem buses for each modem reside between example measurement points V and VI. In the next higher layer, a modem selection & control layer for multimode device based communication is provided. In some embodiments, this layer is controlled by a network decision policy that selects the most desirable network modem for some or all of the data traffic, and when the most desirable network is not available the policy reverts to the next most desirable network until a connection is established provided that one of the networks is available. In some embodiments, certain network traffic, such as verification, control, redundant or secure traffic, is routed to one of the networks even when some or all of the data traffic is routed to another network. This dual routing capability provides for a variety of enhanced security, enhanced reliability or enhanced manageability devices, services or applications. In the next higher layer, a modem firewall is provided. For example, the modem firewall provides for traditional firewall functions, but unlike traditional firewalls, in order to rely on the firewall for verifiable service usage control, such as access control and security protection from unwanted networking traffic or applications, the various service verification techniques and agents described herein are added to the firewall function to verify compliance with service policy and prevent tampering of the service controls. In some embodiments, the modem firewall is implemented farther up the stack, possibly in combination with other layers as indicated in other Figures. In some embodiments, a dedicated firewall function or layer is provided that is independent of the other processing layers, such as the policy implementation layer, the packet forwarding layer and/or the application layer. In some embodiments, the modem firewall is implemented farther down the stack, such as within the modem drivers, below the modem drivers, or in the modem itself. Example measurement point IV resides between the modem firewall layer and an IP queuing and routing layer. As shown, an IP queuing and routing layer is separate from the policy implementation layer where the policy implementation agent implements a portion of the traffic control and/or service usage control policies. As described herein, in some embodiments, these functions are separated so that a standard network stack function can be used for IP queuing and routing, and the modifications necessary to implement the policy implementation agent functions can be provided in a new layer inserted into the standard stack. In some embodiments, the IP queuing and routing layer is

combined with the traffic or service usage control layer. For example, a combined routing and policy implementation layer embodiment can also be used with the other embodiments, such as shown in Figure 12. Measurement point III resides between the IP queuing and routing layer and a policy implementation agent layer. Measurement point II resides between the policy implementation agent layer and the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of Figure 12.

[00108] As shown in Figure 12, the application service interface layer is above the standard networking stack API and, in some embodiments, its function is to monitor and in some cases intercept and process the traffic between the applications and the standard networking stack API. In some embodiments, the application service interface layer identifies application traffic flows before the application traffic flows are more difficult or practically impossible to identify farther down in the stack. In some embodiments, the application service interface layer in this way assists application layer tagging in both the virtual and literal tagging cases. In the case of upstream traffic, the application layer tagging is straight forward, because the traffic originates at the application layer. In some downstream embodiments, where the traffic or service activity classification relies on traffic attributes that are readily obtainable, such as source address or URL, application socket address, IP destination address, time of day or any other readily obtained parameter, the traffic type can be identified and tagged for processing by the firewall agent or another agent as it initially arrives. In other embodiments, as described herein, in the downstream case, the solution is generally more sophisticated when a traffic parameter that is needed to classify the manner in which the traffic flow is to be controlled or throttled is not readily available at the lower levels of the stack, such as association with an aspect of an application, type of content, something contained within TLS, IPSEC or other secure format, or other information associated with the traffic. Accordingly, in some embodiments the networking stack identifies the traffic flow before it is fully characterized, categorized or associated with a service activity, and then passes the traffic through to the application interface layer where the

final classification is completed. In such embodiments, the application interface layer then communicates the traffic flow ID with the proper classification so that after an initial short traffic burst or time period the policy implementation agents can properly control the traffic. In some embodiments, there is also a policy for tagging and setting service control policies for traffic that cannot be fully identified with all sources of tagging including application layer tagging.

[00109] As shown in Figure 12, a service monitor agent, which is also in communication with the agent communication bus 1630, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I through VI, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown.

[00110] **Figure 13** illustrates an embodiment similar to Figure 12 in which some of the service processor is implemented on the modem and some of the service processor is implemented on the device application processor in accordance with some embodiments. In some embodiments, a portion of the service processor is implemented on the modem (e.g., on modem module hardware or modem chipset) and a portion of the service processor is implemented on the device application processor subsystem. It will be apparent to one of ordinary skill in the art that variations of the embodiment depicted in Figure 13 are possible where more or less of the service processor functionality is moved onto the modem subsystem or onto the device application processor subsystem. For example, such embodiments similar to that depicted in Figure 13 can be motivated by the advantages of including some or all of the service processor network communication stack processing and/or some or all of the other service agent functions on the modem subsystem (e.g., and such an approach can be applied to one or more modems). For example, the service processor can be distributed as a standard feature set contained in a modem chipset hardware or software package or modem module hardware or software package, and such a configuration can provide for easier adoption or development by device OEMs, a higher level of differentiation for the chipset or modem module manufacturer, higher levels of performance or service usage control implementation integrity or security, specification or interoperability standardization, and/or other benefits.

[00111] Referring to Figure 13, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for modem MAC/PHY layer at the bottom of the device communications stack. Measurement point IV resides above the modem MAC/PHY layer. The modem firewall layer resides between measurement points IV and III. In the next higher layer, the policy implementation agent is provided, in which the policy implementation agent is implemented on the modem (e.g., on modem hardware). Measurement point II resides between the policy implementation agent and the modem driver layer, which is then shown below a modem bus layer. The next higher layer is shown as the IP queuing and routing layer, followed by the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of Figure 13.

[00112] **Figure 14** illustrates various embodiments of intermediate networking devices that include a service processor for the purpose of verifiable service usage measurement, reporting, and billing reports in accordance with some embodiments. For example, Figures 14(A) through 14(E) illustrate various extended modem alternatives for access network connection through an intermediate modem or networking device combination that has a connection (e.g., LAN connection) to one or more devices 100.

[00113] In some embodiments, device 100 includes a 3G and/or 4G network access connection in combination with the Wi-Fi LAN connection to the device 100. For example, the intermediate device or networking device combination can be a device that simply translates the Wi-Fi data to the WWAN access network without implementing any portion of the service processor 115 as shown in Figure 14(A). In some embodiments, an intermediate device or networking device combination includes a more sophisticated implementation including a networking stack and some embodiments a processor, as is the case for example if the intermediate networking device or networking device combination includes a router function, in which case the service processor 115 can be implemented in part or entirely on the intermediate modem or networking device

combination. The intermediate modem or networking device combination can also be a multi-user device in which more than one user is gaining access to the 3G or 4G access network via the Wi-Fi LAN connection. In the case of such a multi-user network, the access network connection can include several managed service links using multiple instantiations of service processor 115, each instantiation, for example, being implemented in whole or in part on device 100 with the intermediate modem or networking device combination only providing the translation services from the Wi-Fi LAN to the WWAN access network.

[00114] Referring now to Figures 14(B)-(D), in some embodiments, the service processors 115 are implemented in part or in whole on the intermediate modem or networking device combination. In the case where the service processor 115 is implemented in part or in whole on the intermediate modem or networking device combination, the service processor 115 can be implemented for each device or each user in the network so that there are multiple managed service provider accounts all gaining access through the same intermediate modem or networking device combination. In some embodiments, the functions of service processor 115 are implemented on an aggregate account that includes the WWAN access network traffic for all of the users or devices connected to the Wi-Fi LAN serviced by the intermediate modem or networking device combination. In some embodiments, the central provider can also provide an aggregated account service plan, such as a family plan, a corporate user group plan and/or an instant hotspot plan. In the case where there is one account for the intermediate modem or networking device combination, the intermediate modem or networking device combination can implement a local division of services to one or more devices 100 or users in which the services are controlled or managed by the intermediate modem or networking device combination or the device 100, but the management is not subject to service provider control and is auxiliary to the service management or service policy implementation performed by service processors 115. In some embodiments, another service model can also be supported in which there is an aggregate service provider plan associated with one intermediate modem or networking device combination, or a group of intermediate modems or networking device combinations but where each user or device still has its own service plan that is a sub-plan under the aggregate plan so that each user or device has independent service policy implementation with a unique instantiation of service processor 115 rather than aggregate service policy implementation across multiple users in the group with a single instantiation of service processor 115.

[00115] As shown in Figure 14(B), in some embodiments, device 100 includes a Wi-Fi modem, a Wi-Fi modem combined with a 3G and/or 4G WWAN modem on intermediate modem or networking device combination 1510, and the intermediate modem or networking device combination forwards WWAN access network traffic to and from device 100 via the Wi-Fi link. For example, the service processor 115 can be implemented in its entirety on device 100 and the service provider account can be associated exclusively with one device. Similarly, as shown in Figure 14(C), such an implementation can be provided using a different access modem and access network, such as a 2G and/or 3G WWAN, DSL wire line, cable DOCSIS wire line or fiber wire line configuration in place of the 3G and/or 4G access network connection to the intermediate modem or networking device combination 1510. In addition, various other embodiments similarly use DSL as shown in Figures 14(D), USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510, or a femto cell modem and DSL/cable/T1/other combination as shown in Figure 14(E).

[00116] **Figure 15** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including a proxy server(s) 270 in accordance with some embodiments. As shown, Figure 2 includes a proxy server(s) 270 in communication with a 4G/3G/2G wireless network operated by, for example, a central provider. For example, the proxy server(s) 270 can be used to implement and/or assist in providing various techniques described herein, such as service usage measurement and/or other techniques as described herein.

[00117] In some embodiments, it may not be possible to accurately identify every network service access attempt or service usage (e.g., or traffic access) as belonging to a given service usage partition (e.g., a given ambient service usage, background network chatter usage, user service plan usage, emergency service usage, and/or other type of service usage). As used herein, the terms service usage partition, service usage recording partition, service charging bucket, and micro-CDRs are used interchangeably. Accordingly, it is desirable to provide a service charging bucket for traffic that is allowed and not definitively identified as belonging to a known service charging bucket. This allows for techniques to employ an “allow but verify” approach to traffic that is likely to be legitimately associated with an ambient service or a user

service or a network service that is intended to be allowed, but is not definitively identified as being associated with an allowed service.

[00118] As an example, there may be a web site access associated with an ambient service that does not have a reference identifier or other traffic parameter that allows the service processor to associate it with the correct ambient service. In this case, a set of rules can be applied to determine if it is likely that the web site access is a legitimate access given the access control policies that are in place, and if it is the access can be allowed and the traffic usage either recorded in the ambient service charging bucket that it is suspected to be associated with, or the traffic usage can be charged to a network chatter service usage bucket, or the traffic usage can be charged to the user service usage bucket, or the traffic usage may be recorded in a “not classified but allowed” service charging bucket. In some embodiments, in which such traffic is charged to the “not classified but allowed” service usage charging bucket, additional verification measures are employed to ensure that the amount of traffic that is not classified but allowed does not grow too large or become a back-door for service usage errors. For example, the access control policy rules for allowing unclassified traffic can be relatively loose as long as the amount of service usage charges accumulating in the not classified charging bucket remains within certain bounds, and/or the rate of service usage charged to the not classified bucket remains within certain bounds, but if the not classified traffic becomes large or the rate of not classified traffic growth becomes large then the rules governing when to allow not classified traffic can be tightened.

[00119] As another example, a browser application can access a web site that is known to be an ambient service website, and that web site might serve back a series of traffic flows, some of which are associated with the ambient service website through URL identifiers that are known to be part of the website, and other traffic can be associated with the ambient service website by virtue of a referring website tag or header, and some traffic can be returned to the same application with a relatively close time proximity to the other traffic as being identified as ambient traffic. In this example, as long as the not classified traffic service charging bucket does not exceed a given pre-set policy limit on its size, and/or does not grow faster than a given pre-set policy rate, and/or is received within a certain pre-set policy period of time difference from the time that other ambient service charging bucket traffic is received, then the not classified traffic is continued to be allowed. However, if the not classified traffic amount or rate of growth

exceeds the pre-set policy limits, or if the period of time between when verified ambient service traffic is received and the not classified traffic is received exceeds policy limits, then the not classified traffic can be blocked or other action can be taken to further analyze the not classified traffic.

[00120] In some embodiments, it is important to provide a hierarchy of service usage charging rules for the various service usage partitions on a device. As an example, for a given service plan there can be two ambient service charging buckets, a network chatter (e.g., or network overhead) service charging bucket, and a user service plan service charging bucket and it is desirable to make sure that no ambient services or network overhead service or unclassified service is charged to the user service plan, and it is also desirable to ensure that all known ambient service traffic is charged to the appropriate ambient service partner, and it is desirable to ensure that no network overhead service or unclassified service is charged to ambient service partners. In such situations, a service charging bucket hierarchy can be provided as follows: determine if a traffic flow (e.g., or socket) is associated with network overhead, and if so allow it and charge that service bucket, then determine if a traffic flow (or socket) is associated with ambient service #1, and if so allow it and charge that service bucket, then determine if a traffic flow (or socket) is associated with ambient service #2, and if so allow it and charge that service bucket, then determine if a traffic flow (or socket) is associated with not classified traffic, and if so allow it and charge that service bucket, then if the traffic is not associated with any of the above service charging buckets allow it and charge it to the user service plan charging bucket. In another example, if the user has not yet chosen to pay for a user service plan, then the same hierarchical access control and service charging policy can be used except the final step would be: then if the traffic is not associated with any of the above service charging buckets block the traffic. Hierarchical service charging bucket identification such as depicted in these examples can be a crucial aspect of a robust access control policy and/or service charging policy system. Many other access control policy hierarchies and service charging bucket policy hierarchies will now be apparent to one of ordinary skill in the art.

[00121] In some embodiments, the not classified traffic is charged according to service charging rules that rely on the most likely candidate service charging bucket for the traffic. As another example, if the not classified traffic is being delivered to the same application as other

known ambient service traffic and the time difference between delivery of the known ambient service traffic and the not classified traffic is small, then the not classified traffic can be charged to the ambient service in accordance with a pre-set charging policy rule specifying these conditions. Other embodiments that will now be apparent to one of ordinary skill in the art. For example, another charging rule for not classified traffic could be to perform a pro-rata allocation of the not classified traffic to all of the other service charging buckets with the pro-rata allocation being based on the percentage of the total traffic used by the device for each service charging bucket. As another example, the not classified traffic can be charged to a subset of the service charging buckets for the device (e.g., all ambient services plus the network overhead service) in accordance with the pro-rata share for each service included in the pro-rata split.

[00122] In some embodiments, the user service plan agreement is structured so that the user acknowledges that ambient services in which the access connection to the service is sponsored, paid for, and/or partially subsidized by an entity other than the user are a benefit to the user, and/or the user acknowledges that there is no inherent right to free ambient services, and that the service usage accounting system may not always properly characterize usage for a sponsored or subsidized ambient service (e.g., or some other specialized service) in the correct accounting service charging bucket, and, thus, the user service plan account can be charged and/or billed with some of this traffic. By having the user acknowledge a service use agreement of this form then some ambient traffic can be charged to the user service plan account, including, for example, allowed but not classified traffic, excess ambient service usage beyond pre-set policy limits, ambient service usage during busy network periods or on congested network resources, and/or other criteria/measures. In some embodiments, the user might be notified that they are being charged for service activities that are sometimes subsidized or free to the user. As discussed above, it is important to ensure that a not classified service charging bucket does not become a back door for service charging errors or hacking. It will now be apparent to one of ordinary skill in the art that the not classified service usage charges can be verified in a variety of manners, including, for example, observing the size of the not classified service charging bucket as compared to other service usage charges on the device (e.g., total device service usage, ambient service usage, user bucket service usage, and/or other criteria/measures), capping the not classified bucket, and/or capping the rate of growth of the not classified bucket.

[00123] In some embodiments, it is important to verify not only that the total device service usage amount is correct, but that the service usage is being reported in the proper service charging buckets. For example, if the service processor software can be hacked so that it correctly reports the total service usage, but reports user service plan traffic under one or more ambient service buckets, then simply verifying that the total amount of service usage is correct will not be sufficient to prevent the device from obtaining free user service that can be charged to ambient service partners. There are a variety of direct and indirect embodiments to accomplish this verification of service charging bucket divisions. For example, in direct verification embodiments, one or more alternative measures of service usage are employed to cross-check the accuracy of the service charging bucket divisions. In indirect embodiments one of two classes of verification are employed: the size and rate of growth for service charging buckets is analyzed and compared to a pre-set group of policies to detect and/or modify service charging bucket growth that is out of policy; and/or the proper operation of the service processor elements involved in service charging bucket partitioning is verified.

[00124] Various embodiments involving direct verification of service charging bucket usage and/or accounting include the use of network based service usage measures such as CDRs, IPDRs, flow data records (e.g., FDRs – detailed reports of service usage for each service flow, such as network socket connection, opened and used to transmit data to or from the device), accounting records, interim accounting records or other similar usage records to verify that the device is within service policy and/or the device based service usage reports are accurate. Use of such network generated service usage records to directly verify service charging and/or proper service usage policy adherence are described herein. When network address destination and/or source information is available in these records, as described herein, this can be used in some embodiments to verify the service charging bucket accounting provided by the device service processor. In some embodiments, some types of service usage records include real-time data but not necessarily all of the useful information needed to help verify service charging bucket accounting, while other types of service usage records provide more detail (e.g., IP address for destination and source) but do not always arrive in real-time. For example, in some embodiments, FDRs are created each time a new service flow (e.g., network socket connection) is opened and then closed. At the time the service flow is closed, a (e.g., possibly time stamped) data usage record indicating source address, destination address and amount of data transmitted

is created and sent to a charging aggregation function in the network. The charging aggregation function can then forward the FDRs to the service controller for verification or direct accounting of service charging bucket accounting. By comparing the FDR addresses with known ambient service traffic address associations, the partitioning of service charging buckets between one or more ambient services and other services such as a user service plan service charging bucket may be verified. However, in some cases it can be a long period of time for an FDR to be generated when a device service flow (e.g., socket) remains open for a long period of time, as in the case for example with a long file download, a peer to peer connection with a socket keep alive, or a proxy server service with a socket keep alive. In such cases, it can be disadvantageous to have large amounts of data to be transferred without an FDR to confirm device service processor based reports, and in some cases this can provide an opportunity for service processor service reporting hacks. This can be remedied in a variety of ways by using other network reported service usage information to augment the FDR information. For example, start and stop accounting records can sometimes be obtained in some embodiments from a network element such as a service gateway or the AAA servers (e.g., or other network equipment elements depending on the network architecture). Although start and stop records do not possess the detail of service usage information that FDRs, CDRs, IPDRs, interim accounting records or other service usage records possess, they do inform the service controller that a device is either connected to the network or has stopped connecting. If a device is connected to the network and is not transmitting device usage reports or heartbeats, then the service controller is alerted that an error or hacking condition is likely. As another example of how two or more types of network reported service usage information may be used to create a better real time or near real-time check on device service usage, if both FDRs and start/stop accounting records are available, the service controller can send a stop-then-resume service command to the device (e.g., or alternatively send a stop then resume service command to a network equipment element), which will cause the device to terminate all open service flows before re-initiating them, and once the service flows are stopped then the FDR flow records will be completed and transmitted for any service flows that were in process but unreported when the stop service command was issued. This will cause any long term open socket file transfers to be reported in the FDR flow records thus plugging the potential back door hole in the FDR service usage accounting verification method.

[00125] As another example showing how multiple types of network generated service usage accounting records may be used to complement each other and strengthen the verification of service charging bucket accounting partitions, interim data records can be used with FDRs. Interim data records are available in accordance with some embodiments, in which the interim data records are generated on a regularly scheduled basis by a network element (e.g., gateway, base station, HLR, AAA, and/or other network element/function). Interim data records are typically near real time records that report the aggregate traffic usage for the device as of a point in time, but often do not include traffic address information or other traffic details. In embodiments in which both interim accounting records and FDRs are available, when the interim accounting records are indicating service usage that is not being reported in the FDR stream this is evidence that a device has one or more long term socket connections that are open and are not terminating. In this case, the service controller can verify that the device based usage reports are properly accounting for the total amount of service usage reported by the interim accounting records, and/or the service controller can force an FDR report for the open sockets by issuing a stop-resume service command as similarly discussed above.

[00126] As described herein, other embodiments involving direct verification of service charging bucket accounting can be provided. One example is to route ambient service traffic to a proxy server or router programmed to support only the network access allowed for the ambient service and to account for the ambient service usage. Additional proxy servers or routers can be similarly programmed for each ambient service that is part of the device service plan, and in some embodiments, another proxy server or router is programmed to support traffic control and account for the user service plan service access. By comparing the service usage accounting for each of these proxy servers or routers, the device generated service charging bucket accounting can be directly verified. In some embodiments, the usage accounting provided by the proxy servers or routers is used directly for service usage accounting.

[00127] In some embodiments, ambient service partner feedback is used to verify service charging bucket accounting. For example, web servers used by ambient service partners to provide ambient services can identify a user device based on header information embedded in the HTML traffic, and then account for either the service used by the device during the ambient service sessions or account for the number of transactions the user completes. If service usage is

recorded, then it can be reported to the service controller and be used directly to verify ambient service charging bucket accounting. If transactions are all that are recorded, then this can be reported to the service controller and the amount of ambient service used by the device can be compared with the number of transactions completed to determine if the ambient service usage is reasonable or should be throttled or blocked. It will now be apparent to one of ordinary skill in the art that other embodiments can be provided that employ more than one type of network generated service usage records to verify service usage accounting and/or verify service charging bucket accounting.

[00128] Other embodiments involving indirect methods for verifying or controlling service charging bucket accounting include monitoring the size and/or growth rate of ambient service usage. In some embodiments, the access control policy rules call for restricting a given ambient service access when the amount of service usage charges accumulating in the ambient service charging bucket exceed a pre-set policy limit, and/or when the rate of service usage for the ambient service exceeds a pre-set policy limit. For example, once these limits are reached, the ambient service can be throttled back for a period of time, blocked for a period of time, or charged to the user service plan charging bucket. In some embodiments, before these actions are taken the user UI can be used to notify the user of the service policy enforcement action. In some embodiments, indirect verification of service charging bucket accounting includes the various techniques described herein for verifying proper operation of the service processor agent software and/or protecting the service processor agent software from errors, manipulation, or hacking.

[00129] In some embodiments, the device service processor directs traffic destined for a given ambient service to a proxy server or router programmed to support that ambient service, and any traffic control policies and/or access control policies for the ambient service are implemented in the proxy server or router. For example, in such embodiments the proxy server or router can be programmed to only allow access to one or more ambient services that are authorized by the device service plan, with the proxy server or router controlling device access so that other network destinations cannot be reached. Continuing this example embodiment, the proxy server or router can account for the ambient service usage in an ambient service charging bucket as discussed elsewhere. In such proxy server or router ambient service control embodiments, the

same traffic association techniques described elsewhere that allow incoming traffic associated with an ambient service website or other service to be identified, allowed or blocked, potentially throttled, and accounted for in a service charging bucket can be implemented in the proxy server or router programming. Such proxy server or router embodiments can also implement user service plan service charging buckets, user service plan traffic controls, and user service plan access control as discussed herein. In some embodiments, the proxy server or router analyzes the HTML traffic content of the traffic flows as described herein to perform such associations, traffic control and/or service usage accounting. Similarly, in some embodiments, a proxy server or router can provide the “surf-out” capabilities described herein by performing the same surf-out traffic associations (e.g., HTML branch reference associations and/or other branch associations) described herein. It will now be apparent to one of ordinary skill in the art that many of the adaptive ambient service control and service usage charging functions described herein for a service processor can be readily implemented with a proxy server or router that is appropriately programmed.

[00130] In some embodiments, routing of device traffic for one or more ambient services and/or user service plan services to a proxy server or router is accomplished by the device service processor using the device service processor traffic control embodiments described herein. In some embodiments, routing of device traffic for one or more ambient services and/or user service plan services to a proxy server or router is accomplished by dedicated network equipment such as the gateways (e.g. SGSN, GGSN, PDSN, or PDN) , home agents, HLRs or base stations, with the network equipment being provisioned by a service controller (e.g., or other interchangeable network element with similar functions for this purpose) to direct the device traffic to the proxy server or router. In some embodiments, the ambient service traffic or the user service plan traffic is controlled by the proxy server according to a service plan policy set supplied by the service controller (e.g., or equivalent network function for this purpose). The traffic control service policy thus implemented by the proxy server can control traffic based on one or more of the following: period of time, network address, service type, content type, application type, QoS class, time of day, network busy state, bandwidth, and data usage.

[00131] In some embodiments, a proxy server or router is used to verify accounting for a given service, for example, an ambient service. In some embodiments, this is accomplished by the

device service processor directing the desired service flows to a proxy server or router programmed to handle the desired service flows, with the proxy server or router being programmed to only allow access to valid network destinations allowed by the access control policies for the desired service, and the proxy server or router also being programmed to account for the traffic usage for the desired services. In some embodiments, the proxy service usage accounting may then be used to verify device based service usage accounting reported by the service processor. In some embodiments, the accounting thus reported by the proxy server or router can be used directly to account for service usage, such as ambient service usage or user service plan service usage.

[00132] In some embodiments, in which a proxy server is used for device service usage accounting, the proxy server maintains a link to the device service notification UI via a secure communication link, such as the heartbeat device link described herein. For example, the proxy server or router can keep track of device service usage versus service plan usage caps/limits and notify the user device UI through the device communication link (e.g., heartbeat link) between the service controller and the device. In some embodiments, the proxy server/router communicates with a device UI in a variety of ways, such as follows: UI connection through a device link (e.g., heartbeat link), through a device link connected to a service controller (e.g., or other network element with similar function for this purpose), presenting a proxy web page to the device, providing a pop-up page to the device, and/or installing a special portal mini-browser on the device that communicates with the proxy server/router. In some embodiments, the UI connection to the proxy server/router is used as a user notification channel to communicate usage notification information, service plan choices, or any of the multiple services UI embodiments described herein.

[00133] In some embodiments for the proxy server/router techniques for implementing service traffic/access controls and/or service charting bucket accounting, it is desirable to have the same information that is available to the service processor on the device, including, for example, application associated with the traffic, network busy state, QoS level, or other information about the service activity that is available at the device. For example, such information can be used to help determine traffic control rules and/or special services credit is due (e.g., ambient services credit). In some embodiments, information available on the device can be communicated to the

proxy server/router and associated with traffic flows or service usage activities in a variety of ways. For example, side information can be transmitted to the proxy server/router that associates a traffic flow or service activity flow with information available on the device but not readily available in the traffic flow or service activity flow itself. In some embodiments, such side information may be communicated over a dedicated control channel (e.g., the device control link or heartbeat link), or in a standard network connection that in some embodiments can be secure (e.g., TLS/SSL, or a secure tunnel). In some embodiments, the side information available on the device can be communicated to the proxy server/router via embedded information in data (e.g., header and/or stuffing special fields in the communications packets). In some embodiments, the side information available on the device can be communicated to the proxy server/router by associating a given secure link or tunnel with the side information. In some embodiments, the side information is collected in a device agent or device API agent that monitors traffic flows, collects the side information for those traffic flows, and transmits the information associated with a given flow to a proxy server/router. It will now be apparent to one of ordinary skill in the art that other techniques can be used to communicate side information available on the device to a proxy server/router.

[00134] For example, just as the hierarchy of charging rules can be important for implementations in which the service processor is creating the service charging bucket accounting, it can also be important in implementations that use a proxy server or router for service charging bucket accounting. Accordingly, various embodiments described herein for creating a hierarchy of service usage charging rules can be applied to proxy server or proxy router embodiments. It will be apparent to one of ordinary skill in the art that the service charging bucket embodiments and traffic control and access control embodiments described herein for allowed but not classified buckets apply equally to the proxy server/router embodiments. For example, pre-defined service policy rules can be programmed into the proxy server/router to control the traffic flows and/or place usage limits or access limits on an ambient service, or a user service plan service. It will also now be apparent to one of ordinary skill in the art that the embodiments described herein disclosing an initial allowed service access list, temporarily allowing additional service activities until they are determined to be allowed or not allowed, expanding the allowed service activity list, maintaining a not allowed service activity list and expanding the not allowed service activity list also apply equally to proxy server/router

embodiments. Similarly, it will now be apparent to one of ordinary skill in the art that the proxy/server router embodiments can be employed to directly generate the service charging bucket (or micro-CDR) usage reports used to provide further detail and/or billing capabilities for service usage. In some embodiments, in which the device service processor directs traffic to a proxy server/router, there are advantageous design feature embodiments available that can reduce the need to provision network to detect and force specialized device service traffic to the appropriate proxy server/router. For example, this can be done by creating a "usage credit" system for the services supported by the proxy server/router. Total service usage is counted on the one hand by the device service processor, or by other network equipment, or by both. Credit on the other hand for ambient service or other specialized access service usage that is not charged to the user is then provided for services that the device directs through the proxy server/router destination (e.g., URL or route hop) supporting the particular ambient service or other specialized access service. If the device correctly directs traffic to the proxy server/router, then the counting and/or access rules are correctly implemented by the proxy server/router. The service can be thus controlled and/or accounted for. When the service is accounted for, the proxy server/router reports the service charging bucket accounting back to the service controller (e.g., or other network equipment responsible for service charging bucket/ micro CDR mediation) and the user service plan service charging bucket account can be credited for the services. Traffic that reaches the proxy server/router is controlled by the access rules and/or traffic control rules and/or QoS control rules of the proxy server/router programming, so there is no question regarding the type of service that is supported with the service charging buckets that are reported to mediation functions (e.g., mediation functions can be performed by one or more of service controller, usage mediation, billing, AAA, and/or HLR/home agent). As the proxy server/router is in the network and can be physically secured and protected from hacking, there is high confidence that the service control and/or charging rules intended for ambient services or some other specialized service are properly implemented and that the proxy server/router connection is being used for the intended service and not some other unintended hacked service. If the device is somehow hacked or otherwise in error so that the traffic is not directed through the appropriate proxy server/router, then the proxy server/router does not log the traffic in micro CDRs/buckets and no specialized service usage credit is sent to the mediation functions, so there is no usage credit deducted from the device user service plan service usage totals. Thus, the user

pays for the services when the device is hacked to avoid the proxy server/router. The user account service agreement can specify that if the user tampers with software and traffic is not routed to servers then credit will not be provided and user plan will be charged.

[00135] In some proxy server/router embodiments, the usage credit is sometimes recorded by the proxy server/router detecting which device is performing the access. Device identification can be accomplished in a variety of ways including a header/tag inserted into the traffic by the device, a route in the network specified for that device, a secure link (e.g., TLS/SSL, IP Sec, or other secure tunnel), a unique device IP address or other credential (e.g., where proxy server/router has access to an active IP address look up function), a unique proxy server/router address and/or socket for the device.

[00136] In some embodiments, the coordination of the device service controller traffic control elements with a proxy server/router can make it simpler to locate, install, provision and operate the proxy servers. The proxy server/routers do not need to be located “in line” with the access network because it is the device's responsibility to make sure the traffic is routed to the servers/routers or else there is not credit and the user account is charged. In some embodiments, this makes it unnecessary or reduces the need to force device traffic routes in carrier network. In some embodiments, the proxy server/routers can be located in carrier network or on the Internet. If the proxy server/routers are on Internet, then traffic can be authenticated in a firewall before being passed to server/routers to enhance security to attack.

[00137] In some embodiments, the service charging bucket recording software in the proxy server/router can be programmed into an ambient service partners network equipment directly thus eliminating the need for special apparatus. The ambient service partner's equipment (e.g., a web server, load balancer or router) can recognize the device using one of the techniques described above, aggregate the device service charging bucket accounting, and periodically send the usage accounting to the service controller or other network service usage mediation function.

[00138] Programming and/or provisioning the types of ambient services, user service plan services and/or specialized services disclosed in various embodiments described herein can be a complex process. In some embodiments, a simplified user programming interface, also referred to herein as a service design interface, is used to program the necessary policy settings for such

services is desirable. For example, a service design interface is provided that organizes and/or categorizes the various policy settings that are required to set up an ambient service (e.g., or other service) including one or more of the following: a policy list of service activities that are allowed under the ambient service (e.g., or other service), access control policies, rules for implementing and/or adapting an allowed list of network destinations, rules for implementing and/or adapting a blocked list of network destinations, service charging bucket policies, user notification policies, service control, and/or service charging bucket verification policies, actions to be taken upon verification errors. In some embodiments, the required information for one or more of these policy sets is formatted into a UI that organizes and simplifies the programming of the policies. In some embodiments, the UI is partly graphical to help the user understand the information and what settings need to be defined in order to define the service. In some embodiments, the UI is created with an XML interface. In some embodiments, the UI is offered via a secure web connection. In some embodiments, a basic service policy for an ambient service (e.g., or another service) is created that includes one or more of the above service policy settings, and then this service policy set becomes a list or an object that can be replicated and used in multiple service plan policy set definitions (e.g., “dragged and dropped” in a graphical UI). In some embodiments, the resulting set of policies created in this service design interface are then distributed to the necessary policy control elements in the network and/or on the device that act in coordination to implement the service policy set for a given device group. For example, if a service processor is used in conjunction with a service controller, then the service design interface can load the service policy settings subsets that need to be programmed on the service controller and the device service processor into the service controller, and the service controller loads the service controller policy settings subset into the service controller components that control the policies and loads the device policy settings subset to the devices that belong to that device group. In embodiments in which a proxy server/router is used to help control and account for services, in some embodiments, the service design interface loads the service policy settings subsets that need to be programmed on the proxy server/router into the proxy server/router. In embodiments where other network equipment (e.g., gateways, base stations, service usage recording/aggregation/feed equipment, AAA, home agent/HLR, mediation system, and/or billing system) need to be provisioned or programmed, in some embodiments, the service design interface also loads the appropriate device group policy subsets

to each of the equipment elements. Accordingly, various techniques can be used as described herein to greatly simplify the complex task of translating a service policy set or service plan into all the myriad equipment and/or device settings, programming, and/or provisioning commands required to correctly implement the service. It will now be apparent to one of ordinary skill in the art that several of these techniques can similarly be used for the VSP service design interface.

[00139] Those of ordinary skill in the art will appreciate that various other rules can be provided for the rules engine as described herein. Those of ordinary skill in the art will also appreciate that the functions described herein can be implemented using various other network architectures and network implementations (e.g., using various other networking protocols and corresponding network equipment and techniques).

[00140] In device-assisted service (DAS) systems, end-user device agents can assist the network in policy implementation or enforcement. For example, device agents can assist the network in recordkeeping to allocate costs when end-user devices access data services over an access network, enforcing access control or service limit policies for the device, enforcing usage limits, or assisting in notification policies for information regarding network access services that are in communication with the device end user. If a device is configured with a device agent configured to assist the network in policy implementation or enforcement, there may be a device portion of a network policy that is enforced on the device and a network portion of an access network service policy that is enforced by network elements in the network. In some access networks, network-based systems are employed to implement the network portion of the access network service policy, such as, for example, to manage the authentication process of allowing a device onto a network or to determine one or more network policies that should be enforced by the network elements such as access control policy, service usage limits, service usage accounting or billing policy, or service usage notification policy.

[00141] To achieve an overall network service policy, the network portion of the access network service policy may be configured to work in conjunction with the device-based portion of the access network service policy to achieve an overall combined network service policy. If the device agents required to implement the device portion of the access network service policy are not present on the device or are not properly configured, then the overall combined network

service policy can be in error or may not be possible to achieve, potentially resulting in an undesired network service policy implementation. In such cases, it is desirable for a network system to be employed to detect this condition and modify the network portion of an access network service policy enforced by the network-based elements so that a desired network service policy enforcement may be achieved.

[00142] In some embodiments, a device agent that can assist the network in policy implementation or enforcement may be termed a “device policy implementation agent,” which in some embodiments may be part of the service processor.

[00143] Examples of when it may be advantageous to adapt the network portion of an access network service policy in order to account for a missing or improperly configured service processor include but are not limited to: (i) a device credential has been moved to a device that does not have a service processor, (ii) a device credential has been moved to a device with a service processor with a different configuration than the service processor originally associated with the device credential, (iii) a device service processor has been tampered with or has an improper configuration.

[00144] In some embodiments, the service processor is used to assist in classifying service usage into sub-categories for the purpose of usage accounting policy enforcement, access control policy enforcement, service usage limits, or notification policy enforcement that differs according to the category. In some embodiments, the classification can be for one or more device applications. In some embodiments the classification can be for one or more network destinations. In some embodiments the classification can be for one or more network types. In some embodiments a classification of service usage (herein referred to as a sponsored service or an ambient service) can be performed to facilitate allocating access network costs, in whole or in part, associated with the sponsored or ambient service to a service sponsor, the service sponsor being an entity other than the device user.

[00145] What is needed is a network system that detects the presence and proper configuration of a service processor, or lack thereof, in the end-user device, wherein the service processor, if present, enforces a device portion of an access network service policy on a device configured with a device credential, and, if the service processor is present and properly configured, that

causes a first network portion of an access network service policy to be enforced in the network, the first network portion of an access network service policy being configured to provide counterpart policy enforcement to a device portion of an access network service policy to achieve a first desired overall access network service policy; and if the service processor is not present and properly configured, that causes a second network portion of an access network service policy to be enforced in the network that is configured to operate without a device counterpart policy to achieve a second desired overall access network service policy.

[00146] In some embodiments, a network system is used to detect when unscrupulous users attempt to acquire free data services by tampering with a service processor in order to use one service and have the service usage accounting allocated to a second service that is sponsored. For example, if a device sends reports of its data usage to the network, a user might attempt to hack the device so that its reports contain information that is more favorable to the user than it should be, e.g., by reporting less data usage than the device actually used. As another example, a device may contain a “sponsored SIM” card or another credential that allows the device to use a fixed amount of data, possibly associated with a particular service, at a reduced charge or at no charge to the user. Unscrupulous users may attempt to find ways to increase their quantity of free or subsidized data usage with sponsored SIM cards.

[00147] Bandwidth limitations in the wireless access network are making unlimited data plans less attractive to service providers. At the same time, users of end-user devices want to have more control over their devices’ data usage to control costs. The ability to track a device’s data usage with high accuracy, on a more granular level than simply by measuring aggregate data usage, is an important enabler new service offerings that meet both of these needs. For example, accurate tracking of a device’s data usage on a service-by-service or application-by-application basis, or on even finer levels, will allow service providers to offer a la carte service plans that allow users to choose customized application- or service-specific data plans.

[00148] Therefore, there is a need for security measures to prevent policy errors caused by changing device credentials, improper configuration of a service processor, or fraud in DAS systems. In particular, there is a need for tools that allow the network to detect fraudulent end-user device activity.

[00149] Disclosed herein are various embodiments to prevent, detect, or take action in response to moving a device credential from one device to another, improper configuration of a service processor, a missing service processor, or tampering with a service processor in device-assisted services (DAS) systems.

[00150] In some embodiments, the service controller in the network authenticates the service processor and checks that it is reporting the end-user device's usage in the expected manner, e.g., at expected times, including expected information, with expected indicia of authenticity, etc.

[00151] In some embodiments, when the end-user device reports usage, the service controller checks whether the reports sent by the service processor are consistent with reports from a trusted source, such as a network element.

[00152] In some embodiments, when the service controller detects fraudulent or potentially fraudulent activities, the service controller notifies a network administrator or network resource, which can then further evaluate the situation and decide how to respond. In some embodiments, the subscriber's billing rate is increased.

[00153] In some embodiments, a device client configured to implement a device portion of a network access service policy (e.g., an access control policy or traffic control policy, a device software or operating environment security policy, a service usage limit, a service accounting or charging policy, a service notification policy, or another policy) may be termed a "device policy implementation client," which in some embodiments may be part of the service processor. Also without loss of generality, the term "service controller" may be used to refer to a service processor authentication and management system. Both the service processor and service controller may have functions in addition to those described herein.

[00154] In some embodiments, a device is configured with a properly configured service processor responsible for implementing or enforcing a device portion of a first access network service policy. In some embodiments, the device is configured without a properly configured service processor. In some embodiments, a service controller can be configured to determine whether the service processor is present on the device and, if so, whether it is properly configured.

[00155] In some embodiments, if the service controller determines that the device is configured with a properly configured service processor, the service controller causes a network based access network service policy enforcement system to implement or enforce a first network-based portion of the first access network service policy. In this case, because the service controller has verified that a properly configured service processor is present on the device, the service controller system operates under the premise that the device is properly implementing or enforcing the device portion of the first access network service policy. If, however, the service controller determines that a properly configured device service processor is not present on the device, the service controller causes a network-based access network service policy enforcement system to implement or enforce a second network based portion of the first access network service policy. In this case, the service controller system operates under the premise that the device is not properly implementing or enforcing a device portion of an access network service policy.

[00156] In some embodiments, an end-user device is configured with: (1) a wireless modem to connect to a wireless access network (or another network access modem to connect to another type of access network); (2) one or more device credential sources (e.g., a SIM card, a soft-SIM, a universal SIM, an IMSI source, a wireless modem, a phone number source, an IMEI source, an MEID source, a user password or PIN, a MAC address source, an IP address source, a secure device identifier source, a device secure communication encryption key source, etc.) that store a device credential and provide the device credential to one or more network service policy enforcement elements (e.g., AAA, HLR, PCRF, access network authentication system, admission system or log-in system) for the purpose of seeking or gaining admission to the wireless access network (or other access network); and (3) a service processor (e.g., a device client) configured to implement or enforce a device-based portion of a wireless access network service policy and communicate with a network-based service controller in order to provide service processor authentication information configured to allow verification that the service processor is present and properly configured on the device.

[00157] In some embodiments, a network-based system is configured with: (1) one or more network-based device authentication or admission elements (e.g., AAA, HLR, PCRF, access network authentication system, admission system, log-in system, etc.) configured to receive a

device credential from an end-user device that is attempting to receive or is receiving access network services; (2) one or more service policy enforcement elements (e.g., a network gateway, router, GGSN, SGSN, proxy, charging element, notification trigger element, etc.) configured to implement an access network service policy that is associated with the device credential; (3) a service processor authentication and management system (e.g., a service controller) configured to receive service processor authentication information and use the information to verify that the service processor is present and properly configured on the device. In some embodiments, the service processor authentication and management system is further configured to: (a) in the event that the service processor is present and properly configured on the device, cause the access network service policy that is associated with the device credential to be executed as a first network portion of an access network service; or (b) in the event that the service processor is not present on the device and properly configured, cause the access network service policy that is associated with the device credential to be executed as a second network portion of an access network service.

[00158] Without loss of generality, in the following related embodiments the terms, “SIM card” and “SIM” are used to represent a device credential source. As would be appreciated by one of ordinary skill in the art, other device credential sources (e.g., a soft-SIM, a universal SIM, an IMSI source, a wireless modem, a phone number source, an IMEI source, an MEID source, a MAC address source, an IP address source, a secure device identifier source, a device secure communication encryption key source, etc.) can be interchanged with SIM card in many of the embodiments. For example, in embodiments in which a SIM card is moved from one device to another, another type of device credential could be moved instead (e.g., soft SIM, universal SIM, an IMSI source, a wireless modem, a phone number source, an IMEI source, an MEID source, a MAC address source, an IP address source, a secure device identifier source, a device secure communication encryption key source, etc.). As another example, when a user tampers with a service processor associated with a SIM, the user could be tampering with a service processor associated with another type of device credential (e.g., soft SIM, universal SIM, an IMSI source, a wireless modem, a phone number source, an IMEI source, an MEID source, a MAC address source, an IP address source, a secure device identifier source, a device secure communication encryption key source, etc.). There are many other example embodiments where the term “SIM” can be exchanged for another source of device credentials, with the embodiments being too

numerous to list and yet evident to one of ordinary skill in the art in the context of the teachings herein.

[00159] In some embodiments, the one or more device credential sources include a SIM card. In some embodiments, the service controller can be configured to recognize which device or service processor the SIM is associated with, use the SIM and device association to look up a desired device portion of a wireless access network service policy, and communicate the policy to the appropriate device service processor. In some embodiments, the two different device portions of a wireless access network policy are determined according to a device group or user group service policy definition that includes one or more SIM credentials and/or one or more service processor credentials, and these policy definitions are entered in a virtual service provider work station that manages the service controller and/or device service processor policies.

[00160] In some embodiments, the service controller is configured to recognize when the SIM card from a first device with a first service processor has been moved to a second device with a second service processor. In some such embodiments, the service controller can be configured to recognize which device or service processor the SIM is associated with, use the SIM and device association to look up a desired network portion of a wireless access network service policy, and cause the network portion of a wireless access network service policy to be implemented or enforced in one or more network service policy enforcement elements. In some embodiments, the two different network portions of a wireless access network policy are determined according to a device group or user group service policy definition that includes one or more SIM credentials and/or one or more service processor credentials, and these policy definitions are entered in a virtual service provider work station that manages the service controller and/or network service policy enforcement element policies.

[00161] In some embodiments, the one or more device credential sources include a SIM card. In some embodiments, the service controller is configured to detect when a device user has moved the SIM card from a first device configured with a properly configured service processor to a second device that is not configured with a properly configured service processor. In some embodiments, the service controller can be configured to determine that the first device is configured with a properly configured service processor and communicate a device portion of a

wireless access network service policy to the appropriate device service processor. In some embodiments, the device portion of a wireless access network policy is determined according to a device group or user group service policy definition that includes a SIM credential and/or a service processor credential, and these policy definitions are entered in a virtual service provider work station that manages the service controller and/or device service processor policies. In some embodiments, the service controller is configured to determine that the first device is configured with a properly configured service processor and cause a first network portion of a wireless access network service policy to be implemented or enforced in one or more network service policy enforcement elements. In some embodiments the service controller is configured to determine that the second device is not configured with a properly configured service processor and cause a second network portion of a wireless access network service policy to be implemented or enforced in one or more network service policy enforcement elements. In some embodiments, the device portion of a wireless access network policy is determined according to a device group or user group service policy definition that includes a SIM credential, and these policy definitions are entered in a virtual service provider work station that manages the service controller and/or network service policy enforcement element policies.

[00162] In some of these embodiments, the differences between the first network portion of a wireless access network service policy and the second network portion of a wireless access network service policy can include a difference in network access privileges, a difference in allowable network destinations, a difference in service usage accounting or billing for “bulk” access, a difference in service usage accounting or billing for a classification of access, a difference in service usage accounting rates or billing rates for “bulk” access, a difference in service usage accounting rates or billing rates for a classification of access, a difference in sponsored (ambient) service accounting or billing, a difference in service speed or quality, a difference in which networks the device or user has access to, a difference in the service usage notification that is provided to the end user, a difference in roaming service policies or permissions or accounting/billing rates, a quarantining of the device or user access capabilities, differences between (e.g., disabling or otherwise modifying) one or more features of device operation, or suspending the device from access to the network.

[00163] In some embodiments, a SIM and a service processor are associated with a classification of service usage and a corresponding device portion of access network service policy enforcement. The service controller is then responsible for properly authenticating the proper configuration of the service processor in association with the SIM in order to determine the appropriate network portion of network access service policy that should be enforced.

[00164] In some embodiments, a SIM and a service processor are associated with one or more application-specific services wherein the device network access service has policy elements that are specific to a device software or firmware application. A software or firmware application-specific service can include but is not limited to a service with specific policy elements associated with a user application program; an operating system program, library or function; a background application service such as an application update, content caching, software update or other background application service.

[00165] In some embodiments, a SIM and a service processor are associated with one or more network-destination-specific services wherein the device network access service has policy elements that are specific to a network destination or resource. A network destination or resource can include but is not limited to a server, gateway, destination address, domain, website or URL.

[00166] In some embodiments, a SIM and a service processor are associated with any combination of a device application, network destination or resource; a type of network; a roaming condition (e.g., a home or roaming network); a time period; a level of network congestion; a level of network quality-of-service (QoS); and a background or foreground communication.

[00167] In some embodiments, a SIM and a service processor are associated with one or more sponsored services (also referred to herein as ambient services), wherein a portion or all of the service usage accounting for one or more classifications of service usage are accounted to, charged to, or billed to a service sponsor rather than the device user or party who pays for the user service plan. The portion of service that is sponsored can be all of the device access or a portion or classification of the device access. In some embodiments, the classification of the sponsored portion of service (e.g., the identification of the portion of the device's use of the

access network that should be allocated to the service sponsor) is accomplished on the device with a service processor. In some embodiments, the classification of the sponsored portion of service is accomplished in the network using DPI elements, gateway elements, server elements, proxy elements, website elements or web service elements. In some embodiments, the classification of the sponsored portion of service is accomplished with a classification policy implemented by a combination of a service processor on the device (e.g., steering a classification of service to a given network element via a re-direction, re-route, or tunnel [e.g. secure SSL, VPN, APN or other tunnel protocol]) and one or more network elements (e.g., DPI elements, gateway elements, server elements, proxy elements, website elements or web service elements). In some embodiments, the portion of service that is sponsored includes service for one device application or a group of device applications. In some embodiments, the portion of service that is sponsored includes service for a network destination or resource, a server or website, or a group of network destinations, servers or websites. In some embodiments, the portion of service that is sponsored includes service on a specific type of network. In some embodiments, the portion of service that is sponsored includes service on a home network or a roaming network. In some embodiments, the portion of service that is sponsored includes service during a time period. In some embodiments, the portion of service that is sponsored includes service for a certain range of network congestion. In some embodiments, the portion of service that is sponsored can include service for a certain range of network QoS. In some embodiments, the portion of service that is sponsored includes service for a network background or foreground data communication. In some embodiments, the portion of service that is sponsored includes any combination of device application, network destination or resource, a type of network, a roaming condition (e.g., home or roaming network), a time period, a level of network congestion, a level of network QoS, and a background or foreground communication.

[00168] In some embodiments, a SIM (or other source of user credential or device credential, as explained previously) is installed in or present in association with a device configured with a device service processor configuration that provides access network policy enforcement. In such embodiments, one or more network elements can implement or enforce a network-based portion of access network policy enforcement, and the device service processor can be configured to implement or enforce a device-based portion of access network policy enforcement. In some embodiments, one or more SIM credentials can be used at least in part to identify the network-

based portion of access network policy. In some embodiments, one or more SIM credentials can be used at least in part to identify the device-based portion of access network policy.

[00169] In some embodiments that include a SIM module policy association, the policy enforcement includes one or more of access control policy enforcement, service usage limit, access accounting policy enforcement, and access service user notification policy enforcement. In some embodiments, the access control policy enforcement includes one or more of allowing, limiting, blocking, deferring, delaying or traffic shaping device network access for “bulk” access (e.g., “not classified” access), or one or more specific classifications of access network service activities. In some embodiments, the access accounting policy enforcement includes one or more of counting an amount of “bulk” (e.g., “unclassified”) access network service usage, or counting an amount of access network service usage for one or more specific classifications of access network service activities. In some embodiments, the access service notification policy enforcement includes one or more of notifying an end user when a pre-defined service usage condition occurs for “bulk” (e.g. “unclassified”) access network service usage or notifying an end user when a pre-defined service usage condition occurs for one or more specific classifications of access network service activities. Examples of specific classifications of access network service activities include access by an application or OS function, access to one or more network destinations or network resources (such as a web site, domain, IP address or other address identifier, URL, socket tuple, network server, network route or APN, network gateway or proxy, network content source or sub-network). Additional examples of specific classifications of access network service activities include device access to network services with different QoS service levels. In some embodiments, a portion of the policies associated with specific classifications of access network service are implemented or enforced with a device-based service processor, and other portions of access network service policy are enforced in one or more network-based elements.

[00170] In some embodiments in which one or more network elements implement or enforce a network-based portion of access network policy enforcement and a device service processor is configured to implement or enforce a device-based portion of access network policy enforcement, one or more device SIM credentials are identified and used at least in part to determine the policies enforced by the network. In such embodiments, the device service

processor can be relied upon to implement or enforce certain aspects of access network service policy that are not implemented or enforced in the network.

[00171] In some embodiments, a first portion of access network service policy is determined at least in part by one or more SIM credentials and is implemented by one or more network elements, and a second portion of access network service policy is intended to be implemented by a device-based service processor, but the SIM is installed in a device that is not configured with a service processor capable of implementing the second portion of access network service policy. In some such embodiments, a network element identifies whether the SIM is installed in a device that is configured with a service processor capable of implementing the second portion of access network service policy intended to be implemented on the device. In some embodiments, the identification is accomplished by a network system that implements one or more of the following device configuration detection and network policy selection functions: (1) Identify when a SIM whose credentials are used at least in part to identify a network-based portion of access network policy is installed in a device configured to include a service processor capable of implementing or enforcing a device-based portion of access network service policy, and provision a first network-based service policy in one or more network-based policy enforcement elements that implement or enforce access network service policy; (2) Identify when a SIM whose credentials are used at least in part to identify the network-based portion of access network policy is installed in a device that is not configured to include a service processor capable of implementing or enforcing a device-based portion of access network service policy and implement a second network-based service policy in one or more network-based policy enforcement elements that implement or enforce access network service policy.

[00172] In some embodiments, when it is determined that a SIM whose credentials are used at least in part to identify the network-based portion of access network policy is installed in a device configured to include a service processor capable of implementing or enforcing a device-based portion of access network service policy, a network-based service policy provisioning system provisions a first network-based service policy into one or more network elements (e.g., programs or sends the policy to one or more network elements) and also provisions a device-based service policy into a device service processor. In some embodiments, when it is determined that a SIM whose credentials are used at least in part to identify the network-based

portion of access network policy is installed in a device that is not configured to include a service processor capable of implementing or enforcing a device-based portion of access network service policy, a network-based service policy provisioning system provisions a second network-based service policy into one or more network elements, and there is no policy provisioning for a device-based service processor.

[00173] Such embodiments are advantageous, for example, when a device-based service processor is capable of implementing or enforcing a network access service policy that has fine grain classification aspects that are not otherwise implemented or enforced in the network. For example, in some embodiments a SIM is installed in a first device configuration that includes a device-based service processor capable of classifying access network service usage associated with one or more device software applications and enforce a policy for access control, service limit, access accounting or access service notification for that classification. In this case a first set of network-based access network service policies may be provisioned into the network elements that implement or enforce access network service policy. If the same SIM is installed in a second device configuration that does not include the described service processor capability, a second set of network-based access network service policies may be provisioned into the network elements that implement or enforce access network service policy. In such embodiments, the first device configuration can include a trusted access control or service limit policies in the service processor that determine the network access allowances for one or more applications, and the first network service policies are configured to facilitate this device-based application access control or service limitation. In contrast, the second device configuration, having no service processor, has no trusted access control or service limitation policies, and therefore the second network service policies may be configured in a manner that allows access only if the service plan or service account associated with the SIM (or second device or SIM user) includes permissions for “bulk” access, “unclassified” access, or access that is classified by the network and not by the device.

[00174] In some embodiments, the second network service policies are configured to modify the classification of network access services in accordance with capabilities that exist only in the network without the assistance of a device-assisted classification component.

[00175] In some embodiments, the second network service policies include a second access service accounting or charging rate that is different than the access service accounting or charging rate of the first network service policies. For example, the method of service accounting or service charging to the end user in the case where the SIM is installed in a device configuration that includes a service processor capability (e.g., the device is capable of performing service classification, accounting, control or notification functions) can be different than the method of service accounting or service charging to the end user in the case where the SIM is installed in a device configuration that does not include the service processor capability. For example, if the SIM is installed in a device configuration that includes a service processor capability, a given application (e.g., social networking application, email application, search application, voice application, news application, etc.) might have a first service accounting or charging policy defining a first charging measure (e.g., time-based usage for an application, website, content type, service type QoS class; or e.g., megabyte-based usage for an application, website, content type, service type QoS class, etc.) and/or first charging rate (e.g., \$X per minute; or e.g., \$Y per megabyte, etc.) when the device configuration includes a service processor capability, whereas when the SIM is not installed in a device configuration that includes a service processor capability, all traffic may be rated in the same manner (e.g., time-based or megabyte-based), potentially with a higher price. In some embodiments, when the SIM is not installed in a device configuration that includes a service processor capability, the device network access permissions are altered, or the device's communications may be quarantined or blocked.

[00176] In some embodiments, when a SIM is installed in a device with a first device configuration, the service processor is configured to differentially treat one or more classifications of access network service activities based on network congestion level, time of day, QoS level or background/foreground access (e.g., background content caching or background upload of device/user analytics, background software or OS updates, background application/server communications, etc.), but the same SIM can alternatively be installed in a device without such service processor capabilities (e.g., a device with a second device configuration). In such an embodiment, one or more of the network-based portions of access control or service limitation policy, network-based portion of accounting or charging policy, or network-based portion of user notification policy can be varied depending on whether the SIM is

installed in a device with the first device configuration or the second device configuration. For example, if the SIM is recognized by the network in association with the first device configuration, a lower accounting rating or service usage price can be applied to traffic that is (i) allocated to background status, (ii) is controlled based on network congestion level, (iii) is controlled based on time of day, (iv) is controlled based on a lower QoS classification allowance, etc., whereas if the SIM is recognized by the network in association with the second device configuration, a single, potentially higher accounting rating or service usage price can be applied. In some embodiments, if the SIM is recognized by the network in association with the second device configuration the device network access permissions can be altered, or the device's communications can be quarantined or blocked.

[00177] In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that includes a service processor service usage charging capability, one or more network elements are configured to zero-rate the device access (i.e., the one or more network elements will not apply the service usage accounting recorded by one or more network elements to the user's bill), and user service accounting or charging is turned over to a service controller that receives service usage accounting or charging information from the service processor.

[00178] In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, one or more network elements are configured to zero-rate the device access (i.e., the one or more network elements will not apply the service usage accounting recorded by one or more network elements to the user's bill), and user service accounting or charging is turned over to one or more proxy gateway/servers configured to account or charge for device service usage.

[00179] In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, the one or more proxy gateway/servers perform additional traffic access control

or service limitation policy implementation or enforcement for the one or more classifications of service usage.

[00180] In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, the one or more proxy gateway/servers perform additional service usage classification for the purpose of service usage accounting, access control, service limiting or user notification.

[00181] In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that does not include a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, network elements other than the proxy gateway/servers account for service usage, potentially at a different rate than when a SIM is determined by a network element to be installed in a device configuration that includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications.

[00182] In some embodiments in which the device configuration includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, the device routing, re-directing, or steering is accomplished by routing, re-directing, or steering the device traffic for one or more service usage classifications to a specific network destination or resource associated with the proxy gateway/server. In some embodiments, the routing, re-directing, or steering is accomplished using a secure tunnel through the network. In some embodiments the routing, re-directing, or steering is accomplished with a VPN or APN tunnel.

[00183] In some embodiments, a network-based service charging policy system is used in conjunction with a user service agreement confirmation system, wherein the user agreement confirmation system provides confirmation that the user has agreed to access service usage terms that stipulate a first rate of access service usage accounting or charging when a SIM is detected in association with a device configuration that includes a service processor capability, and a second rate of access service usage accounting or charging when a SIM is detected in association

with a device configuration that does not include a service processor capability. In some embodiments, if a user removes or tampers with a device configuration that includes a service processor capability, or if a user installs a SIM in a device that is not configured with a service processor capability, the user service usage billing conditions are changed. In some embodiments, depending on the device configuration (e.g., with or without a service processor capability), the user is billed at a different rate for “bulk” service usage, or is billed at a different rate for one or more classifications of service usage.

[00184] In some embodiments, a network-based service charging policy system is used in conjunction with a user service agreement confirmation system, wherein the user agreement confirmation system provides confirmation that the user has agreed to access service usage terms that stipulate a first set of access service privileges when a SIM is detected in association with a device configuration that includes a service processor capability, and a second set of access service privileges when a SIM is detected in association with a device configuration that does not include a service processor capability. In some embodiments, if a user removes or tampers with a device configuration that includes a service processor capability, or if a user installs a SIM in a device that is not configured with a service processor capability, the user service usage permissions are modified. In some embodiments, this modification can include altering the allowed network destinations, altering the allowed network services, altering the allowed network resources, quarantining access or blocking access.

[00185] In some embodiments the presence of a device service processor in combination with a SIM results in the service controller providing advantageous network access services to the user. Examples include but are not limited to the sponsored services discussed herein, user-paid application-based services (e.g., user-paid services where access for one or more device applications is included in a service allowance with potentially lower cost than overall internet access), user-paid destination services (e.g., user-paid services where access for one or more network destinations or resources is included in a service allowance with potentially lower cost than overall internet access), roaming services (e.g., services that aid the user when the device is connected to a roaming network, such as by informing the user that she is roaming and asking if she wishes to continue or block roaming service usage, up to date roaming service usage indication or cost indication, roaming service rate indications, allowing a user to decide which

device service usage classifications he wishes to allow while roaming, etc.), or service usage notification services (e.g., providing the user with an update of how much service usage or cost has been incurred, informing the user of what service plans are available, informing the user when a service plan sign up may be advantageous to the user based on an activity or group of activities the user is attempting, or providing the user with a set of service plan sign up choices that can be selected and purchased in a device user interface (UI), etc.). In some embodiments, these user services are made possible by the capabilities of the service processor on the device in conjunction with a specific configuration of a service controller or other network elements on an access service provider network.

[00186] In some embodiments, if the SIM for a first network service provider is removed from the device and another SIM for a second network or service provider is installed, the user may not have access to the same services. In some embodiments, the service processor on the device detects that the SIM has been changed and informs the user through a device user interface (UI) notification that if the user changes SIMS or service provider networks, the user will lose certain services. In some embodiments, the services that will be lost are listed in a UI notification. In some embodiments the UI notification states that if the user wishes to regain access to certain services, the user can re-install the original SIM.

[00187] In some embodiments, one or more network elements determine whether an end-user device has an active service processor. In some embodiments, a service controller in the network authenticates the service processor.

[00188] In some embodiments, the service controller performs authentication of the service processor to ensure that it is present and properly configured to implement a device portion of an access network service policy. Figures 16 and 17 show a system diagram for a device service processor to service controller communication link that can aid in secure communication and service processor authentication and verification functions.

[00189] Figure 16 is a functional diagram illustrating service control device link 1691 of service processor 115 and the service control service link 1638 of service controller 122 in accordance with some embodiments. In particular, service control device link 1691 of service processor 115 and service control service link 1638 of service controller 122 as shown in Figure

16 provide for secure control plane communication over service control link 1653 between service processor 115 and service controller 122 in accordance with some embodiments. Various embodiments include two or three layers of encryption in the service control link, with one embodiment or layer being implemented in the encrypt functions (2408, 2428) and decode functions (2412, 2422), and another embodiment or layer implemented in the transport services stack (2410, 2420). An optional third embodiment or layer of encryption is implemented below the transport services stack, for example, with IPSEC or another IP layer encryption, VPN or tunneling scheme. For example, various known security encryption techniques can be implemented in the encrypt functions (2408, 2428), with public/private or completely private keys and/or signatures so that very strong levels of security for service processor control plane traffic can be achieved even through the basic transport services (2410, 2420) implemented with standard secure or open Internet networking protocols, such as TLS or TCP. For example, the service processor agent communications local to the device can be conducted to and from the service controller elements via service control device link 1691 connection to agent communication bus 1630. The combination of service control device link 1691 and agent communication bus 1630, which in some embodiments is also securely encrypted or signed, provides a seamless, highly secure, asynchronous control plane connection between the service processor and service controller server elements and the service controller and service controller agents that works over a wide range of access networks, such as any access network that has the capability to connect IP or TCP traffic to another TCP or IP endpoint on the access network, another private network or over the Internet. As described herein, in some embodiments, agent communication bus 1630 also provides a fourth level of encrypted or signed communication to form a secure closed system on the device for agent to agent communication, for example, making it very difficult or practically impossible for software or applications to gain access to one or more of the a service processor agents on the device in any way other than service control device link 1691. In this way, in some embodiments, agent communication bus 1630 and the service processor agents can only be accessed by one another as necessary or permitted by agent communication policies, or by the service controller or other authorized network function with proper security credentials communicating over service control device link 1691. Additionally, in some embodiments, communications between a subset of two or more agents, or between one or more agents and one or more service controller server elements are encrypted with unique

keys or signatures in such a way that a fourth level of security providing private point to point, point to multipoint, or multipoint to multipoint secure communication lines is provided.

[00190] In some embodiments, all of service control device link 1691 communications are transformed into a continuous control plane connection, with a frequency based on the rate of service usage, a minimum set period between connections, and/or other methods for establishing communication frequency. In some embodiments, this heartbeat function provides a continuous verification link by which the service controller verifies that the service processor and/or device are operating properly with the correct service policies being implemented. In view of the following heartbeat function embodiments described herein, it will be apparent to one of ordinary skill in the art that different approaches for implementing the various heartbeat embodiments are possible, and it will be clear that there are many ways to achieve the essential features enabling a reliable, sometimes continuous control link and verification function for the purpose of assisting control of service usage in a verifiable manner. As shown, inside service processor 115, service control device link 1691 includes heartbeat send counter 2402 in communication with agent communication bus 1630. For example, heartbeat send counter 2402 can provide a count for triggering when a service processor 115 communication (e.g., periodic communication based on a heartbeat mechanism) should be sent to service controller 122, and heartbeat buffer 2404, also in communication with agent communication bus 1630, buffers any such information for the next service processor 115 communication, in accordance with various heartbeat based embodiments, as similarly described herein. Heartbeat buffer 2404 is in communication with framing element 2406 and encrypt element 2408 for framing and encrypting any service processor 115 communications transmitted to service controller 122 by transport services stack 2410 over service control link 1653. Similarly, as shown inside service controller 122, service control server link 1638 includes heartbeat send counter 2434 in communication with service controller network 2440, and heartbeat buffer 2432, also in communication with service controller network 2440, which buffers any such information for the next service controller 122 communication, in accordance with various heartbeat based embodiments, as similarly described herein. Heartbeat buffer 2432 is in communication with framing element 2430 and encrypt element 2428 for framing and encrypting any such service controller 122 communications transmitted to service processor 115 by transport services stack 2420 over service control link 1653.

[00191] As also shown inside service processor 115 of Figure 16, service control device link 1691 includes decode element 2412 for decoding any received service controller 122 communications (e.g., decrypting encrypted communications), unpack element 2414 for unpacking the received service controller 122 communications (e.g., assembling packetized communications), and agent route 2416 for routing the received service controller 122 communications (e.g., commands, instructions, heartbeat related information or status reports, policy related information or configuration settings and/or updates, challenge/response queries, agent refreshes and/or new software for installation) to the appropriate agent of service processor 115. Similarly, as shown inside service controller 122, service control server link 1638 also includes decode element 2422 for decoding any received service processor 115 communications (e.g., decrypting encrypted communications), unpack element 2424 for unpacking the received service processor 115 communications (e.g., assembling packetized communications), and agent route 2426 for routing the received service processor 115 communications (e.g., responses to instructions and/or commands, heartbeat related information or status reports, policy related information or configuration settings and/or updates, challenge/response queries, agent status information, network service/cost usage and/or any other reporting related information) to the appropriate agent of service controller 122. Accordingly, as described herein with respect to various embodiments, the various secure communications between service controller 122 and service processor 115 can be performed using the embodiment as shown in Figure 16, and those of ordinary skill in the art will also appreciate that a variety of other embodiments can be used to similarly provide the various secure communications between service controller 122 and service processor 115 (e.g., using different software and/or hardware architectures to provide secure communications, such as using additional and/or fewer elements/functions or other design choices for providing such secure communications).

[00192] In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided, and the following embodiments (e.g., as shown and described with respect to Figure 17) teach such a structure that packs the various service processor agent control plane communications and the various service controller element control plane connections into a format that does not consume excessive bandwidth to enable a continuous control plane connection between the device and service controller. In some embodiments, an efficient and effective communication framing structure between the service

processor and service controller is provided to buffer such communication messages for some period of time before framing and transmitting, such as in a heartbeat frequency that is based on rate of service usage. In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided to allow for the frame to be easily packed, encrypted, decoded, unpacked and the messages distributed. In view of the various embodiments described herein, it will be apparent to one of ordinary skill in the art that many framing structures will work for the intended purpose of organizing or framing agent communications and the uniqueness and importance of combining such a system element with the device service controller functions, the service processor functions, the service control verification functions and/or the other purposes.

[00193] Figure 17 is a functional diagram illustrating a framing structure of service processor communication frame 2502 and service controller communication frame 2522 in accordance with some embodiments. In particular, service control device link 1691 of service processor 115 and service control service link 1638 of service controller 122 (e.g., as shown in Figure 16) provide for secure control plane communication over service control link 1653 between service processor 115 and service controller 122 using communication frames in the format of service processor communication frame 2502 and service controller communication frame 2522 as shown in Figure 17 in accordance with some embodiments. As shown, service processor communication frame 2502 includes service processor framing sequence number 2504, time stamp 2506, agent first function ID 2508, agent first function message length 2510, agent first function message 2512, and, assuming more than one message is being transmitted in this frame, agent Nth function ID 2514, agent Nth function message length 2516, and agent Nth function message 2518. Accordingly, service processor communication frame 2502 can include one or more messages as shown in Figure 17, which can depend on networking frame length requirements and/or other design choices. Similarly, as shown, service controller communication frame 2522 includes service controller framing sequence number 2524, time stamp 2526, agent first function ID 2528, agent first function message length 2530, agent first function message 2532, and, assuming more than one message is being transmitted in this frame, agent Nth function ID 2534, agent Nth function message length 2536, and agent Nth function message 2538. Accordingly, service controller communication frame 2522 can include one or

more messages as shown in Figure 17, which can depend on networking frame length requirements and/or other design choices.

[00194] Figures 18A through 18E, 19A through 19G, and 20A through 20C present numerous embodiments that can be used in isolation or in combination by a service controller in authenticating the service processor to ensure that it is present and properly configured to implement a device portion of an access network service policy. Figures 18A through 18E provide tables summarizing various service processor heartbeat functions and parameters (e.g., implemented by various agents, components, and/or functions implemented in software and/or hardware) in accordance with some embodiments. Many of these heartbeat functions and parameters are similarly described above, and the tables shown in Figures 18A-E are not intended to be an exhaustive summary of these heartbeat functions and parameters, but rather are provided as an aid in understanding these functions and parameters in accordance with some heartbeat based embodiments described herein.

[00195] Figures 19A through 19G provide tables summarizing various device based service policy implementation verification techniques in accordance with some embodiments. Many of these device based service policy implementation verification techniques are similarly described above, and the tables shown in Figures 19A-G are not intended to be an exhaustive summary of these device based service policy implementation verification techniques, but rather are provided as an aid in understanding these techniques in accordance with some device based service policy embodiments described herein.

[00196] Figures 20A through 20C provide tables summarizing various techniques for protecting the device based service policy from compromise in accordance with some embodiments. Many of these techniques for protecting the device based service policy from compromise are similarly described above, and the tables shown in Figures 20A-C are not intended to be an exhaustive summary of these techniques for protecting the device based service policy from compromise, but rather are provided as an aid in understanding these techniques in accordance with some device based service policy embodiments described herein.

[00197] Figure 21 illustrates an example embodiment of a process to start or stop a data session with SGSN notification. End-user device 100 attempts to start a data session by sending a GPRS

Attach message to SGSN 2230. SGSN 2230 notifies service controller 122 that end-user device 100 has started a data session. Service controller 122 waits for a pre-determined time, for example, one minute, to receive a login or authentication request from service processor 115. In some embodiments, service controller 122 sets a login timer. If service controller 122 receives the login or authentication request before the timer expires, it attempts to authenticate service processor 115.

[00198] One or more authentication errors may occur when service controller 122 attempts to authenticate service processor 115. For example, service processor 115 may have invalid credentials. As another example, service processor 115 may send invalid application or kernel signatures. As another example, service processor 115 may report end-user device “root” detection errors. As another example, service processor 115 may contact service controller 122 using an identifier that is already in use by a different end-user device.

[00199] If service controller 122 does not receive the request from service processor 115 within the pre-determined time, or if service controller 122 is unable to authenticate service processor 115 for some reason, service controller 122 assumes that either (1) end-user device 100 does not contain a service processor, and is therefore unable to participate in device-assisted services, or (2) although end-user device 100 has a service processor, service processor 115 has been disabled. Service controller 122 sends a notification (“No active SP” message) to data rating element 2220 to indicate that end-user device 100 does not have the ability to provide the information necessary for data mediation element 2210 to generate detailed data usage reports, e.g., “micro-CDRs.” In some embodiments, service controller 122 sends a trigger to the network to indicate that end-user device 100 should be charged for usage at “standard” bulk rates. In some embodiments, service controller 122 specifies a “standard” bulk rate charging code in the CDRs it sends to data mediation element 2210. In some embodiments, data rating element 2220 determines data usage by end-user device 100 based on carrier-based records.

[00200] If service controller 122 receives the login or authentication request from service processor 115 within the pre-determined time and successfully authenticates service processor 115, service controller 122 sends a notification (“Device OK” message) to data rating element 2220 to indicate that end-user device 100 has a service processor and is capable of supporting

device-assisted services. In some embodiments, data rating element 2220 expects to receive “micro-CDR” reports from data mediation element 2210 when service controller 122 has determined that end-user device 100 has an active service processor. In some embodiments, data rating element 2220 determines usage based on the micro-CDRs, which contain more granular information than ordinary CDRs. For example, whereas an ordinary CDR might simply report that an end-user device used 100 Megabytes (MB) of data, a set of micro-CDRs might report that the end-user device used 15 MB of e-mail, 35 MB of social networking, and 50 MB of streaming video.

[00201] In some embodiments, data mediation element 2210 sends carrier-based usage reports (e.g., CDRs) to service controller 122. Service controller 122 queries usage database 2200 for device-based usage reports (e.g., micro-CDRs) for end-user device 100. Service controller 122 determines the data usage of end-user device 100 from the carrier-based usage reports. Service controller 122 determines the data usage of end-user device 100 from the device-based usage reports. Service controller 122 compares the usage determined from the carrier-based usage reports to the usage determined from the device-based usage reports. If service controller 122 determines that the two usage measures do not match (e.g., are not identical or are not within a threshold of each other), service controller 122 sends a notification (e.g., a fraud alert) to data rating element 2220 to indicate that the end-user device is in a fraud state, and data rating element 2220 should bill usage for end-user device 100 based on carrier-based usage reports. Service controller 122 sends the carrier-based usage reports and device-based usage reports to data mediation element 2210.

[00202] When the “GPRS detach” message is received by SGSN 2230, SGSN 2230 sends a notification to service controller 122 that the data session for end-user device 100 is closed.

[00203] Figure 22 illustrates an example embodiment of a process to start or stop a data session with GGSN notification. The process is similar to that described with reference to Figure 21, except in how the data session starts and ends. End-user device 100 starts a data session by sending data traffic to GGSN 2240. GGSN 2240 recognizes the start of a new data session and notifies service controller 122 that end-user device 100 has started a data session. When GGSN

2240 determines that the data session has closed, it sends a notification to service controller 122 that the data session for end-user device 100 is closed.

[00204] As discussed above, in some embodiments a device service processor can provide information to assist in classification of service usage for any combination of device application, network destination or resource, a type of network, roaming condition (e.g., home or roaming network), a time period, a level of network congestion, a level of network QoS, and a background or foreground communication. In some embodiments, when a service processor provides service usage for a classification of service usage involving one or more of device application, network destination or resource, a type of network, roaming condition (e.g., home or roaming network), a time period, a level of network congestion, a level of network QoS, and a background or foreground communication, service processor 115 generates a service usage report, called a “micro-CDR,” that is then communicated to a network element (e.g., a service controller). The micro-CDR provides a service usage accounting breakdown in finer detail (e.g., including information about a device application, network destination or resource, a type of network, roaming condition (e.g., home or roaming network), a time period, a level of network congestion, a level of network QoS, and a background or foreground communication) than a “bulk” CDR that does not provide such a usage accounting breakdown.

[00205] In some embodiments, a device is configured to receive access network services and is further configured to include a service processor capability to account for one or more service activity classifications and send the accounting to a service controller. In some embodiments the service controller is configured to communicate at least a portion of the service processor service accounting as a service usage credit to a service usage reconciliation system. Note that a service usage reconciliation system is also referred to herein in various embodiments as a service usage mediation system or similar term involving mediation. In some embodiments, the service usage reconciliation system is configured to remove a credit from a user service accounting or usage bill. In some embodiments, the service usage credit that is removed from a user service accounting or usage bill is allocated to sponsor service accounting or bill.

[00206] In some embodiments it is advantageous to reconcile the micro-CDR service usage accounting reports received from a service processor against a trusted source. In some

embodiments, this is accomplished through a system that provides usage credit for one or more micro-CDR usage reports that are reconciled with or validated by a trusted source. In some embodiments, if such credit is provided, the corresponding usage is removed from the user “bulk” usage and re-assigned to the user according to service usage accounting rules associated with the micro-CDR classification. In some embodiments the micro-CDR accounting rules can be designed to account micro-CDR service usage report accounting to a paid user service classification (e.g., a device application based service accounting, a network destination or resource based service accounting, a roaming service usage accounting, etc.). In some embodiments, the micro-CDR accounting rules can be designed to account micro-CDR service usage report accounting to a sponsored service classification (e.g., a sponsored device application based service accounting, a sponsored network destination or resource-based service accounting, a sponsored background classification of service usage, a sponsored content source classification of service usage, a sponsored shopping service, etc.).

[00207] In some embodiments the trusted source used to validate micro-CDR service usage classification reports is an FDR (flow data record) source that reports a detailed level of classification that indicates network source or destination (e.g., domain, URL, IP address, etc.) and possibly one or more ports and protocols. In some embodiments, the source of the FDR is a network element. In some embodiments the source of the FDR is a device agent. In some embodiments, the agent that generates the FDR report is located in a secure execution environment on the device. In some embodiments, the agent that generates the FDR report is located in a secure hardware environment on the device. In some embodiments, the agent that generates the FDR report uses a secure transmission protocol with the service controller that is sequenced and signed and/or encrypted in a manner wherein if the sequence of FDR reports or the content of FDR reports is tampered with, then an FDR integrity violation may be detected by the service controller. In some embodiments, a communication from the service controller to the agent generating the FDR reports is sequenced and signed and/or encrypted in a manner wherein if the sequence of FDR reports or the content of FDR reports is tampered with, then an FDR integrity violation may be detected by the agent generating the FDR reports. In some embodiments, when the agent generating the FDR reports detects an FDR integrity violation, the agent generating the FDR reports causes device access to be quarantined or blocked for one or more access networks. In some embodiments, other device communication links than access

network links can also be quarantined or blocked, including one or more of wired device access ports (e.g., Ethernet, USB, firewire, etc.), Bluetooth, WiFi, and near field communications.

[00208] In some embodiments, the trusted source used to validate micro-CDR service usage classification reports is a network-based element such as a server, gateway, proxy or router that processes the classification of service associated with the micro-CDR. In some embodiments, the network-based element classifies service usage associated with the micro-CDR, measures the service usage, and provides a service usage classification report back to a service controller so that it can be reconciled against the micro-CDR reports.

[00209] In some embodiments, a device is configured to receive access network services and is further configured to include a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers. In some such embodiments, a service usage reconciliation system is configured to receive device service usage information (e.g., a credit amount) from the one or more proxy gateway/servers, and the service usage information is used in removing an amount (e.g., a credit amount) from service usage allocated to or charged to a user bill by the service usage reconciliation system. In some embodiments, the device routing is accomplished by routing, re-directing, or steering device traffic for one or more service usage classifications to a specific network destination or resource associated with the proxy gateway/server. In some embodiments, the routing, re-directing, or steering is accomplished using a secure tunnel through the network. In some embodiments the routing, re-directing, or steering is accomplished using an SSL, VPN or APN tunnel.

[00210] In some embodiments, a device service processor classifies service usage according to a service classification policy and routes, re-directs, or steers the traffic associated with the classification policy to a network element (e.g., a server, gateway, proxy or router that processes the classification of service associated with the micro-CDR) that generates the micro-CDR for that service usage accounting. In this manner, the device can associate service usage for device applications or OS functions with a specific network destination that in turn further processes the traffic and generates the appropriate micro-CDRs that are sent to the service controller for reconciliation (e.g., mediation) as described above. The service processor can steer the traffic

classified according to the classification policy by re-directing the traffic to the network destination associated with the appropriate network element, routing the traffic to the network destination associated with the appropriate network element, or tunneling or securely tunneling (e.g. SSL, VPN, APN) the traffic to the network destination associated with the appropriate network element.

[00211] In some embodiments, the trusted source used to validate micro-CDR service usage classification reports is a server or website that provides the service, and the validation is provided in the form of good customer feedback associated with a user credential, a service processor credential or a device credential that can be used to determine which device or user to provide the credit to. For example, if a website is associated with the service usage classification defined for a micro-CDR, and the website is visited by a device with a given device credential or user credential, and the website servers track the number of visits, number of transactions, amount of business generated, amount of data communicated or another measure of device interaction with the website, then a summary of this device interaction with the website can be communicated to the service controller and the service controller can provide credit for the micro-CDR.

[00212] In some embodiments, another means of limiting the possibility of improper service usage accounting due to improper configuration of a service processor or tampering with a service processor can be accomplished by capping the amount of service over a given period of time that is allowed for a given micro-CDR service usage classification category (e.g., by limiting the amount of service usage in a given period of time for one or more service usage classifications including a device application, network destination or resource, a type of network, a roaming condition (e.g., home or roaming network), a time period, a level of network congestion, a level of network QoS, or a background or foreground communication). In some embodiments, capping the amount of service over a given period of time that is allowed for a given micro-CDR service usage classification category is advantageous as a way of limiting service usage costs for a user-paid service that is based on a specific classification of service usage. In some embodiments, capping the amount of service over a given period of time that is allowed for a given micro-CDR service usage classification category is advantageous as a way of limiting service usage costs for a sponsored service that is based on a specific classification of

service usage. In some embodiments, the possibility of service usage report tampering for one or more micro-CDR service usage classification categories is limited by combining reconciliation of service usage using one or more of start/stop accounting, CDR feedback, FDR feedback, etc., and setting a limit on the usage that is allowed for one or more of the micro-CDR service usage classification categories.

[00213] In some embodiments, the possibility of service usage report tampering for one or more micro-CDR service usage classification categories is limited by comparing the total service usage for all combined micro-CDR service usage classifications against the total amount of service used in bulk CDR reports received from a trusted source.

[00214] In some embodiments using associative classification (also referred to as adaptive ambient service usage classification), some service usage that can not be directly identified as belonging to a give micro-CDR service usage classification is assigned to the micro-CDR service usage classification based on one or more of: (i) time proximity with one or more known service usage flows identified as belonging to the micro-CDR classification, (ii) a maximum amount of service usage (e.g., byte count) that has occurred since one or more known service usage flows that belong the micro-CDR classification were identified, or (iii) the fact that the unidentified service usage is associated with the same application as one or more known service usage flows that belong to the micro-CDR classification.

[00215] In some such associative classification (adaptive ambient service classification) embodiments, service usage fraud exposure can be limited by setting a limit on the amount of service usage that can be “unaccounted for” so that if the majority of usage can be classified as belonging to a micro-CDR service usage classification category, the unaccounted-for service usage is allowed to be accounted for in the same micro-CDR accounting. In this manner, if fraudulent service usage activity results in a large percentage of service usage that is not known to be classified as belonging to the micro-CDR usage classification category, a micro-CDR accounting integrity violation can be declared. Service usage above the limits that cannot be reconciled (accounted for) can alternatively be accounted for (e.g., charged to the user) at an agreed-upon contract rate. In some embodiments, the agreed-upon rate is as high or higher than the rate for user paid bulk services (e.g., higher than the rate at which sponsored and specialized

application or website based services are billed). In some embodiments, the user is sent a notification by the service controller that the user is being billed at the higher rate. In some embodiments, the user signs up to a service agreement wherein the user agrees to be billed at the higher rate in the event that the service processor is compromised or the micro-CDR accounting is compromised.

[00216] In some embodiments, the micro-CDR reports include the amount of service usage that was identified by the service processor as known to belong to the micro-CDR service usage category. In some embodiments, a flow identifier (e.g., domain, URL, IP address, port, or device application associated with [originating or terminating] the flow) can be provided in the micro-CDR reports for service usage known to belong to the micro-CDR classification. In some embodiments, the service controller samples or scans these “known good” micro-CDR flow identifiers to ensure that the flows do in fact belong to the micro-CDR service usage classification, and if they do not a micro-CDR accounting integrity violation can be declared. In some embodiments a flow identifier (e.g., domain, URL, IP address, port, or device application associated with [originating or terminating] the flow) can be provided in the micro-CDR reports for service usage that cannot be classified as belonging to the micro-CDR classification. In some embodiments, the service controller samples or scans these “unknown” micro-CDR flow identifiers to determine if the service destination patterns indicate fraudulent service usage that is inconsistent with micro-CDR classification policies, and if so a micro-CDR accounting integrity violation can be declared.

[00217] In some embodiments, a SIM that is expected to be installed in a device configured with a properly configured service processor is allocated a relatively small service usage cap in a network portion of an access network service usage policy so that the device can connect to the network and allow the service processor to authenticate with the service controller. By limiting the initial amount of service usage allowed prior to the service processor authentication with the service controller, it is not possible to get a large amount of service prior to ensuring that a properly configured service processor is present on the device. In some embodiments, once the device service processor is authenticated, an increment can be added to the usage limit in the network portion of the access network service policy. In some embodiments, additional usage limit increments can be added to the network portion of the access network service policy as

device service processor generated CDRs, FDRs or micro-CDRs are received by the service controller. In some embodiments, if at any time the flow of CDRs, FDRs or micro-CDRs from the device is tampered with or stopped, the service controller stops incrementing the usage limit in the network portion of access network service policy, and the device access is denied.

Alternatively, in some embodiments, rather than stopping service when a service processor is removed or tampered with, the network portion of the access network service policy calls for the application of a higher rate of billing as compared to one or more micro-CDR billing rates for micro-CDR credits provided by the service controller (e.g., user paid application based services, user paid website based services, user paid content services, sponsored application based services, sponsored website based services or sponsored content based services). In some embodiments, if the service processor ceases to send micro-CDRs to the service controller, the user ceases to be credited for the micro-CDR service usage and all usage is billed at a bulk rate that may be higher than the micro-CDR service rates.

[00218] In some embodiments, a SIM is provided or sold to a user wherein the SIM is associated with sponsored services that are based on network access service policies configured in the network policy enforcement elements and a service controller. In such embodiments, the problem arises that the SIM may be installed in a device that does not have a properly configured service processor, giving rise to the possibility that a user could receive unintended free services with the sponsored SIM. Embodiments described above can be used to limit the amount of access the SIM is allowed to receive prior to service processor authentication with the service controller by limiting the initial service usage amount allowed in the initial network portion of access network service policy. However, if a number of sponsored SIMs are readily available and inexpensive or free, a user could potentially swap several SIMs into the device and remove each SIM when the service controller fails to authenticate the service processor. In some embodiments, the service controller recognizes the SIM and a second device credential (e.g., an IMEI, a modem credential or a device credential) the first time the sponsored SIM acquires service usage and fails to authenticate the service processor for that device. Once the service processor fails to authenticate with the service controller, the service controller re-sets the network portion of the access network service policy to deny service the next time a SIM attempts to authenticate with the device credential associated with the original SIM.

[00219] In some embodiments, good customer feedback may be used as a micro-CDR credit source directly without a service processor on the device. For example, in some embodiments, a website is associated with the service usage classification defined for a micro-CDR, and the website or server that is visited by a device with a given device credential or user credential tracks one or more of the number of visits, number of transactions, amount of business generated, amount of data communicated or another measure of device interaction with the website or server, creates a summary report of this device interaction with the website or server, and then communicates the summary report to a service controller. The service controller can then reconcile the good customer feedback summary report of the device interaction with the website or server by applying a user service usage credit rating rule to deduct a bulk portion of service usage from the user account and add a classification of service usage to the user account that is rated for billing purposes by a rating rule for the given micro-CDR classification. Alternatively, the service controller can deduct a portion of the good customer micro-CDR service usage accounting or billing from the user account and add it to a sponsor entity account, such as the entity that provides the website or server service. In this way, a micro-CDR service usage charging system can be implemented in a network for classification service usage with specialized service usage classification rating, for both user paid classification and sponsored classifications, without the need for a service processor on the device.

[00220] Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

CLAIMS

WHAT IS CLAIMED IS:

1. A network system, comprising:
 - one or more network elements configured to receive a device credential from an end-user device; and
 - a service processor authentication and management system configured to:
 - obtain service processor authentication information, and
 - using the service processor authentication information, facilitate execution of an end-user device service processor authentication procedure.
2. The network system recited in claim 1, wherein at least one of the one or more network elements is an AAA, an HLR, a PCRF, an access network authentication system, an admission system, or a log-in system.
3. The network system recited in claim 1, wherein at least one of the one or more service policy enforcement elements is a gateway, a router, a GGSN, a SGSN, a proxy, a charging element, or a notification trigger element.
4. The network system recited in claim 1, wherein authenticating the service processor on the end-user device comprises verifying that the service processor is present and configured in an expected manner.
5. The network system recited in claim 1, further comprising one or more service policy enforcement elements configured to implement an access network service policy associated with the device credential, and wherein the service processor authentication and management system is further configured to cause the access network service policy associated with the device credential to be executed as a first network portion of an access network service when the end-user device service processor authentication procedure is successful.

6. The network system recited in claim 1, further comprising one or more service policy enforcement elements configured to implement an access network service policy associated with the device credential, and wherein the service processor authentication and management system is further configured to cause the access network service policy associated with the device credential to be executed as a second network portion of an access network service when the end-user device service processor authentication procedure is unsuccessful.

7. The network system recited in claim 1, wherein the device credential is information from a SIM card, information from a soft SIM, information from a universal SIM, an IMSI, a wireless modem identifier, a phone number, an IMEI, an MEID, a MAC address, an IP address, a secure device identifier, or a device secure communication encryption key.

8. The network system recited in claim 1, wherein the service processor authentication and management system is further configured to:

- associate a first device credential with a first end-user device;

- determine whether a received device credential, associated with an authenticating end-user device, is the first device credential;

- determine whether the authenticating end-user device is the first end-user device;

- enforce a first access network control policy when the received device credential is the first device credential and the authenticating end-user device is the first end-user device; and

- enforce a second access network control policy when the received device credential is not the first device credential or the authenticating end-user device is not the first end-user device.

9. The network system recited in claim 8, wherein the second access network control policy differs from the first access network control policy in one or more of a network access privilege, an allowable network destination, a service usage accounting or billing policy, a service usage rate, a service speed or quality, an allowed access network, a user notification, a roaming policy or permission, effect on a device operation.

10. The network system recited in claim 8, wherein the first end-user device comprises a properly-configured service processor.

11. The network system recited in claim 8, wherein the second end-user device does not include a properly-configured service processor.

12. The network system recited in claim 8, wherein the second access network control policy is configured to suspend or block network access by the authenticating end-user device.

13. An end-user device, comprising:

a modem for enabling the end-user device to access available network data services over an access network;

one or more device credential sources configured to store a device credential; and

a service processor configured to:

enforce a device-based portion of a wireless access network service policy; and

communicate with a network-based service controller to provide service processor authentication information configured to assist the network-based service controller in authenticating the service processor.

14. The end-user device recited in claim 13, wherein the service processor authentication information is the device credential.

15. The end-user device recited in claim 13, wherein the device credential is information from a SIM card, information from a soft SIM, information from a universal SIM, an IMSI, a wireless modem identifier, a phone number, an IMEI, an MEID, a MAC address, an IP address, a secure device identifier, or a device secure communication encryption key.

16. A network system, comprising:

memory configured to store a trusted usage data report associated with an end-user device; and

one or more network elements configured to:

receive a usage data report from the end-user device;

obtain the trusted usage data report associated with the end-user device; and

reconcile the usage data report from the end-user device and the trusted usage data report associated with the end-user device.

17. The network system recited in claim 16, wherein the trusted usage data report associated with the end-user device is generated by a network element.

18. The network system recited in claim 16, wherein the trusted usage data report associated with the end-user device is generated by an end-user device software or firmware agent in a secure execution environment.

19. The network system recited in claim 18, wherein the trusted usage data report associated with the end-user device is received from a good customer feedback source.

20. The network system recited in claim 19, wherein the good customer feedback source is a website or server that tracks one or more of a number of visits by the end-user device, a number of transactions associated with the end-user device, an amount of business generated in association with the end-user device, an amount of data communicated by or to the end-user device, or another measure of the end-user device's interaction with the website or server.

21. The network system recited in claim 16, wherein the network-generated usage data report associated with the end-user device is a flow data record.

22. The network system recited in claim 16, wherein the one or more network elements are further configured to credit a user account associated with the end-user device based on reconciling the usage data report from the end-user device and the network-generated usage data report associated with the end-user device.

23. A network system, comprising:

one or more network elements configured to:

receive a data usage report associated with an end-user device from a good customer feedback source, and

based on the data usage report from the good customer feedback source, reduce a bulk data usage amount associated with a user account.

24. A network system, comprising:

one or more network elements configured to detect a service usage indication associated with an end-user device; and

a service controller configured to:

- determine that a device credential is intended to be associated with a service processor on the end-user device;
- receive the service usage indication associated with the end-user device;
- detect a specified condition; and
- declare a service processor integrity violation upon detecting the specified condition.

25. The network system recited in claim 24, wherein the specified condition is that the service controller is unable to complete a service processor authentication procedure.

26. The network system recited in claim 24, wherein the service controller is further configured to receive a device-originated service usage indication from the service processor, and wherein the specified condition is that the service usage indication is inconsistent with the device-originated service usage indication.

27. The network system recited in claim 24, wherein the service controller is further configured to receive a device-originated service usage indication from the service processor, and wherein the specified condition is that either the service usage indication or the device-originated service usage indication is inconsistent with a service usage policy.

28. The network system recited in claim 24, wherein the device credential is information from a SIM card, information from a soft SIM, information from a universal SIM, an IMSI, a wireless modem identifier, a phone number, an IMEI, an MEID, a MAC address, an IP address, a secure device identifier, or a device secure communication encryption key.

29. The network system recited in claim 24, wherein at least one of the one or more network elements is a GGSN, an SGSN, a charging gateway, a AAA function, an HLR, a router, or a server.

30. The network element recited in claim 24, wherein the service usage indication associated with the end-user device is one or more of a start accounting message, a stop accounting message, a charging data record, a flow data record, or a service usage measure.

31. The network element recited in claim 25, wherein the service controller is unable to complete the service processor authentication procedure when the service processor does not communicate with the service controller within a predetermined amount of time after the service controller receives the service usage indication associated with the end-user device.

ABSTRACT OF THE DISCLOSURE

Disclosed herein are various embodiments to prevent, detect, or take action in response to the moving a device credential from one device to another, the improper configuration of a service processor, a missing service processor, or the tampering with a service processor in device-assisted services (DAS) systems.

Figure 1

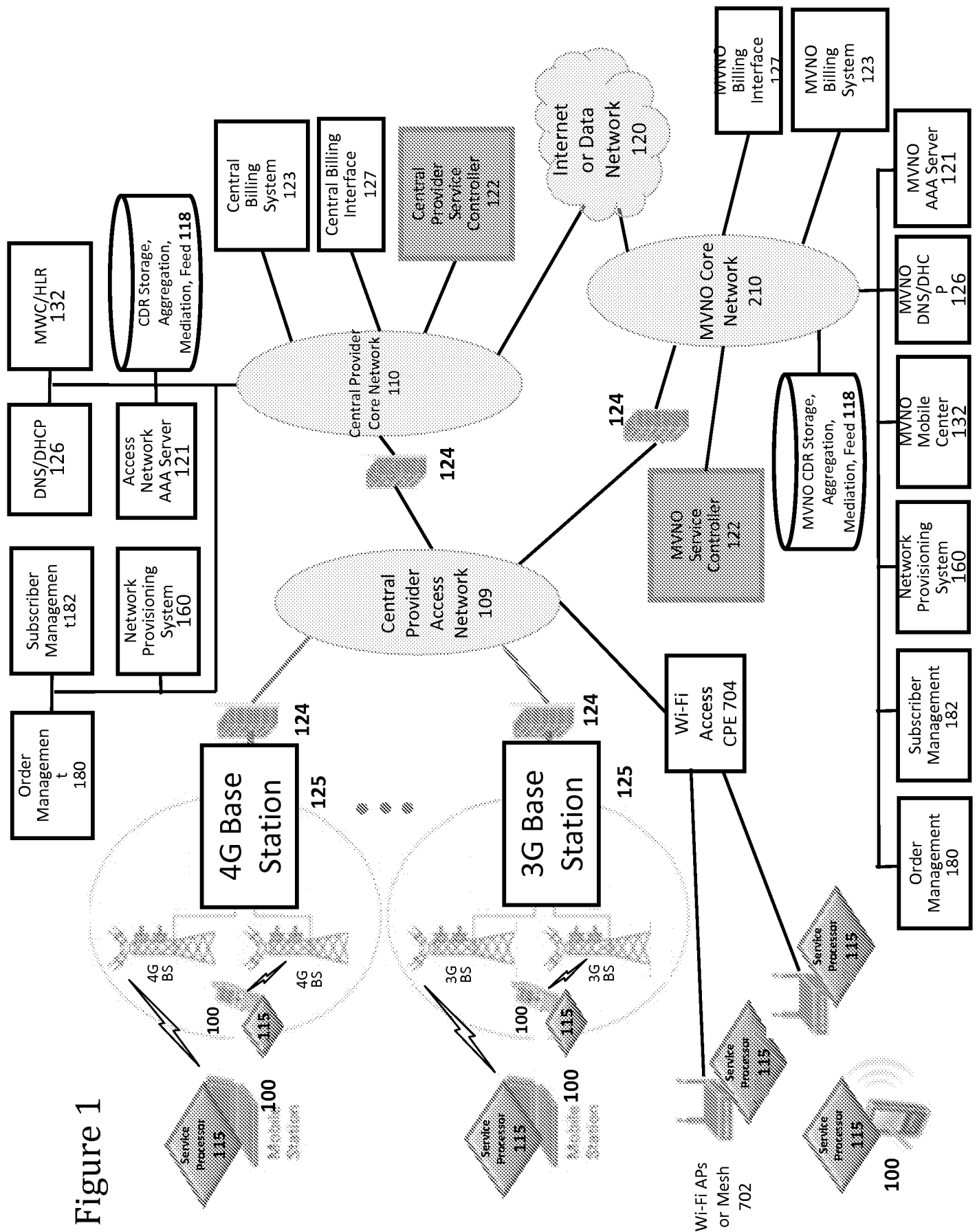


Figure 2

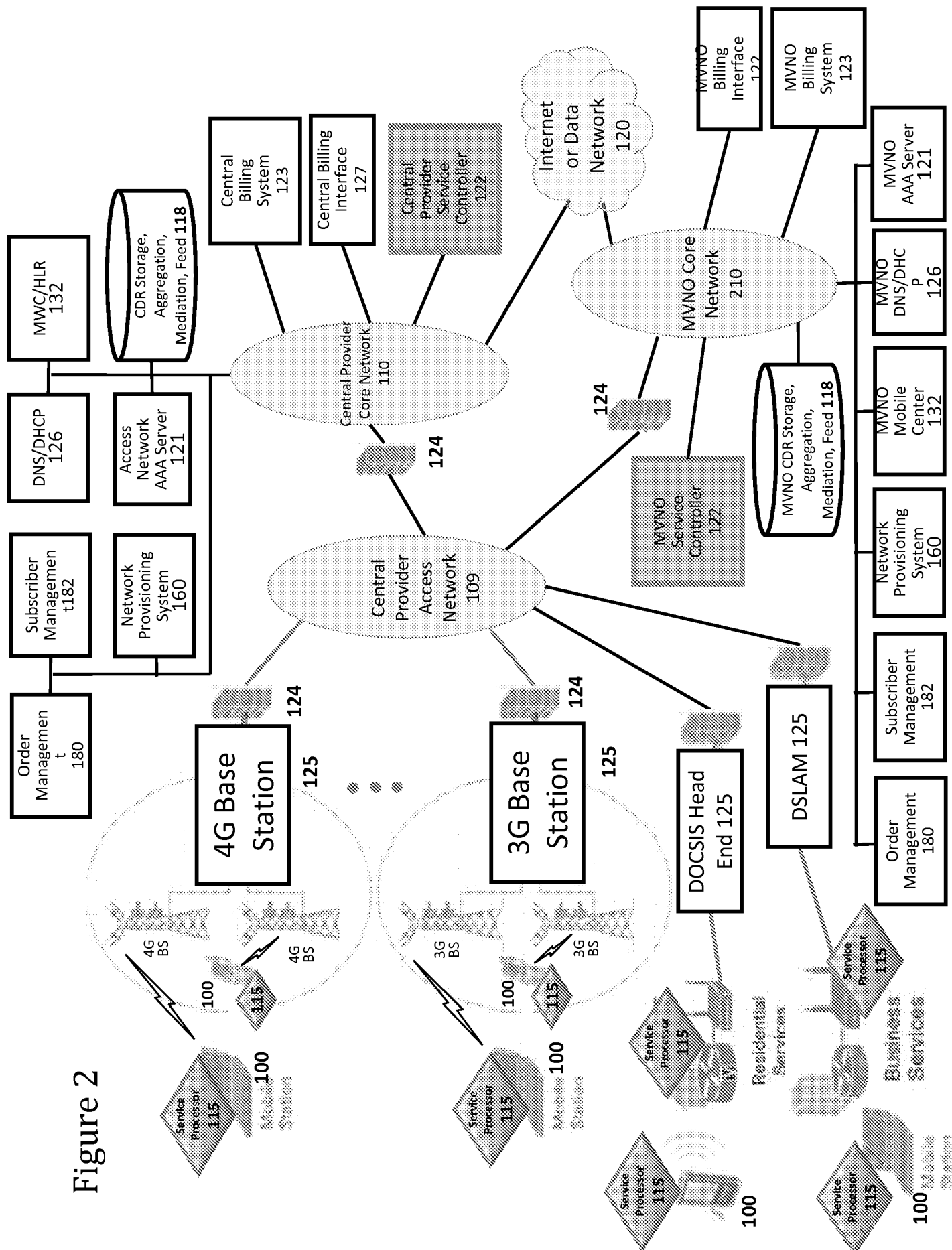


Figure 3

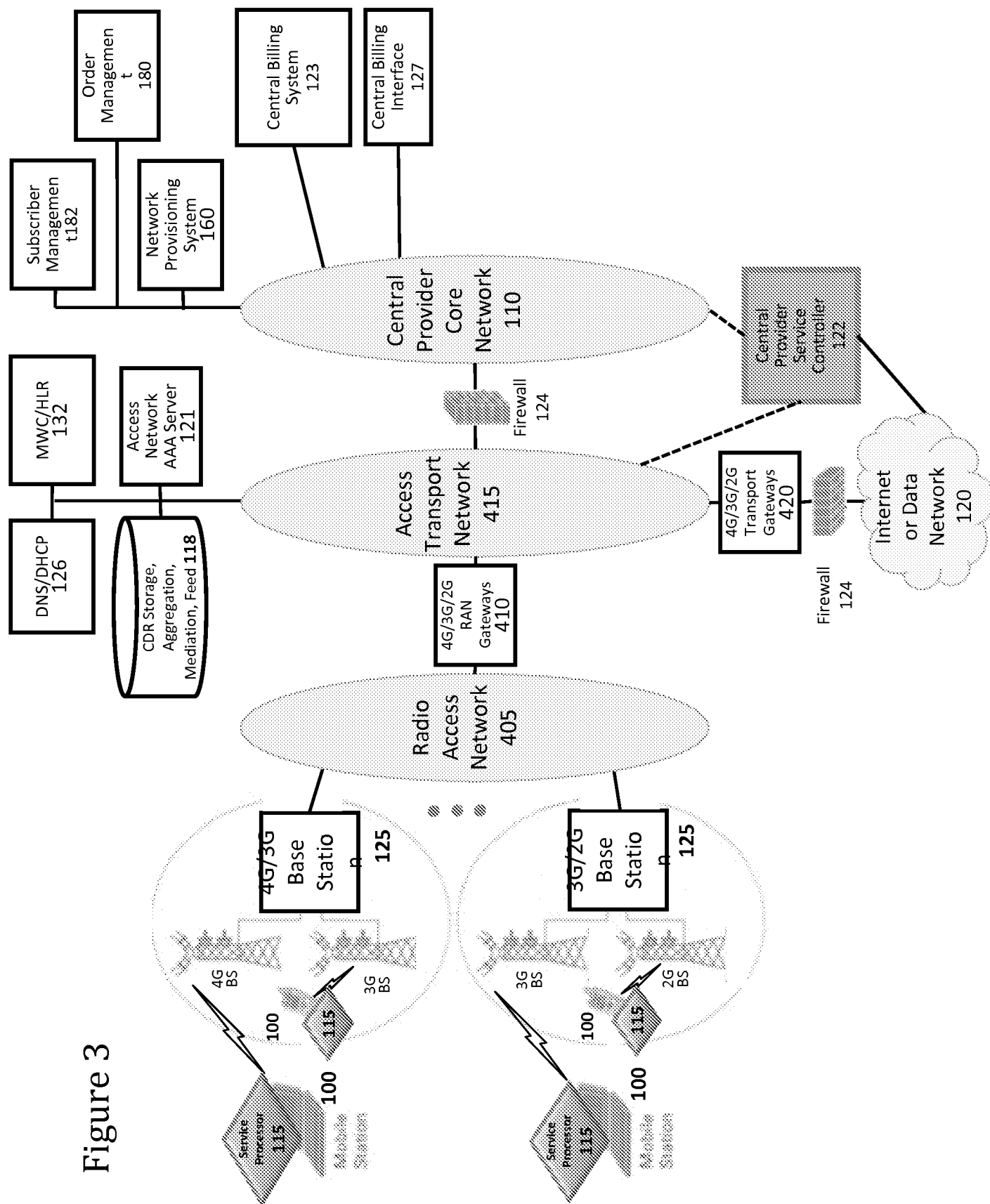


Figure 4

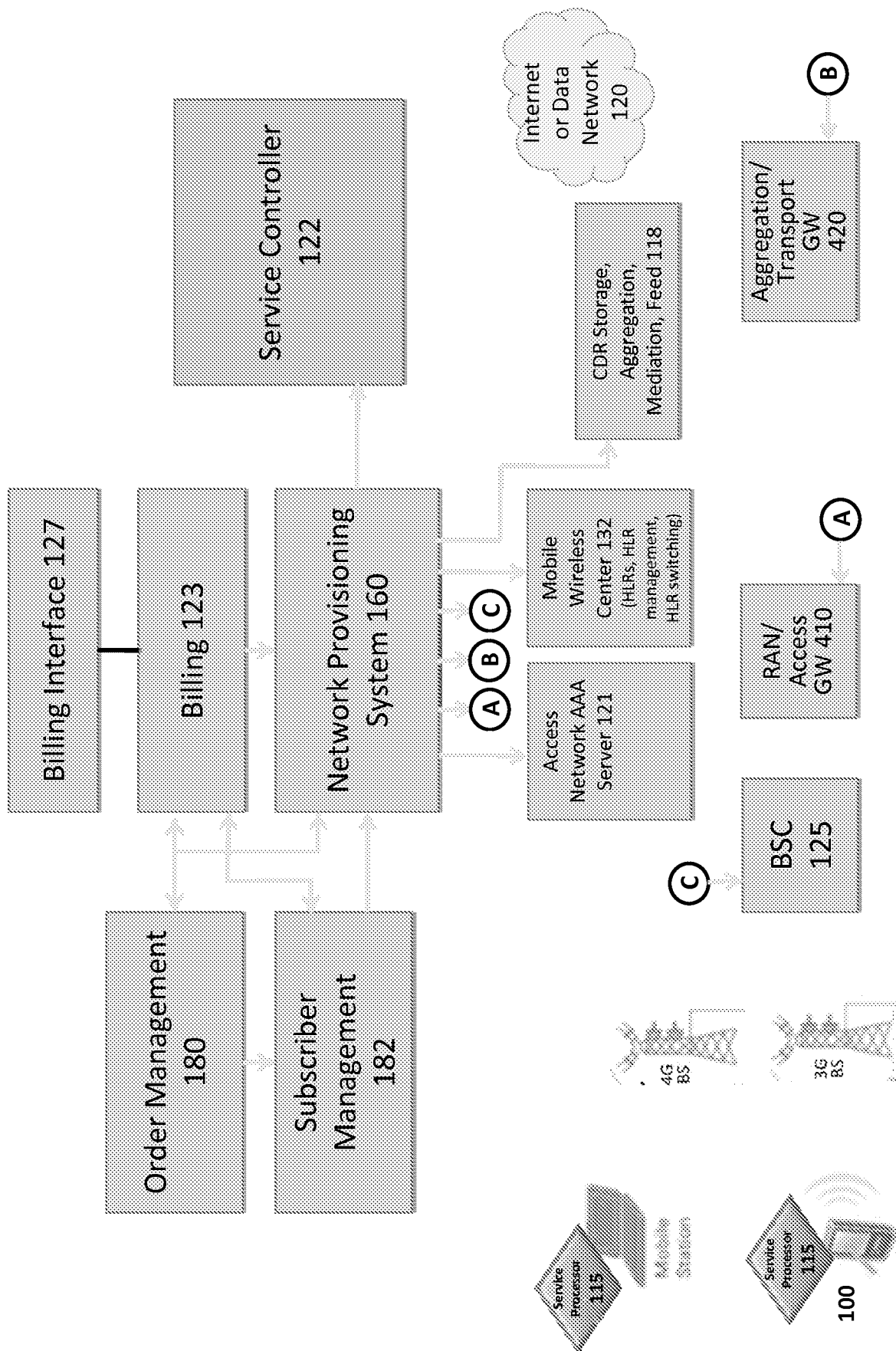


Figure 5

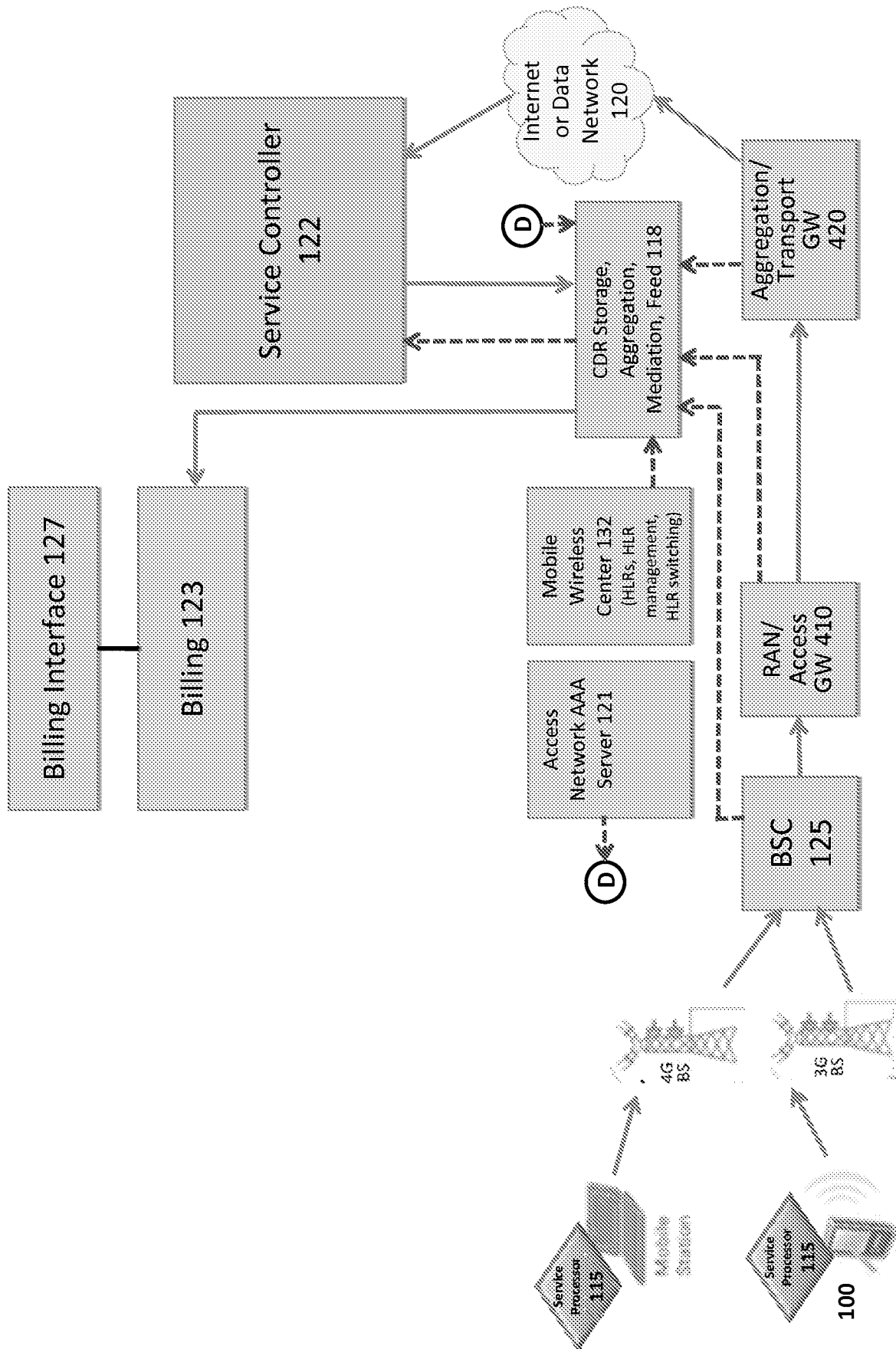


Figure 6

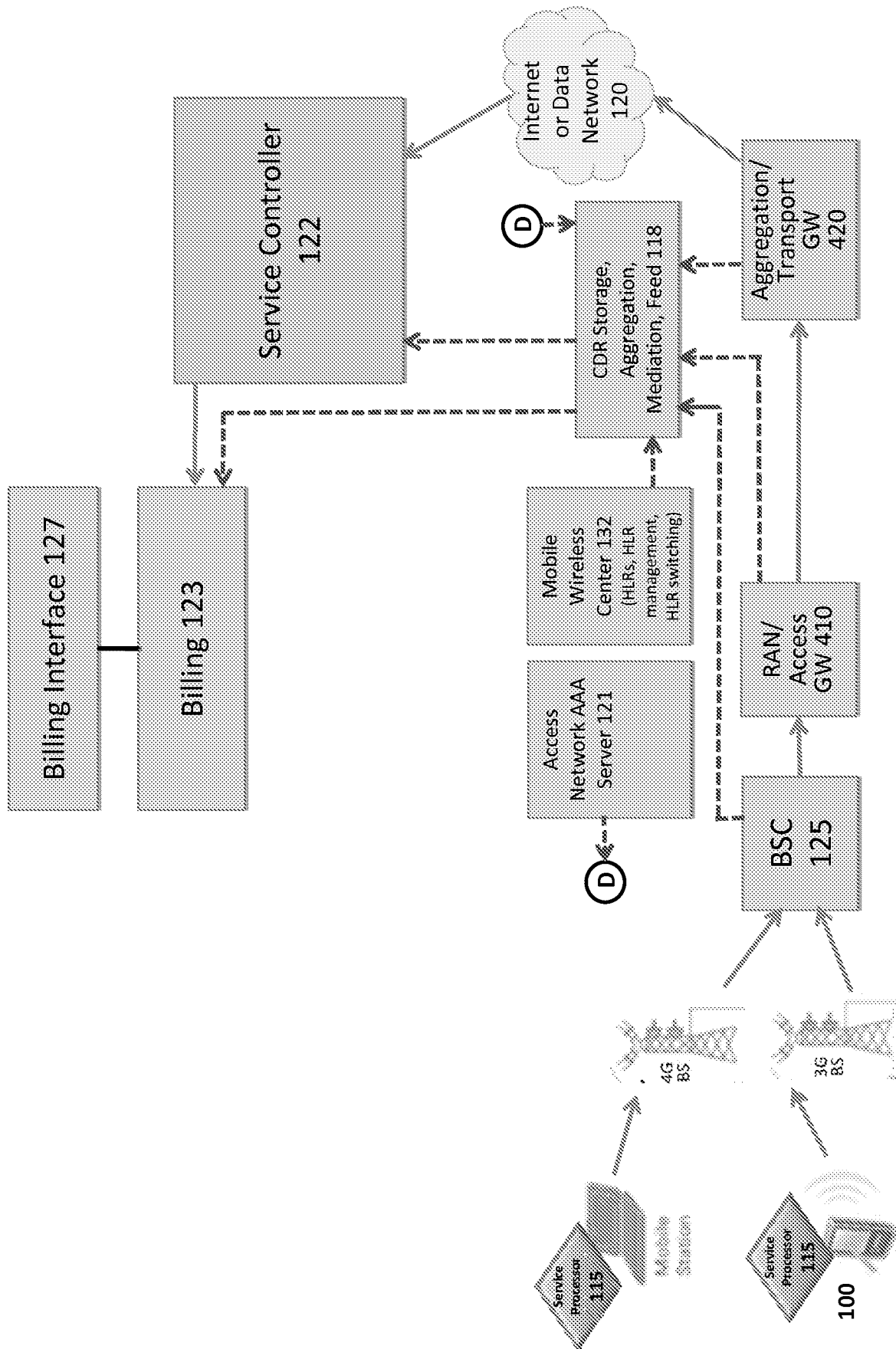


Figure 7

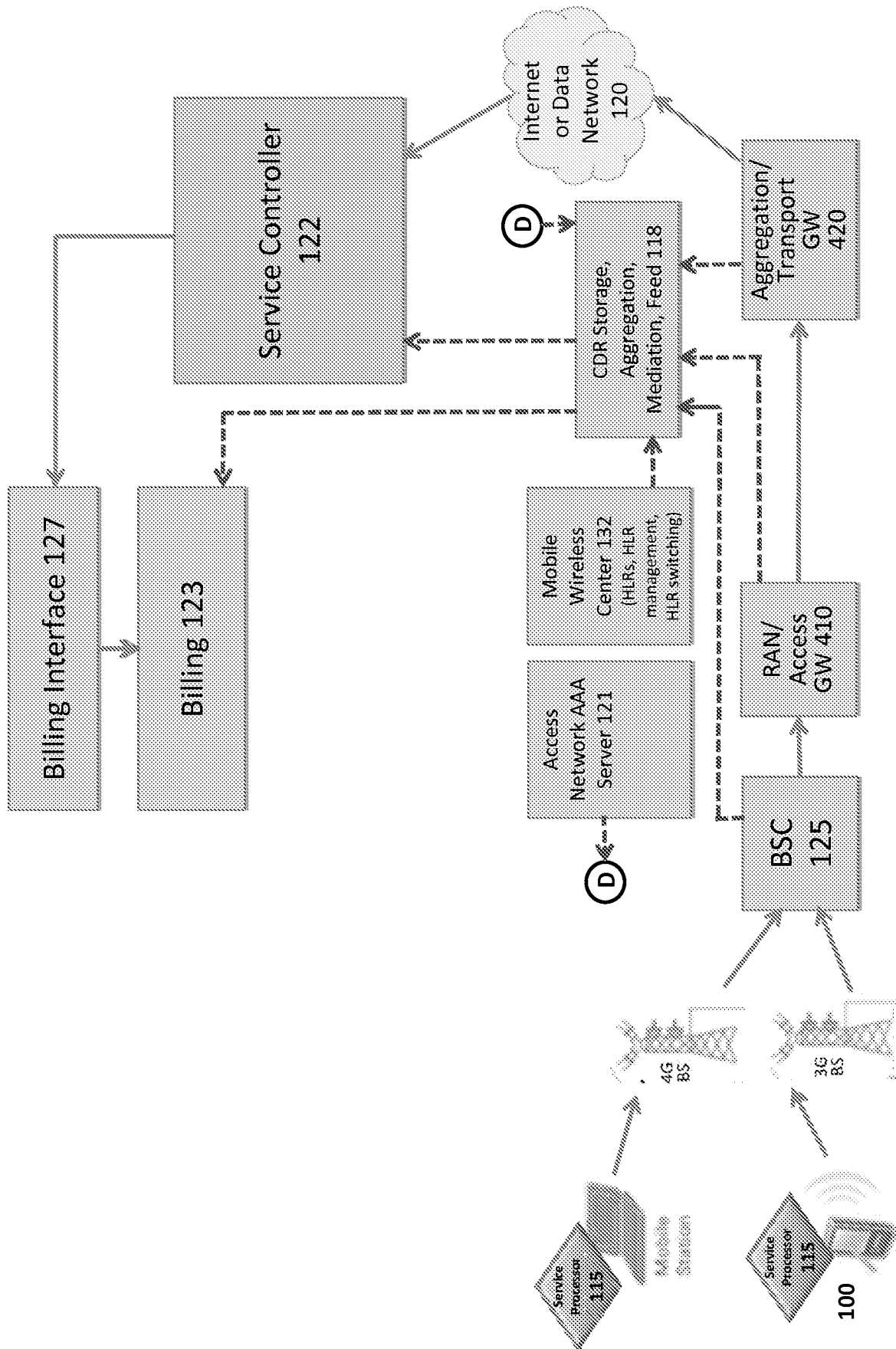
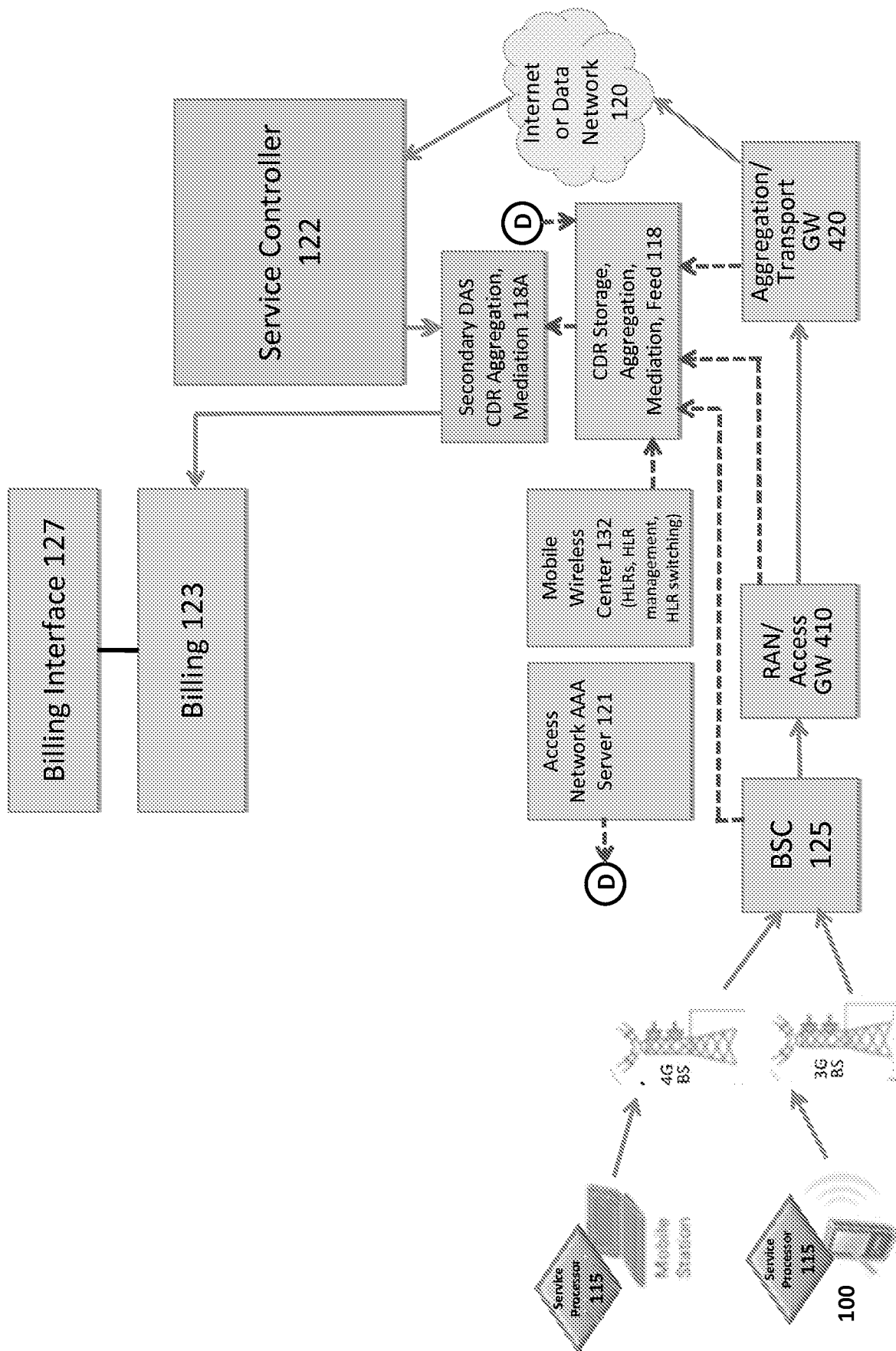


Figure 8



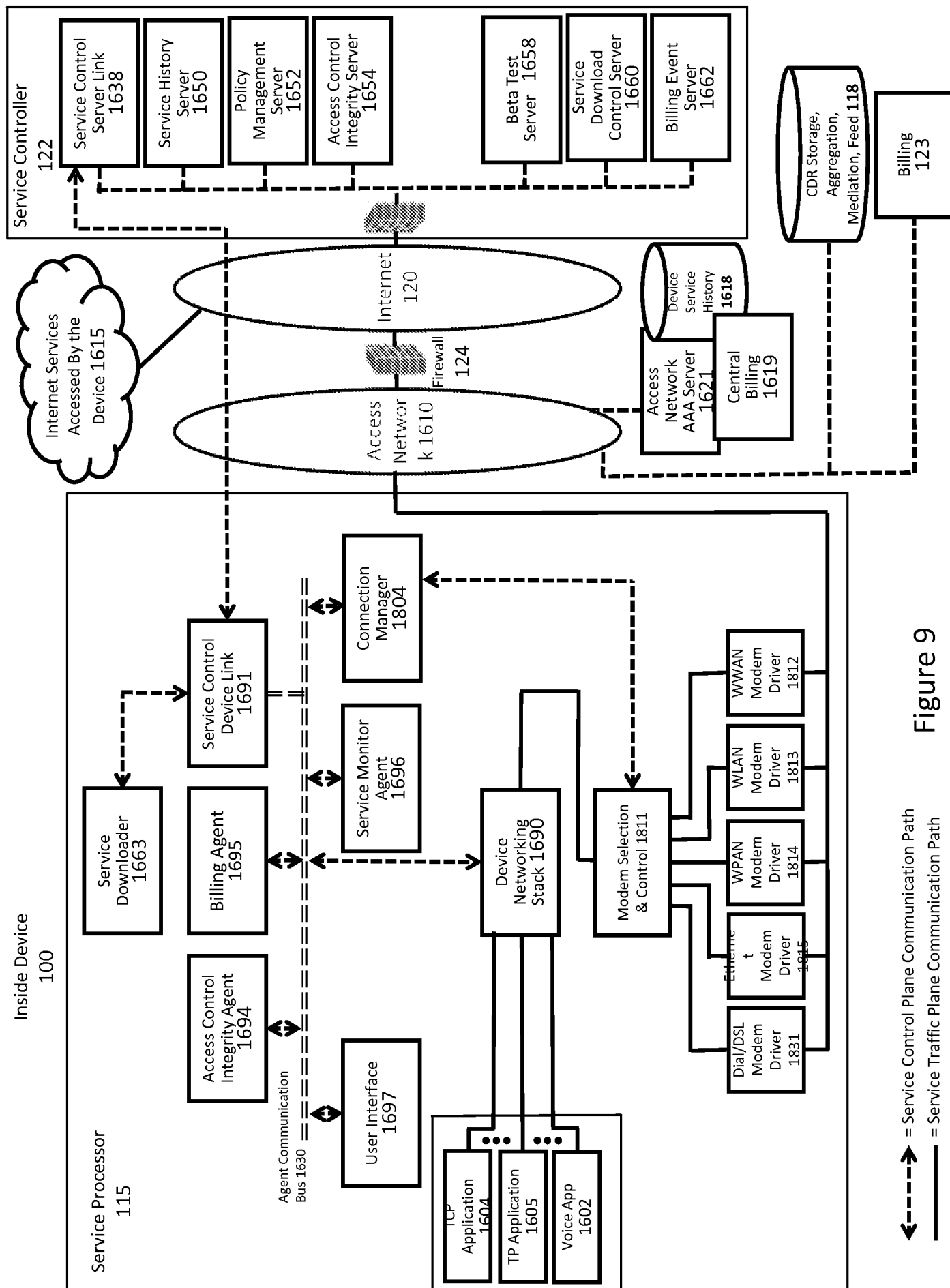


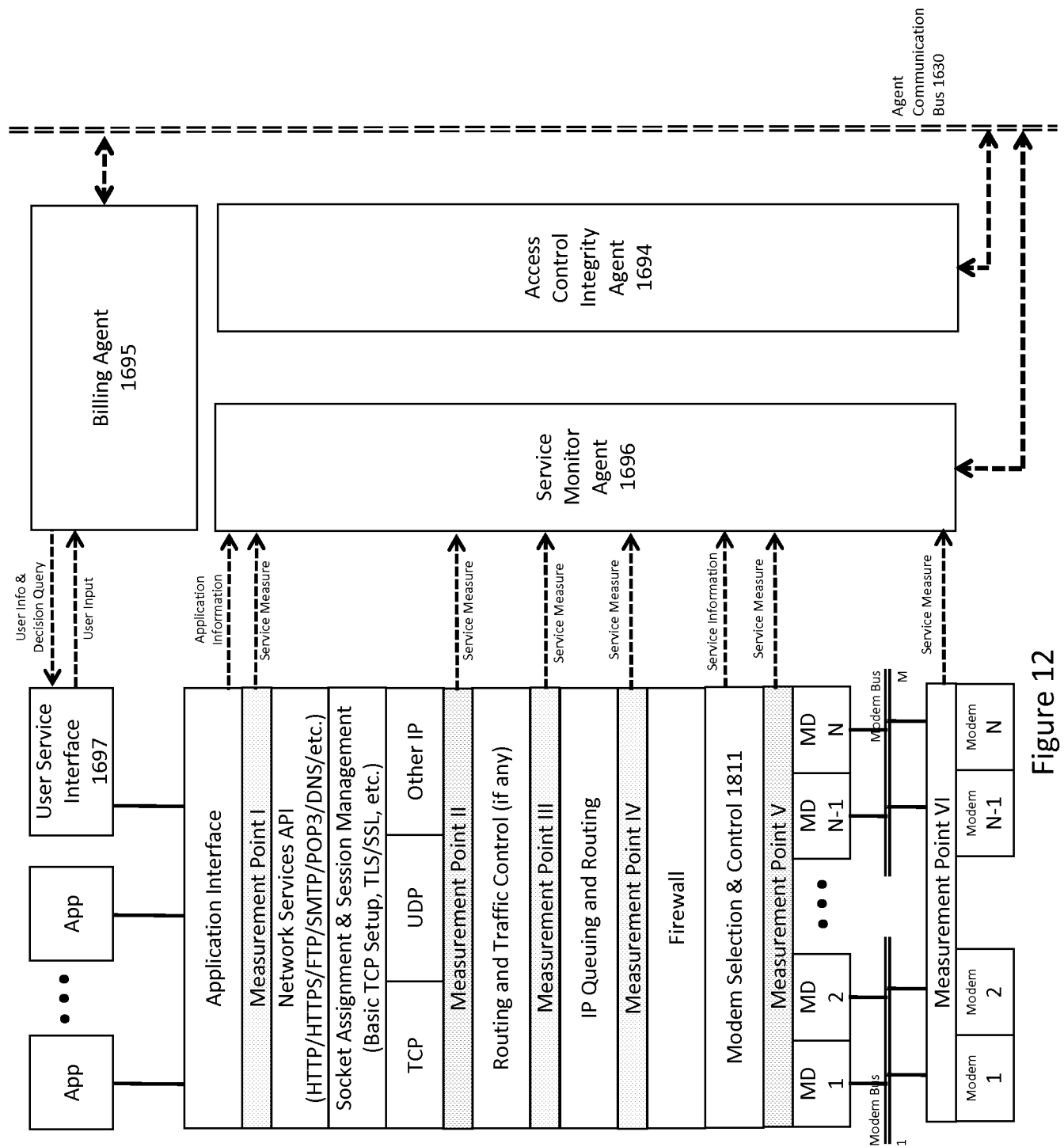
Figure 9

Service Processor 115 Embodiment	Partial Summary of Embodiment Functions
Service Control Device Link 1691	Device side control plane link for connecting Service Processor 415 to Service Controller. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Agent 1694	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected. In some embodiments, verifies configuration of other agents or performs challenge-response sequence testing. In some embodiments, monitors software loading activity, protected memory access or communication with Service Processor agents to detect unauthorized changes to Service Processor software or configuration.
Service Monitor Agent 1696	Records and reports device service usage. In some embodiments, assists in communicating application tagging of traffic flows through the networking stack policy implementation. In some embodiments, maintains a history and provides reports or summary reports of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection.
Billing Agent 1695	Detects and reports billing events. In some embodiments interacts with the User Interface Agent 497 to provide the user with service plan options, accept service plan selections, provide notification on service usage levels, provide options on service usage control policy, accept choices on service usage policy, provide transaction options or accept transaction choices. In some embodiments, interacts with Transaction Servers 134 to conduct ecommerce transactions with central billing.
User Interface 1697	Provide service interface to users.
Service Downloader 1663	Provides a download function to install or update service software elements on the device.
Connection Manager 1804	Provides a control and supervision function for one or more modem drivers or modems that connect to an access network.
Modem Selection and Control 1811	Selects the access network connection.
Modem Drivers 1831, 1815, 1814, 1813, 1812	Converts data traffic into modem bus traffic for one or more modems.
Modems 2141, 2125, 2124, 2123, 2122	Connects the device to one or more networks.

Figure 10

Service Controller 122 Element	Partial Summary of Embodiment Functions
Service Control Server Link 1638	Network side control plane link for connecting Service Controller 122 and Service Processor 115 device agents. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Server 1654	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected.
Service History Server 1650	Collects and records service usage reports from the Access Network AAA Server 1621 and the Service Monitor Agent 1696. In some embodiments, maintains a history of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection. In some embodiments, this activity summary is further analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.
Central Provider Billing System 123	Provides mediation function for central provider billing events. Accepts service plan changes. In some embodiments, provides updates on device service usage, service plan limits or service policies.
Billing Event Server 1662	In some embodiments, collects billing events, provides service plan information to the Service Processor 115, provides service usage updates to the Service Processor 115, serves as interface between device and central Provider Billing System 123, or provides trusted third party function for certain ecommerce billing transactions.
Service Download Control Server 1660	Provides a download function to install or update service software elements on the device.

Figure 11



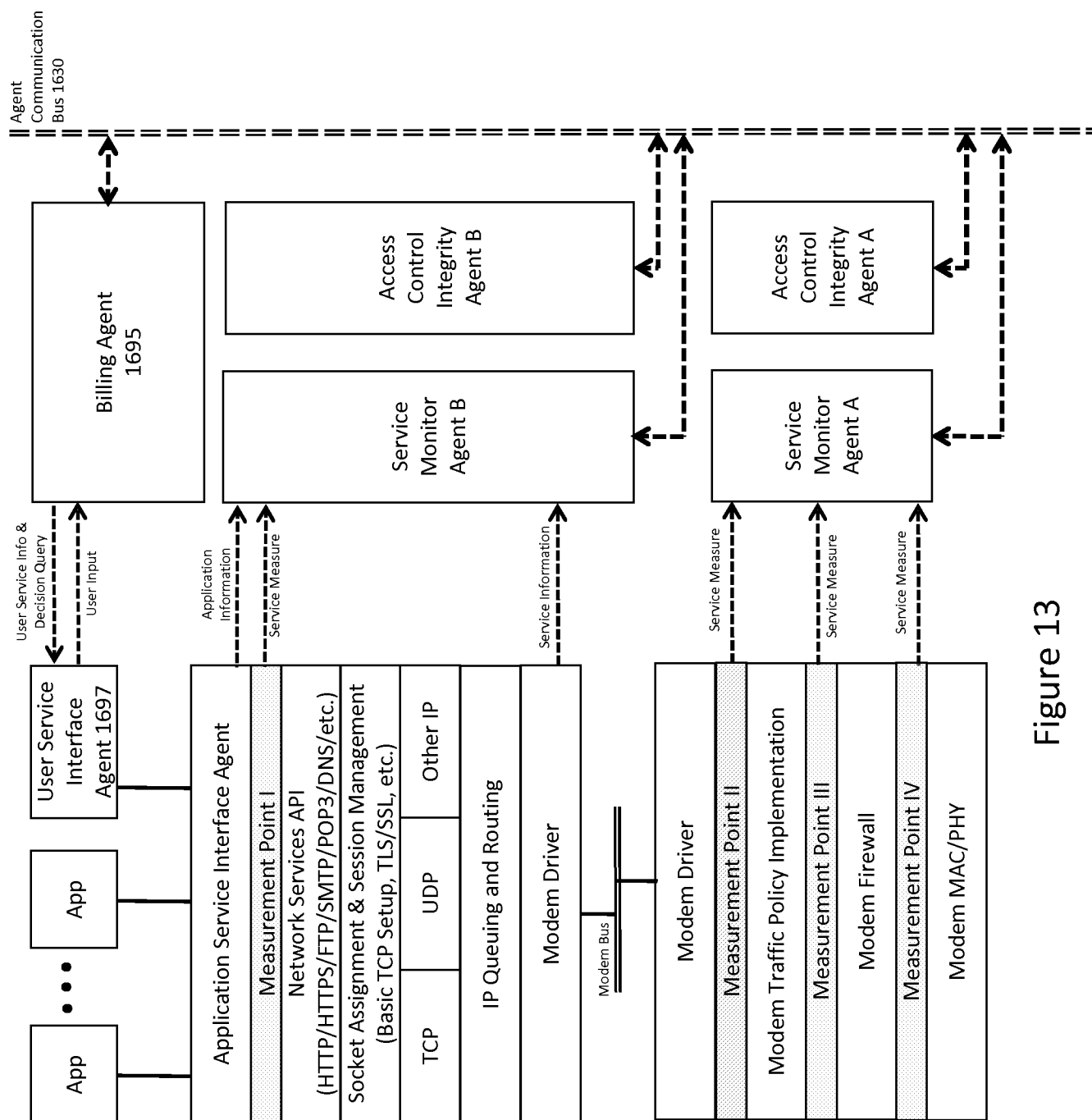


Figure 13

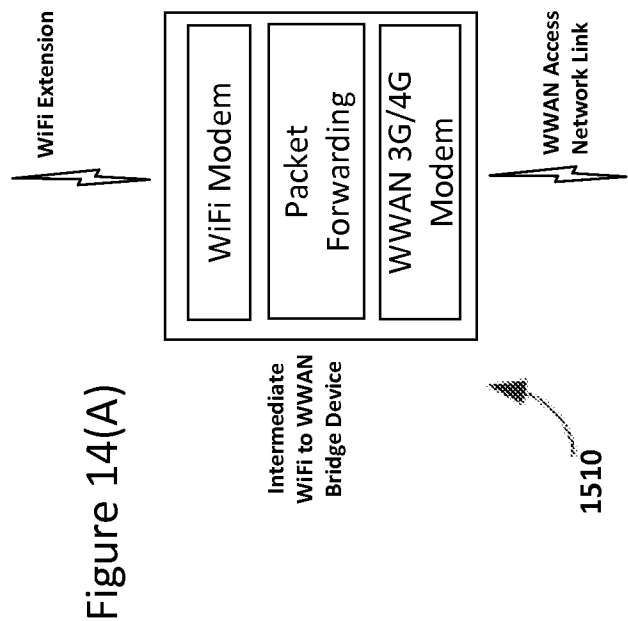
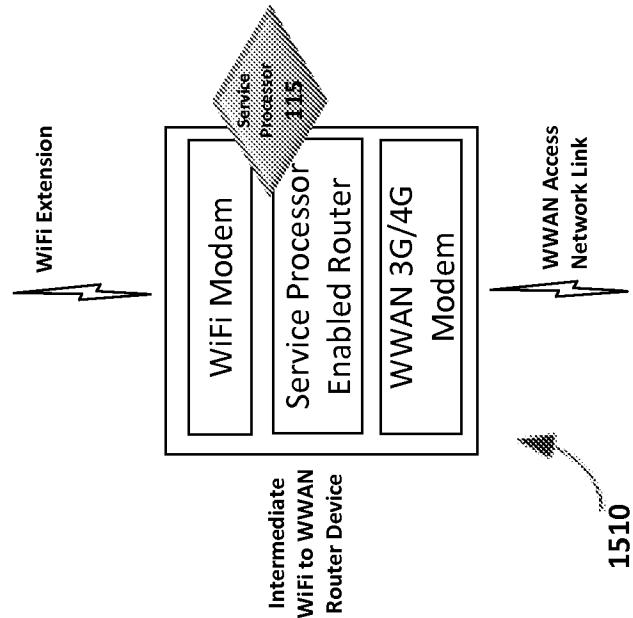
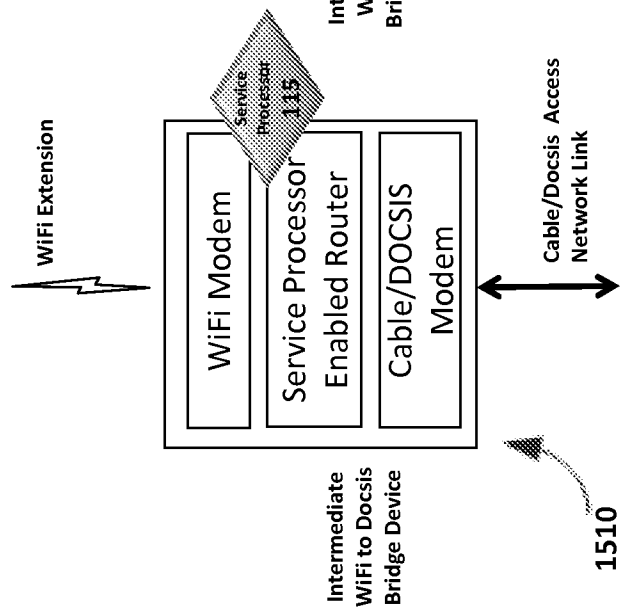
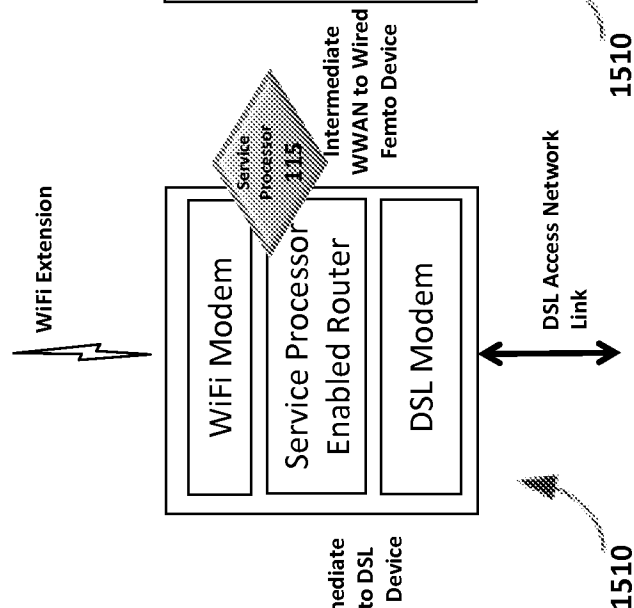
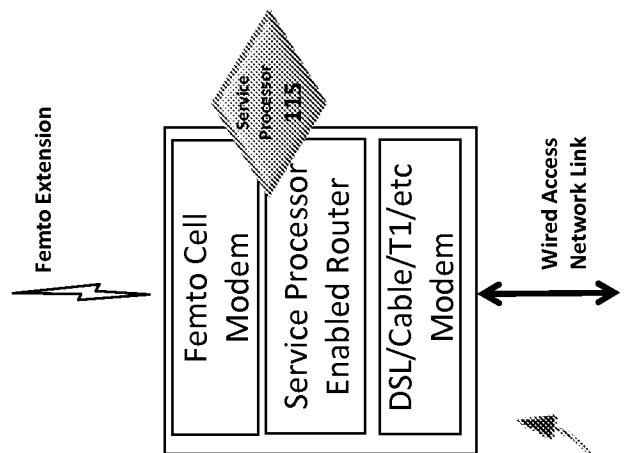


Figure 14



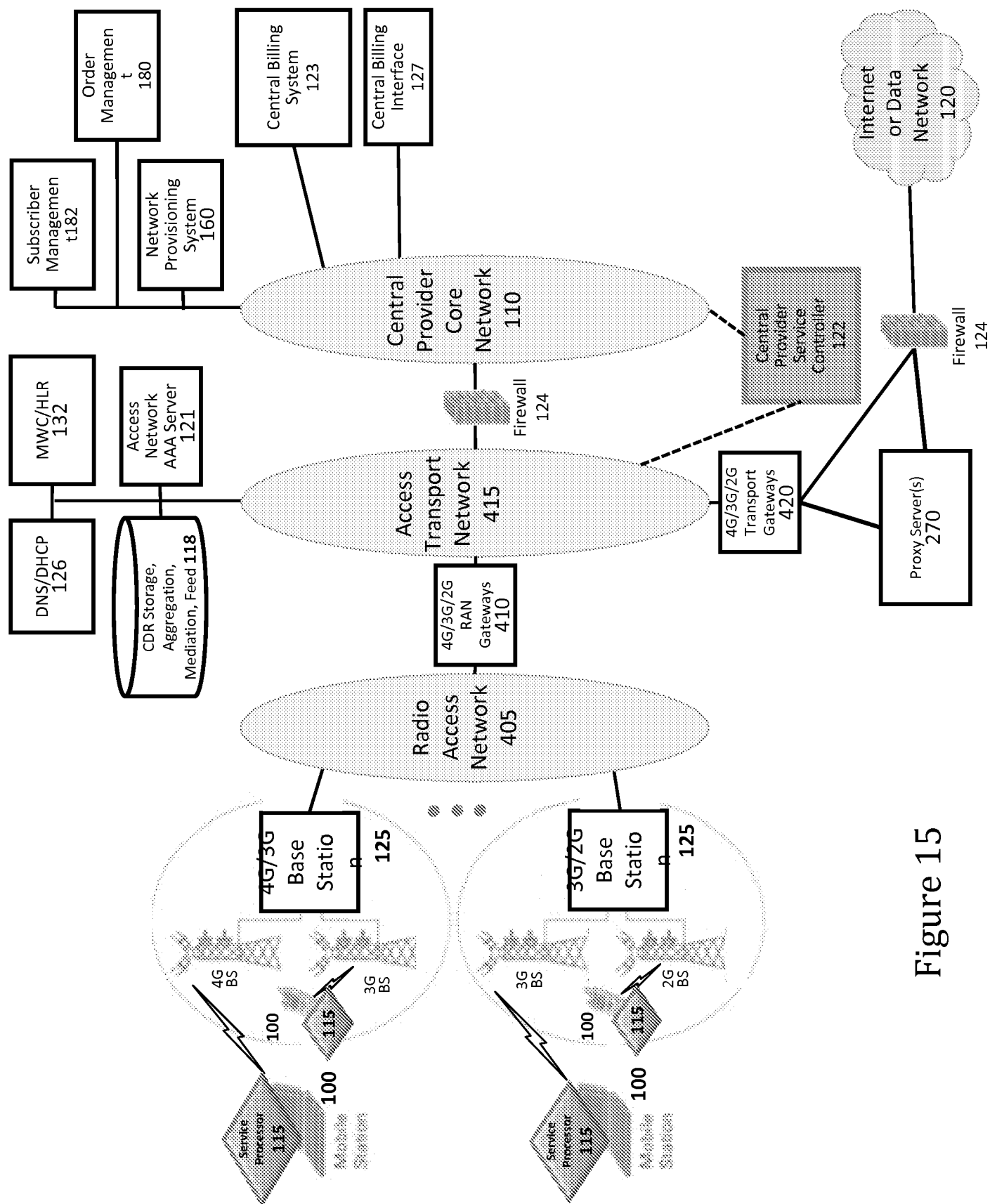


Figure 15

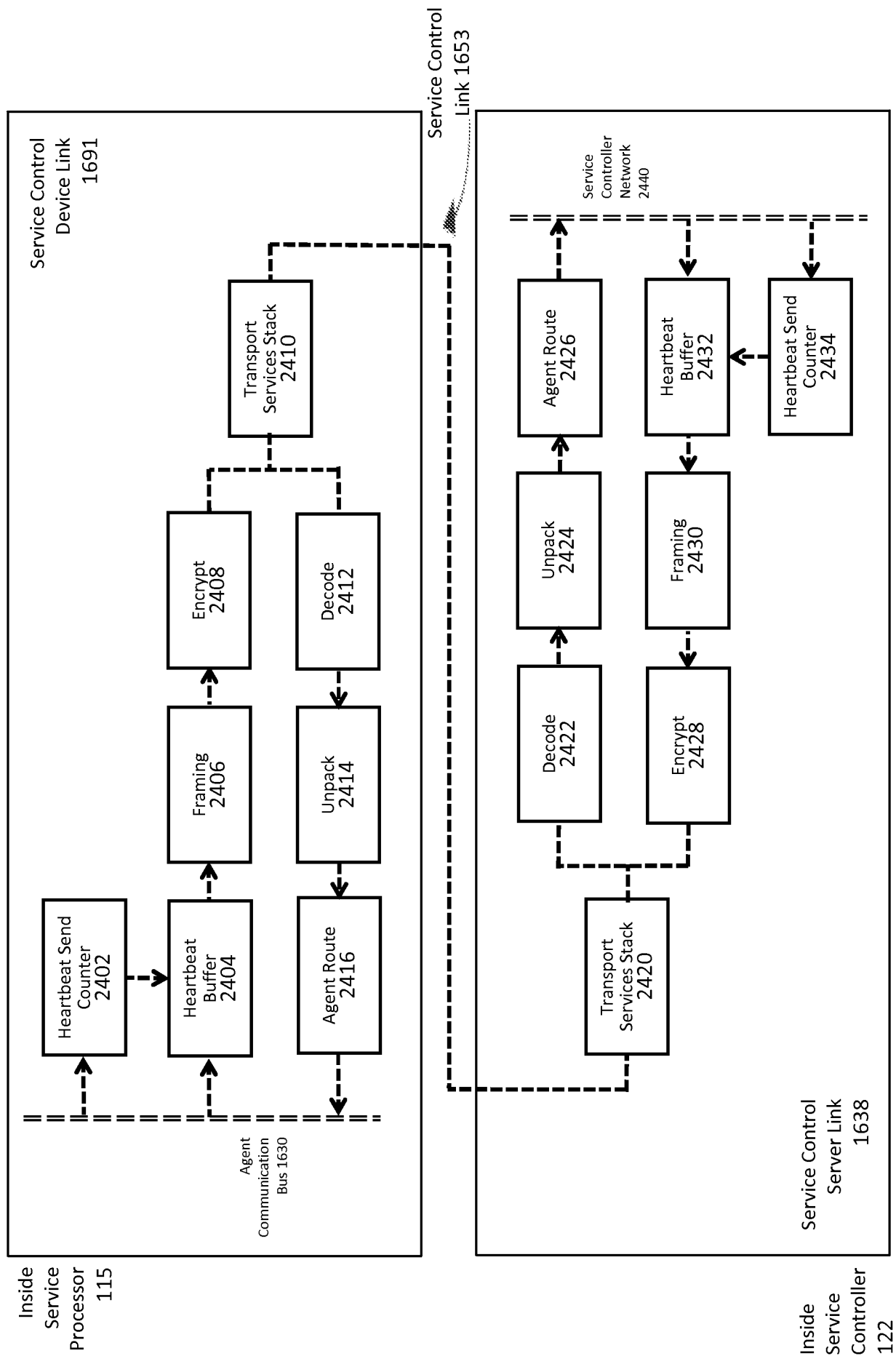


Figure 16

Service Processor Framing Sequence # 2504	Time Stamp 2506	Agent Function #1 ID 2508	Agent Function #1 Message Length 2510	Agent Function #1 Message 2512	...	Agent Function #N ID 2514	Agent Function #N Message Length 2516	Agent Function #N Message 2518
---	--------------------	------------------------------------	---	---	-----	------------------------------------	---	---

Service Processor Communication Frame 2502

Service Controller Framing Sequence # 2524	Time Stamp 2526	Agent Function #1 ID 2528	Agent Function #1 Message Length 2530	Agent Function #1 Message 2532	...	Agent Function #N ID 2534	Agent Function #N Message Length 2536	Agent Function #N Message 2538
--	--------------------	------------------------------------	---	---	-----	------------------------------------	---	---

Service Controller Communication Frame 2522

Figure 17

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Access control integrity report	Contains the latest results of the Access Control Integrity agents Service Processor system checks and reports any error events.	Not necessary to report in every heartbeat if there are no errors. Can report only on error, set a minimum frequency or respond to Service Controller polling.
Service monitor report	Reports filtered summary of Service Monitor Agent measurements. Summary reduces control traffic and filters out unauthorized private information.	Every heartbeat. Some embodiments link this to amount of data usage in the data path to keep overhead low. Report immediately upon polling from Service Controller.
Billing event report	Reports any billing activity since the last heartbeat. Billing events may include service usage events, transaction events, bill by account records, bill by account offset reports, or any other event that results in a billing event report.	Send upon billing event. Report immediately upon polling from Service Controller.
Service Processor settings report	Reports service policy settings for all Service Processor agents.	Not necessary to send every heartbeat. Some embodiments link this to amount of data usage to reduce overhead. Can report every N heartbeats. Report immediately upon polling from Service Controller.
Customer resource management report	Reports filtered summary of Service Monitor Agent measurements or filtered summary of other device or user activity such as service preferences, advertisement behavior and location. Summary reduces control traffic and filters out unauthorized private information.	Not necessary to send every heartbeat. Some embodiments link this to amount of data usage to reduce overhead. Can report every N heartbeats. Report immediately upon polling from Service Controller.
Responses to Service Processor agent queries	Sends agent responses to challenge-response queries from the Service Controller.	Report immediately upon polling from Service Controller.
Location tracking service update	Reports filtered summary of location tracking information. Summary reduces control traffic and filters out unauthorized private information.	Not necessary to send every heartbeat. Some embodiments call for a minimum time based transmission frequency.
Service usage based transmission frequency	Lowers overhead by buffering and reserving heartbeat communications from agents and servers until a certain amount of data has been transmitted or received in the network, or a certain amount of service has been consumed. When the parameters are chosen properly, this can result in the network control plane traffic overhead being a small percentage of data path traffic or result in the control plane traffic cost being a small percentage of the service usage cost.	Ranges depending on settings. For example, if there are 5 agents messages that typically need to be communicated, and each message is less than 100 bytes, and Service Processor heartbeat framing plus network overhead would result in a packet size of less than 1,000 bytes, and the heartbeat packet is transmitted when 10,000,000 bytes have been communicated over the data path, then the overhead loss due to one heartbeat packet in each direction is less than 0.02%.
Constant frequency transmissions	Since the device may be off line for long periods of time where the Service Control Processor needs to verify service control integrity, in some embodiments it can be advantageous to transmit heartbeat packets at a minimum rate regardless of data traffic activity. This is accomplished by setting a timer that sends queued heartbeat packets on a regular schedule.	Ranges depending on settings and applications.
Service Controller polled transmissions	In some embodiments, the Service Controller may poll the Service Processor for a heartbeat transmission at which time the Service Processor will frame and transmit all queued heartbeat messages.	Ranges depending on applications. In some embodiments this is used as an on demand function while in others it is used as a way to set heartbeat transmission timing functions in the Service Controller.
Service Processor polled transmissions	In some embodiments, the Service Processor polls the Service Controller for a heartbeat transmission at which time the Service Controller will frame and transmit all queued heartbeat messages.	Ranges depending on applications. In some embodiments this is used as an on demand function while in others it is used as a way to set heartbeat transmission timing functions in the Service Processor.

Figure 18A

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Agent self-check reports	Agent reports results of various agent self-diagnosis procedures to ensure that the agent is properly configured, operating properly, properly implementing service control policy or has not been tampered with. [provide examples which are extensions of typical software security self diagnosis reporting]	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Environment reports	One or more agents scan the storage or execution environment for one or more of the agents to identify potential threats to the integrity of the service implementation or agent integrity and makes a report. In one example embodiment, a scan is done to determine if unauthorized software or hardware is executing in a secure agent environment. In another embodiment, a scan is done to determine the software that has been loaded into a portion of the device operating environment, memory or storage, and the software list is referenced against a known threat list. In another example embodiment, the list of entities that accessed one or more agents is scanned to determine if an unauthorized access to an agent has occurred. In another embodiment a scan is performed to determine if unauthorized access to secure execution environment, memory or storage has occurred. In another example embodiment, the network access pattern for the device is logged and analyzed to determine if there is an access pattern that is known to be associated with a threat to service or agent control integrity. In another example embodiment, the internal device software, memory or peripheral access pattern is logged and analyzed to determine if there is an access pattern that is known to be associated with a threat to service or agent control integrity.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
User notification response reports	Billing agent, UI agent or another agent logs user notification events and the response of the user to the notification event. In some embodiments these events may be cross-referenced to the notification policy that should be in force on the device and the device service usage to ensure that the proper notification sequences are being adhered to. In other embodiments, the user notification responses are logged and used to document user choices to notification events, billing event decisions, service control decisions or service cost control decisions. In some embodiments, the user may be asked to provide a password, biometric signature, hardware key or other mechanism to positively identify that the user is in possession of the device or to verify that the service is operating properly or is implemented properly. In some embodiments, the user may be asked to acknowledge a service coverage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service coverage acknowledgement.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device, for example when there has been a user notification sequence action with the user. In some embodiments, the report is generated when there is a verification error of some kind that is identified.

Figure 18B

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
User warning response reports	Billing agent, UI agent or another agent logs user warning events and the response of the user to warning event. In some embodiments the user response is used to determine if the user is in positive control of the device. In some embodiments the response is used to confirm that the user acknowledges a billing overage or other service cost event. In some embodiments, the user may be asked to provide a password, biometric signature, hardware key or other mechanism to positively identify that the user is in possession of the device or to verify that the service is operating properly or is implemented properly.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device, for example when there has been a warning sequence action with the user. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Agent communication log reports	Reports entities that established or attempted to establish communication with the agents. In one embodiment, reports a list of entities and the number of times the entity communicated or attempted to communicate with the agent. In another embodiment, reports an error flag when unauthorized entities attempt to establish communication with an agent.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Service usage synchronization data	IPDR or other data that is used to synchronize the device service usage counters. In some embodiments the data is time stamped so that the service usage at a point in time may be reconciled between the local device usage count and the network based usage count, and then the local device usage count since the point in time may be used to estimate the present real-time usage count. In some embodiments, the service usage data from the device is used by the network as the actual service usage or billing data base for the device. In other embodiments, a bill by account function is included in the service usage synchronization data so that the service usage may be billed to different accounts other than a single or main user account.	Service usage synchronization is continuous with each heartbeat in some embodiments. In other embodiments service usage synchronization is based on a push from the Service Controller or other network function that sends the IPDR information to the device. In other embodiments, the device requests a synchronization data transmission.
Service cost synchronization data	Information to reconcile a service cost estimate on the local device with a service cost count from a network based function. Similar to the service usage count, in some embodiments the service cost information is time stamped so that service cost at a point in time may be reconciled between the device and the network based function, and then a local measure of service cost may be used to estimate the present real-time service cost. In some embodiments the local service cost is determined by taking recorded billing events and looking up the cumulative cost of one or more billing events using a service usage to cost look up data base stored locally on the device or available from a network function. In some embodiments, service cost estimation is done entirely in the network and the result is pushed out to the device UI. In other embodiments service cost estimation is done in the device based on local usage estimates and a local usage to cost lookup table.	Service cost synchronization is continuous with each heartbeat in some embodiments. In other embodiments service cost synchronization is based on a push from the Service Controller or other network function that sends the IPDR information to the device. In other embodiments, the device requests a synchronization data transmission.

Figure 18C

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Available network information and roaming information	Device receives available network or available roaming service provider information from a network function. The available network or roaming service information may include the potential network service or roaming service a device or user may choose to select, or the network service or roaming service the user has already selected. In some embodiments this information includes service cost information to aid the device or the user in determining the potential or actual costs of service usage while using the available network or roaming network. In some embodiments the service cost information is used to help the user in selecting the available network provider or roaming service provider. In some embodiments the available network cost information or roaming cost information is combined with a measure of expected or possible service usage to estimate how much a typical usage scenario may cost. In some embodiments, the available network information or roaming information is used to help the user estimate the present available network or roaming service charges for services used to date. In some embodiments service usage is recorded and sent to a network function that estimates the current service cost. In other embodiments the service cost is estimated locally on the device based on a service usage estimate and a service usage to cost look up function. In other embodiments, the service cost is derived by querying the available network or roaming network billing system.	In some embodiments available network information or roaming information is requested by the device. In other embodiments, the information is periodically updated by the Service Controller or other network function that contains the information.
System messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display a system messages or screen that is generated by a network function or server to the end user and possibly report user inputs to the UI message or screen. Examples include, etc.	System messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments, some system messages are generated in response to user input or requests. In other embodiments, system messages are generated on a regular time table or in accordance with a certain amount of service usage.
UI screen messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display user interface message or screen that is generated by a network function or serve to the end user and possibly report user inputs to the UI message or screen. Examples include service usage UI, service choice UI, upgrade UI, transaction UI, marketing UI, billing UI, user identify confirmation UI, user service warning UI, user potential service tamper response request UI, etc.	UI screen messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments, some user UI messages are generated in response to user input or requests. In other embodiments, UI messages are generated on a regular time table or in accordance with a certain amount of service usage.
Local agent check-in history	Logs and reports agent check-ins or self-reports that are made to a local agent integrity verification function.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.

Figure 18D

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Software install report	Logs and reports one or more aspects of software installs that have occurred on the device.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified. In some embodiments, the report is generated when new SW is installed.
Test billing event	In some embodiments the Service Controller or other network function may send or cause a test billing event wherein the device triggers a local billing sequence for the purpose of verifying that the billing sequence is properly logged, conducted and reported. The billing sequence can be related to a service usage event or sequence, a transaction event or sequence, or any other event or sequence that should result in a billing event.	In some embodiments, the test billing event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.
Test service event	In some embodiments the service Controller or other network function may send or cause a service usage event wherein the device triggers a local service usage event or sequence for the purpose of verifying that the service usage event or sequence is properly logged and reported.	In some embodiments, the test service usage event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.

Figure 18E

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify service usage measure in network is consistent with expected service behavior	Network service usage measure is in conflict with expected service usage. Examples: traffic usage outside limits, address access outside limits, data rate outside limits, traffic shaping rules not being followed.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify service usage measure at device is consistent with expected service behavior	Device service usage measure is in conflict with expected service usage. Examples: traffic usage too high, address access outside limits, email accessed against policy.	Same as above.
Verify service usage measure in network is consistent with service usage measure at device	Device service usage measure varies significantly from network service usage measure	Same as above.
Verify service usage measure at one point in device is consistent with service usage measure at a second point in device	Service usage measure at one point in device stack that is inconsistent with another point indicates error or potential parasitic usage	Same as above. In some embodiments, the differences in service measures on the device may be used to evaluate the nature of the service usage policy implementation problem.
Verify that service policies in effect are as intended	Service policy setting queries result in settings that are different than intended	In some embodiments, reset service policies and see if error persist. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 19A

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify presence of Service Processor agents	Agent does not respond to agent communication or query-response	<p>In some embodiments, run dynamic agent load. In some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions:</p> <p>In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify configuration of Service Processor agents	Agent configuration audit or configuration self-check fails.	<p>In some embodiments, run dynamic agent load. In some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify billing events are reported or are reported properly	Billing Agent query reveals logged billing events that have not been reported.	<p>In some embodiments, perform a billing event test to determine if the billing event reporting sequence is operating properly. In some embodiments, run dynamic agent load. In some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>

Figure 19B

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
<p>Verify network reported service usage measure are consistent with reported device billing data.</p>	<p>Billing agent is not properly reporting billing events for service usage, transactions, bill by account, or other billing event functions.</p>	<p>In some embodiments, perform a service usage test to determine if the service usage reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
<p>Verify device reported service usage measure are consistent with reported device billing data.</p>	<p>Billing agent reports are inconsistent with service usage reports.</p>	<p>In some embodiments, perform a billing event test to determine if the billing event reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, perform a service usage test to determine if the service usage reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>

Figure 19C

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Send test billing event through device and verify it is reported.	Test billing event is nor properly reported by the device.	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify device reports billing events reported from transaction servers.	Transaction server receipts do not correspond with billing events from device.	In some embodiments, perform checks to determine of transaction server receipts are valid. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify activation tracking system presence, configuration or operation	Activation tracking service is not present, is not providing scheduled network activity reporting, or is exhibiting erroneous reports.	In some embodiments the response is to place the device ID, on a list of devices suspected of having activation tracking functions that have been tampered with for the purpose of central provider billing reconciliation. In some embodiments, install a new copy of the activation tracking service agent software either from a locally stored device copy or a network download. In some embodiments where authorization exists to manage device software and some aspects of service tracking, run further checks on device service integrity such as agent query-response. In some embodiments where authorization exists to manage a device access service connection, send error message to device UI, suspend device or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Verify device standing or service plan standing	No service plan on record or device not authorized	In some embodiments, if device is not yet activated with a service plan, provide UI with activation sequence. In some embodiments, if device is not authorized for service on one of the networks controlled by the Service Controller, send the UI an error message instructing the user how to proceed. In some embodiments, configure the Service Processor for the ambient service intended for that device. In some embodiments, download the appropriate Service Processor agent software that is appropriate for that device.

Figure 19D

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify proper operation of Service Processor agents	Check input to output relationship on Policy Implementation agent, Firewall agent. Check billing event reports to verify events are being recorded. Check application and traffic inspection tagging system correctly tagging traffic. Verify Service Processor heartbeat reports proper agent integrity self-checks, cross-checks and query/response sequences with Service Controller.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Service Processor heartbeat response reports	One or more of the heartbeat reports indicate an error in operation, configuration, or tamper and error prevention system. Heartbeat function not functioning properly but device is still indicating service usage on the network.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Test service event	Service usage reporting system does not properly report test service usage event	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing test event to determine if the device is properly reporting billing events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 19E

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Load a fresh version of Service Processor software and perform integrity reports	After fresh load of Access Control Integrity Agent, agent discovers one or more of the other agents are corrupted.	Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify Service Processor code configuration with agent self diagnosis checks	One or more of the agents indicates an error after running a self-check.	Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify that device uses service only after being authorized	Device gains access to the network and does not check in with the Access Control Integrity Server and service measures indicate device is on the network.	In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 19F

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify user standing	User does not respond with proper response to UI query such as request for ID., password or biometric input. This process may be part of handling a suspected error.	In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis. In some embodiments, the user may be asked to acknowledge a service coverage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service coverage acknowledgement.
Agent communications log	Unauthorized communications with one or more agents is detected	In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 19G

Service Policy Implementation Tamper or Error Protection Technique	Example Error Trigger Criteria	Example Error Responses
Detect or block device networking activity that is potentially harmful for the operation of Service Processor.	Network activity is observed in service monitor reports that fit known patterns that indicated harmful software may be present on device.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized Service Processor software from being loaded.	Access Control Integrity Agent discovers software that is on a known malicious list.	Same as above.
Detect or block unauthorized access of protected Service Processor software or hardware memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized communication with Service Processor software or hardware.	Unauthorized communication is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure loader with signed SW installed into protected memory	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure encrypted communication between Service Processor agents.	Secure communication link is in error or unauthorized access is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh agents with communication links that are in error or entire Service Processor. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure encrypted communication between Service Processor and Service Controller.	Service Processor communication is lost.	Send error message to device UI (if possible), suspend device, place on SPAN, place on watch list, place on further action list or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Execution of Service Processor software within secure memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.

Figure 20A

Service Policy Implementation Tamper or Error Protection Technique	Example Error Trigger Criteria	Example Error Responses
Storage of service processor software in secure memory	Secure memory violation or Service Processor stored in non-secure memory	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detection or removal of software thought to be harmful to Service Processor operation.	Unauthorized software is detected.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Recording and reporting of software loading signatures, software activity signatures or network activity signatures for later identification of threat sequences.	Unauthorized software or malicious network activity is detected	Same as above.
Implement critical Service Processor software as a self-refreshing program that resists corruption by running self-audit and reinstall processes such as placing audit function in inaccessible memory or OS functions or bios.	Re-installation function alerts that re-installation has been required. Continued re-installations or failure to re-install alert increases severity of warnings.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Encrypted agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code encryption	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Obfuscated agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code obfuscation	Same as above.
Unique agent identification numbers and signatures	Agent is discovered to have an incorrect ID, or fails signature	Same as above.
Secure agent communication bus	Agent communication bus monitoring discovers unauthorized communication or other unauthorized access to one or more agents is discovered	Same as above.
Agent level message encryption	Agent is found to be communicating without the required level of agent communication encryption	Same as above.

Figure 20B

Service Policy Implementation Tamper or Error Protection Technique	Example Error Trigger Criteria	Example Error Responses
Service control link message level encryption	Unauthorized communication traffic is discovered on service control link	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Service control link transport layer encryption	Unauthorized communication traffic is discovered on service control link	Same as above.
Agent communication access permissions	Unauthorized communication is discovered with one or more agents	Same as above.
Agent communication log	Unauthorized communication is discovered with one or more agents	Same as above.
Encrypted agent code for downloads	Agent download is found to have incorrect or absent encryption or signature	Same as above.
Secure downloader memory	Unauthorized access to or storage in secure downloader memory is discovered	Same as above.

Figure 20C

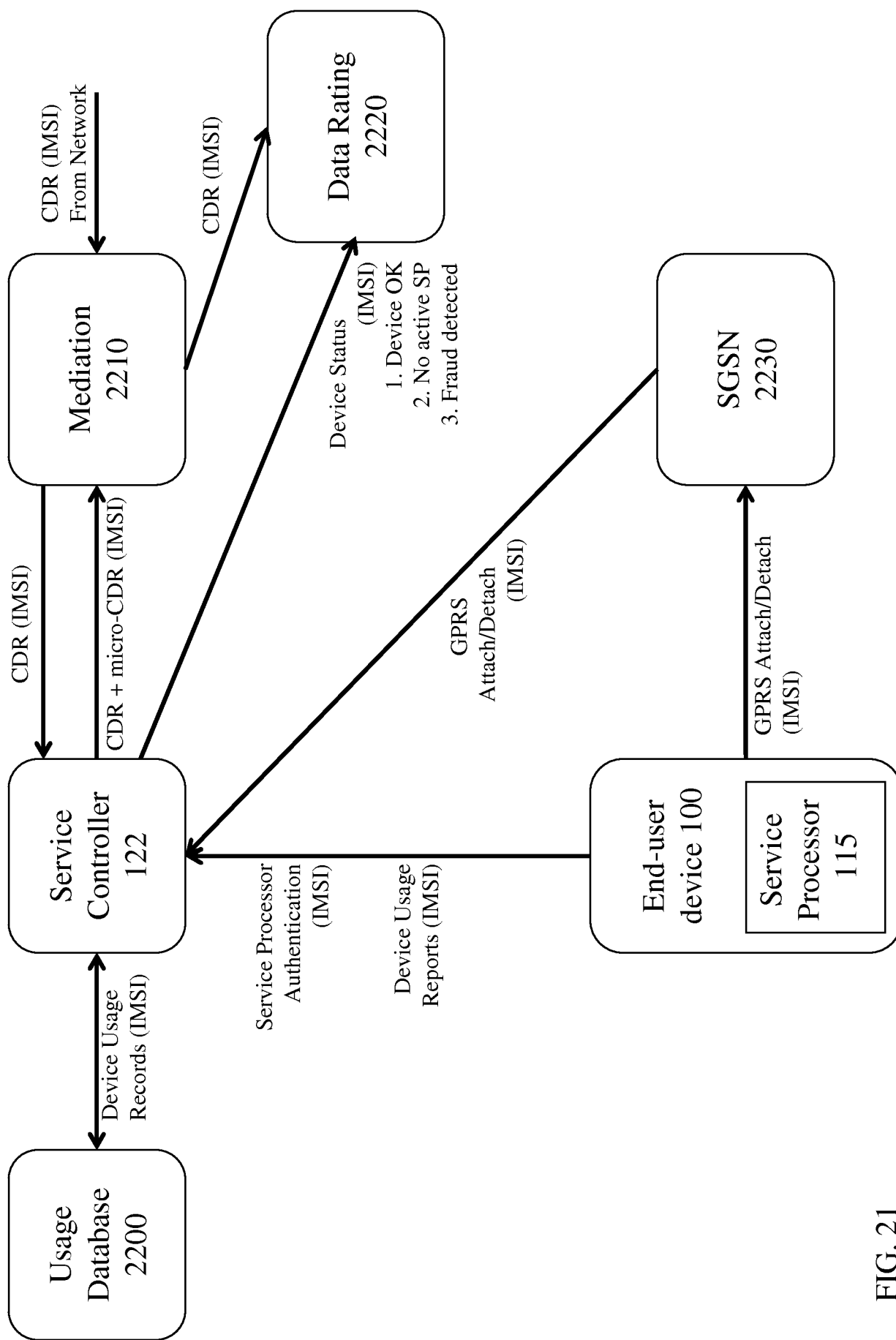


FIG. 21

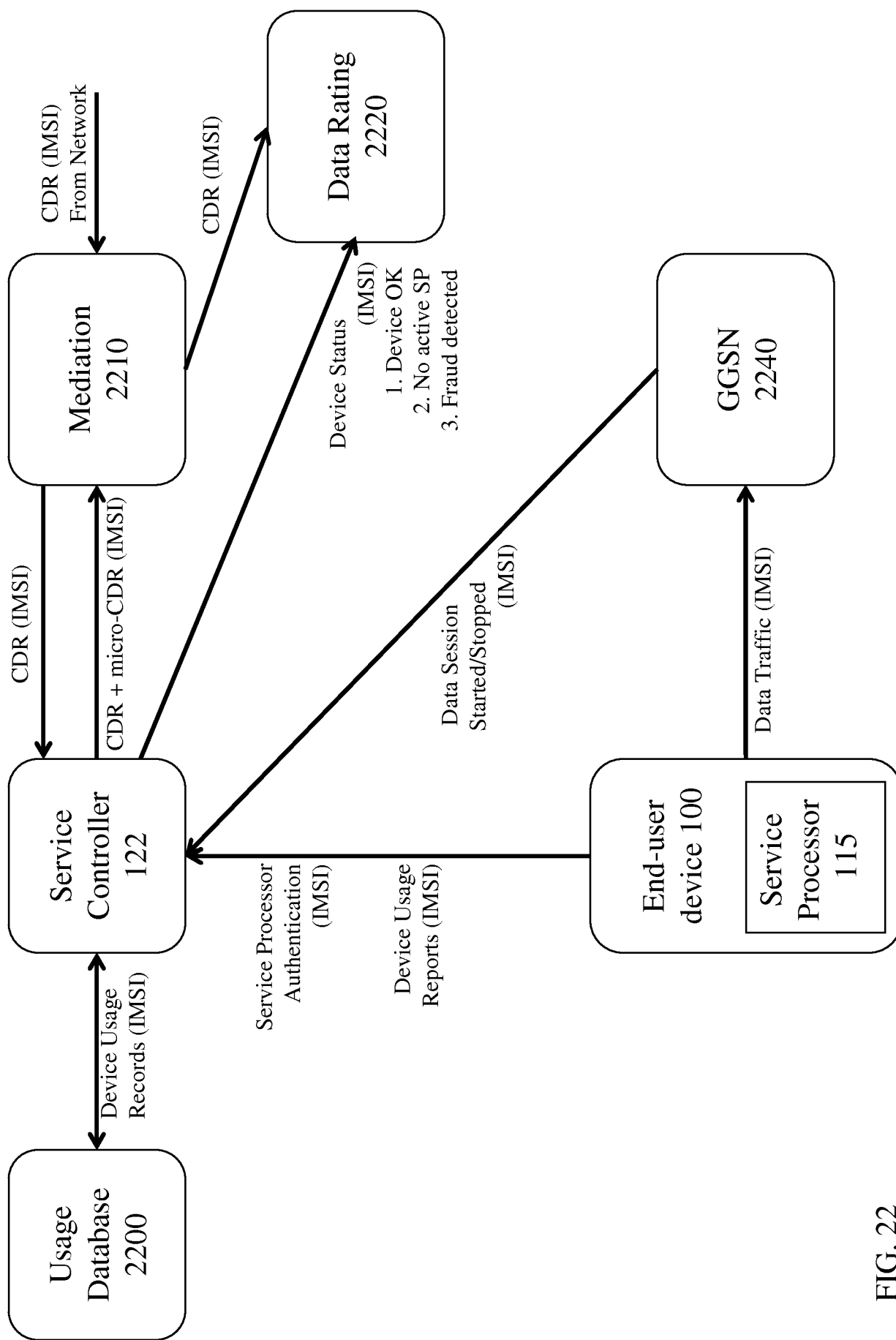


FIG. 22

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	Adapting Network Policies Based on Device Service Processor Configuration			
First Named Inventor/Applicant Name:	Gregory G. Raleigh			
Filer:	Marc A. Sockol/Linda Brost			
Attorney Docket Number:	26WV-160511 [RALEP034]			
Filed as Small Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	82	82
Utility Search Fee	2111	1	270	270
Utility Examination Fee	2311	1	110	110
Pages:				
Utility Appl Size fee per 50 sheets >100	2081	1	135	135
Claims:				
Claims in excess of 20	2202	11	26	286
Independent claims in excess of 3	2201	2	110	220

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1103

Electronic Acknowledgement Receipt

EFS ID:	10995137
Application Number:	13237827
International Application Number:	
Confirmation Number:	1814
Title of Invention:	Adapting Network Policies Based on Device Service Processor Configuration
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	69849
Filer:	Marc A. Sockol/Linda Brost
Filer Authorized By:	Marc A. Sockol
Attorney Docket Number:	26WV-160511 [RALEP034]
Receipt Date:	20-SEP-2011
Filing Date:	
Time Stamp:	20:10:56
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 1103
RAM confirmation Number	12068
Deposit Account	504561
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		160511-RALEP034-ApplicationA-092011.pdf	94767	yes	2
			952befc8769e06142d380b78a824ee04c9ada56a		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal of New Application		1	1	
	Authorization for Extension of Time all replies		2	2	
Warnings:					
Information:					
2	Specification	160511-RALEP034-ApplicationB-092011.pdf	470235	no	103
			769a163b896e5be3510826a7c0ca41e4c8ba9155		
Warnings:					
Information:					
3	Drawings-only black and white line drawings	160511-RALEP034-ApplicationC-092011.pdf	1495917	no	34
			4ca67786a321b3f4d6a6da403be4e15f386fa9c		
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	39938	no	2
			8511c82acff5f1b59393ce6b65f6c15edb1647ca		
Warnings:					
Information:					
Total Files Size (in bytes):			2100857		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

SCORE Placeholder Sheet for IFW Content

Application Number: 13237827

Document Date: 9/20/2011

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (<http://es/ScoreAccessWeb/>).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/237,827	
APPLICATION AS FILED - PART I							
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)	RATE(\$)	FEE(\$)	
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	95	N/A		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	310	N/A		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	125	N/A		
TOTAL CLAIMS (37 CFR 1.16(j))	31	minus 20 = *	11	x 30 =	330		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	5	minus 3 = *	2	x 125 =	250		
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			155			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					0.00		
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	1265	TOTAL	
APPLICATION AS AMENDED - PART II							
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	x =	x =	=
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =	x =	=
	Application Size Fee (37 CFR 1.16(s))						
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
				TOTAL ADD'L FEE		TOTAL ADD'L FEE	
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	x =	x =	=
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =	x =	=
	Application Size Fee (37 CFR 1.16(s))						
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
				TOTAL ADD'L FEE		TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.							



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/237,827	09/20/2011	Gregory G. Raleigh	26WV-160511 [RALEP034]

CONFIRMATION NO. 1814

FORMALITIES LETTER



OC000000050127234

69849
SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
390 Lytton Avenue
Palo Alto, CA 94301

Date Mailed: 10/03/2011

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing.

A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.

Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of \$65 for a small entity in compliance with 37 CFR 1.27, must be submitted.

SUMMARY OF FEES DUE:

Total fee(s) required within **TWO MONTHS** from the date of this Notice is \$65 for a small entity

- \$65 Surcharge.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
<https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/afesschaye/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
13/237,827	09/20/2011	2447	1103	26WV-160511 [RALEP034]	31	5

CONFIRMATION NO. 1814

69849
SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
390 Lytton Avenue
Palo Alto, CA 94301

FILING RECEIPT



OC000000050127233

Date Mailed: 10/03/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Gregory G. Raleigh, Residence Not Provided;
James Lavine, Residence Not Provided;

Power of Attorney: None

Domestic Priority data as claimed by applicant

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.)

If Required, Foreign Filing License Granted: 09/29/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/237,827**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Adapting Network Policies Based on Device Service Processor Configuration

Preliminary Class

709

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER**Title 35, United States Code, Section 184****Title 37, Code of Federal Regulations, 5.11 & 5.15****GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Examiner:

Gregory G. Raleigh, et al.

Not Yet Assigned

Serial No. 13/237,827

Art Unit: 2447

Filed: September 20, 2011

Conf. No.: 1814

Title: Adapting Network Policies Based on Device Service Processor Configuration

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

Sir:

Prior to examination of the above-referenced application, please enter the following amendments and consider the following remarks:

In the Specification:

Please replace Paragraphs [0001] through [0003] on Pages 1 through 4 of the specification with the following paragraphs [0001] through [0003]:

-- **[0001]** This application is a continuation-in-part of and incorporates by reference the following U.S. pending non-provisional patent applications: U.S. serial No. 12/380,759 filed March 2, 2009, entitled "Verifiable Device Assisted Service Policy Implementation," U.S. serial No. 12/380,779 filed March 2, 2009, entitled "Device Assisted Service Profile Management with User Preference, Adaptive Policy, Network Neutrality, and User Privacy," U.S. serial No. 12/380,758 filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Monitoring with Reporting, Synchronization, and Notification," U.S. serial No. 12/380,778 filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Billing with Integrated Accounting, Mediation Accounting, and Multi-Account," U.S. serial No. 12/380,768 filed March 2, 2009, entitled "Network Based Service Policy Implementation with Network Neutrality and User Privacy," U.S. serial No. 12/380,767 filed March 2, 2009, entitled "Network Based Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy," U.S. serial No. 12/380,780 filed March 2, 2009, entitled "Automated Device Provisioning and Activation," U.S. serial No. 12/380,755 filed March 2, 2009, entitled "Device Assisted Ambient Services," U.S. serial No. 12/380,756 filed March 2, 2009, entitled "Network Based Ambient Services," U.S. serial No. 12/380,770 filed March 2, 2009, entitled "Network Tools for Analysis, Design, Testing, and Production of Services," U.S. serial No. 12/380,771 filed March 2, 2009, entitled "Verifiable Service Billing for Intermediate Networking Devices" (issued as U.S. Patent No. 8,023,425 on September 20, 2011), U.S. serial No. 12/380,772 filed March 2, 2009, entitled "Roaming Services Network and Overlay Networks," U.S. serial No. 12/380,782 filed March 2, 2009, entitled "Open Development System for Access Service Providers," U.S. serial No. 12/380,783 filed March 2, 2009, entitled "Virtual Service Provider Systems," U.S. serial No. 12/380,757 filed March 2, 2009, entitled "Service Activation Tracking System," U.S. serial No. 12/380,781 filed March 2, 2009, entitled "Open Transaction Central Billing System," U.S. serial No. 12/380,774 filed March 2, 2009, entitled "Verifiable and Accurate Service Usage Monitoring for Intermediate Networking Devices," U.S. serial No.

12/380,773 filed March 2, 2009, entitled "Verifiable Service Policy Implementation for Intermediate Networking Devices," U.S. serial No. 12/380,769 filed March 2, 2009, entitled "Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy for Intermediate Networking Devices," U.S. serial No. 12/380,777 filed March 2, 2009, entitled "Simplified Service Network Architecture," U.S. serial No. 12/695,019 filed January 27, 2010, entitled "Device Assisted CDR Creation, Aggregation, Mediation, and Billing," U.S. serial No. 12/695,020 filed January 27, 2010, entitled "Adaptive Ambient Services," U.S. serial No. 12/694,445 filed January 27, 2010, entitled "Security Techniques for Device Assisted Services," U.S. serial No. 12/694,451 filed January 27, 2010, entitled "Device Group Partitions and Settlement Platform," U.S. serial No. 12/694,455 filed January 27, 2010, entitled "Device Assisted Services Install," U.S. serial No. 12/695,021 filed January 27, 2010, entitled "Quality of Service for Device Assisted Services," U.S. serial No. 12/695,980 filed January 28, 2010, entitled "Enhanced Roaming Services and Converged Carrier Networks with Device Assisted Services and a Proxy," U.S. serial No. 13/134,028 filed May 25, 2011, entitled "Device-Assisted Services for Protecting Network Capacity," U.S. serial No. 13/134,005 filed May 25, 2011, entitled "System and Method for Wireless Network Offloading" and U.S. serial No. 13/229,580 filed September 9, 2011 entitled "Wireless Network Service Interfaces." This application claims priority to and incorporates by reference the following U.S. pending provisional patent applications: U.S. provisional serial No. 61/384,456 filed September 20, 2010, entitled "Securing Service Processor with Sponsored SIMs," U.S. provisional serial No. 61/385,020 filed September 21, 2010, entitled "Service Usage Reconciliation System Overview," U.S. provisional serial No. 61/387,243 filed September 28, 2010, entitled "Enterprise and Consumer Billing Allocation for Wireless Communication Device Service Usage Activities," and U.S. provisional serial No. 61/387,247 filed September 28, 2010, entitled "Secured Device Data Records," U.S. provisional serial No. 61/389,547 filed October 4, 2010, entitled "User Notifications for Device Assisted Services," U.S. provisional serial No. 61/407,358 filed October 27, 2010, entitled "Service Controller and Service Processor Architecture," U.S. provisional serial No. 61/418,507 filed December 1, 2010, entitled "Application Service Provider Interface System," U.S. provisional serial No. 61/418,509 filed December 1, 2010, entitled "Service Usage Reporting Reconciliation and Fraud Detection for Device Assisted Services," U.S. provisional serial No. 61/420,727 filed December 7, 2010, entitled "Secure Device Data Records," U.S.

provisional serial No. 61/422,565 filed December 13, 2010, entitled "Service Design Center for Device Assisted Services," U.S. provisional serial No. 61/422,572 filed December 13, 2010, entitled "System Interfaces and Workflows for Device Assisted Services," U.S. provisional serial No. 61/422,574 filed December 13, 2010, entitled "Security and Fraud Detection for Device Assisted Services," U.S. provisional serial No. 61/435,564 filed January 24, 2011, entitled "Framework for Device Assisted Services," and U.S. provisional serial No. 61/472,606 filed April 6, 2011, entitled "Managing Service User Discovery and Service Launch Object Placement on a Device."

[0002] Further, this application incorporates by reference the following U.S. provisional patent applications: U.S. provisional serial No. 61/206,354 filed January 28, 2009, entitled "Services Policy Communication System and Method," U.S. provisional serial No. 61/206,944 filed February 4, 2009, entitled "Services Policy Communication System and Method," U.S. provisional serial No. 61/207,393 filed February 10, 2009, entitled "Services Policy Communication System and Method," U.S. provisional serial No. 61/207,739 filed February 13, 2009, entitled "Services Policy Communication System and Method," U.S. provisional serial No. 61/270,353 filed July 6, 2009, entitled "Device Assisted CDR Creation, Aggregation, Mediation and Billing," U.S. provisional serial No. 61/275,208 filed August 25, 2009, entitled "Adaptive Ambient Services," U.S. provisional serial No. 61/237,753 filed August 28, 2009, entitled "Adaptive Ambient Services," U.S. provisional serial No. 61/252,151 filed October 15, 2009, entitled "Security Techniques for Device Assisted Services," U.S. provisional serial No. 61/252,153 filed October 15, 2009, entitled "Device Group Partitions and Settlement Platform," U.S. provisional serial No. 61/264,120 filed November 24, 2009, entitled "Device Assisted Services Install," U.S. provisional serial No. 61/264,126 filed November 24, 2009, entitled "Device Assisted Services Activity Map," U.S. provisional serial No. 61/348,022 filed May 25, 2010, entitled "Device Assisted Services for Protecting Network Capacity," U.S. provisional serial No. 61/381,159 filed September 9, 2010, entitled "Device Assisted Services for Protecting Network Capacity," U.S. provisional serial No. 61/381,162 filed September 9, 2010, entitled "Service Controller Interfaces and Workflows." The following applications, U.S. serial No. 12/380,759 filed March 2, 2009, entitled "Verifiable Device Assisted Service Policy Implementation," U.S. serial No. 12/380,779 filed March 2, 2009, entitled "Device Assisted

Service Profile Management with User Preference, Adaptive Policy, Network Neutrality, and User Privacy," U.S. serial No. 12/380,758 filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Monitoring with Reporting, Synchronization, and Notification," U.S. serial No. 12/380,778 filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Billing with Integrated Accounting, Mediation Accounting, and Multi-Account," U.S. serial No. 12/380,768 filed March 2, 2009, entitled "Network Based Service Policy Implementation with Network Neutrality and User Privacy," U.S. serial No. 12/380,767 filed March 2, 2009, entitled "Network Based Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy," U.S. serial No. 12/380,780 filed March 2, 2009, entitled "Automated Device Provisioning and Activation," U.S. serial No. 12/380,755 filed March 2, 2009, entitled "Device Assisted Ambient Services," U.S. serial No. 12/380,756 filed March 2, 2009, entitled "Network Based Ambient Services," U.S. serial No. 12/380,770 filed March 2, 2009, entitled "Network Tools for Analysis, Design, Testing, and Production of Services," U.S. serial No. 12/380,772 filed March 2, 2009, entitled "Roaming Services Network and Overlay Networks," U.S. serial No. 12/380,782 filed March 2, 2009, entitled "Open Development System for Access Service Providers," U.S. serial No. 12/380,783 filed March 2, 2009, entitled "Virtual Service Provider Systems," U.S. serial No. 12/380,757 filed March 2, 2009, entitled "Service Activation Tracking System," U.S. serial No. 12/380,781 filed March 2, 2009, entitled "Open Transaction Central Billing System," U.S. serial No. 12/380,774 filed March 2, 2009, entitled "Verifiable and Accurate Service Usage Monitoring for Intermediate Networking Devices," U.S. serial No. 12/380,771 filed March 2, 2009, entitled "Verifiable Service Billing for Intermediate Networking Devices" (issued as U.S. Patent No. 8,023,425 on September 20, 2011), U.S. serial No. 12/380,773 filed March 2, 2009, entitled "Verifiable Service Policy Implementation for Intermediate Networking Devices," U.S. serial No. 12/380,777 filed March 2, 2009, entitled "Simplified Service Network Architecture," U.S. serial No. 12/695,019 filed January 27, 2010, entitled "Device Assisted CDR Creation, Aggregation, Mediation, and Billing," U.S. serial No. 12/695,020 filed January 27, 2010, entitled "Adaptive Ambient Services," U.S. serial No. 12/694,445 filed January 27, 2010, entitled "Security Techniques for Device Assisted Services," U.S. serial No. 12/694,451 filed January 27, 2010, entitled "Device Group Partitions and Settlement Platform," U.S. serial No. 12/694,455 filed January 27, 2010, entitled "Device Assisted Services Install," U.S. serial No. 12/695,021 filed January 27, 2010, entitled "Quality of

Service for Device Assisted Services," U.S. serial No. 12/695,980 filed January 28, 2010, entitled "Enhanced Roaming Services and Converged Carrier Networks with Device Assisted Services and a Proxy" claim priority to U.S. provisional serial No. 61/206,354 filed January 28, 2009, entitled "Services Policy Communication System and Method." The following applications, U.S. serial No. 12/380,759 filed March 2, 2009, entitled "Verifiable Device Assisted Service Policy Implementation," U.S. serial No. 12/380,779 filed March 2, 2009, entitled "Device Assisted Service Profile Management with User Preference, Adaptive Policy, Network Neutrality, and User Privacy," U.S. serial No. 12/380,758 filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Monitoring with Reporting, Synchronization, and Notification," U.S. serial No. 12/380,778 filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Billing with Integrated Accounting, Mediation Accounting, and Multi-Account," U.S. serial No. 12/380,768 filed March 2, 2009, entitled "Network Based Service Policy Implementation with Network Neutrality and User Privacy," U.S. serial No. 12/380,767 filed March 2, 2009, entitled "Network Based Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy," U.S. serial No. 12/380,780 filed March 2, 2009, entitled "Automated Device Provisioning and Activation," U.S. serial No. 12/380,755 filed March 2, 2009, entitled "Device Assisted Ambient Services," U.S. serial No. 12/380,756 filed March 2, 2009, entitled "Network Based Ambient Services," U.S. serial No. 12/380,770 filed March 2, 2009, entitled "Network Tools for Analysis, Design, Testing, and Production of Services," U.S. serial No. 12/380,772 filed March 2, 2009, entitled "Roaming Services Network and Overlay Networks," U.S. serial No. 12/380,782 filed March 2, 2009, entitled "Open Development System for Access Service Providers," U.S. serial No. 12/380,783 filed March 2, 2009, entitled "Virtual Service Provider Systems," U.S. serial No. 12/380,757 filed March 2, 2009, entitled "Service Activation Tracking System," U.S. serial No. 12/380,781 filed March 2, 2009, entitled "Open Transaction Central Billing System," U.S. serial No. 12/380,774 filed March 2, 2009, entitled "Verifiable and Accurate Service Usage Monitoring for Intermediate Networking Devices," U.S. serial No. 12/380,771 filed March 2, 2009, entitled "Verifiable Service Billing for Intermediate Networking Devices" (issued as U.S. Patent No. 8,023,425 on September 20, 2011), U.S. serial No. 12/380,773 filed March 2, 2009, entitled "Verifiable Service Policy Implementation for Intermediate Networking Devices," U.S. serial No. 12/380,777 filed March 2, 2009, entitled "Simplified Service Network Architecture," U.S. serial

No. 12/695,019 filed January 27, 2010, entitled "Device Assisted CDR Creation, Aggregation, Mediation, and Billing," U.S. serial No. 12/695,020 filed January 27, 2010, entitled "Adaptive Ambient Services," U.S. serial No. 12/694,445 filed January 27, 2010, entitled "Security Techniques for Device Assisted Services," U.S. serial No. 12/694,451 filed January 27, 2010, entitled "Device Group Partitions and Settlement Platform," U.S. serial No. 12/694,455 filed January 27, 2010, entitled "Device Assisted Services Install," U.S. serial No. 12/695,021 filed January 27, 2010, entitled "Quality of Service for Device Assisted Services," U.S. serial No. 12/695,980 filed January 28, 2010, entitled "Enhanced Roaming Services and Converged Carrier Networks with Device Assisted Services and a Proxy" claim priority to U.S. provisional serial No. 61/206,944 filed February 4, 2009, entitled "Services Policy Communication System and Method." The following applications, U.S. serial No. 12/380,759 filed March 2, 2009, entitled "Verifiable Device Assisted Service Policy Implementation," U.S. serial No. 12/380,779 filed March 2, 2009, entitled "Device Assisted Service Profile Management with User Preference, Adaptive Policy, Network Neutrality, and User Privacy," U.S. serial No. 12/380,758 filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Monitoring with Reporting, Synchronization, and Notification," U.S. serial No. 12/380,778 filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Billing with Integrated Accounting, Mediation Accounting, and Multi-Account," U.S. serial No. 12/380,768 filed March 2, 2009, entitled "Network Based Service Policy Implementation with Network Neutrality and User Privacy," U.S. serial No. 12/380,767 filed March 2, 2009, entitled "Network Based Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy," U.S. serial No. 12/380,780 filed March 2, 2009, entitled "Automated Device Provisioning and Activation," U.S. serial No. 12/380,755 filed March 2, 2009, entitled "Device Assisted Ambient Services," U.S. serial No. 12/380,756 filed March 2, 2009, entitled "Network Based Ambient Services," U.S. serial No. 12/380,770 filed March 2, 2009, entitled "Network Tools for Analysis, Design, Testing, and Production of Services," U.S. serial No. 12/380,772 filed March 2, 2009, entitled "Roaming Services Network and Overlay Networks," U.S. serial No. 12/380,782 filed March 2, 2009, entitled "Open Development System for Access Service Providers," U.S. serial No. 12/380,783 filed March 2, 2009, entitled "Virtual Service Provider Systems," U.S. serial No. 12/380,757 filed March 2, 2009, entitled "Service Activation Tracking System," U.S. serial No. 12/380,781 filed March 2, 2009, entitled "Open Transaction Central Billing System," U.S. serial

No. 12/380,774 filed March 2, 2009, entitled "Verifiable and Accurate Service Usage Monitoring for Intermediate Networking Devices," U.S. serial No. 12/380,771 filed March 2, 2009, entitled "Verifiable Service Billing for Intermediate Networking Devices" (issued as U.S. Patent No. 8,023,425 on September 20, 2011), U.S. serial No. 12/380,773 filed March 2, 2009, entitled "Verifiable Service Policy Implementation for Intermediate Networking Devices," U.S. serial No. 12/380,777 filed March 2, 2009, entitled "Simplified Service Network Architecture," U.S. serial No. 12/695,019 filed January 27, 2010, entitled "Device Assisted CDR Creation, Aggregation, Mediation, and Billing," U.S. serial No. 12/695,020 filed January 27, 2010, entitled "Adaptive Ambient Services," U.S. serial No. 12/694,445 filed January 27, 2010, entitled "Security Techniques for Device Assisted Services," U.S. serial No. 12/694,451 filed January 27, 2010, entitled "Device Group Partitions and Settlement Platform," U.S. serial No. 12/694,455 filed January 27, 2010, entitled "Device Assisted Services Install," U.S. serial No. 12/695,021 filed January 27, 2010, entitled "Quality of Service for Device Assisted Services," U.S. serial No. 12/695,980 filed January 28, 2010, entitled "Enhanced Roaming Services and Converged Carrier Networks with Device Assisted Services and a Proxy," claim priority to U.S. provisional serial No. 61/207,393 filed February 10, 2009, entitled "Services Policy Communication System and Method." The following applications, U.S. serial No. 12/380,759 filed March 2, 2009, entitled "Verifiable Device Assisted Service Policy Implementation," U.S. serial No. 12/380,779 filed March 2, 2009, entitled "Device Assisted Service Profile Management with User Preference, Adaptive Policy, Network Neutrality, and User Privacy," U.S. serial No. 12/380,758 filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Monitoring with Reporting, Synchronization, and Notification," U.S. serial No. 12/380,778 filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Billing with Integrated Accounting, Mediation Accounting, and Multi-Account," U.S. serial No. 12/380,768 filed March 2, 2009, entitled "Network Based Service Policy Implementation with Network Neutrality and User Privacy," U.S. serial No. 12/380,767 filed March 2, 2009, entitled "Network Based Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy," U.S. serial No. 12/380,780 filed March 2, 2009, entitled "Automated Device Provisioning and Activation," U.S. serial No. 12/380,755 filed March 2, 2009, entitled "Device Assisted Ambient Services," U.S. serial No. 12/380,756 filed March 2, 2009, entitled "Network Based Ambient Services," U.S. serial No. 12/380,770 filed March 2, 2009, entitled "Network

Tools for Analysis, Design, Testing, and Production of Services," U.S. serial No. 12/380,772 filed March 2, 2009, entitled "Roaming Services Network and Overlay Networks," U.S. serial No. 12/380,782 filed March 2, 2009, entitled "Open Development System for Access Service Providers," U.S. serial No. 12/380,783 filed March 2, 2009, entitled "Virtual Service Provider Systems," U.S. serial No. 12/380,757 filed March 2, 2009, entitled "Service Activation Tracking System," U.S. serial No. 12/380,781 filed March 2, 2009, entitled "Open Transaction Central Billing System," U.S. serial No. 12/380,774 filed March 2, 2009, entitled "Verifiable and Accurate Service Usage Monitoring for Intermediate Networking Devices," U.S. serial No. 12/380,771 filed March 2, 2009, entitled "Verifiable Service Billing for Intermediate Networking Devices" (issued as U.S. Patent No. 8,023,425 on September 20, 2011), U.S. serial No. 12/380,773 filed March 2, 2009, entitled "Verifiable Service Policy Implementation for Intermediate Networking Devices," U.S. serial No. 12/380,777 filed March 2, 2009, entitled "Simplified Service Network Architecture," U.S. serial No. 12/695,019 filed January 27, 2010, entitled "Device Assisted CDR Creation, Aggregation, Mediation, and Billing," U.S. serial No. 12/695,020 filed January 27, 2010, entitled "Adaptive Ambient Services," U.S. serial No. 12/694,445 filed January 27, 2010, entitled "Security Techniques for Device Assisted Services," U.S. serial No. 12/694,451 filed January 27, 2010, entitled "Device Group Partitions and Settlement Platform," U.S. serial No. 12/694,455 filed January 27, 2010, entitled "Device Assisted Services Install," U.S. serial No. 12/695,021 filed January 27, 2010, entitled "Quality of Service for Device Assisted Services," U.S. serial No. 12/695,980 filed January 28, 2010, entitled "Enhanced Roaming Services and Converged Carrier Networks with Device Assisted Services and a Proxy," claim priority to U.S. provisional serial No. 61/207,739 filed February 13, 2009, entitled "Services Policy Communication System and Method." The following applications, U.S. serial No. 12/695,019 filed January 27, 2010, entitled "Device Assisted CDR Creation, Aggregation, Mediation, and Billing," U.S. serial No. 12/694,451 filed January 27, 2010, entitled "Device Group Partitions and Settlement Platform," U.S. serial No. 12/695,980 filed January 28, 2010, entitled "Enhanced Roaming Services and Converged Carrier Networks with Device Assisted Services and a Proxy," claim priority to U.S. provisional serial No. 61/270,353 filed July 6, 2009, entitled "Device Assisted CDR Creation, Aggregation, Mediation and Billing." The following application, U.S. serial No. 12/695,020 filed January 27, 2010, entitled "Adaptive Ambient Services," claims priority to U.S. provisional serial No. 61/275,208

filed August 25, 2009, entitled "Adaptive Ambient Services." The following application, U.S. serial No. 12/695,020 filed January 27, 2010, entitled "Adaptive Ambient Services," claims priority to U.S. provisional serial No. 61/237,753 filed August 28, 2009, entitled "Adaptive Ambient Services." The following applications, U.S. serial No. 12/694,445 filed January 27, 2010, entitled "Security Techniques for Device Assisted Services," U.S. serial No. 12/695,021 filed January 27, 2010, entitled "Quality of Service for Device Assisted Services" claim priority to U.S. provisional serial No. 61/252,151 filed October 15, 2009, entitled "Security Techniques for Device Assisted Services." The following applications, U.S. serial No. 12/694,451 filed January 27, 2010, entitled "Device Group Partitions and Settlement Platform," U.S. serial No. 12/695,021 filed January 27, 2010, entitled "Quality of Service for Device Assisted Services" claim priority to U.S. provisional serial No. 61/252,153 filed October 15, 2009, entitled "Device Group Partitions and Settlement Platform." The following application, U.S. serial No. 12/694,455 filed January 27, 2010, entitled "Device Assisted Services Install" claims priority to U.S. provisional serial No. 61/264,120 filed November 24, 2009, entitled "Device Assisted Services Install." The following application, U.S. serial No. 12/695,019 filed January 27, 2010, entitled "Device Assisted CDR Creation, Aggregation, Mediation, and Billing" claims priority to U.S. provisional serial No. 61/264,126 filed November 24, 2009, entitled "Device Assisted Services Activity Map." The following applications, U.S. serial No. 13/134,028 filed May 25, 2011, entitled "Device-Assisted Services for Protecting Network Capacity" and U.S. serial No. 13/134,005 filed May 25, 2011, entitled "System and Method for Wireless Network Offloading" claim priority to U.S. provisional serial No. 61/348,022 filed May 25, 2010, entitled "Device Assisted Services for Protecting Network Capacity." The following application, U.S. serial No. 13,229,580 filed September 9, 2011 entitled "Wireless Network Service Interfaces" claims priority to U.S. provisional serial No. 61/381,159 filed September 9, 2010, entitled "Device Assisted Services for Protecting Network Capacity." The following application, U.S. serial No. 13,229,580 filed September 9, 2011 entitled "Wireless Network Service Interfaces" claims priority to U.S. provisional serial No. 61/381,162 filed September 9, 2010, entitled "Service Controller Interfaces and Workflows."

[0003] All of the above patents and applications are hereby incorporated by reference. --

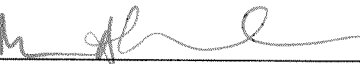
REMARKS

Applicants respectfully request entry of the preliminary amendment set forth in this paper.
Paragraphs [0001] through [0003] of the specification are being replaced herein.

The undersigned authorizes any fees which may be required, or credit any overpayment to
Deposit Account No. 50-4561. Should the Examiner have any questions or need any additional
information regarding this communication, the Examiner is invited to contact the undersigned at
the telephone number shown below.

Respectfully submitted,

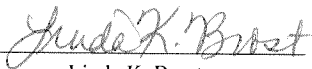
Date: December 13, 2011

By: 
Marc A. Sockol
Reg. No. 40,823
Customer Number 69849
Sheppard Mullin Richter & Hampton LLP
379 Lytton Avenue
Palo Alto, CA 94301-1432
Telephone: (650) 815-2600

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being
attached or enclosed) is being filed electronically via EFS-Web
addressed to the Commissioner for Patents on:

Date: December 13, 2011

By: 

Linda K. Brost

Electronic Acknowledgement Receipt

EFS ID:	11608982
Application Number:	13237827
International Application Number:	
Confirmation Number:	1814
Title of Invention:	Adapting Network Policies Based on Device Service Processor Configuration
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	69849
Filer:	Marc A. Sockol/Linda Brost
Filer Authorized By:	Marc A. Sockol
Attorney Docket Number:	26WV-160511 [RALEP034]
Receipt Date:	13-DEC-2011
Filing Date:	20-SEP-2011
Time Stamp:	19:42:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		160511-RALEP034-PrelimAmendNotofChgofEntity Status121311.pdf	276048 8cb8ce23450c3912996b50bdda0d437e924b1ea0	yes	13

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Transmittal Letter	1	1
	Miscellaneous Incoming Letter	2	2
	Preliminary Amendment	3	12
	Applicant Arguments/Remarks Made in an Amendment	13	13

Warnings:

Information:

Total Files Size (in bytes):	276048
-------------------------------------	--------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM <i>(to be used for all correspondence after initial filing)</i>		Application Number	13/237,827
		Filing Date	September 20, 2011
		First Named Inventor	Gregory G. Raleigh, et al.
		Art Unit	2447 Conf. No. 1814
		Examiner Name	Not Yet Assigned
Total Number of Pages in This Submission	13	Attorney Docket Number	26WV-160511 [RALEP034]

ENCLOSURES (Check all that apply)		
☐ Fee Transmittal Form ☐ Fee Attached ☒ Preliminary Amendment (11 pgs.) ☐ After Final ☐ Affidavits/declaration(s) ☐ Extension of Time Request ☐ Express Abandonment Request ☐ Information Disclosure Statement with PTO/SB/08a/b ☐ Certified Copy of Priority Document(s) ☐ Reply to Missing Parts/Incomplete Application ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53	☐ Drawing(s) ☐ Licensing-related Papers ☐ Petition ☐ Petition to Convert to a Provisional Application ☐ Power of Atty. to Prosecute Applications [PTO/SB/80] (1 pg.) ☐ Terminal Disclaimer ☐ Request for Refund ☐ CD, Number of CD(s) _____ ☐ Landscape Table on CD	☐ After Allowance Communication to TC ☐ Appeal Communication to Board of Appeals and Interferences ☐ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) ☐ Proprietary Information ☐ Status Letter ☒ Other Enclosure(s) (please identify below): Notice of Change of Entity Status from Large to Small (1 pg.)
Remarks You are hereby authorized to charge any additional fee required or credit any overpayment to Deposit Account No. 50-4561.		
SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT		
Firm Name	Sheppard, Mullin, Richter & Hampton LLP	
Signature		
Printed name	Marc A. Sockol	
Date	December 13, 2011	Reg. No. 40,823

CERTIFICATE OF ELECTRONIC TRANSMISSION			
I hereby certify that this correspondence is being filed electronically via EFS-Web addressed to the Commissioner for Patents on the date shown below:			
Signature			
Typed or printed name	Linda K. Brost	Date	December 13, 2011

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Examiner:

Gregory G. Raleigh, et al.

Not Yet Assigned

Serial No. 13/237,827

Art Unit: 2447

Filed: September 20, 2011

Conf. No.: 1814

Title: Adapting Network Policies Based on Device Service Processor Configuration

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

NOTICE OF CHANGE OF ENTITY STATUS FROM LARGE TO SMALL

Dear Sir:

The Applicant herein is now entitled to claim small entity status for the above-referenced patent application, and shall henceforth pay fees due at the small entity rate.

Please change your records to reflect this change in entity status.

No fee should be required for this change of entity status, but if such fee is determined to be owed, please charge Deposit Account No. 50-4561 for the same.

Respectfully submitted,

Date: December 13, 2011

By: 

Marc A. Sockol
Reg. No. 40,823
Customer Number 69849
Sheppard Mullin Richter & Hampton LLP
379 Lytton Avenue
Palo Alto, CA 94301-1432

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 13/237,827		Filing Date 09/20/2011		☐ To be Mailed		
APPLICATION AS FILED – PART I											
(Column 1)			(Column 2)			SMALL ENTITY ☒ OR		OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR		RATE (\$)	FEE (\$)			
☒ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	82			N/A				
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A				N/A				
☒ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	110			N/A				
TOTAL CLAIMS (37 CFR 1.16(j))	minus 20 =	*	X \$ =				X \$ =				
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$ =				X \$ =				
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))			If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).								
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))											
			TOTAL	192			TOTAL				
APPLICATION AS AMENDED – PART II											
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY			
AMENDMENT	12/13/2011	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR		RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 31	Minus	** 31	= 0	X \$30 =			0	X \$ =	
	Independent (37 CFR 1.16(h))	* 5	Minus	***5	= 0	X \$125 =			0	X \$ =	
	☐ Application Size Fee (37 CFR 1.16(s))										
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
					TOTAL ADD'L FEE	0			TOTAL ADD'L FEE		
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY			
AMENDMENT	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR		RATE (\$)	ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(i))	*	Minus	**	=			X \$ =		X \$ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=			X \$ =		X \$ =	
	☐ Application Size Fee (37 CFR 1.16(s))										
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
					TOTAL ADD'L FEE				TOTAL ADD'L FEE		
<p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.</p>											

Legal Instrument Examiner:
/ANGELA JONES/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Examiner:

Gregory G. Raleigh, et al.

Not Yet Assigned

Serial No. 13/237,827

Art Unit: 2447

Filed: September 20, 2011

Conf. No.: 1814

Title: Adapting Network Policies Based on Device Service Processor Configuration

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO NOTICE TO FILE MISSING PARTS UNDER 37 C.F.R. 1.53(b)

Dear Sir:

In response to the Notice to File Missing Parts of Application mailed on October 3, 2011, in the above-identified application, enclosed herewith are the missing parts needed to complete filing of the above-identified patent application. The signed declaration for patent application is enclosed herewith under 37 C.F.R. §§1.27 and 1.16(e).

☒ Small entity status is proper for the assignee under 37 C.F.R. §§1.9 and 1.27.

The fees associated with the filing of this response are shown below:

	Fees
Missing Parts Surcharge (small entity)	\$ 65.00
☒ Extension of Time Fee – 1 Month (small entity)	\$ 75.00
TOTAL FEE ENCLOSED (small entity) -	= \$140.00

- ☐ No additional fee is required for this _____.
- ☒ Please charge Deposit Account No. 50-4561 in the amount of \$140.00.
- ☒ The Commissioner is hereby authorized to charge any additional fees and credit any overpayments to Deposit Account No. 50-4561.
- ☒ Charge any patent application processing fees under 37 C.F.R. 1.17.

Respectfully submitted,

Date: January 3, 2012

By: _____



Marc A. Sockol
Reg. No. 40,823
Customer Number 69849
Sheppard Mullin Richter & Hampton LLP
379 Lytton Avenue
Palo Alto, CA 94301-1432
(650) 815-2600

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

**DECLARATION FOR UTILITY OR
DESIGN
PATENT APPLICATION
(37 CFR 1.63)**Declaration
Submitted
With Initial
Filing

OR

Declaration
Submitted after Initial
Filing (surcharge
(37 CFR 1.16 (f))
required)

Attorney Docket Number	26WV-160511 [RALEP034]
First Named Inventor	Gregory G. Raleigh, et al.
COMPLETE IF KNOWN	
Application Number	13/237,827
Filing Date	September 20, 2011
Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned

I hereby declare that: (1) Each inventor's residence, mailing address, and citizenship are as stated below next to their name; and (2) I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Adapting Network Policies Based on Device Service Processor Configuration

(Title of the Invention)

the application of which



is attached hereto

OR

was filed on (MM/DD/YYYY) 09/20/2011 as United States Application Number or PCT InternationalApplication Number 13/237,827 and was amended on (MM/DD/YYYY) _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

Authorization To Permit Access To Application by Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the above-identified patent application is filed access to the above-identified patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the above-identified patent application is filed to have access to the above-identified patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the above-identified patent application with respect to: 1) the above-identified patent application-as-filed; 2) any foreign application to which the above-identified patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the above-identified patent application; and 3) any U.S. application-as-filed from which benefit is sought in the above-identified patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing the Authorization to Permit Access to Application by Participating Offices.

[Page 1 of 4]

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance completing the form, call 1-800-PTO-9199 and select option 2.

W02-WEST:1LKB1404072195.1

DECLARATION — Utility or Design Patent Application

Claim of Foreign Priority Benefits

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 2 of 4]

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent ApplicationDirect all
correspondence to:The address
associated with
Customer Number:

69849

OR

Correspondence
address below

Name

Address

City

State

Zip

Country

Telephone

Email

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available. Petitioner/applicant is advised that documents which form the record of a patent application (such as the PTO/SB/01) are placed into the Privacy Act system of records DEPARTMENT OF COMMERCE, COMMERCE-PAT-7, System name: *Patent Application Files*. Documents not retained in an application file (such as the PTO-2038) are placed into the Privacy Act system of COMMERCE/PAT-TM-10, System name: *Deposit Accounts and Electronic Funds Transfer Profiles*.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR:

A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])

Family Name or Surname

Gregory G.

Raleigh

Inventor's Signature

Date

12/12/11

Residence: City

State

Country

Citizenship

Woodside

California

U.S.

U.S.

Mailing Address

131 Fox Hollow Road

City

State

Zip

Country

Woodside

California

94062

U.S.

Additional inventors or a legal representative are being named on the 1 supplemental sheet(s) PTO/SB/02A or 02LR attached hereto

[Page 3 of 4]

W02-WEST:1LKB1404072195.1

DECLARATION	ADDITIONAL INVENTOR(S) Supplemental Sheet Page <u>4</u> of <u>4</u>
--------------------	--

Name of Additional Joint Inventor, if any:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any))		Family Name or Surname	
James		Lavine	
Inventor's Signature 		Date <u>12/8/11</u>	
Residence: City	State	U.S. Country	U.S. Citizenship
8 Heavenly Way			
Mailing Address			
Mill Valley City	California State	94941 Zip	U.S. Country
Name of Additional Joint Inventor, if any:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any))		Family Name or Surname	
Inventor's Signature		Date	
Residence: City	State	Country	Citizenship
Mailing Address			
City	State	Zip	Country
Name of Additional Joint Inventor, if any:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any))		Family Name or Surname	
Inventor's Signature		Date	
Residence: City	State	Country	Citizenship
Mailing Address			
City	State	Zip	Country

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	13237827			
Filing Date:	20-Sep-2011			
Title of Invention:	Adapting Network Policies Based on Device Service Processor Configuration			
First Named Inventor/Applicant Name:	Gregory G. Raleigh			
Filer:	Marc A. Sockol/Linda Brost			
Attorney Docket Number:	26WV-160511 [RALEP034]			
Filed as Small Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Late filing fee for oath or declaration	2051	1	65	65
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:	Page 208 of 2483			

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension - 1 month with \$0 paid	2251	1	75	75
Miscellaneous:				
Total in USD (\$)				140

Electronic Acknowledgement Receipt

EFS ID:	11751975
Application Number:	13237827
International Application Number:	
Confirmation Number:	1814
Title of Invention:	Adapting Network Policies Based on Device Service Processor Configuration
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	69849
Filer:	Marc A. Sockol/Linda Brost
Filer Authorized By:	Marc A. Sockol
Attorney Docket Number:	26WV-160511 [RALEP034]
Receipt Date:	03-JAN-2012
Filing Date:	20-SEP-2011
Time Stamp:	21:05:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 140
RAM confirmation Number	8092
Deposit Account	504561
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		160511-RALEP034-MPResponse010312.pdf	242015 517985ab938cb6af50f6285c6482d82a35e d3d15	yes	7

Multipart Description/PDF files in .zip description

Document Description	Start	End
Transmittal Letter	1	1
Applicant Response to Pre-Exam Formalities Notice	2	3
Oath or Declaration filed	4	7

Warnings:**Information:**

2	Fee Worksheet (SB06)	fee-info.pdf	32301 bcbfda8ebf6ae78f96158cdbe9e46794c3a6c ade3	no	2
---	----------------------	--------------	--	----	---

Warnings:**Information:**

Total Files Size (in bytes):	274316
-------------------------------------	--------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM (to be used for all correspondence after initial filing)		Application Number	13/237,827
		Filing Date	September 20, 2011
		First Named Inventor	Gregory G. Raleigh, et al.
		Art Unit	2447 Conf. No. 1814
		Examiner Name	Not Yet Assigned
Total Number of Pages in This Submission	7	Attorney Docket Number	26WV-160511 [RALEP034]

ENCLOSURES (Check all that apply)		
☐ Fee Transmittal Form ☐ Fee Attached ☐ Preliminary Amendment ☐ After Final ☐ Affidavits/declaration(s) ☐ Extension of Time Request ☐ Express Abandonment Request ☐ Information Disclosure Statement with PTO/SB/08a/b ☐ Certified Copy of Priority Document(s) ☐ Reply to Missing Parts/Incomplete Application ☒ Reply to Missing Parts under 37 CFR 1.52 or 1.53 (2 pgs.)	☐ Drawing(s) ☐ Licensing-related Papers ☐ Petition ☐ Petition to Convert to a Provisional Application ☐ Power of Atty. to Prosecute Applications [PTO/SB/80] (1 pg.) ☐ Terminal Disclaimer ☐ Request for Refund ☐ CD, Number of CD(s) _____ ☐ Landscape Table on CD	☐ After Allowance Communication to TC ☐ Appeal Communication to Board of Appeals and Interferences ☐ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) ☐ Proprietary Information ☐ Status Letter ☒ Other Enclosure(s) (please identify below): Declaration for Utility Patent Application (4 pgs.)
Remarks You are hereby authorized to charge any additional fee required or credit any overpayment to Deposit Account No. 50-4561.		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT			
Firm Name	Sheppard, Mullin, Richter & Hampton LLP		Customer No. 69849
Signature			
Printed name	Marc A. Sockol		
Date	January 3, 2012	Reg. No.	40,823

CERTIFICATE OF ELECTRONIC TRANSMISSION			
I hereby certify that this correspondence is being filed electronically via EFS-Web addressed to the Commissioner for Patents on the date shown below:			
Signature			
Typed or printed name	Linda K. Brost	Date	January 3, 2012

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/237,827	
APPLICATION AS FILED - PART I							
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	95		N/A	
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	310		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	125		N/A	
TOTAL CLAIMS (37 CFR 1.16(j))	31 minus 20 =	*	x 30 =	330	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	5 minus 3 =	*	x 125 =	250			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			155			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
			TOTAL	1265		TOTAL	
* If the difference in column 1 is less than zero, enter "0" in column 2.							
APPLICATION AS AMENDED - PART II							
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	x =	OR	x =
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =	OR	x =
	Application Size Fee (37 CFR 1.16(s))					OR	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR	
			TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	x =	OR	x =
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =	OR	x =
	Application Size Fee (37 CFR 1.16(s))					OR	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR	
			TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.							



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
13/237,827	09/20/2011	2447	1168	26WV-160511 [RALEP034]	31	5

CONFIRMATION NO. 1814

UPDATED FILING RECEIPT

69849

SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
379 Lytton Avenue
Palo Alto, CA 94301



OC000000051927716

Date Mailed: 01/11/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Gregory G. Raleigh, Woodside, CA;
James Lavine, Mill Valley, CA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CIP of 12/380,759 03/02/2009
and is a CIP of 12/380,758 03/02/2009
and is a CIP of 12/380,768 03/02/2009
and is a CIP of 12/380,767 03/02/2009
and is a CIP of 12/380,780 03/02/2009
and said 12/380,758 03/02/2009
is a CIP of 12/380,755 03/02/2009
This application 13/237,827
is a CIP of 12/380,756 03/02/2009
and is a CIP of 12/380,770 03/02/2009
and said 12/380,755 03/02/2009
is a CIP of 12/380,771 03/02/2009 PAT 8023425
and is a CIP of 12/380,772 03/02/2009
and said 12/380,756 03/02/2009
is a CIP of 12/380,783 03/02/2009
and said 12/380,772 03/02/2009
is a CIP of 12/380,757 03/02/2009
and is a CIP of 12/380,781 03/02/2009
and is a CIP of 12/380,774 03/02/2009
and is a CIP of 12/380,773 03/02/2009

and is a CIP of 12/380,769 03/02/2009
and is a CIP of 12/380,777 03/02/2009

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.)

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 09/29/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/237,827**

Projected Publication Date: 04/19/2012

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Adapting Network Policies Based on Device Service Processor Configuration

Preliminary Class

709

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:



Practitioners associated with the Customer Number:

69849

OR



Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:



The address associated with Customer Number:

69849

OR

☐ Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone			Email

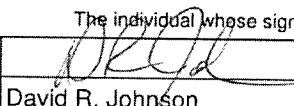
Assignee Name and Address:

Headwater Partners I, LLC
350 Marine Parkway, Suite 300
Redwood City, California 94065
U.S.A.

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date: 18 MARCH, 2011
Name	David R. Johnson	Telephone: 650-517-2782
Title	Chief Financial Officer	

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Examiner:

Gregory G. Raleigh, et al.

Not Yet Assigned

Serial No.: 13/237,827

Art Unit: 3627

Filed: September 20, 2011

Conf. No.: 1814

Title: Adapting Network Policies Based on Device Service Processor Configuration

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**INFORMATION DISCLOSURE STATEMENT PURSUANT TO
37 C.F.R. §§1.97(b)**

Sir:

In accordance with the duty of disclosure under 37 CFR §1.56 and pursuant to 37 CFR §§1.97-1.98, Applicant hereby notifies the U.S. Patent and Trademark Office of the references listed on the enclosed Form PTO-SB/08A. Pursuant to the USPTO's waiver of the requirements under 37 CFR 1.98(a)(2)(i) for submitting a copy of each cited U.S. patent, we are not submitting copies of U.S. patents and/or patent publications cited.

The present Information Disclosure Statement is being filed more than three months after the filing date but before receiving the first Office Action. Accordingly, no fee or certification is needed.

The submission of the listed documents is not intended as an admission that any such document constitutes prior art against the claims of the present application. Applicant reserves the right to dispute any of the listed documents as prior art during examination. Furthermore, Applicant does not waive any right to take any action that would be appropriate to antedate or otherwise remove any listed document as a competent reference against the claims of the

present application. The submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made or that no other material information may exist.

The Examiner is requested to initial the enclosed Form PTO/SB/08A and return a copy thereof to the undersigned.

No fee is believed to be due relative to this submission, but if for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. 50-4561.

Respectfully submitted,

Date: April 12, 2012

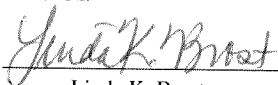
By: 

Marc A. Sockol, Reg. No. 40,823
Attorney for Applicants
Customer Number 69849
Sheppard, Mullin, Richter & Hampton LLP
379 Lytton Avenue
Palo Alto, CA 94301-1432
Telephone: (650) 815-2600

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: April 12, 2012

By: 

Linda K. Brost

Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet 1 of 17

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		5,577,100	11-19-1996	McGREGOR et al	
		5,892,900	04-06-1999	GINTER et al	
		5,940,472	08-17-1999	NEWMAN et al	
		6,047,268	04-04-2000	BARTOLI et al	
		6,078,953	06-20-2000	VAID et al	
		6,098,878	08-08-2000	DENT et al	
		6,141,686	10-31-2000	JACKOWSKI et al	
		6,148,336	11-14-2000	THOMAS et al	
		6,198,915	03-06-2001	McGREGOR et al	
		6,263,055	07-17-2001	GARLAND et al	
		6,449,479	09-10-2002	SANCHEZ, Eduardo	
		6,532,235	03-11-2003	BENSON et al	
		6,532,579	03-11-2003	SATO et al	
		6,539,082	03-25-2003	LOWE et al	
		6,563,806	05-13-2003	YANO et al	
		6,574,321	06-03-2003	COX et al	
		6,603,969	08-05-2003	VUORISTO et al.	
		6,639,975	10-28-2003	O'NEAL et al	
		6,650,887	11-18-2003	McGREGOR et al	
		6,651,101	11-18-2003	GAI et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				
	F01	EP 1463238 A1	09-29-2004	Alcatel		
	F02	EP 1739518 A1	01-03-2007	Research In Motion Limited		
	F03	EP 1772988 A1	04-11-2007	Huawei Technologies Co., LTD.		

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet

2

of

17

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		6,658,254	12-02-2003	PURDY et al.	
		6,684,244	01-27-2004	GOLDMAN et al	
		6,725,031	04-20-2004	WATLER et al	
		6,785,889	08-31-2004	WILLIAMS, Peter	
		6,829,696	12-07-2004	BALMER et al	
		6,920,455	07-19-2005	WESCHLER, Paul	
		6,952,428	10-04-2005	NECKA et al	
		6,965,667	11-15-2005	TRABANDT et al	
		6,996,076	02-07-2006	FORBES et al	
		6,998,985	02-14-2006	REISMAN et al	
		7,027,408	04-11-2006	NABKEL, et al.	
		7,042,988	05-09-2006	JUITT et al	
		7,058,968	06-06-2006	ROWLAND et al	
		7,092,696	08-15-2006	HOSAIN et al	
		7,142,876	11-28-2006	TROSSEN et al	
		7,158,792	01-02-2007	COOK et al	
		7,174,174	02-06-2007	BORIS et al	
		7,180,855	02-20-2007	LIN	
		7,197,321	03-27-2007	ERSKINE et al	
		7,242,920	04-10-2007	MORRIS, Robert P.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				
	F04	EP 1978772 A1	10-08-2008	British Telecomm. Public Ltd. Co.		
	F05	WO 1999/065185 A3	12-16-1999	British Telecomm. Public Ltd. Co.		
	F06	WO 2003/014891 A2	02-20-2003	The Boeing Company		

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet

3

of

17

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		7,245,901	07-17-2007	McGREGOR et al	
		7,280,816	10-09-2007	FRATTI et al	
		7,280,818	10-09-2007	CLAYTON, Steve	
		7,289,489	10-30-2007	KUNG et al	
		7,290,283	10-30-2007	COPELAND III, John A.	
		7,317,699	01-08-2008	GODFREY et al	
		7,322,044	01-22-2008	HRASTAR, Scott E.	
		7,324,447	01-29-2008	MORFORD	
		7,325,037	01-29-2008	LAWSON, Karen L.	
		7,349,695	03-25-2008	OOMMEN et al	
		7,353,533	04-01-2008	WRIGHT et al	
		7,356,337	04-08-2008	FLORENCE	
		7,373,136	05-13-2008	WATLER et al	
		7,401,338	07-15-2008	BOWEN et al	
		7,403,763	07-22-2008	MAES, Stephane H.	
		7,418,253	08-26-2008	KAVANAHA, Alan	
		7,421,004	09-02-2008	FEHER, Kamilo	
		7,450,591	11-11-2008	KORLING, et al.	
		7,486,185	02-03-2009	CULPEPPER et al	
		7,516,219	04-07-2009	MOGHADDAM et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				
	F07	WO 2003/058880 A1	07-17-2003	Telia AB		
	F08	WO 2004/028070 A1	04-01-2004	Credant Technologies, Inc.		
	F09	WO 2004/077797 A2	09-10-2004	Boston Comm. Group, Inc.		

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet

4

of

17

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		7,574,731	08-11-2009	FASCENDA, Anthony C.	
		7,580,857	08-25-2009	VanFLEET, et al.	
		7,617,516	11-10-2009	HUSLAK, et al.	
		7,620,065	11-17-2009	FALARDEAU, Eric	
		7,620,162	11-17-2009	AARON et al	
		7,647,047	01-12-2010	MOGHADDAM et al	
		7,668,903	02-23-2010	EDWARDS, et al.	
		7,720,505	05-18-2010	GOPI, et al.	
		7,747,240	06-29-2010	BRISCOE et al	
		7,797,204	09-14-2010	BALENT, Bruce F.	
		7,848,768	12-07-2010	OMORI, et al.	
		7,868,778	01-11-2011	KENWRIGHT, David Norris	
		7,873,705	01-18-2011	KALISH, Dan	
		7,882,029	02-01-2011	WHITE, Craig R.	
		7,929,960	04-19-2011	MARTIN et al	
		7,937,069	05-03-2011	RASSAM, Frederic	
		7,941,184	05-10-2011	PRENDERGAST et al	
		7,957,511	06-07-2011	DRUDIS et al	
		7,975,184	07-05-2011	GOFF et al	
		7,986,935	07-26-2011	D'SOUZA et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				
	F10	WO 2004/095753 A2	11-04-2004	Motorola Inc.		
	F11	WO 2006/004467 A1	01-12-2006	Telefonaktiebolaget LM Ericsson		
	F12	WO 2006/050758 A1	05-18-2006	Telefonaktiebolaget LM Ericsson		

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet

5

of

17

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		8,005,459	08-23-2011	BALSILLIE, Jim	
		8,010,080	08-30-2011	THENTHIRUPERAI, et al.	
		8,010,081	08-30-2011	ROSKOWSKI, Steve	
		8,015,133	09-06-2011	WU, et al	
		8,015,234	09-06-2011	LUM et al	
		2002/0022472	02-21-2002	WATLER et al	
		2002/0120540	08-29-2002	KENDE et al	
		2002/0131404	09-19-2002	MEHTA et al	
		2002/0138601	09-26-2002	PIPONIUS et al	
		2002/0176377	11-28-2002	HAMILTON	
		2002/0199001	12-26-2002	WENOCUR et al	
		2003/0004937	01-02-2003	SALMENKAITA et al	
		2003/0005112	01-03-2003	KRAUTKREMER, Todd Joseph	
		2003/0013434	01-16-2003	ROSENBERG et al	
		2003/0050070	03-13-2003	MASHINSKY et al	
		2003/0050837	03-13-2003	KIM	
		2003/0088671	05-08-2003	KLINKER et al	
		2003/0133408	07-17-2003	CHENG et al	
		2003/0161265	08-28-2003	CAO et al	
		2003/0182420	09-25-2003	JONES et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				
	F13	WO 2006/073837 A2	07-13-2006	Symbol Technologies, Inc.		
	F14	WO 2006/077481 A1	07-27-2006	TrueContext Corporation		
	F15	WO 2006/130960 A1	12-14-2006	Mobidia, Inc.		

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

American LegalNet, Inc.
www.FormsWorkflow.com

Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet

6

of

17

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		2003/0182435	09-25-2003	REDLICH et al	
		2003/0224781	12-04-2003	MILFORD et al	
		2003/0229900	12-11-2003	REISMAN	
		2003/0236745	12-25-2003	HARTSELL et al	
		2004/0019539	01-29-2004	RAMAN et al	
		2004/0030705	02-12-2004	BOWMAN-AMUAH et al	
		2004/0044623	03-04-2004	WAKE et al	
		2004/0047358	03-11-2004	CHEN et al	
		2004/0073672	04-15-2004	FASCENDA	
		2004/0082346	04-29-2004	SKYTT et al	
		2004/0098715	05-20-2004	AGHERA et al	
		2004/0103193	05-27-2004	PANDYA et al	
		2004/0127200	07-01-2004	SHAW et al	
		2004/0132427	07-08-2004	LEE et al	
		2004/0168052	08-26-2004	CLISHAM et al	
		2004/0198331	10-07-2004	COWARD et al	
		2004/0236547	11-25-2004	RAPPAPORT et al	
		2004/0249918	12-09-2004	SUNSHINE	
		2005/0021995	01-27-2005	LAL et al	
		2005/0048950	03-03-2005	MORPER	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				
	F16	WO 2007/001833 A2	01-04-2007	Symbol Technologies, Inc.		
	F17	WO 2007/014630 A1	02-08-2007	Telefonaktiebolaget LM Ericsson		
	F18	WO 2007/018363 A1	02-15-2007	Upresto, Inc.		

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

American LegalNet, Inc.
www.FormsWorkFlow.com

Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet	7	of	17
-------	---	----	----

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		2005/0055291	03-10-2005	BEVENTE et al	
		2005/0055309	03-10-2005	WILLIAMS et al	
		2005/0060266	03-17-2005	DEMELLO et al	
		2005/0097516	05-05-2005	DONNELLY et al	
		2005/0107091	05-19-2005	VANNITHAMBY et al	
		2005/0128967	06-16-2005	SCOBIE	
		2005/0166043	07-28-2005	ZHANG et al	
		2005/0183143	08-18-2005	ANDERHOLM et al	
		2005/0198377	09-08-2005	FERGUSON et al	
		2005/0216421	09-29-2005	BARRY et al	
		2005/0228985	10-13-2005	YLIKOSKI et al	
		2005/0238046	10-27-2005	HASSAN et al	
		2005/0246282	11-03-2005	NASLUND et al	
		2005/0250508	11-10-2005	GUO et al	
		2005/0254435	11-17-2005	MOAKLEY et al	
		2005/0266825	12-01-2005	CLAYTON	
		2005/0266880	12-01-2005	GUPTA	
		2006/0014519	01-19-2006	MARSH et al	
		2006/0019632	01-26-2006	CUNNINGHAM et al	
		2006/0026679	02-02-2006	ZAKAS	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD- YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				
	F19	WO 2007/053848 A1	05-10-2007	Mobile Armor, LLC		
	F20	WO 2007/069245 A2	06-21-2007	Yoggie Sec. Systems, Inc.		
	F21	WO 2007/107701 A2	09-27-2007	British Telecomm. Public Ltd. Co.		

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

American LegalNet, Inc.
www.FormsWorkFlow.com

Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet

8

of

17

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		2006/0034256	02-16-2006	ADDAGATLA et al	
		2006/0040642	02-23-2006	BORIS et al	
		2006/0045245	03-02-2006	AARON et al	
		2006/0048223	03-02-2006	LEE et al	
		2006/0072646	04-06-2006	FEHER et al	
		2006/0085543	04-01-2006	HRASTAR et al	
		2006/0112016	05-25-2006	ISHIBASHI	
		2006/0143098	06-29-2006	LAZARIDIS	
		2006/0165060	07-27-2006	DUA, Robin	
		2006/0178917	08-10-2006	MIKURAK	
		2006/0178918	08-10-2006	MIKURAK	
		2006/0183462	08-17-2006	KOLEHMAINEN et al	
		2006/0190314	08-24-2006	HERNANDEZ	
		2006/0199608	09-07-2006	DUNN et al	
		2006/0206904	09-14-2006	WATKINS et al	
		2006/0218395	09-28-2006	MAES	
		2006/0233108	10-19-2006	KRISHNAN, Murali R.	
		2006/0233166	10-19-2006	BOU-DIAB et al	
		2006/0236095	10-19-2006	SMITH et al	
		2006/0242685	10-26-2006	HEARD et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				
	F22	WO 2008/017837 A1	02-14-2008	Symbian Software Limited		
	F23	WO 2008/051379 A2	05-02-2008	Verizon Services Corp.		
	F24	WO 2008/066419 A1	06-05-2008	Telefonaktiebolaget LM Ericsson		

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet

9

of

17

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		2006/0258341	11-16-2006	MILLER et al	
		2006/0291477	12-28-2006	CROAK et al	
		2007/0019670	01-25-2007	FALARDEAU	
		2007/0022289	01-25-2007	ALT et al	
		2007/0036312	02-15-2007	CAI et al	
		2007/0055694	03-08-2007	RUGE et al	
		2007/0076616	04-05-2007	NGO et al	
		2007/0093243	04-26-2007	KAPADEKAR et al	
		2007/0100981	05-03-2007	ADAMCZYK et al	
		2007/0101426	05-03-2007	LEE et al	
		2007/0104126	05-10-2007	CALHOUN et al	
		2007/0130315	06-07-2007	FRIEND et al	
		2007/0140113	06-21-2007	GEMELOS	
		2007/0140275	06-21-2007	BOWMAN et al	
		2007/0198656	08-23-2007	MAZZAFERRI et al	
		2007/0220251	09-20-2007	ROSENBERG et al	
		2007/0226225	09-27-2007	YIU et al	
		2007/0243862	10-18-2007	COSKUN et al	
		2007/0248100	10-25-2007	ZUBERI et al	
		2007/0255848	11-01-2007	SEWALL, et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				
	F25	WO 2008/080139 A1	07-03-2008	Integrated Mobile, Inc.		
	F26	WO 2008/080430 A1	07-10-2008	Telecom Italia S.P.A.		
	F27	WO 2008/099802 A1	08-21-2008	NEC Corporation		

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet

10

of

17

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		2007/0259673	11-08-2007	WILLARS et al	
		2007/0263558	11-15-2007	SALOMONE	
		2007/0274327	11/29/2007	KAARELA et al	
		2007/0294395	12-20-2007	STRUB et al	
		2007/0298764	12-27-2007	CLAYTON, Steve	
		2008/0005561	01-03-2008	BROWN et al	
		2008/0010452	01-10-2008	HOLTZMAN et al	
		2008/0039102	02-14-2008	SEWALL, et al	
		2008/0049630	02-28-2008	KOZISEK et al	
		2008/0052387	02-28-2008	HEINZ et al	
		2008/0059474	03-01-2008	LIM, Keng	
		2008/0059743	03-06-2008	BYCHKOV et al	
		2008/0064367	03-13-2008	NATH et al	
		2008/0060066	03-06-2008	WYNN et al	
		2008/0062900	03-13-2008	RAO	
		2008/0066149	03-01-2008	LIM, Keng	
		2008/0066150	03-01-2008	LIM, Keng	
		2008/0082643	04-03-2008	STORRIE et al	
		2008/0083013	04-03-2008	SOLIMAN et al	
		2008/0095339	04-24-2008	ELLIOTT et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				
	F28	WO 2010/088413 A1	08-05-2010	Headwater Partners I LLC		

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet

11

of

17

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		2008/0098062	04-24-2008	BALIA	
		2008/0109679	05-08-2008	WRIGHT et al	
		2008/0120688	05-22-2008	QIU et al	
		2008/0127304	05-29-2008	GINTER et al	
		2008/0130534	06-28-2005	TOMIOKA, Tazuko	
		2008/0130656	06-05-2008	KIM et al	
		2008/0132268	06-05-2008	CHOI-GROGAN et al	
		2008/0134330	06-05-2008	KAPOOR et al	
		2008/0147454	06-19-2008	WALKER et al.	
		2008/0160958	04-03-2008	ABICHANDANI et al	
		2008/0162637	07-03-2008	ADAMCZYK et al	
		2008/0162704	04-03-2008	POPLETT et al	
		2008/0164304	07-10-2008	NARASIMHAN	
		2008/0167027	07-10-2008	GAUTIER et al	
		2008/0167033	07-10-2008	BECKERS, Michel	
		2008/0168523	07-10-2008	ANSARI et al	
		2008/0177998	07-24-2008	APSANGI et al	
		2008/0183812	07-31-2008	PAUL et al	
		2008/0189760	08-07-2008	ROSENBERG et al	
		2008/0207167	08-28-2008	BUGENHAGEN	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet

12

of

17

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		2008/0212470	09-04-2008	CASTANEDA et al	
		2008/0221951	09-11-2008	STANFORTH et al	
		2008/0222692	09-11-2008	ANDERSSON et al	
		2008/0225748	09-18-2008	KHEMANI et al	
		2008/0229385	09-18-2008	FEDER et al	
		2008/0229388	09-18-2008	MAES, Stephane H.	
		2008/0256593	10-16-2008	VINBERG	
		2008/0268813	10-30-2008	MAES, Stephane H.	
		2008/0298230	12-01-2008	LUFT et al	
		2008/0305793	12-11-2008	GALLAGHER et al	
		2008/0311885	12-18-2008	DAWSON et al	
		2008/0316923	12-25-2008	FEDDERS et al	
		2008/0318547	12-25-2008	BALLOU et al	
		2008/0318550	12-25-2008	DEATLEY	
		2008/0319879	12-25-2008	CARROLL et al	
		2009/0005005	01-01-2009	FORSTALL et al	
		2009/0054030	02-26-2009	GOLDS, David	
		2009/0068984	03-12-2009	BURNETT	
		2009/0077622	03-19-2009	BAUM et al	
		2009/0125619	05-14-2009	ANTANI, Snehal S.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

American LegalNet, Inc.
www.FormsWorkFlow.com

Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet

13

of

17

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		2009/0180391	07-16-2009	PETERSEN et al	
		2009/0197585	08-06-2009	AARON, Jeffrey A.	
		2009/0257379	10-15-2009	ROBINSON et al	
		2009/0271514	10-29-2009	THOMAS et al	
		2009/0287921	11-19-2009	ZHU et al	
		2009/0286507	11-19-2009	O'NEAL et al	
		2009/0288140	11-19-2009	HUBER et al	
		2010/0017506	01-21-2010	FADELL	
		2010/0043068	02-18-2010	VARADHAN et al	
		2010/0071053	03-18-2010	ANSARI et al	
		2010/0082431	04-01-2010	RAMER et al	
		2010/0188975	07-29-2010	RALEIGH, Gregory G.	
		2010/0188990	07-29-2010	RALEIGH, Gregory G.	
		2010/0188992	07-29-2010	RALEIGH, Gregory G.	
		2010/0188994	07-29-2010	RALEIGH, Gregory G.	
		2010/0191576	07-29-2010	RALEIGH, Gregory G.	
		2010/0191612	07-29-2010	RALEIGH, Gregory G.	
		2010/0191846	07-29-2010	RALEIGH, Gregory G.	
		2010/0192170	07-29-2010	RALEIGH, Gregory G.	
		2010/0192212	07-29-2010	RALEIGH, Gregory G.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				

Examiner
SignatureDate
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

American LegalNet, Inc.
www.FormsWorkFlow.com

Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [JRALEP034]

Sheet	14	of	17
-------	----	----	----

U. S. PATENT DOCUMENTS

[illegible]

FOREIGN PATENT DOCUMENTS

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ "Number" ⁴ "Kind Code" ⁵ (if known)				

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet 15 of 17

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
	N01	Author Unknown, 3GPP TS 23.203, V8.4.0, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture (Release 8), December 2008	
	N02	Author Unknown, 3GPP TS 23.401, V8.4.0, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 8), December 2008	
	N03	Author Unknown, "Overview of GSM, GPRS, and UMTS," Chapter 2, November 4, 2008	
	N04	Author Unknown, Hewlett-Packard, "IP Multimedia Services Charging," a White Paper from HP, January 2006	
	N05	Author Unknown, Kindle™ User's Guide 3rd Edition, Copyright 2004-2009	
	N06	No author/date indicated. "Data Roaming Tariffs - Transparency Measures." Obtained from EUROPA - Europe's Information Society Thematic Portal website, June 24, 2011: "http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm."	
	N07	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	
	N08	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	
	N09	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	
	N10	DIKAIKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet 16 of 17

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
	N11	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	
	N12	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	
	N13	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	
	N14	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	
	N15	LI, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	
	N16	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standardization Efforts," IEEE Communications Magazine, June 2004	
	N17	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	
	N18	KYRIAKAKOS et al., "Ubiquitous Service Provision in Next Generation Mobile Networks," Proceedings of the 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004	
	N19	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	
	N20	OPPLIGER, Rolf, "Internet Security: Firewalls and Beyond," Communications of the ACM, May 1997, Vol. 40, No. 5	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995 no Persons are required to respond to a collection of information unless it contains a valid OMR control number

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	13/237,827
Filing Date	September 20, 2011
First Named Inventor	Gregory G. Raleigh, et al.
Art Unit	3627
Examiner Name	Not Yet Assigned
Attorney Docket Number	26WV-160511 [RALEP034]

Sheet 17 of 17

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
	N21	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	
	N22	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	
	N23	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	
	N24	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 2004	
	N25	Search Report and Written Opinion mailed 20 January 2012 from International Serial Number PCT/US2011/052420 filed 20 September 2011	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PATENT COOPERATION TREATY

N25

From the INTERNATIONAL SEARCHING AUTHORITY

To: MARK SOCKOL
SHEPPARD, MULLIN, RICHTER & HAMPTON
LLP
390 LYTTON AVENUE
PALO ALTO, CA 94301

PCT

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT AND
THE WRITTEN OPINION OF THE INTERNATIONAL
SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 26WV-160511 [RALEP034]	Date of mailing (day/month/year) 20 JAN 2012
International application No. PCT/US2011/052420	International filing date (day/month/year) 20 September 2011
Applicant HEADWATER PARTNERS I LLC	
FOR FURTHER ACTION See paragraphs 1 and 4 below	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 – 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.
3. ☐ **With regard to any protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:**
- ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.
- ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of 18 months from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

Within 19 months from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later); otherwise, the applicant must, within 20 months from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of 30 months (or later) will apply even if no demand is filed within 19 months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 Telephone No. PCT OSP: 571-272-7774
---	--

Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 26WV-160511 [RALEP034]	FOR FURTHER ACTION see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/US2011/052420	International filing date (day/month/year) 20 September 2011	(Earliest) Priority Date (day/month/year) 20 September 2010
Applicant HEADWATER PARTNERS I LLC		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the language, the international search was carried out on the basis of:

- ☒ the international application in the language in which it was filed.
☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c. ☐ With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2. ☐ Certain claims were found unsearchable (see Box No. II).

3. ☐ Unity of invention is lacking (see Box No. III).

4. With regard to the title,

- ☒ the text is approved as submitted by the applicant.
☐ the text has been established by this Authority to read as follows:

5. With regard to the abstract,

- ☒ the text is approved as submitted by the applicant.
☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

- a. the figure of the drawings to be published with the abstract is Figure No. 1
☒ as suggested by the applicant.
☐ as selected by this Authority, because the applicant failed to suggest a figure.
☐ as selected by this Authority, because this figure better characterizes the invention.
- b. ☐ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2011/052420

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 15/16 (2011.01)

USPC - 726/7

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) - G06F 7/00, 15/16, 17/00; H04L 29/08 (2011.01)

USPC - 726/1-7, 12, 17-19, 20

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

MicroPatent, Google Scholar

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2010/088413 A1 (RALEIGH) 05 August 2010 (05.08.2010) entire document	1-7 and 13-31
Y		8-12
Y	US 2008/0010452 A1 (HOLTZMAN et al) 10 January 2008 (10.01.2008) entire document	8-12
Y	US 2004/0249918 A1 (SUNSHINE) 09 December 2004 (09.12.2004) entire document	11
A	US 2008/0060066 A1 (WYNN et al) 06 March 2008 (06.03.2008) entire document	1-31

☐ Further documents are listed in the continuation of Box C.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

21 December 2011

Date of mailing of the international search report

20 JAN 2012

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: MARK SOCKOL
SHEPPARD, MULLIN, RICHTER & HAMPTON
LLP
390 LYTTON AVENUE
PALO ALTO, CA 94301

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Applicant's or agent's file reference 26WV-160511 [RALEP034]		Date of mailing (day/month/year) 20 JAN 2012
FOR FURTHER ACTION See paragraph 2 below		
International application No. PCT/US2011/052420	International filing date (day/month/year) 20 September 2011	Priority date (day/month/year) 20 September 2010
International Patent Classification (IPC) or both national classification and IPC IPC(8) - G06F 15/16 (2011.01) USPC - 726/7		
Applicant HEADWATER PARTNERS I LLC		

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Date of completion of this opinion 21 December 2011	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	--	---

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITYInternational application No.
PCT/US2011/052420

Box No. 1 Basis of this opinion

1. With regard to the language, this opinion has been established on the basis of:
- ☒ the international application in the language in which it was filed.
- ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2. ☐ This opinion has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a)).
3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:
- a. (means)
- ☐ on paper
- ☐ in electronic form
- b. (time)
- ☐ in the international application as filed
- ☐ together with the international application in electronic form
- ☐ subsequently to this Authority for the purposes of search
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2011/052420

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	8-12	YES
	Claims	1-7 and 13-31	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-31	NO
Industrial applicability (IA)	Claims	1-31	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-7 and 13-31 lack novelty under PCT Article 33(2) as being anticipated by Raleigh (WO 2010/088413 A1).

Regarding claim 1, Raleigh discloses a network system (Abstract; the invention is to a wireless network which supports one or more devices in wireless communication), comprising: one or more network elements configured to receive a device credential from an end-user device (Paragraphs [0065] and [0149]; the system has network equipment (elements) including a service controller (122) which can provide authentication credentials to other networking equipment); and a service processor authentication and management system (Paragraphs [0035], [0038] and [0065]; the invention includes a system and/or process that generates network device authentication and provisioning to allow devices into the network system. Wherein the device assisting functions reside in a service processor (115)) configured to: obtain service processor authentication information (Paragraphs [0035], [0038] and [0065]; the invention includes a system and/or process that generates network device authentication and provisioning to allow devices into the network system. Wherein the device assisting functions reside in a service processor (115)), and using the service processor authentication information, facilitate execution of an end-user device service processor authentication procedure (Paragraphs [0035] and [0099]; an Authentication, Authorization and Accounting (AAA) access network server (1621) provides access control and authorization functions for the device access layer to allow the devices onto a central provider network).

Regarding claim 2, Raleigh discloses the network system recited in claim 1, wherein at least one of the one or more network elements is an AAA (Paragraph [0099]; the system uses an Access Network AAA server), an HLR (Paragraph [0041]; an HLR is used), a PCRF, an access network authentication system (Paragraph [0099]; the system uses an Authentication, Authorization and Accounting (AAA) access network server (1621)), an admission system, or a log-in system (Paragraph [0052]; the system uses a log-in system wherein the end user is required to enter a unique log-in).

Regarding claim 3, Raleigh discloses the network system recited in claim 1, wherein at least one of the one or more service policy enforcement elements is a gateway, a router, a GGSN, a SGSN, a proxy (Paragraph [00144]; the system uses gateways, routers GGSN, SGSN and proxy servers to route traffic (enforce traffic policies)), a charging element, or a notification trigger element (Paragraph [0091]; the system provides policy service control based on trigger events).

Regarding claim 4, Raleigh discloses the network system recited in claim 1, wherein authenticating the service processor on the end-user device comprises verifying that the service processor is present and configured in an expected manner (Paragraph [0091]; the service controller verifies device service policy and the verification error conditions that can indicate a mismatch in service measure and service policy can include unauthorized network access, unauthorized network speed, and other conditions).

Regarding claim 5, Raleigh discloses the network system recited in claim 1, further comprising one or more service policy enforcement elements configured to implement an access network service policy associated with the device credential (Paragraph [00142]; a user can be notified of a service policy enforcement action related to access control policy rules), and wherein the service processor authentication and management system is further configured to cause the access network service policy associated with the device credential to be executed as a first network portion of an access network service when the end-user device service processor authentication procedure is successful (Paragraph [00143]; the proxy server or router can be programmed to only allow access to one or more ambient services (a first or second network portion) that are authorized by the device service plan (credentials)).

Regarding claim 6, Raleigh discloses the network system recited in claim 1, further comprising one or more service policy enforcement elements configured to implement an access network service policy associated with the device credential (Paragraph [00142]; a user can be notified of a service policy enforcement action related to access control policy rules), and wherein the service processor authentication and management system is further configured to cause the access network service policy associated with the device credential to be executed as a second network portion of an access network service when the end-user device service processor authentication procedure is unsuccessful (Paragraph [00143]; the proxy server or router can be programmed to only allow access to one or more ambient services (a first or second network portion) that are authorized by the device service plan (credentials)).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2011/052420

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claim 7, Raleigh discloses the network system recited in claim 1, wherein the device credential is information from a SIM card, information from a soft SIM, information from a universal SIM, an IMSI, a wireless modem identifier, a phone number, an IMEI, an MEID, a MAC address, an IP address (Paragraphs [00105] and [00149]; an IP address can be used to verify policy control and service usage is only obtained by the current user(s)), a secure device identifier (Paragraph [0045]; the device sends an identifier for usage activity), or a device secure communication encryption key (Paragraph [0087]; the device can communication through secure communications using IP layer encryption techniques).

Regarding claim 13, Raleigh discloses an end-user device, comprising: a modem for enabling the end-user device to access available network data services over an access network (Paragraph [0118]; the invention uses a modem or network device which allows access to a 3G or 4G network via a wireless connection); one or more device credential sources configured to store a device credential (Paragraphs [0052] and [0056]; the system has a CDR storage, aggregation, mediation feed (118) which stores service usage information and unique log-in (credentials) for end users); and a service processor (Paragraphs [0035], [0038] and [0065]; the invention includes a system and/or process that generates network device authentication and provisioning to allow devices into the network system. Wherein the device assisting functions reside in a service processor (115) configured to: enforce a device-based portion of a wireless access network service policy (Abstract and Paragraphs [0142] and [0144]; the device service processor controls and enforces device service plans and device service traffic to ensure service policies are implemented. As mentioned in the abstract the network is a wireless network); and communicate with a network-based service controller to provide service processor authentication information configured to assist the network-based service controller in authenticating the service processor (Paragraphs [0065] and [0149]; the system has network equipment (elements) including a service controller (122) which can provide authentication credentials (authentication information) to other networking equipment).

Regarding claim 14, Raleigh discloses the end-user device recited in claim 13, wherein the service processor authentication information is the device credential (Paragraphs [0065] and [0149]; the system has network equipment (elements) including a service controller (122) which can provide authentication credentials (authentication information) to other networking equipment).

Regarding claim 15, Raleigh discloses the end-user device recited in claim 13, wherein the device credential is information from a SIM card, information from a soft SIM, information from a universal SIM, an IMSI, a wireless modem identifier, a phone number, an IMEI, an MEID, a MAC address, an IP address (Paragraphs [00105] and [00149]; an IP address can be used to verify policy control and service usage is only obtained by the current user(s)), a secure device identifier (Paragraph [0045]; the device sends an identifier for usage activity), or a device secure communication encryption key (Paragraph [0087]; the device can communication through secure communications using IP layer encryption techniques).

Regarding claim 16, Raleigh discloses a network system (Abstract; the invention is to a wireless network which supports one or more devices in wireless communication), comprising: memory configured to store a trusted usage data report associated with an end-user device (Paragraph [0092]; the service controller (122) includes a service history server (1650) which collects and stores records service usage or service activity reports from an Access Network AAA server); and one or more network elements configured to: receive a usage data report from the end-user device (Paragraph [0092]; the service controller (122) includes a service history server (1650) which collects and stores records service usage or service activity reports from an Access Network AAA server. The usage or service activity reports can be verified and sent to other servers and/or one or more agents); obtain the trusted usage data report associated with the end-user device (Paragraph [0092]; the service controller (122) includes a service history server (1650) which collects and stores records service usage or service activity reports from an Access Network AAA server. The usage or service activity reports can be verified and sent to other servers and/or one or more agents); and reconcile the usage data report from the end-user device and the trusted usage data report associated with the end-user device (Paragraph [0092]; the service controller (122) includes a service history server (1650) which collects and stores records service usage or service activity reports from an Access Network AAA server. The usage or service activity reports can be verified and sent to other servers and/or one or more agents).

Regarding claim 17, Raleigh discloses the network system recited in claim 16, wherein the trusted usage data report associated with the end-user device is generated by a network element (Paragraph [0092]; the usage report is generated by the service controller (122) and the service history server (1650)).

Regarding claim 18, Raleigh discloses the network system recited in claim 16, wherein the trusted usage data report associated with the end-user device is generated by an end-user device software or firmware agent in a secure execution environment (Fig. 9 and Paragraphs [0092] and [00106]; service history reports can be generated from the device and include various service tracking information which is later reported to the service history server (1650). The service processor functions are implemented as secure software).

Regarding claim 19, Raleigh discloses the network system recited in claim 18, wherein the trusted usage data report associated with the end-user device is received from a good customer feedback source (Paragraph [0095]; the network traffic analysis server (1656- good customer feedback source) collects/receives service usage history for devices and/or groups of devices and analyzes the service usage).

Regarding claim 20, Raleigh discloses the network system recited in claim 19, wherein the good customer feedback source is a website or server (Paragraph [0095]; the network traffic analysis server (1656- good customer feedback source) collects/receives service usage history for devices and/or groups of devices and analyzes the service usage) that tracks one or more of a number of visits by the end-user device, a number of transactions associated with the end-user device, an amount of business generated in association with the end-user device, an amount of data communicated by or to the end-user device (Paragraph [00142]; the amount of service usage can be a tracked measure), or another measure of the end-user device's interaction with the website or server (Paragraph [0095]; the network traffic analysis server (1656- good customer feedback source) collects/receives service usage history for devices and/or groups of devices and analyzes the service usage).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/052420

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 21, Raleigh discloses the network system recited in claim 16, wherein the network-generated usage data report associated with the end-user device is a flow data record (Paragraph [00138]; the data can be stored in a flow data record (FDR)).

Regarding claim 22, Raleigh discloses the network system recited in claim 16, wherein the one or more network elements are further configured to credit a user account associated with the end-user device based on reconciling the usage data report from the end-user device and the network-generated usage data report associated with the end-user device (Paragraph [0148]; the system uses charging usage reports to determine the total service usages and can apply credit to a user for services not used or charged).

Regarding claim 23, Raleigh discloses a network system (Abstract; the invention is to a wireless network which supports one or more devices in wireless communication), comprising: one or more network elements configured to: receive a data usage report associated with an end-user device from a good customer feedback source (Paragraphs [0095] and [00141]; the network traffic analysis server (1656- good customer feedback source) collects/receives service usage history for devices and/or groups of devices and analyzes the service usage. Also ambient partner feedback is used to verify service charging accounting), and based on the data usage report from the good customer feedback source, reduce a bulk data usage amount associated with a user account (Paragraph [00141]; the service usage reported from the service partner's feedback is compared to the number of transactions completed to determine if the ambient usage is reasonable or should the ambient service be throttled (reduced) or blocked completely).

Regarding claim 24, Raleigh discloses a network system (Abstract; the invention is to a wireless network which supports one or more devices in wireless communication), comprising: one or more network elements configured to detect a service usage indication associated with an end-user device (Paragraphs [0052] and [0056]; the system has a CDR storage, aggregation, mediation feed (118) which stores service usage information and unique log-in (credentials) for end users); and a service controller configured to: determine that a device credential is intended to be associated with a service processor on the end-user device (Paragraphs [0065] and [0149]; the system has network equipment (elements) including a service controller (122) which can provide authentication credentials to other networking equipment); receive the service usage indication associated with the end-user device (Paragraph [0095]; the network traffic analysis server (1656- good customer feedback source) collects/receives service usage history for devices and/or groups of devices and analyzes the service usage); detect a specified condition (Paragraph [0088]; the system can include an access control integrity server (1654) which collects device information on service policies and can cross check information to identify integrity breaches (specified conditions)); and declare a service processor integrity violation upon detecting the specified condition (Paragraph [0088]; the system can initiate action when a service policy violation or system integrity breach is suspected).

Regarding claim 25, Raleigh discloses the network system recited in claim 24, wherein the specified condition is that the service controller is unable to complete a service processor authentication procedure (Paragraph [00133]; the service charge usage must be received within a certain pre-set policy time difference from the time that other ambient service charging traffic is received for the condition to be verified).

Regarding claim 26, Raleigh discloses the network system recited in claim 24, wherein the service controller is further configured to receive a device-originated service usage indication from the service processor (Paragraph [0092]; the service controller (122) includes a service history server (1650) which collects and stores records service usage or service activity reports from an Access Network AAA server. The usage or service activity reports can be verified and sent to other servers and/or one or more agents), and wherein the specified condition is that the service usage indication is inconsistent with the device-originated service usage indication (Paragraphs [0088]-[0091]; the system can initiate action when a service policy violation or system integrity breach is suspected wherein the integrity check can be based on service usage).

Regarding claim 27, Raleigh discloses the network system recited in claim 24, wherein the service controller is further configured to receive a device-originated service usage indication from the service processor (Paragraph [0092]; the service controller (122) includes a service history server (1650) which collects and stores records service usage or service activity reports from an Access Network AAA server. The usage or service activity reports can be verified and sent to other servers and/or one or more agents), and wherein the specified condition is that either the service usage indication or the device originated service usage indication is inconsistent with a service usage policy (Paragraphs [0088]-[0091]; the system can initiate action when a service policy violation or system integrity breach is suspected wherein the integrity check can be based on service usage).

Regarding claim 28, Raleigh discloses the network system recited in claim 24, wherein the device credential is information from a SIM card, information from a soft SIM, information from a universal SIM, an IMSI, a wireless modem identifier, a phone number, an IMEI, an MEID, a MAC address, an IP address (Paragraphs [00105] and [00149]; an IP address can be used to verify policy control and service usage is only obtained by the current user(s)), a secure device identifier (Paragraph [0045]; the device sends an identifier for usage activity), or a device secure communication encryption key (Paragraph [0087]; the device can communication through secure communications using IP layer encryption techniques).

Regarding claim 29, Raleigh discloses the network system recited in claim 24, wherein at least one of the one or more network elements is a GGSN, an SGSN (Paragraph [00144]; the system uses gateways, routers GGSN, SGSN and proxy servers to route traffic (enforce traffic policies)), a charging gateway, a AAA function (Paragraph [0099]; the system uses an Access Network AAA server), an HLR (Paragraph [0041]; an HLR is used), a router, or a server (Paragraph [00144]; the system uses gateways, routers GGSN, SGSN and proxy servers to route traffic (enforce traffic policies)).

Regarding claim 30, Raleigh discloses the network element recited in claim 24, wherein the service usage indication associated with the end-user device is one or more of a start accounting message, a stop accounting message, a charging data record, a flow data record (Paragraph [00138]; the data can be stored in a flow data record (FDR)), or a service usage measure (Paragraph [0092]; the service controller (122) includes a service history server (1650) which collects and stores records service usage or service activity reports from an Access Network AAA server. The usage or service activity reports can be verified and sent to other servers and/or one or more agents).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/052420

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claim 31, Raleigh discloses the network element recited in claim 25, wherein the service controller is unable to complete the service processor authentication procedure when the service processor does not communicate with the service controller within a predetermined amount of time after the service controller receives the service usage indication associated with the end-user device (Paragraph [00133]; the service charge usage must be received within a certain pre-set policy time difference from the time that other ambient service charging traffic is received).

Claims 8-10 and 12 lack an inventive step under PCT Article 33(3) as being obvious over Raleigh (WO 2010/088413 A1) in view of Holtzman et al. (US 2008/0010452 A1; hereinafter Holtzman).

Regarding claim 8, Raleigh discloses the network system recited in claim 1, wherein the service processor authentication and management system is further configured to: associate a first device credential with a first end-user device (Paragraph [00149]; a unique device IP address or other credentials can be used to provide and determine device access rights). Raleigh does not disclose determining whether a received device credential, associated with an authenticating end-user device, is the first device credential; determine whether the authenticating end-user device is the first end-user device; enforce a first access network control policy when the received device credential is the first device credential and the authenticating end-user device is the first end-user device; and enforce a second access network control policy when the received device credential is not the first device credential or the authenticating end-user device is not the first end-user device. However, in disclosing a system for providing access certificates (abstract), Holtzman teaches determining whether a received device credential, associated with an authenticating end-user device, is the first device credential (Fig. 18 and Paragraph [0215]; the system stores a list of credentials for entities and determines which entities can have unlimited (first access policy), somewhat limited (second access policy), or blacklisted (third access policy), access based on the policies and authentication of the entity); determine whether the authenticating end-user device is the first end-user device (Fig. 18 and Paragraph [0215]; the system stores a list of credentials for entities and determines which entities can have unlimited (first access policy), somewhat limited (second access policy), or blacklisted (third access policy), access based on the policies and authentication of the entity); enforce a first access network control policy when the received device credential is the first device credential and the authenticating end-user device is the first end-user device (Fig. 18 and Paragraph [0215]; the system stores a list of credentials for entities and determines which entities can have unlimited (first access policy), somewhat limited (second access policy), or blacklisted (third access policy), access based on the policies and authentication of the entity); and enforce a second access network control policy when the received device credential is not the first device credential or the authenticating end-user device is not the first end-user device (Fig. 18 and Paragraph [0215]; the system stores a list of credentials for entities and determines which entities can have unlimited (first access policy), somewhat limited (second access policy), or blacklisted (third access policy), access based on the policies and authentication of the entity). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include determining whether a received device credential, associated with an authenticating end-user device, is the first device credential; determine whether the authenticating end-user device is the first end-user device; enforce a first access network control policy when the received device credential is the first device credential and the authenticating end-user device is the first end-user device; and enforce a second access network control policy when the received device credential is not the first device credential or the authenticating end-user device is not the first end-user device in the invention of Raleigh as taught by Holtzman, so only allowed entities are given access (Holtzman; Paragraph [0215]).

Regarding claim 9, Raleigh discloses the network system recited in claim 8, but Raleigh does not disclose wherein the second access network control policy differs from the first access network control policy in one or more of a network access privilege, an allowable network destination, a service usage accounting or billing policy, a service usage rate, a service speed or quality, an allowed access network, a user notification, a roaming policy or permission, effect on a device operation. Holtzman teaches wherein the second access network control policy differs from the first access network control policy in one or more of a network access privilege (Fig. 18 and Paragraph [0215]; the system stores a list of credentials for entities and determines which entities can have unlimited (first access policy), somewhat limited (second access policy), or blacklisted (third access policy), access based on the policies and authentication of the entity), an allowable network destination, a service usage accounting or billing policy, a service usage rate, a service speed or quality, an allowed access network, a user notification, a roaming policy or permission, effect on a device operation. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein the second access network control policy differs from the first access network control policy in one or more of a network access privilege, an allowable network destination, a service usage accounting or billing policy, a service usage rate, a service speed or quality, an allowed access network, a user notification, a roaming policy or permission, effect on a device operation in the invention of Raleigh as taught by Holtzman, so only allowed entities are given access (Holtzman; Paragraph [0215]).

Regarding claim 10, Raleigh as modified discloses the network system recited in claim 8, wherein Raleigh discloses wherein the first end-user device comprises a properly-configured service processor (Paragraph [0029]; the system can include a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor).

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITYInternational application No.
PCT/US2011/052420

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

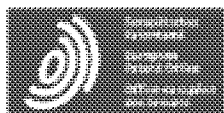
Continuation of:

Regarding claim 12, Raleigh as modified discloses the network system recited in claim 8, wherein Raleigh discloses wherein the second access network control policy is configured to suspend or block network access by the authenticating end-user device (Paragraph [0099]; the Access Network AAA server (1621) can restrict, suspend or limit network access as necessary).

Claim 11 lacks an inventive step under PCT Article 33(3) as being obvious over Raleigh (WO 2010/088413 A1) in view of Holtzman et al. (US 2008/0010452 A1; hereinafter Holtzman) in further view of Sunshine (US 2004/0249918 A1).

Regarding claim 11, Raleigh discloses the network system recited in claim 8, but Raleigh does not disclose wherein the second end-user device does not include a properly-configured service processor. However in disclosing a system for configuring a service processor (Abstract), Sunshine teaches wherein the second end-user device does not include a properly-configured service processor (Abstract; a second service process can be configured from a first service processor). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein the second end-user device does not include a properly-configured service processor in the invention of Raleigh as taught by Holtzman, so a service processor can be configured by another service processor which already has proper configuration parameters (Sunshine; Abstract).

Claims 1-31 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.



Espacenet

Ref. No. F01

Bibliographic data: EP1463238 (A1) — 2004-09-29

Device for local management of security processes of a telecommunication network equipment

Inventor(s): MARILLY EMMANUEL [FR]; BETGE-BREZETZ STEPHANE [FR]; MARTINOT OLIVIER [FR]; CHEVANNE MICHEL [FR]; DELEGUE GERARD [FR] [±]

Applicant(s): CIT ALCATEL [FR] [±]

Classification:
 - **international:** **G06F13/00; H04L12/24; H04L12/26;**
 (IPC1-7): H04L12/24; H04L12/26
 - **European:** H04L12/24A2; H04L12/24D;
H04L12/24E1B; H04L12/24E4A;
H04L12/24S3; H04L12/26M

Application number: EP20040290706 20040315

Priority number (s): FR20030003835 20030328

Also published as: EP1463238 (B1) US2004193711 (A1) JP2004303241 (A) FR2853109 (A1) ES2245774 (T3) more

Abstract of EP1463238 (A1)

The device is embedded in a network equipment and has a safety management module (MAE) adapting the configuration of the equipment (NE) according to a management data stored in a management information base (MIB). The module modifies a policy of measurement of parameter values of a network and/or modifies policy of sending report to network management system (NMS) and/or modifies operation mode of the network equipment. An independent claim is also included for a communication network.

Last updated: 5.12.2011 Worldwide Database 5.7.31; 92p

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
29.09.2004 Bulletin 2004/40

(51) Int. Cl.⁷: H04L 12/24, H04L 12/26

(21) Numéro de dépôt: 04290706.3

(22) Date de dépôt: 15.03.2004

(84) Etats contractants désignées:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Etats d'extension désignés:
AL HR LT LV MK

• Betge-Brezetz, Stéphane
75015 Paris (FR)
• Martinot, Olivier
91210 Draveil (FR)
• Chevanne, Michel
92140 Clamart (FR)
• Deleigue, Gérard
94230 Cachan (FR)

(30) Priorité: 28.03.2003 FR 0303835

(71) Demandeur: ALCATEL
75008 Paris (FR)

(74) Mandataire: Chaffraix, Sylvain et al
Compagnie Financière Alcatel
Département de Propriété Industrielle,
5, rue Noël Pons
92734 Nanterre Cedex (FR)

(72) Inventeurs:
• Marilly, Emmanuel
92160 Antony (FR)

(54) **Dispositif de gestion locale de procédés d'assurance pour un équipement de réseau de communications**

(57) Un dispositif embarqué (D) est dédié à la gestion locale d'assurance pour un équipement de réseau (NE) d'un réseau de communications (N) équipé d'un système de gestion de réseau (NMS), ledit équipement (NE) présentant une configuration choisie et comportant des moyens (MM) de mesure de valeurs de paramètre (s) du réseau et une base d'informations de gestion

(MIB) stockant des données de gestion représentatives des valeurs mesurées. Le dispositif (D) comprend des moyens de gestion (MAE) chargés d'adapter la configuration de l'équipement (NE) en fonction d'au moins les données de gestion stockées dans la base d'informations de gestion (MIB) et de règles, dites d'assurance, choisies.

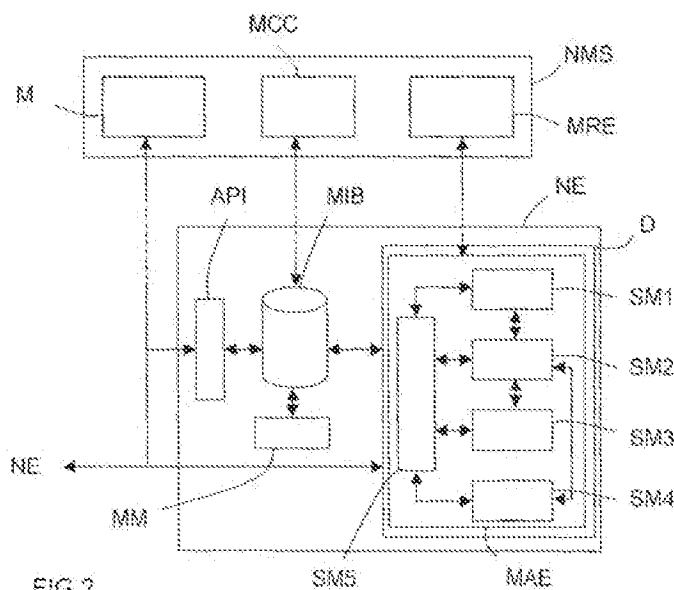


FIG. 2

Description

[0001] L'invention concerne les réseaux de communications, et plus particulièrement ceux offrant une assurance de continuité de service(s).

[0002] De nombreux réseaux de communications mettent en œuvre des procédés d'assurance qui contrôlent l'exécution d'activités de maintenance préventives et réactives destinées à assurer à leurs clients la continuité de la disponibilité de services, définis en termes de qualité de service (QoS). A cet effet, les réseaux disposent d'un système de gestion de réseau (ou NMS pour « Network Management System ») qui analyse continuellement l'état des ressources et les performances de manière à anticiper ou détecter des problèmes ou pannes et à déterminer les actions à entreprendre de sorte que les clients ne soient pas pénalisés.

[0003] Une telle analyse centralisée repose sur la collection d'un très grand nombre de données d'information et d'alarmes auprès des nombreux équipements de réseau, chargés d'effectuer des mesures de valeurs de paramètre(s) du réseau, et plus précisément auprès de leurs bases d'informations de gestion (ou MIB pour « Management Information Base ») chargées de stocker les données de gestion représentatives des valeurs mesurées. Une fois collectées, par exemple via un collecteur SNMP, les données sont stockées dans une base de données d'archivage, par exemple de type Oracle, et alimentent des modules de calcul qui mettent en œuvre des formules ou équations prédéfinies.

[0004] Une telle solution est par exemple décrite dans l'article « Real-Time Performance Monitoring and Anomaly Detection in the Internet: and Adaptive, Objective-Driven, Mix-and-Match Approach » de L. Lawrence Ho, Christopher J. Macey and Ronald G. Hiller.

[0005] Un tel procédé d'assurance centralisé requiert l'emploi de bases de données de très grandes capacités, nécessite des temps de calcul importants et consomme de la bande passante (lors de la collecte), ce qui nuit aux performances du réseau.

[0006] Certaines tentatives ont été faites vers l'utilisation d'agents embarqués dans des éléments réseaux, mais les aspects décisionnels demeurent dans un organe centralisé et présentent les mêmes défauts que la solution précédente. De plus, ces tentatives ne concernent pas l'assurance.

[0007] Des exemples de telles tentatives peuvent être trouvées dans les brevets américains US 6 272 537 et US 6 086.

[0008] L'invention a donc pour but d'améliorer la situation.

[0009] Elle propose à cet effet un dispositif de gestion locale d'assurance pour un équipement de réseau de communications présentant une configuration choisie et comportant des moyens de mesure de valeurs de paramètre(s) du réseau et une base d'informations de gestion (MIB) stockant des données de gestion représentatives des valeurs mesurées.

[0010] Ce dispositif se caractérise par le fait qu'il comporte des moyens de gestion chargés d'adapter la configuration de l'équipement dans lequel il est implanté (ou embarqué) en fonction, notamment, des données de gestion stockées dans sa base d'informations de gestion et de règles, dites d'assurance, choisies, définissant une politique locale d'assurance.

[0011] En d'autres termes, l'invention consiste à intégrer dans des équipements (ou noeuds) du réseau un dispositif d'assurance embarqué de sorte qu'ils puissent assurer localement au moins une partie du procédé d'assurance géré par le NMS.

[0012] Le dispositif d'assurance embarqué, selon l'invention, pourra comporter des caractéristiques complémentaires qui pourront être prises séparément et/ou en combinaison, et en particulier :

- des moyens de gestion capables d'adapter la configuration de leur équipement en fonction de données d'informations provenant d'au moins un autre équipement de réseau,
- une adaptation consistant en une modification de la politique de mesure de paramètre(s) et/ou une modification de la politique d'envoi de rapport (ou « reporting ») au NMS,
- une adaptation consistant en une modification du mode de fonctionnement de l'équipement,
- des moyens de gestion comprenant des moyens d'analyse de paramètres du réseau capables de délivrer des données d'information représentatives de l'évolution temporelle, sur un intervalle choisi, de certaines valeurs de paramètre(s) du réseau (comme par exemple le trafic ou l'état d'un routeur) qui sont stockées dans la MIB. Dans ce cas, les moyens d'analyse peuvent être agencés de manière à délivrer des données d'information représentatives d'une analyse de tendance et/ou d'une analyse de profils ou de signatures (ou « baselines ») et/ou d'une analyse de discontinuité et/ou d'une agrégation de valeurs de paramètres du réseau. Par ailleurs, ces moyens d'analyse peuvent être configurables, notamment dans le but de mettre en œuvre de nouveaux calculs, relatifs aux paramètres du réseau, transmis par le NMS.
- des moyens de gestion comprenant des moyens d'alarme chargés de déclencher l'envoi d'une alarme et/ou de données d'information au NMS et/ou à au moins un autre équipement de réseau, en fonction de règles d'assurance choisies. De telles données d'information et alarmes sont par exemple représentatives de résultat(s) d'analyse(s) ou d'agrégation(s) de données effectuée(s) par les moyens d'analyse et/ou de valeur(s) de paramètre(s) du réseau stockées dans la MIB. Par ailleurs, les moyens d'alarme peuvent être configurables.
- des moyens de gestion comprenant des moyens d'observation du réseau définissant un agent de mesure de flux de type « bout-en-bout » (ou « end-to-end »).

te-ent »), et délivrant des données d'informations. Dans ce cas, les moyens d'observation du réseau peuvent être configurables.

- des moyens de gestion comprenant des moyens de gestion d'accords de niveau de service (ou SLA pour « Service Level Agreement ») délivrant des données d'informations. Dans ce cas, les moyens de gestion d'accords de niveau de service peuvent être configurables,
- des moyens de gestion capables d'effectuer des tests, par exemple de mesure(s) active(s) ou d'aide au diagnostic. Ces tests peuvent notamment permettre de faire remonter une information agrégée ou le résultat du test (par exemple le temps pris pour une opération de type TCP) au niveau de la couche NMS,
- des moyens de gestion capables d'assurer leur gestion en fonction d'un calendrier, de sorte que certaines (ou toutes les) fonctions d'assurance ou tests ne soient effectuées que certains jours de la semaine ou du mois ou à certaines heures, par exemple,
- des moyens de gestion comprenant des moyens de contrôle chargés de gérer le fonctionnement (et notamment la configuration) des moyens d'analyse, des moyens d'alarme, des moyens d'observation du réseau et des moyens de gestion d'accords de niveau de service, en fonction des règles d'assurance choisies et des données d'informations qu'ils délivrent. De tels moyens de contrôle peuvent se présenter sous la forme d'un moteur de règles (ou « rule engine ») dans lequel sont stockées les règles d'assurance choisies. Par ailleurs, ces moyens de contrôle peuvent être configurables,
- des moyens de gestion configurables,
- des moyens de gestion et/ou des moyens d'analyse et/ou des moyens et/ou des moyens de contrôle et/ou des moyens d'observation du réseau et/ou des moyens de gestion d'accords de niveau de service agencés de manière à pouvoir être configurés par le NMS via une interface de langage de programmation (ou API pour « Application Programming Interface ») et éventuellement via la MIB. Dans ce cas, la MIB peut être configurée ou programmée par le NMS via l'API,
- des moyens de gestion et/ou des moyens d'analyse et/ou des moyens d'alarme et/ou des moyens d'observation du réseau et/ou des moyens de gestion d'accords de niveau de service et/ou des moyens de contrôle agencés de manière à pouvoir être configurés par le NMS via des commandes dédiées, telles que des « Command Line Interface » (ou CLI).

[0013] L'invention concerne également un équipement de réseau muni d'un dispositif du type de celui présenté ci-avant. L'invention convient plus particulièrement, bien que de façon non restrictive, aux équipe-

ments de réseau tels que les routeurs, les commutateurs (ou « switchs ») et les pare-feux (ou « firewalls »).

[0014] L'invention propose également un réseau de communications équipé d'un système de gestion de réseau (NMS) et d'une multiplicité d'équipements de réseau du type de celui présenté ci-avant. Dans un mode de réalisation de type distribué, chaque équipement de réseau peut être agencé de manière à délivrer au système de gestion de réseau des alarmes et/ou des données d'information de types différents.

[0015] L'invention peut notamment être mise en œuvre dans toutes les technologies réseaux qui doivent être gérées, et notamment dans les réseaux de transmission (par exemple de type WDM, SONET, SDH), de données (par exemple de type Internet-IP ou ATM) ou de voix (par exemple de type classique, mobile ou NGN).

[0016] D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et des dessins annexés, sur lesquels :

- la figure 1 illustre de façon schématique un réseau de communications comprenant un système de gestion de réseau (NMS) et des équipements de réseau selon l'invention, et
- la figure 2 illustre de façon schématique un exemple de réalisation d'un équipement de réseau selon l'invention.

[0017] Les dessins annexés pourront non seulement servir à compléter l'invention, mais aussi contribuer à sa définition, le cas échéant.

[0018] L'invention a pour objet de permettre la gestion locale, par des équipements de réseau, d'une partie du procédé d'assurance géré par le système de gestion de réseau (ou NMS pour « Network Management System ») d'un réseau de communications.

[0019] Comme cela est illustré sur la figure 1, un réseau de communications N comporte schématiquement une multiplicité d'équipements de réseau NEi (ici $i = 1, 2$, mais il peut prendre d'importe quelle valeur), comme par exemple des serveurs équipés d'un pare-feu ou (« firewall »), des commutateurs (ou « switchs »), des routeurs périphériques (ou « edge routers ») ou des routeurs de cœur (ou « core routers »), pouvant échanger des données, selon un protocole de gestion de réseau, avec un système de gestion de réseau, et notamment avec son serveur de gestion NMS.

[0020] Chaque équipement NEi comporte classiquement une base d'informations de gestion MIB (« Management Information Base »), également appelée base d'instances d'objets. Chaque MIB stocke des données de gestion représentatives de valeurs de champs d'information qui caractérisent l'équipement NEi associé. Certains de ces champs d'information désignent des paramètres du réseau dont les valeurs instantanées sont mesurées par des sondes MM implantées dans, ou gérées par, l'équipement NEi. Par ailleurs,

chaque MIB est associée à une définition de base d'informations de gestion (non représentée), également appelée définition de MIB, stockée dans le système de gestion de réseau et accessible au serveur de gestion NMS.

[0021] Dans ce qui suit, on considère à titre d'exemple non limitatif que le réseau de communications N est de type internet (IP) et que le protocole de gestion du réseau est le protocole SNMP (pour « Simple Network Management Protocol » RFC 2571-2580). Bien entendu, l'invention s'applique à d'autres types de réseau, comme par exemple aux réseaux de transmission de type WDM, SONET ou SDH, de données de type ATM, ou de voix de type classique, mobile ou NGN, et à d'autres protocoles de gestion de réseau, comme par exemple TL1, CORBA ou CMISE/CMIP.

[0022] Par ailleurs, on considère dans ce qui suit que les équipements de réseau NEi sont des routeurs périphériques (ou de bordure) agissant en tant qu'agents d'observation de flux de type « bout-en-bout » (ou « end-to-end »). Ces routeurs sont généralement placés aux frontières du réseau et permettent l'établissement de liens avec d'autres réseaux. Ces agents sont généralement destinés à effectuer des mesures de bout en bout pour des problèmes d'échelle (ou « scalability »). Mais, bien entendu, l'invention n'est pas limitée à ce seul type d'équipement de réseau. Elle concerne tous les équipements de réseau capables d'échanger des données de gestion avec le NMS, et notamment les routeurs périphériques qui n'agissent pas en tant qu'observateurs, les routeurs de cœur, les commutateurs et les pare-feux.

[0023] Chaque équipement de réseau NEi est généralement configuré spécifiquement de manière à transmettre au NMS (ou couche NMS) des données d'information représentatives de mesures qu'il a effectuées avec sa ou ses sondes MM et qu'il a stockées dans sa MIB, ainsi que des alarmes signalant des problèmes ou des pannes. La configuration est généralement définie par une ou plusieurs politiques. Par exemple, une première politique est relative aux conditions d'envoi (ou « reporting ») de valeurs mesurées par l'équipement NEi à l'aide de ses sondes MM. Une deuxième politique peut concerner la ou les mesures de paramètre(s) que l'équipement NEi doit effectuer avec sa ou ses sondes MM. Une troisième politique peut concerner le mode de fonctionnement de l'équipement NEi. Ces politiques sont habituellement définies pour chaque équipement NEi par un module de configuration MC du NMS. Elles sont transmises aux équipements NEi, via le réseau N, à l'aide du protocole de gestion (ici SNMP).

[0024] Mais, le NMS, et notamment son module de collection MCC (ou « collector »), peut également, lorsqu'il l'estime nécessaire, adresser à un équipement de réseau NEi des requêtes pour qu'il lui transmette les valeurs de certains des champs d'information qui sont stockés dans sa MIB. C'est ce que l'on appelle, en anglais, le « polling ».

[0025] Comme cela est mieux illustré sur la figure 2, l'invention propose un dispositif de gestion locale d'assurance D destiné à être soit implanté (ou embarqué) dans un équipement NEi, soit intégré dans un boîtier externe raccordé directement à un équipement NEi. Dans ce qui suit, on considère que le dispositif D est embarqué dans un équipement NEi.

[0026] Ce dispositif D selon l'invention comporte un module d'assurance MAE (ou module de gestion locale d'assurance) chargé d'adapter la configuration de l'équipement NEi, dans lequel il est embarqué, en fonction de règles, dites d'assurance, choisies, des données de gestion stockées dans sa MIB, et d'éventuelles données d'information qu'il reçoit des autres équipements de réseau.

[0027] On entend ici par « adapter », le fait de modifier une politique de mesure de paramètre(s) (voire mettre en place une nouvelle politique de mesure(s) ou reconfigurer la politique de mesure(s)) et/ou une politique d'envoi de rapport (ou « reporting ») au NMS et/ou le mode de fonctionnement de l'équipement NEi, initialement défini(s) par le module de configuration MC du NMS.

[0028] Par ailleurs, on entend par « règles d'assurance », des règles définissant la politique d'assurance locale de l'équipement compte tenu des valeurs prises par certains paramètres du réseau, stockées dans sa MIB, ou d'événements extérieurs, tels qu'une action de la couche NMS ou d'un autre routeur.

[0029] Le module d'assurance embarqué MAE permet ainsi d'embarquer dans un équipement NEi certaines fonctions d'assurance de manière à le rendre « plus intelligent », à limiter le nombre d'informations qui transitent dans le réseau, et éventuellement à permettre sa reconfiguration partielle, en fonction de règles d'assurance.

[0030] Afin de gérer localement la politique d'assurance, le module d'assurance MAE comporte préférentiellement un premier sous-module SM1 chargé d'appliquer un ou plusieurs traitements aux valeurs de certains champs d'information stockés dans la MIB. Plus précisément, ces traitements consistent à appliquer aux valeurs des champs d'information choisis, en fonction de règles d'assurance dédiées, des formules ou des équations, définies par le module de configuration MC du NMS, afin de délivrer des données d'information.

[0031] Par exemple, le premier sous-module SM1 est chargé d'effectuer des analyses de tendance sur un intervalle choisi (ou suivant un calendrier prédéfini), utiles aux anticipations de problèmes ou de pannes. Il peut notamment signaler que le pourcentage d'utilisation d'un CPU d'un routeur va atteindre un seuil critique dans une heure, ou que la bande passante d'un LSP va dépasser le seuil choisi dans deux heures.

[0032] Il peut être également chargé d'effectuer des analyses de profils ou de signatures (ou « baselines »). Cela est notamment utile lorsque l'on cherche, par exemple, à reconnaître ou identifier un profil caractéris-

tique d'utilisation, tel qu'une attaque spécifique d'un routeur, ou un mode de facturation (ou « billing »).

[0033] Il peut être également chargé d'effectuer des analyses de discontinuité de flux ou de trafic. Par exemple, en cas de surcharge d'un réseau, des paquets sont supprimés (ou « dropped »), si bien que la détection d'une discontinuité sur le paramètre de suppression (de 0 à x) permet d'informer que l'on a effectivement des paquets supprimés.

[0034] Il peut encore être chargé d'effectuer des agrégations de valeurs de paramètres du réseau, par exemple pour appliquer des formules du module de collection de données MCC dans le routeur ou pour calculer une moyenne sur une période donnée (par exemple la bande passante moyenne utilisée au cours de la dernière semaine). Dans ce cas, les valeurs agrégées peuvent être stockées dans la MIB et en être extraites sur requête de polling issue du module de collection MCC du NMS.

[0035] A titre d'exemple illustratif, le premier sous-module SM1 peut être chargé d'estimer l'évolution prévisionnelle (ou tendance) du nombre de paquets abandonnés (« dropped »), ainsi que l'évolution prévisionnelle de la bande passante utilisée et/ou de la charge de calcul (CPU) de l'équipement NEI. Il peut être également agencé pour effectuer des tests, par exemple de mesure(s) active(s) ou d'aide au diagnostic. Ces tests peuvent notamment permettre de faire remonter une information agrégée ou le résultat du test (par exemple le temps pris pour une opération de type TCP) au niveau de la couche NMS.

[0036] Préférentiellement, le premier sous-module SM1 délivre des données d'informations représentatives du résultat de ses analyses (ou estimations) à un (cinquième) sous-module de gestion (SM5), qui décide des actions à entreprendre en fonction de la politique d'assurance locale de son équipement NEI.

[0037] Le module d'assurance MAE comporte également de préférence un deuxième sous-module SM2 chargé de déclencher l'envoi d'alarme(s) et/ou de données d'information (ou rapports) sur ordre du cinquième sous-module SM5, en fonction de règles d'assurance qui lui sont dédiées.

[0038] Mais, on peut également envisager que le premier sous-module SM1 alimente le deuxième sous-module SM2 en données d'information, de sorte qu'il leur applique certaines des règles d'assurance et décide soit de leur envoi, soit de l'émission d'une alarme, à destination du NMS, et plus précisément d'un module de réception d'événements MRE, et/ou d'au moins un autre équipement de réseau.

[0039] Dans l'exemple illustré d'un routeur périphérique de type « bout-en-bout », le module d'assurance MAE comporte également de préférence un troisième sous-module SM3 chargé d'observer le réseau, et notamment le trafic de type « bout-en-bout », en fonction de règles d'assurance qui lui sont dédiées. Par exemple, on dispose d'une sonde embarquée, pour effectuer

les mesures de bout-en-bout. Cette sonde embarquée est alors configurée de manière à déterminer le flux à étudier et les résultats des mesures alimentent des règles d'assurance dédiées. Par exemple, l'une de ces règles peut être : « si entre deux routeurs périphériques on mesure deux flux différents, alors on agrège la mesure des deux flux pour limiter le calcul ».

[0040] Dans ce cas, le troisième sous-module SM3 définit ce que l'homme de l'art appelle un agent de mesure de flux « bout-en-bout » (ou « end-to-end »).

[0041] Préférentiellement, le troisième sous-module SM3 délivre des données d'informations représentatives du résultat de ses observations (ou mesures) au (cinquième) sous-module de gestion (SM5), qui décide des actions à entreprendre en fonction de la politique d'assurance locale de son équipement NEI. Mais, on pourrait également envisager que le troisième sous-module SM3 alimente le deuxième sous-module SM2 en données d'informations, de sorte qu'il leur applique certaines des règles d'assurance et décide soit de leur envoi, soit de l'émission d'une alarme, à destination du NMS, et plus précisément d'un module de réception d'événements MRE, et/ou d'au moins un autre équipement de réseau.

[0042] Par ailleurs, et comme illustré sur la figure 2, le module d'assurance MAE peut comporter un quatrième sous-module SM4 chargé de gérer localement certains accords de niveau de service (ou SLA pour « Service Level Agreement »), en fonction de règles d'assurance qui lui sont dédiées. Par exemple, le sous-module SM4 connaît l'accord de niveau de service (SLA) d'un client, de sorte qu'il peut être chargé de vérifier si ce SLA est bien respecté, et générer une alarme (ou données d'informations) si ce n'est pas le cas (ou si la situation se dégrade).

[0043] Préférentiellement, le quatrième sous-module SM4 délivre des données d'informations représentatives de comptes-rendus de gestion au cinquième sous-module SM5, qui décide des actions à entreprendre en fonction de la politique d'assurance locale de son équipement NEI. Mais, on pourrait également envisager que le quatrième sous-module SM4 alimente le deuxième sous-module SM2 en données d'information, de sorte qu'il leur applique certaines des règles d'assurance et décide soit de leur envoi, soit de l'émission d'une alarme, à destination du NMS, et plus précisément d'un module de réception d'événements MRE, et/ou d'au moins un autre équipement de réseau.

[0044] Comme indiqué plusieurs fois ci-avant, le module d'assurance MAE comporte un cinquième sous-module SM5 (ou module de contrôle) chargé de contrôler le fonctionnement des autres sous-modules (ici SM1 à SM4). Plus préférentiellement, ce cinquième sous-module SM5 se présente sous la forme d'un moteur de règles (ou « rule engine ») dans lequel sont stockées toutes les règles d'assurance dédiées aux autres sous-modules. Il s'agit par exemple d'un « Java expert System Shell ».

[0045] Alors que chaque sous-module SM1 à SM4 effectue des calculs et/ou des analyses et/ou des rapports définis à partir de règles d'assurance dédiées, le cinquième sous-module SM5 gère préférentiellement l'ensemble desdites règles d'assurance dédiées. Par « gérer l'ensemble des règles », on entend ici gérer les conditions et les actions définies par les différentes règles.

[0046] Le cinquième sous-module SM5 a plus précisément deux fonctions principales.

[0047] Une première fonction consiste à ordonner au deuxième sous-module SM2 de générer une alarme, ou d'adresser un rapport, à destination de la couche NMS (ou d'un autre équipement du réseau), parce qu'en appliquant une règle d'assurance à des données délivrées par l'un des autres sous-modules SM1 à SM4, il s'est aperçu que la condition correspondante n'était pas satisfaite.

[0048] Par exemple, il ordonne la génération d'une alarme parce que les données d'analyse délivrées par le premier sous-module SM1 ne satisfont pas la condition qui leur est associée par la politique locale d'assurance, ou parce que le quatrième sous-module SM4 l'a averti qu'un SLA qu'il gère localement n'était pas respecté.

[0049] Une seconde fonction consiste à décider de l'adaptation de la configuration de l'équipement NEI, et notamment du module d'assurance embarqué MAE, en fonction des données d'informations qu'il reçoit des autres sous-modules SM1 à SM4 et des règles d'assurance qui définissent la politique locale d'assurance.

[0050] Par exemple, compte tenu des résultats d'analyse de certains paramètres du réseau, fournis par le premier sous-module SM1, le cinquième sous-module SM5 peut décider de modifier son mode d'analyse ou bien demander au deuxième sous-module SM2 d'adresser une alarme à la couche NMS de sorte qu'elle adresse de nouvelles formules d'analyse. Il peut également décider de modifier un calendrier d'analyses, par exemple effectuées par le premier sous-module SM1.

[0051] Lorsque le cinquième sous-module SM5 décide de modifier le fonctionnement (ou la configuration) de l'un des sous-modules SM1 à SM4, il lui adresse les instructions correspondantes, ce qui revient à lui demander de modifier ses calculs et/ou analyses et/ou rapports. De même, le cinquième sous-module SM5 peut, lorsque la politique locale l'y autorise, être chargé de rétroagir sur la configuration du routeur via un module de reconfiguration embarqué.

[0052] Il est important de noter que les actions de reconfiguration (ou de modification de fonctionnement) décidées par le cinquième sous-module SM5 sont définies par les règles d'assurance de la politique locale. En d'autres termes, le cinquième sous-module SM5 ne fait qu'ordonner l'exécution d'actions prédéfinies.

[0053] Le cinquième sous-module SM5 peut également appliquer des règles d'assurance choisies à des données d'information provenant d'autres équipements

de réseau NEI. En effet, un équipement NEI peut être chargé de transmettre des valeurs qu'il a mesurées et/ou agrégées à un autre équipement NEI équipé d'un dispositif D chargé de traiter ces valeurs de manière à générer de nouvelles données d'information qui peuvent être ensuite remontées au NMS ou envoyées à un autre équipement NEI.

[0054] La politique d'assurance locale peut être par exemple définie comme suit :

- si la tendance, estimée par le premier sous-module SM1, du nombre de paquets abandonnés augmente de plus de 5%, alors une alarme de tendance doit être émise,
- si la bande passante utilisée, analysée par le premier sous-module SM1, demeure inférieure à un premier seuil, alors la valeur de la bande passante utilisée doit être transmise chaque jour au module de collection MCC du NMS,
- si la bande passante utilisée, analysée par le premier sous-module SM1, est comprise entre un premier et un second seuil, alors la valeur moyenne de la bande passante utilisée doit être transmise toutes les heures au module de collection MCC du NMS,
- si l'intervalle de temps, estimé par le premier sous-module SM1, pour que la bande passante utilisée atteigne le second seuil, est inférieur à deux heures, alors une alarme de tendance doit être émise,
- si la charge de calcul (CPU) de l'équipement NEI, estimée par le premier sous-module SM1, est supérieure à 80%, alors les analyses de tendances ne doivent plus être effectuées,
- si la perte de paquets, estimée par le premier sous-module SM1, augmente de 5%, alors la taille des mémoires tampons (« buffers ») doit être augmentée de 5%.

[0055] En d'autres termes la politique d'assurance locale consiste ici, d'une première part, à transmettre chaque jour la mesure de la bande passante si le comportement de l'équipement NEI est normal, mais à activer les analyses de tendance et à augmenter la fréquence d'envoi des rapports si le comportement change, d'une deuxième part, à interrompre toutes les tâches impliquant un paramètre si la valeur de ce paramètre devient critique, et d'une troisième part, à modifier le fonctionnement interne de l'équipement NEI, représenté par un paramètre, en fonction de la variation dudit paramètre.

[0056] De préférence, le module d'assurance MAE est configurable à distance, via le réseau N, par le module de configuration MC du NMS. Plus précisément, chaque sous-module SM1 à SM5 est préférentiellement configurable. Cela permet en effet d'adapter à distance, le fonctionnement de chaque sous-module SM en fonction des circonstances, par exemple du fait de l'évolution du réseau N, et/ou en fonction des besoins, par exemple lorsque le gestionnaire d'assurance centralisé

du NMS a besoin de disposer des valeurs de nouveaux paramètres, ou de paramètres agrégés complémentaires, ou encore de nouvelles analyses réelles ou prospectives (envoi de nouvelles formules ou équations).

[0057] Deux modes de configuration peuvent être envisagés. Un premier mode consiste à transmettre indirectement les données de configuration au module d'assurance MAE via une interface de langage de programmation (ou API pour « Application Programming Interface ») implantée dans l'équipement NEI, ainsi qu'éventuellement via la MIB. Cette interface API peut également, et avantageusement, permettre au module de configuration MC du NMS de configurer ou de programmer la MIB, de sorte qu'elle ne soit pas de type statique. Le module d'assurance MAE peut en effet coopérer avec la MIB pour se configurer et définir de nouvelles entrées dans la MIB, afin de pouvoir accéder à ces nouvelles entrées. Dans ce cas, on accède à la MIB via des requêtes SNMP (« GET » et « SET »), ce qui permet une configuration aisée (voire même une gestion des droits et de la sécurité des échanges avec SNMP 3); la MIB permet d'avoir une interface « normalisée » du fait que ses champs sont accessibles via des OIDs (pour « Object Identifiers ») bien définis. On entend ici par « Object Identifier », un identifiant objet d'une variable MIB que l'on souhaite récupérer. Un tel identifiant est généralement normalisé, par exemple par le standard RFC 1213 pour la MIB II.

[0058] Un second mode consiste à transmettre directement les données de configuration au module d'assurance MAE à l'aide de commandes dédiées, telles que des « Command Line Interface » (ou CLI).

[0059] Le module d'assurance MAE peut être réalisé sous la forme de circuits électroniques, de modules logiciels (ou informatiques), ou d'une combinaison de circuits et de logiciels.

[0060] L'invention ne se limite pas aux modes de réalisation de dispositif de gestion locale d'assurance et d'équipement de réseau décrits ci-avant, seulement à titre d'exemple, mais elle englobe toutes les variantes que pourra envisager l'homme de l'art dans le cadre des revendications ci-après.

[0061] Ainsi, dans ce qui précède on a décrit des équipements de réseau capables de gérer localement le procédé d'assurance supervisé par le NMS. Mais, on peut envisager un fonctionnement distribué dans lequel certains au moins des équipements de réseau sont équipés de dispositifs de gestion locale d'assurance simplifiés, chargés de transmettre des alarmes et/ou des données d'informations spécifiques et complémentaires à un serveur d'assurance du NMS. Bien entendu, dans ce cas les équipements de réseau demeurent capables d'adapter leur configuration en fonction des valeurs des données de gestion stockées dans leur MIB.

[0062] Par ailleurs, on a décrit un mode de réalisation dans lequel le dispositif selon l'invention était implanté ou embarqué dans l'équipement de réseau. Mais, le dispositif selon l'invention peut être agencé sous la forme

d'un élément externe implanté dans un boîtier directement raccordé à l'équipement de réseau.

7 Revendications

1. Dispositif (D) de gestion locale d'assurance pour un équipement de réseau (NE) d'un réseau de communications (N) équipé d'un système de gestion de réseau (NMS), ledit équipement (NE) présentant une configuration choisie et comportant des moyens (MM) de mesure de valeurs de paramètre (s) du réseau et une base d'informations de gestion (MIB) propre à stocker des données de gestion représentatives desdites valeurs mesurées, **caractérisé en ce qu'il comprend des moyens de gestion (MAE) agencés pour adapter la configuration dudit équipement (NE) en fonction d'au moins lesdites données de gestion stockées dans ladite base d'informations de gestion (MIB) et de règles, dites d'assurance, choisies, définissant une politique locale d'assurance, ladite adaptation consiste en une modification d'une politique de mesure de paramètre (s) et/ou une modification d'une politique d'envoi de rapport audit système de gestion de réseau (NMS).**
2. Dispositif selon la revendication 1, **caractérisé en ce que** lesdits moyens de gestion (MAE) sont agencés pour adapter ladite configuration en fonction de données d'informations provenant d'au moins un autre équipement de réseau (NE).
3. Dispositif selon l'une des revendications 1 et 2, **caractérisé en ce que** ladite adaptation consiste en une modification de son mode de fonctionnement.
4. Dispositif selon l'une des revendications 1 à 3, **caractérisé en ce que** lesdits moyens de gestion (MAE) comprennent des moyens d'analyse (SM1) agencés pour déterminer, en fonction de certaines desdites règles d'assurance choisies, des données d'information représentatives de l'évolution temporelle, sur un intervalle choisi, de valeurs de paramètre(s) du réseau stockées dans ladite base d'informations de gestion (MIB).
5. Dispositif selon la revendication 4, **caractérisé en ce que** lesdits moyens d'analyse (SM1) sont agencés pour délivrer des données d'information représentatives d'une analyse de tendance et/ou d'une analyse de profils ou de signatures et/ou d'une analyse de discontinuité et/ou d'une agrégation de valeurs de paramètres du réseau.
6. Dispositif selon l'une des revendications 4 et 5, **caractérisé en ce que** lesdits moyens d'analyse (SM1) sont configurables.

7. Dispositif selon la revendication 6, **caractérisé en ce que** lesdits moyens d'analyse (SM1) sont agencés pour mettre en oeuvre de nouveaux calculs, relatifs aux paramètres du réseau, reçus dudit système de gestion de réseau (NMS). 7
8. Dispositif selon l'une des revendications 1 à 7, **caractérisé en ce que** lesdits moyens de gestion (MAE) comprennent des moyens d'alarme (SM2) propres à déclencher l'envoi d'une alarme et/ou de données d'information audit système de gestion de réseau (NMS) et/ou à au moins un autre équipement de réseau (NE), en fonction de certaines desdites règles d'assurance choisies. 10
9. Dispositif selon la revendication 8, **caractérisé en ce que** lesdits moyens d'alarme (SM2) sont configurables. 15
10. Dispositif selon l'une des revendications 8 et 9, **caractérisé en ce que** lesdites données d'information et lesdites alarmes sont représentatives d'un résultat d'analyse, effectuée par lesdits moyens d'analyse (SM1), et/ou d'une agrégation de données, effectuée par lesdits moyens d'analyse (SM1), et/ou d'une valeur de paramètre du réseau stockée dans ladite base d'informations de gestion (MIB). 20
11. Dispositif selon l'une des revendications 1 à 10, **caractérisé en ce que** lesdits moyens de gestion (MAE) comprennent des moyens d'observation du réseau (SM3) définissant un agent de mesure de flux de type « bout-en-bout », et agencés pour déterminer des données d'information représentatives dudit flux de type bout-en-bout en fonction de certaines desdites règles d'assurance choisies. 25
12. Dispositif selon la revendication 11, **caractérisé en ce que** lesdits moyens d'observation du réseau (SM3) sont configurables. 30
13. Dispositif selon l'une des revendications 1 à 12, **caractérisé en ce que** lesdits moyens de gestion (MAE) comprennent des moyens de gestion d'accords de niveau de service (SM4) agencés pour déterminer des données d'information représentatives de ladite gestion des accords en fonction de certaines desdites règles d'assurance choisies. 35
14. Dispositif selon la revendication 13, **caractérisé en ce que** lesdits moyens de gestion d'accords de niveau de service (SM4) sont configurables. 40
15. Dispositif selon l'une des revendications 2 à 14, **caractérisé en ce que** lesdits moyens de gestion (MAE) comprennent des moyens de contrôle (SM5) propres à gérer le fonctionnement desdits moyens d'analyse (SM1), desdits moyens d'alarme (SM2), 45
- desdits moyens d'observation du réseau (SM3) et desdits moyens de gestion d'accords de niveau de service (SM4), en fonction de certaines au moins desdites règles d'assurance choisies.
16. Dispositif selon la revendication 15, **caractérisé en ce que** lesdits moyens de contrôle (SM5) sont alimentés en données d'information par lesdits moyens d'analyse (SM1) et/ou lesdits moyens d'observation du réseau (SM3) et/ou lesdits moyens de gestion d'accords de niveau de service (SM4), et sont agencés pour ordonner auxdits moyens d'alarme (SM2) de générer des alarmes et/ou des rapports en cas de détection du non respect d'une règle d'assurance par des données d'information reçues. 50
17. Dispositif selon l'une des revendications 15 et 16, **caractérisé en ce que** lesdits moyens de contrôle (SM5) sont agencés sous la forme d'un moteur de règles (« rule engine ») stockant lesdites règles d'assurance choisies. 55
18. Dispositif selon l'une des revendications 15 à 17, **caractérisé en ce que** lesdits moyens de contrôle (SM5) sont configurables. 60
19. Dispositif selon l'une des revendications 1 à 18, **caractérisé en ce que** lesdits moyens de gestion (MAE) sont propres à être configurés par ledit système de gestion de réseau (NMS) via une interface de langage de programmation (API) dudit équipement (NE). 65
20. Dispositif selon l'une des revendications 1 à 19, **caractérisé en ce que** lesdits moyens de gestion (MAE) sont propres à être configurés par ledit système de gestion de réseau (NMS) via une interface de langage de programmation (API) dudit équipement (NE) et via ladite base d'informations de gestion (MIB). 70
21. Dispositif selon l'une des revendications 19 et 20, **caractérisé en ce que** lesdits moyens d'analyse (SM1) et/ou lesdits moyens d'alarme (SM2) et/ou lesdits moyens d'observation du réseau (SM3) et/ou lesdits moyens de contrôle (SM5) et/ou lesdits moyens de gestion d'accords de niveau de service (SM4) sont propres à être configurés par ledit système de gestion de réseau (NMS), via ladite interface de langage de programmation (API). 75
22. Dispositif selon l'une des revendications 19 et 20, **caractérisé en ce que** lesdits moyens d'analyse (SM1) et/ou lesdits moyens d'alarme (SM2) et/ou lesdits moyens d'observation du réseau (SM3) et/ou lesdits moyens de contrôle (SM5) et/ou lesdits moyens de gestion d'accords de niveau de service (SM4) sont propres à être configurés par ledit sys-

tème de gestion de réseau (NMS), via ladite interface de langage de programmation (API) et via ladite base d'informations de gestion (MIB).

ce qu'il comprend une multiplicité d'équipements de réseau (NE) selon l'une des revendications 26 à 29.

23. Dispositif selon l'une des revendications 1 à 22, **caractérisé en ce que** lesdits moyens de gestion (MAE) sont propres à être configurés par ledit système de gestion de réseau (NMS) via des commandes dédiées.

27 31. Réseau selon la revendication 30, **caractérisé en ce que** chaque équipement (NE) est agencé pour délivrer audit système de gestion de réseau (NMS) des alarmes et/ou des données d'information de types différents.

24. Dispositif selon la revendication 23, **caractérisé en ce que** lesdits moyens d'analyse (SM1) et/ou lesdits moyens d'alarme (SM2) et/ou lesdits moyens d'observation du réseau (SM3) et/ou desdits moyens de gestion d'accords de niveau de service (SM4) et/ou lesdits moyens de contrôle (SM5) sont agencés pour être configurés par ledit système de gestion de réseau (NMS) via des commandes dédiées.

30 32. Utilisation des dispositif, équipement et réseau de communications selon l'une des revendications précédentes dans les technologies réseaux devant être gérées.

25. Dispositif selon l'une des revendications 23 et 24, **caractérisé en ce que** lesdites commandes sont de type « Command Line Interface ».

33 33. Utilisation selon la revendication 32, **caractérisé en ce que** lesdites technologies réseaux sont choisies dans un groupe comprenant les réseaux de transmission, en particulier de type WDM, SONET et SDH, de données, en particulier de type Internet-IP et ATM, et de voix, en particulier de type classique, mobile et NGN.

26. Equipement de réseau (NE) pour un réseau de communications (N) équipé d'un système de gestion de réseau (NMS), ledit équipement (NE) présentant une configuration choisie et comportant des moyens (MM) de mesure de valeurs de paramètre (s) du réseau et une base d'informations de gestion (MIB) propre à stocker des données de gestion représentatives desdites valeurs mesurées, **caractérisé en ce qu'il comprend un dispositif (D) selon l'une des revendications précédentes.**

35 25 30

27. Equipement selon la revendication 26, **caractérisé en ce qu'il comprend une interface de langage de programmation (API), et en ce que** ladite base d'informations de gestion (MIB) est propre à être configurée par ledit système de gestion de réseau (NMS) via ladite interface de langage de programmation (API).

35 40

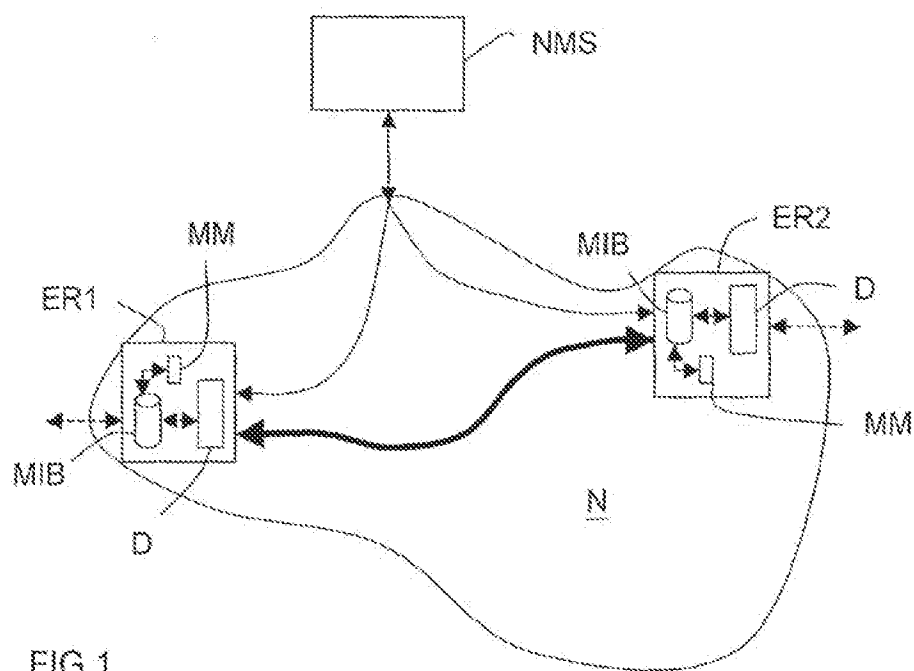
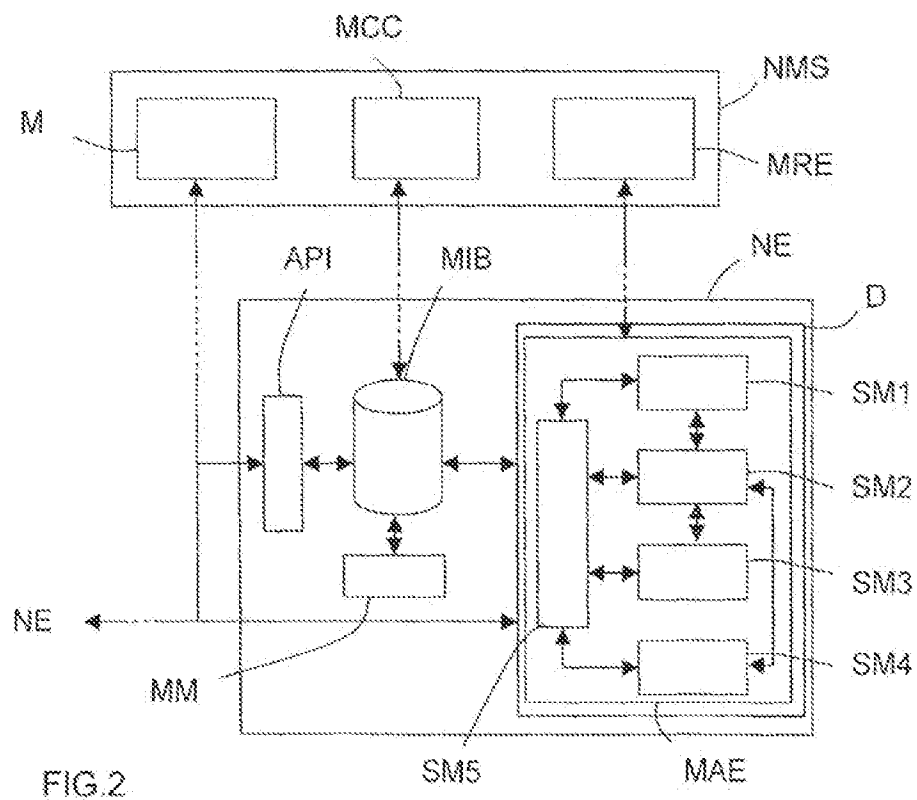
28. Equipement selon l'une des revendications 26 et 27, **caractérisé en ce qu'il comprend une interface de langage de programmation (API), et en ce que** ladite base d'informations de gestion (MIB) est propre à être programmée par ledit système de gestion de réseau (NMS) via ladite interface de langage de programmation (API).

45 50

29. Equipement selon l'une des revendications 26 à 28, **caractérisé en ce qu'il est choisi dans un groupe comprenant au moins les routeurs, les commutateurs et les pare-feu.**

55

30. Réseau de communications (N) comportant un système de gestion de réseau (NMS), **caractérisé en**





Office européen
des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 04 29 0706

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (HPLC.7)
X	HO L L ET AL: "REAL-TIME PERFORMANCE MONITORING AND ANOMALY DETECTION IN THE INTERNET: AN ADAPTIVE, OBJECTIVE-DRIVEN, MIX-AND-MATCH APPROACH" BELL LABS TECHNICAL JOURNAL, WILEY, CA, US, vol. 4, no. 4, octobre 1999 (1999-10), pages 23-40, XP000902469 ISSN: 1089-7689 * abrégé * * page 24, colonne de droite - page 35, colonne de droite * * page 38, colonne de droite, alinéa 2 - page 39, colonne de gauche, alinéa 1 * -----	1-33	H04L12/24 H04L12/26
X	US 6 272 537 B1 (KEKIC MIODRAG M ET AL) 7 août 2001 (2001-08-07) * colonne 7, ligne 20 - ligne 65 * * colonne 8, ligne 42 - colonne 9, ligne 8 * * colonne 13, ligne 50 - colonne 85, ligne 11 * -----	1-33	DOMAINES TECHNIQUES RECHERCHES (HPLC.7)
X	FR 2 774 191 A (INST EURECOM) 30 juillet 1999 (1999-07-30) * abrégé * * page 1, ligne 2 - ligne 8 * * page 3, ligne 5 - ligne 7 * * page 3, ligne 12 - ligne 17 * * page 4, ligne 12 - ligne 17 * * page 5, ligne 1 - page 6, ligne 3 * * page 7, ligne 1 - ligne 12 * * page 11, ligne 12 - page 16, ligne 6 * * figures 2,6,7 * ----- -/-	1-33	H04L
Le présent rapport a été établi pour toutes les revendications			
Lieu de la recherche	Date d'achèvement de la recherche	Examinateur	
Munich	27 juillet 2004	Le Bras, P	
CATÉGORIE DES DOCUMENTS CITÉS		T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande U : cité pour d'autres raisons S : membre de la même famille, document correspondant	
X : particulièrement pertinent à lui seul V : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non écrite P : document prioritaire			

EP 04 29 0706 (1999-07-30)



Office européen
des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande

EP 04 29 0706

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication poursuivie	CLASSEMENT DE LA DEMANDE (int.Cl.7)
X	US 6 085 243 A (BANTHIA PRAKASH C ET AL) 4 juillet 2000 (2000-07-04) * abrégé * * colonne 1, ligne 17 - ligne 20 * * colonne 3, ligne 52 - colonne 5, ligne 10 * * colonne 5, ligne 52 - ligne 54 * * colonne 5, ligne 65 - colonne 6, ligne 26 * * colonne 6, ligne 44 - ligne 45 * * colonne 7, ligne 12 - ligne 23 * * colonne 8, ligne 14 - colonne 10, ligne 58 * * colonne 12, ligne 2 - ligne 4 * * colonne 14, ligne 11 - ligne 21 * *****	1-33	
			DOMAINES TECHNIQUES RECHERCHES (int.Cl.7)
Le présent rapport a été établi pour toutes les revendications			
Lieu de la recherche		Date d'établissement de la recherche	Examineur
Munich		27 juillet 2004	Le Bras, P
CATEGORIE DES DOCUMENTS CITES X : particulièrement pertinent à lui seul ✓ : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : artère plan technologique O : divulgation non écrite P : document prioritaire T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant			

EPO: 12694 1505 03 05 (PRAK02)

**ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE
RELATIF A LA DEMANDE DE BREVET EUROPEEN NO.**

EP 04 29 0706

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.

Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

27-07-2004

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 6272537	B1	07-08-2001	AUCUN	
FR 2774191	A	30-07-1999	FR 2774191 A1	30-07-1999
US 6085243	A	04-07-2000	AU 5661198 A	03-07-1998
			CA 2275235 A1	18-06-1998
			EP 0956680 A1	17-11-1999
			GB 2335124 A	08-09-1999
			WO 9826541 A1	18-06-1998
			US 5922044 A	13-07-1999
			US 6069274 A	28-12-1999
			US 6108782 A	22-08-2000
			WO 9843170 A1	01-10-1998

Pour tout renseignement concernant cette annexe, voir Journal Officiel de l'Office européen des brevets, No 12/02



(11) **EP 1 739 518 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication: **03.01.2007 Bulletin 2007/01** (51) Int Cl.: **G06F 1/00 (2006.01)**

(21) Application number: **05254068.9**

(22) Date of filing: **29.06.2005**

<p>(84) Designated Contracting States: AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR Designated Extension States: AL BA HR LV MK YU</p> <p>(71) Applicant: Research In Motion Limited Waterloo, Ontario N2L 3W8 (CA)</p> <p>(72) Inventors: • Adams, Neil P. Waterloo Ontario N2K 4E4 (CA)</p>	<p>• Little, Herbert A. Waterloo Ontario N2T 2V8 (CA)</p> <p>(74) Representative: Roberts, Gwilym Vaughan et al Kilburn & Strode 20 Red Lion Street London WC1R 4JP (GB)</p>
---	---

(54) **System and method for privilege management and revocation**

(57) The present disclosure relates generally to the management of privileges associated with certain applications that are accessible by users of electronic equipment, such as, for example, networked computers, mobile wireless communications devices, and the like. In particular, the disclosure is directed to systems and methods for managing privileges associated with particular applications and for revoking these privileges in a timely and robust manner. For example, the device keeps track of which applications get access to which privileges. When policies or application control changes, the system detects which privileges have been revoked for which

applications. This can be accomplished by simply comparing the old set of privileges with the new set of privileges. For each revoked privilege for a given application, the system determiner if the application has ever accessed that privilege in the past. If an application has accessed a privilege that is now revoked at any time in the past, the device is reset. To ensure that privileges that may be passed between applications are not overlooked, the device is arranged to perform a reset if any revoked privilege accessible by the device is one that may be passed between applications.

EP 1 739 518 A1

Description

BACKGROUND

1. Field of the Invention

[0001] The present invention relates generally to the management of privileges associated with certain applications that are accessible by users of electronic equipment, such as, for example, networked computers, mobile wireless communications devices, and the like. In particular, the disclosure is directed to systems and methods for managing privileges associated with particular applications and for revoking these privileges in a timely and robust manner.

2. Related Art

[0002] It is well known that certain electronic equipment, such as, for example, networked computers, mobile wireless communications devices, and the like, include applications resident on such equipment that may have access to certain privileges that enable the applications to perform various functions. Typically, a system administrator may use IT policy and application control to set the privileges associated with various applications present on the equipment that is subject to the administrator's control. Examples of privileges may include, for example, allowing an application to use inter-process communication (IPC), enabling the opening of internal and external connections, enabling the injection of browser filters, enabling Bluetooth™ functionality, enabling use of e-mail, enabling the use of personal information management (PIM) functionality, use of application program interface (API), etc. It is important for the system administrator be able to track which applications have access to which privileges, and to be able to revoke privileges on an as needed basis.

[0003] For example, if an application has access to a privilege, and the system administrator revokes that privilege, the application should immediately, or within a small window of time, be denied access to that privilege. In other words, the privilege should be revoked as soon as possible. Events that might trigger a revocation of privileges may include, for example, an application being loaded before the IT administrator/application control data is present on the device, an application is discovered to be a rogue application, or company policy changes, resulting in limiting the use or availability of certain applications and/or privileges associated therewith.

[0004] Regardless of the reason for privilege revocation, such revocation must be accomplished in a secure manner and in a manner that prevents possible work arounds by malicious applications or individuals. In general, according to current privilege revocation schemes, privilege checking is typically performed on the first access to a privilege. For example, applications communicate with IPC using the application registry. Once an ap-

plication has a reference (e.g., pointer) to the application registry, it is difficult to take this reference away from the application. In another example, if an application has passed some of its privileges to another application using IPC, conventional systems can detect that the first application has access to IPC, but there is no way to detect that the other application has been passed the privilege(s).

[0005] Therefore, there remains a need for a system and method for effectively managing privileges associated with applications, and in particular, when privilege revocation is required, to revoke these privileges in a timely and robust manner.

SUMMARY

[0006] In view of the foregoing, we have now identified an efficient, accurate, robust and easy to implement system and method for managing privileges associated with particular applications and for revoking these privileges in a timely and reliable manner.

[0007] According to an exemplary embodiment an application having privileges that are to be revoked may be shut down. When this application is restarted, access to revoked privileges will be denied. In order to keep track of which applications need to be shut down and reset, the system must keep track of which applications have accessed which privileges. To enable monitoring of the privileges accessed by applications, each time an application uses a privilege, the system records the application identifier and which privilege has been accessed. This may be done in any of a number of conventional methods, such as, for example, a data table listing the application identifier and corresponding accessed privilege(s) associated with the application identifier. When the system administrator, or any other authority, institutes a change in privileges, the system accesses the record of which applications have accessed which privileges. A comparison of accessed privileges with the privileges to be revoked is performed. Each application that has accessed a privilege that is to be revoked is identified by the system and then shut down. When the application is restarted, the application will not have access to any of the revoked privileges.

[0008] In another embodiment, a device reset may be performed. By resetting a device, the system is brought to a known state. According to this embodiment, a system administrator, or any other authority, specifies that a device must be reset when a new policy that revokes (or changes) privileges is instituted. A device reset may be instituted at any time the administrator or authority deems it necessary to do so. For example, a device reset may be done whenever a new policy that includes privilege revocation is instituted. However, this may result in numerous unnecessary device reset events that are potentially inconvenient to the user and may interfere with use of the device. Alternatively, the system may keep track of which devices include which applications, and use this

information to determine a less intrusive device reset schedule. For example, resetting only those devices having applications that may potentially be affected by the policy change.

[0009] In yet another advantageous embodiment, aspects of previously described embodiments are combined to provide effective privilege management and revocation. According to this exemplary embodiment, the system administrator or other authority has no actual control over when a device is reset. The administrator merely manages the privileges of the system and particular applications. The device itself is responsible for resetting when necessary. In this embodiment, the device keeps track of which applications get access to which privileges. When policies or application control changes, the system detects which privileges have been revoked for which applications. This can be accomplished by simply comparing the old set of privileges with the new set of privileges. For each revoked privilege for a given application, the system determines if the application has ever accessed that privilege in the past. As noted above, the system has been keeping track of these since the system was first started up. If an application has accessed a privilege that is now revoked at any time in the past, the device is reset. For some privileges (e.g., IPC), it still cannot be determined whether a privilege has been used as a result of being passed from another application. To overcome the potential for missing a revocation of privileges when applications pass privileges between themselves, if, for example, IPC (or any other privilege that is able to be passed between applications) is revoked from any application, regardless of if the system has detected that the application has accessed the privilege, the device must be reset. This reset will bring the device back to a known state. Device reset will only be done when necessary, thus limiting the number of resets and solving the problem associated with privileges that have been passed between applications.

[0010] Each of these embodiments is useful in a variety of privilege management environments ranging from a low-level low-priority where a modest level of privilege revocation security is needed, resulting in a less robust system, to a highly important ultra-robust environment where user inconvenience is secondary to the need for absolute certainty of privilege revocation.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] These and other embodiments along with their attendant advantages are described herein with reference to the following drawings in which like reference numerals refer to like elements, and wherein:

FIG. 1 is a block diagram showing a computer network and communication system in which electronic devices running applications having access to associated privileges are used;

FIG. 2 is a block diagram of a wireless mobile communication device as an example of an electronic device running applications having access to associated privileges;

FIG. 3 is a flow diagram illustrating a method of revoking privileges according to an exemplary embodiment;

FIG. 4 is a flow diagram illustrating a method of revoking privileges according to another exemplary embodiment; and

FIG. 5 is a flow diagram illustrating yet another method of revoking privileges according to another exemplary embodiment.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

[0012] FIG. 1 is a block diagram showing a computer network and communication system in which electronic devices running applications having access to associated privileges are used. The computer network 18 includes, for example, various networked computers 28 and, optionally, a message server 26, all linked via a Local Area Network (LAN) 30. The communication system includes a Wide Area Network (WAN) 12 coupled to a computer system 14, a wireless network gateway 16 and the LAN 30 of the computer network 18. The wireless network gateway 16 is also connected to a wireless communication network 20 in which a wireless mobile communication device 22 (hereinafter "mobile device"), is configured to operate. The entire system 10 is typically managed by, among others, a system administrator or like authority 32.

[0013] The computer system 14 may be a desktop or laptop personal computer that is configured to communicate with the WAN 12 or any other suitable network, such as, for example, the Internet. Personal computers, such as the computer system 14, typically access the Internet via an Internet Service Provider (ISP), Application Service Provider (ASP), or the like.

[0014] The LAN 30 is an example of a typical working computer network environment, in which multiple computers 28 are connected in a network. The computer network 18 is typically located behind a security firewall 24. Within the LAN 30, a message server 26, operating on a computer behind the firewall 24 may act as the primary interface for the owner of the computer network 18 to exchange messages both within the LAN 30 and with other external messaging clients via the WAN 12. Known message servers include, for example, Microsoft Outlook™, Lotus Notes™, Yahoo!™ Messenger, AOL Instant Messenger, or any other client-server or peer-to-peer, or similar messaging clients with various architectures. Messages received by the message server 26 are distributed to mailboxes for user accounts addressed in

the received messages, and are then accessed by a user through a messaging client operating on a computer system 28. The foregoing is merely an exemplary description illustrating a client-server architecture, and in no way implies that such architecture is necessary, as other suitable architectures known to those skilled in the art may be used.

[0015] Although only a message server 26 is shown in the LAN 30, those skilled in the art will appreciate that a LAN may include other types of servers supporting resources that are shared between the networked computer systems 28, and that the message server 26 may also provide additional functionality, such as dynamic database storage for data such as, but not limited to, calendars, to-do lists, task lists, e-mail and documentation. The message server 26 and electronic messaging are described for illustrative purposes only. Systems and methods for managing and revoking privileges are applicable to a wide range of electronic devices, and are in no way limited to electronic devices with messaging capabilities.

[0016] The wireless gateway 16 provides an interface to a wireless network 20, through which messages may be exchanged with a mobile device 22. Such functions as addressing of the mobile device 22, encoding or otherwise transforming messages for wireless transmission, and any other interface functions are performed by the wireless gateway 16. The wireless gateway 16 may be configured to operate with more than one wireless network 20, in which case the wireless gateway 16 also determines a most likely network for locating a given mobile device 22 and possibly track mobile devices as users roam between countries or networks.

[0017] The mobile device 22 is, for example, a data communication device, a voice communication device, a dual-mode communication device such as many modem cellular telephones having both data and voice communications functionality, a multiple-mode device capable of voice, data and other types of communications, a personal digital assistant (PDA) enabled for wireless communications, or a laptop or desktop computer system with a wireless modem.

[0018] Any computer system with access to the WAN 12 may exchange messages with the mobile device 22 through the wireless network gateway 16. Alternatively, private wireless network gateways such as wireless Virtual Private Network (VPN) routers could be implemented to provide a private interface to a wireless network. A wireless VPN router implemented in the LAN 30 provides a private interface from the LAN 30 to one or more mobile devices such as 22 through the wireless network 20. A private interface to a mobile device 22 may also effectively be extended to entities outside the LAN 30 by providing a message forwarding or redirection system that operates with the message server 26. Such a message redirection system is disclosed in United States Patent No. 6,219,694, which is hereby incorporated into this application by reference. In this type of system, incoming

messages received by the message server 26 and addressed to a user of a mobile device 22 are sent through the wireless network interface, either a wireless VPN router, the wireless gateway 16, or another interface, for example, to the wireless network 20 and to the user's mobile device 22. Another alternate interface to a user's mailbox on a message server 26 may be a Wireless Application Protocol (WAP) gateway. Through a WAP gateway, a list of messages in a user's mailbox on the message server 26, and possibly each message or a portion of each message, may be sent to the mobile device 22. A wireless network 20 normally delivers messages to and from communication devices such as the mobile device 22 via RF transmissions between base stations and devices. The wireless network 20 may, for example, be a data-centric wireless network, a voice-centric wireless network, or a dual-mode network that can support both voice and data communications over the same infrastructure. Recently developed networks include Code Division Multiple Access (CDMA) networks and General Packet Radio Service (GPRS) networks. So-called third-generation (3G) networks like Enhanced Data rates for Global Evolution (EDGE) and Universal Mobile Telecommunications Systems (UMTS) are currently under development. Older data-centric networks include, but are not limited to, the Mobitex™ Radio Network ("Mobitex"), and the DataTAC™ Radio Network ("DataTAC"). Voice-centric data networks such as Personal Communication System (PCS) networks, including Global System for Mobile Communications (GSM) and Time Division Multiple Access (TDMA) systems, have been available in North America and world-wide for several years.

[0019] FIG. 2 is a block diagram of an exemplary wireless mobile communication device as an example of an electronic device. However, it should be understood that the systems and methods disclosed herein may be used with many different types of devices, such as personal digital assistants (PDAs), desktop computers, or the like.

[0020] The mobile device 500 is preferably a two-way communication device having at least voice and data communication capabilities. The mobile device 500 preferably has the capability to communicate with other computer systems on the Internet. Depending on the functionality provided by the mobile device, the mobile device may be referred to as a data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device (with or without telephony capabilities). As mentioned above, such devices are referred to generally herein as mobile devices.

[0021] The mobile device 500 includes a transceiver 511, a microprocessor 538, a display 522, non-volatile memory 524, random access memory (RAM) 526, auxiliary input/output (I/O) devices 528, a serial port 530, a keyboard 532, a speaker 534, a microphone 536, a short-range wireless communications subsystem 540, and may also include other device sub-systems 542. The transceiver 511 preferably includes transmit and receive

antennas 516, 518, a receiver (Rx) 512, a transmitter (Tx) 514, one or more local oscillators (LOs) 513, and a digital signal processor (DSP) 520. Within the non-volatile memory 524, the mobile device 500 includes a plurality of software modules 524A-524N that can be executed by the microprocessor 538 (and/or the DSP 520), including a voice communication module 524A, a data communication module 524B, and a plurality of other operational modules 524N for carrying out a plurality of other functions.

[0022] The mobile device 500 is preferably a two-way communication device having voice and data communication capabilities. Thus, for example, the mobile device 500 may communicate over a voice network, such as any of the analog or digital cellular networks, and may also communicate over a data network. The voice and data networks are depicted in FIG. 2 by the communication tower 519. These voice and data networks may be separate communication networks using separate infrastructure, such as base stations, network controllers, etc., or they may be integrated into a single wireless network. References to the network 519 should therefore be interpreted as encompassing both a single voice and data network and separate networks.

[0023] The communication subsystem 511 is used to communicate with the network 519. The DSP 520 is used to send and receive communication signals to and from the transmitter 514 and receiver 512, and also exchange control information with the transmitter 514 and receiver 512. If the voice and data communications occur at a single frequency, or closely-spaced set of frequencies, then a single LO 513 may be used in conjunction with the transmitter 514 and receiver 512. Alternatively, if different frequencies are utilized for voice communications versus data communications or the mobile device 500 is enabled for communications on more than one network 519, then a plurality of LOs 513 can be used to generate frequencies corresponding to those used in the network 519. Although two antennas 516, 518 are depicted in FIG. 2, the mobile device 500 could be used with a single antenna structure. Information, which includes both voice and data information, is communicated to and from the communication module 511 via a link between the DSP 520 and the microprocessor 538,

[0024] The detailed design of the communication subsystem 511, such as frequency band, component selection, power level, etc., is dependent upon the communication network 519 in which the mobile device 500 is intended to operate. For example, a mobile device 500 intended to operate in a North American market may include a communication subsystem 511 designed to operate with the Mobitex or DataTAC mobile data communication networks and also designed to operate with any of a variety of voice communication networks, such as AMPS, TDMA, CDMA, PCS, etc., whereas a mobile device 500 intended for use in Europe may be configured to operate with the GPRS data communication network and the GSM voice communication network. Other types

of data and voice networks, both separate and integrated, may also be utilized with the mobile device 500.

[0025] Communication network access requirements for the mobile device 500 also vary depending upon the type of network 519. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each device. In GPRS data networks, however, network access is associated with a subscriber or user of the mobile device 500. A GPRS device typically requires a subscriber identity module ("SIM"), which is required in order to operate the mobile device 500 on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM, but the mobile device 500 is unable to carry out functions involving communications over the network 519, other than any legally required operations, such as '911' emergency calling.

[0026] After any required network registration or activation procedures have been completed, the mobile device 500 is able to send and receive communication signals, preferably including both voice and data signals, over the network 519. Signals received by the antenna 516 from the communication network 519 are routed to the receiver 512, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation and decoding, to be performed using the DSP 520. In a similar manner, signals to be transmitted to the network 519 are processed, including modulation and encoding, for example, by the DSP 520 and are then provided to the transmitter 514 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 519 via the antenna 518. Although a single transceiver 511 is shown for both voice and data communications, in alternative embodiments, the mobile device 500 may include multiple distinct transceivers, such as a first transceiver for transmitting and receiving voice signals, and a second transceiver for transmitting and receiving data signals, or a first transceiver configured to operate within a first frequency band, and a second transceiver configured to operate within a second frequency band.

[0027] In addition to processing the communication signals, the DSP 520 also provides for receiver and transmitter control. For example, the gain levels applied to communication signals in the receiver 512 and transmitter 514 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 520. Other transceiver control algorithms could also be implemented in the DSP 520 in order to provide more sophisticated control of the transceiver 511.

[0028] The microprocessor 538 preferably manages and controls the overall operation of the mobile device 500. Many types of microprocessors or microcontrollers could be used here, or, alternatively, a single DSP 520

could be used to carry out the functions of the microprocessor 538. Low-level communication functions, including at least data and voice communications, are performed through the DSP 520 in the transceiver 511. High-level communication applications, including the voice communication application 524A, and the data communication application 524B are stored in the non-volatile memory 524 for execution by the microprocessor 538. For example, the voice communication module 524A may provide a high-level user interface operable to transmit and receive voice calls between the mobile device 500 and a plurality of other voice devices via the network 519. Similarly, the data communication module 524B may provide a high-level user interface operable for sending and receiving data, such as e-mail messages, files, organizer information, short text messages, etc., between the mobile device 500 and a plurality of other data devices via the network 519.

[0029] The microprocessor 538 also interacts with other device subsystems, such as the display 522, RAM 526, auxiliary I/O devices 528, serial port 530, keyboard 532, speaker 534, microphone 536, a short-range communications subsystem 540 and any other device subsystems generally designated as 542. For example, the modules 524A-N are executed by the microprocessor 538 and may provide a high-level interface between a user of the mobile device and the mobile device. This interface typically includes a graphical component provided through the display 522, and an input/output component provided through the auxiliary I/O devices 528, keyboard 532, speaker 534, or microphone 536. Additionally, the microprocessor 538 is capable of running a variety of applications that may be present in the device non-volatile memory 524, including applications that have access to various privileges, as will be described in more detail herein.

[0030] Some of the subsystems shown in FIG. 2 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as keyboard 532 and display 522 may be used for both communication-related functions, such as entering a text message for transmission over a data communication network, and device-resident functions such as a calculator or task list or other PDA type functions.

[0031] Operating system software used by the microprocessor 538 is preferably stored in a persistent store such as the non-volatile memory 524. In addition to the operating system and communication modules 524A-N, the non-volatile memory 524 may include a file system for storing data. The non-volatile memory 524 may also include data stores for owner information and owner control information. The operating system, specific device applications or modules, or parts thereof, may be temporarily loaded into a volatile store, such as RAM 526 for faster operation. Moreover, received communication signals may also be temporarily stored to RAM 526, before permanently writing them to a file system located in the

non-volatile memory 524. The non-volatile memory 524 may be implemented, for example, with Flash memory, non-volatile RAM, or battery backed-up RAM.

[0032] An exemplary application module 524N that may be loaded onto the mobile device 500 is a PIM application providing PDA functionality, such as calendar events, appointments, and task items. This module 524N may also interact with the voice communication module 524A for managing phone calls, voice mails, etc., and may also interact with the data communication module 524B for managing e-mail communications and other data transmissions. Alternatively, all of the functionality of the voice communication module 524A and the data communication module 524B may be integrated into the PIM module.

[0033] The non-volatile memory 524 preferably provides a file system to facilitate storage of PIM data items on the device. The PIM application preferably includes the ability to send and receive data items, either by itself, or in conjunction with the voice and data communication modules 524A, 524B, via the wireless network 519. The PIM data items are preferably seamlessly integrated, synchronized and updated, via the wireless network 519, with a corresponding set of data items stored or associated with a host computer system, thereby creating a mirrored system for data items associated with a particular user.

[0034] The mobile device 500 is manually synchronized with a host system by placing the mobile device 500 in an interface cradle, which couples the serial port 530 of the mobile device 500 to a serial port of the host system. The serial port 530 may also be used to insert owner information and owner control information onto the mobile device 500 and to download other application modules 524N for installation on the mobile device 500. This wired download path may further be used to load an encryption key onto the mobile device 500 for use in secure communications, which is a more secure method than exchanging encryption information via the wireless network 519.

[0035] Owner information, owner control information and additional application modules 524N may be loaded onto the mobile device 500 through the network 519, through an auxiliary I/O subsystem 528, through the short-range communications subsystem 540, or through any other suitable subsystem 542, and installed by a user in the non-volatile memory 524 or RAM 526. Such flexibility in application installation increases the functionality of the mobile device 500 and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the mobile device 500.

[0036] When the mobile device 500 is operating in a data communication mode, a received signal, such as a text message or a web page download, will be processed by the transceiver 511 and provided to the microproces-

sor 538, which preferably further processes the received signal for output to the display 522, or, alternatively, to an auxiliary I/O device 528. Owner information, owner control information, commands or requests related to owner information or owner control information, and software applications received by the transceiver 511 are processed as described above. A user of mobile device 500 may also compose data items, such as email messages, using the keyboard 532, which is preferably a complete alphanumeric keyboard laid out in the QWERTY style, although other styles of complete alphanumeric keyboards such as the known DVORAK style may also be used. User input to the mobile device 500 is further enhanced with the plurality of auxiliary I/O devices 528, which may include a thumbwheel input device, a touchpad, a variety of switches, a rocker input switch, etc. The composed data items input by the user are then transmitted over the communication network 519 via the transceiver 511.

[0037] When the mobile device 500 is operating in a voice communication mode, the overall operation of the mobile device 500 is substantially similar to the data mode, except that received signals are output to the speaker 534 and voice signals for transmission are generated by a microphone 536. In addition, the secure messaging techniques described above might not necessarily be applied to voice communications. Alternative voice or audio I/O devices, such as a voice message recording subsystem, may also be implemented on the mobile device 500. Although voice or audio signal output is accomplished through the speaker 534, the display 522 may also be used to provide an indication of the identity of a calling party, the duration of a voice call, or other voice call related information. For example, the microprocessor 538, in conjunction with the voice communication module 524A and the operating system software, may detect the caller identification information of an incoming voice call and display it on the display 522.

[0038] A short-range communications subsystem 540 is also included in the mobile device 500. For example, the subsystem 540 may include an infrared device and associated circuits and components, or a Bluetooth or 802.11 short-range wireless communication module to provide for communication with similarly-enabled systems and devices. Thus, owner information insertion, owner control information insertion, and application loading operations as described above may be enabled on the mobile device 500 via the serial port 530 or other short-range communications subsystem 540.

[0039] FIG. 2 represents a specific example of an electronic device in which owner control systems and methods described herein may be implemented. Implementation of such systems and methods in other electronic devices having further, fewer, or different components than those shown in FIG. 2 would occur to one skilled in the art to which this application pertains and are therefore considered to be within the scope of the present application.

[0040] FIG. 3 is a flow diagram illustrating a method of revoking privileges according to an exemplary embodiment. In this example, an application having privileges that are to be revoked may be shut down. When the application is restarted, access to revoked privileges will be denied. In order to keep track of which applications need to be shut down and reset, the system must keep track of which applications have access to which privileges. To accomplish this, for example, the system monitors and detects use of privileges by applications 300. The system may record an application identifier associated with a particular application and which privilege has been accessed by the application 302. This may be accomplished in any number of conventional methods that are readily apparent to those skilled in the art. For example, a data table listing the application identifier and having pointers directed to privilege(s) accessed by the application or associated with the application identifier. The system then continues to monitor the system for any change, for example, a change in IT policy, that might result in a revocation of privileges 304. So long as no such change is detected in decision block 304, the system continues to monitor and keep track of applications and associated privileges.

[0041] Upon a detection of a change that would result in revocation of privileges being accessed by applications in the system by the decision block 304, such as, for example, a change in IT policy, a comparison of the recorded data relating to the accessed privileges with a listing of the new privileges is performed 306. For example, the application identifiers and associated accessed privileges recorded in step 302 are compared to the new privilege list, or to a list of revoked privileges 306. The changes discussed herein are typically instituted and administered by a system administrator or other authority who has responsibility for operation and management of the system.

[0042] As a result of the comparison 306, each application that has accessed a privilege(s) to be revoked is identified 308 by the system. Upon identification of these applications, the system implements a shut down of these identified applications 310. When these applications are restarted 312, the applications will not have access to any of the revoked privileges. The system will continue to monitor and detect the accessing of privileges and associated applications as described above.

[0043] In another embodiment, as illustrated in the flow diagram of FIG. 4, a device reset may be performed. According to this example, all devices in the system are monitored 400. A system administrator or other authority specifies, for example, that whenever there is a change in system policy that requires revocation or changes in privileges 402, all devices in the system must be reset 404. Resetting the devices brings the system to a known state, i.e., a state in which the system knows which applications have access to which privileges throughout the system. Upon restarting these applications 406 after the device reset 404, the applications will no longer have

access to any of the revoked privileges. According to this example, a device reset may be instituted any time the system administrator or authority deems it necessary to do so. For example, a device reset may be done whenever a new policy that includes privilege revocation is instituted. As a result, this solution may invoke numerous (potentially unnecessary) device reset events that may be intrusive and inconvenient for the users. However, this embodiment provides very robust and timely privilege revocation, and is thus suitable to highly secure systems where privilege management is more important than user convenience.

[0044] Turning now to FIG. 5, another advantageous embodiment implementing features of both embodiments described above with respect to FIGS. 3 and 4 is illustrated. According to this example, aspects of the previously described embodiments are combined to provide highly effective and timely privilege management and revocation. In this example, the system administrator or authority has no actual control over when a device is reset. The administrator or authority merely manages the privileges of the system and of particular applications. The device itself is responsible for resetting as needed.

[0045] In this example, the device monitors which applications of the device have access to which privileges 600, and a log of privileges for the device is kept 602. The device monitors whether policies or application control changes are made in the system 604. If there is no change detected 604, the device continues to monitor applications and keep a log of privileges for the device 600, 602. If a change in policy or application control is detected in step 604, the system determines which privileges have been revoked for which applications by comparing the old set of privileges in the log with the new set of privileges received from the system administrator 606. The device then determines if any revoked privileges are present on the device 608. If revoked privileges are detected, e.g., if an application has accessed a privilege at any time in the past that has now been revoked, the device will reset 610. As described above, resetting the device brings the system to a known state in which all applications and privileges are known. After the device is reset 610, it is restarted 612. Upon restart 612, the device applications will have access to the correct privileges. Advantageously, if no revoked privileges are detected in step 608, the device performs another check to ensure that no privileges that have been passed between application have been missed. As explained above, for some privileges, e.g., IPC, it cannot be determined whether a privilege has been used as a result of being passed from another application. To overcome the potential for missing revocation of privileges when applications pass privileges between themselves, the system checks for privileges that are able to be passed between applications (e.g., IPC) 614. If a privilege that is able to be passed between applications is revoked from any application, regardless of if the system has detected that the application has accessed the privilege 614, the device must

be reset 610 to bring the system to a known state. After resetting, the device is restarted 612, and will now have the only have access to the correct privileges. In this manner, device reset will only be performed when necessary, thus limiting the number of resets and solving the problem associated with privileges that go undetected due to their ability to be passed between applications.

[0046] While this disclosure describes specific exemplary embodiments, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the exemplary embodiments described herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention, as defined in the following claims.

Claims

1. A method for managing privileges associated with applications in an electronic system, comprising:
 - monitoring devices in the electronic system to detect use of privileges by applications being run by the device;
 - recording which applications have accessed which privileges;
 - detecting a change in privileges of the system;
 - comparing recorded privileges previously accessed by applications with a set of privilege changes;
 - identifying any privileges to be revoked based on a result of said comparing step;
 - when a privilege to be revoked is identified, shutting down an application that has previously accessed the revoked privilege; and
 - restarting any application that was shut down for having accessed a revoked privilege.
2. A method according to claim 1, wherein said step of recording, comprises:
 - storing an application identifier associated with an application that has accessed a privilege; and
 - associating said identifier with the privilege accessed by the application.
3. A method according to claim 2, wherein said recording is stored in a data table listing the application identifier and privileges associated therewith.
4. A method according to claim 1, wherein said set of privilege changes comprises privileges to be revoked.
5. A method according to claim 1, wherein said set of privilege changes comprises a listing of all privileges available for use, and does not include privileges to

be revoked.

6. A method according to claim 1, wherein said devices comprise a wireless mobile electronic communication device. 5
7. A method according to claim 1, further comprising continuously repeating the steps.
8. A method according to claim 1, wherein said change in privileges is a result of a change in system IT policy. 10
9. A method for managing privileges in a system comprising electronic devices having applications resident on said devices, comprising: 15
 - monitoring electronic devices that are present in the system;
 - detecting a change in privileges available to said electronic devices; and 20
 - resetting said electronic devices in response to detection of a change in privileges.
10. A method according to claim 9, wherein said change in privileges is a result of a change in system IT policy. 25
11. A method according to claim 9, wherein said change in privileges includes an indication that privileges are to be revoked. 30
12. A method according to claim 9, wherein a system administrator determines when said resetting step is performed. 35
13. A method according to claim 9, wherein said step of resetting said electronic devices brings said system to a known state. 40
14. A method according to claim 13, further comprising restarting said electronic devices after said devices have been reset.
15. A method according to claim 9, wherein said electronic devices include a mobile wireless communications device. 45
16. A method for managing privileges in a system comprising a plurality of electronic devices, said method comprising: 50
 - monitoring, by each device of the system, which applications on each device have access to which privileges; 55
 - recording privileges accessible via applications resident on each device of the system;
 - detecting a change in privileges available to said

devices in said system;
 comparing an old set of privileges with a new set of privileges, said new set of privileges corresponding to said change in privileges;
 determining if any privileges are to be revoked based on said comparison;
 resetting each device that has access to a privilege that is to be revoked;
 determining whether any privileges to be revoked are able to be passed between applications; and
 when a privilege to be revoked is able to be passed between applications, resetting each device that has access to said privilege.

17. A method according to claim 16, wherein said change in privileges is a result of a change in system IT policy.
18. A method according to claim 16, wherein said change in privileges includes an indication that privileges are to be revoked
19. A method according to claim 16, wherein said step of resetting said electronic devices brings said system to a known state.
20. A method according to claim 19, further comprising restarting said electronic devices after said devices have been reset.
21. A method according to claim 16, wherein said electronic devices include a mobile wireless communications device.
22. A system for managing privileges in a network comprising a plurality of electronic devices, said system comprising:

a processor resident in each device of the system, for monitoring which applications on each device have access to which privileges;
 a memory for recording privileges accessible via applications resident on each device of the system; and
 wherein said processor is operable to:

detect a change in privileges available to said devices in said system;
 compare an old set of privileges with a new set of privileges, said new set of privileges corresponding to said change in privileges;
 determine if any privileges are to be revoked based on said comparison;
 reset each device that has access to a privilege that is to be revoked; and
 determine whether any privileges to be revoked are able to be passed between ap-

plications, and when a privilege to be revoked is able to be passed between applications, resetting each device that has access to said privilege.

5

10

15

20

25

30

35

40

45

50

55

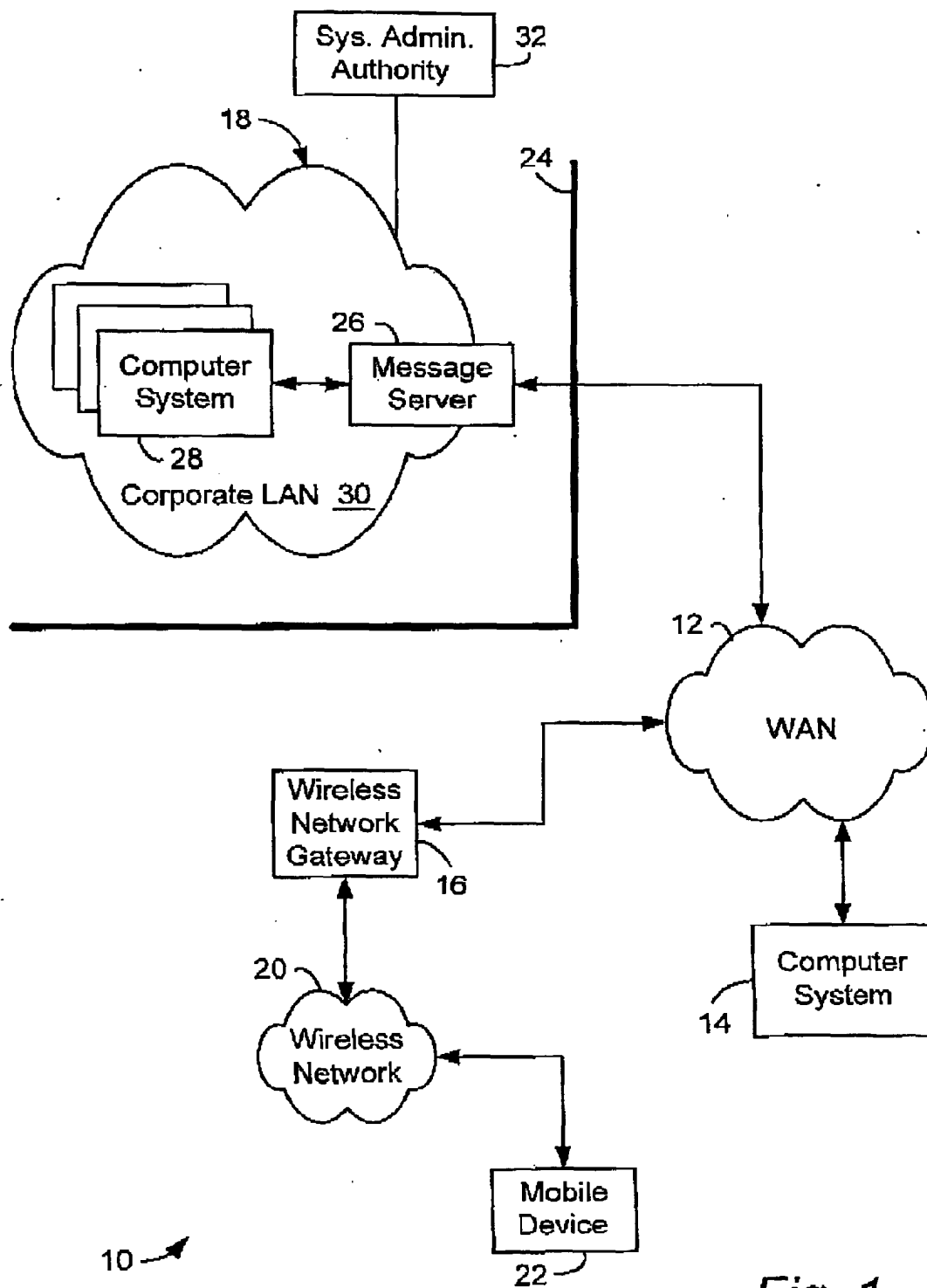


Fig. 1

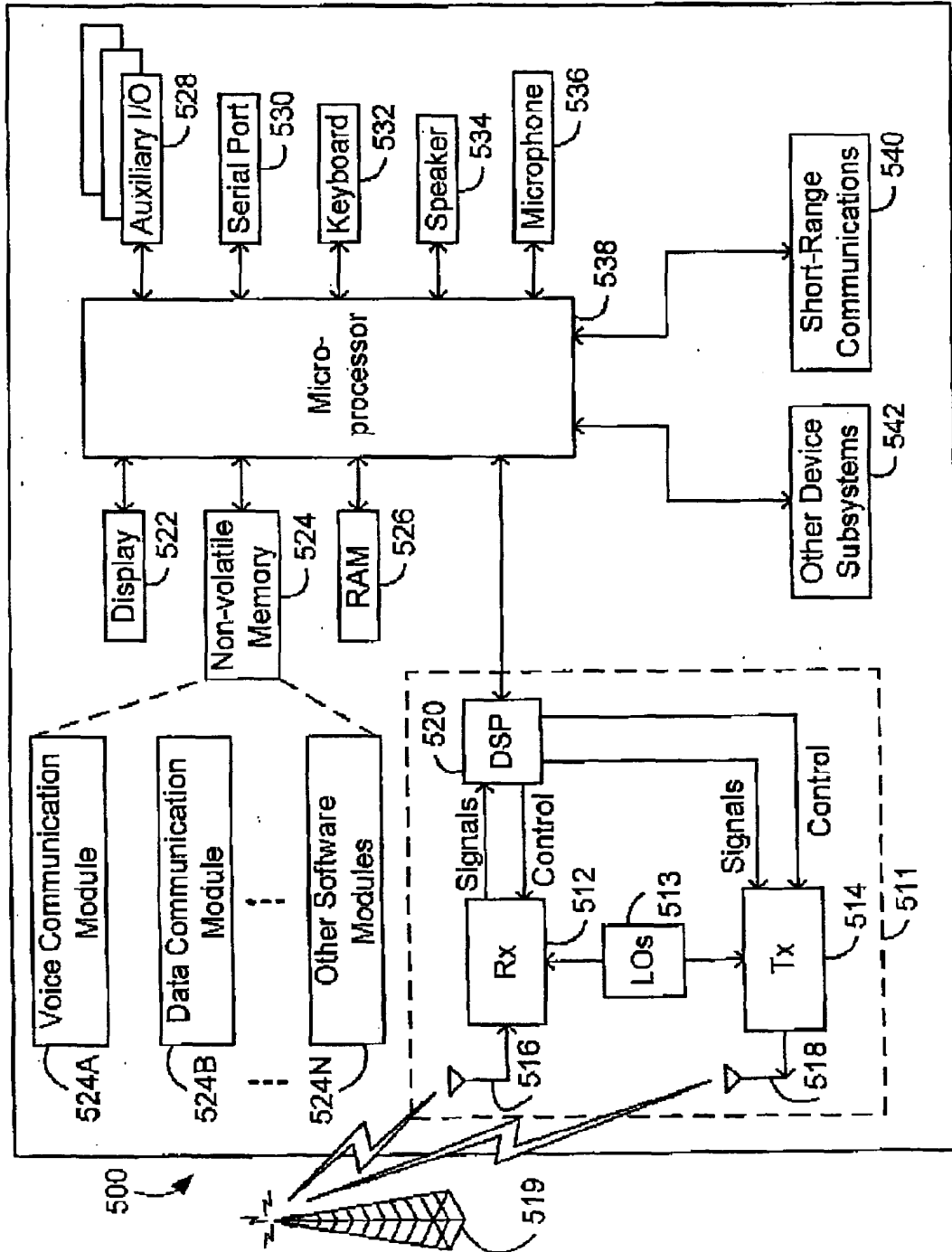
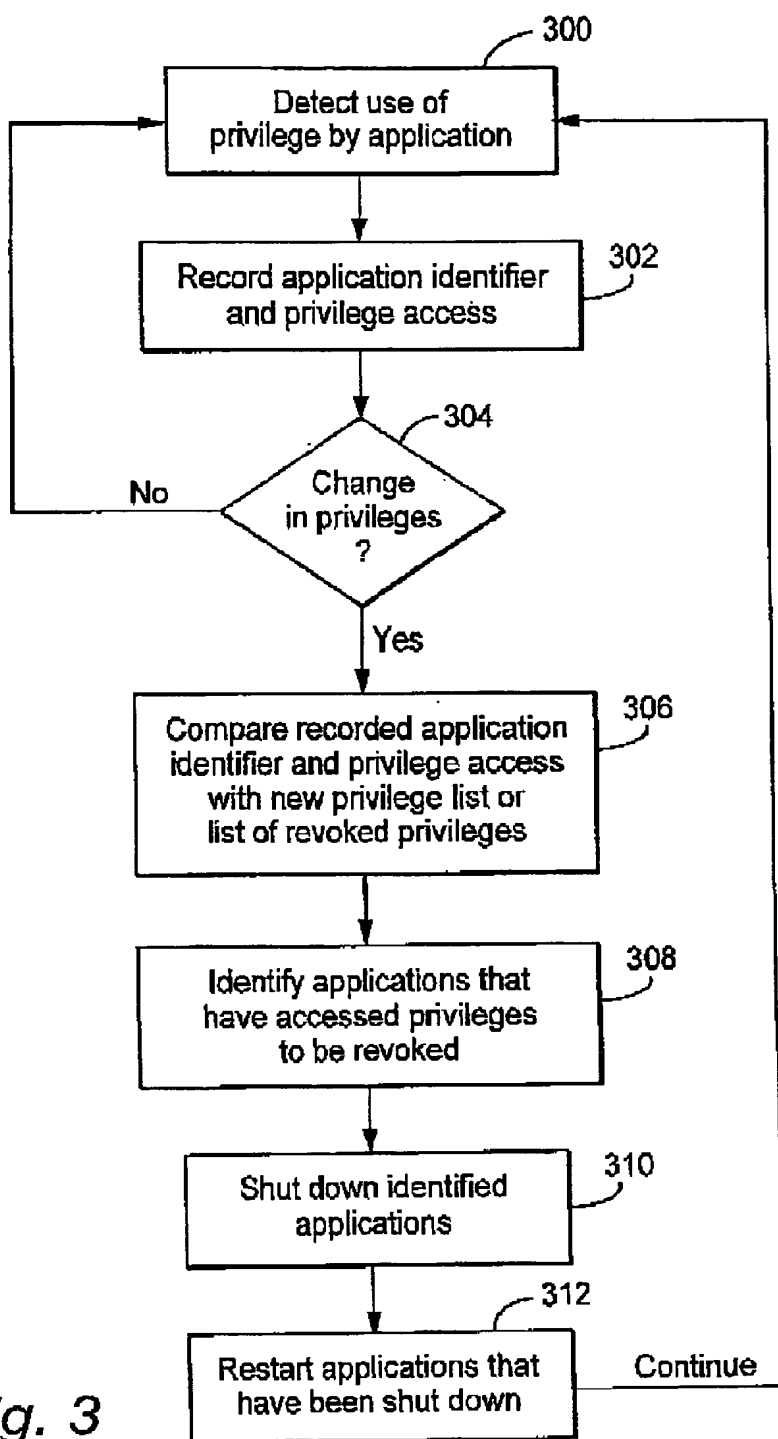
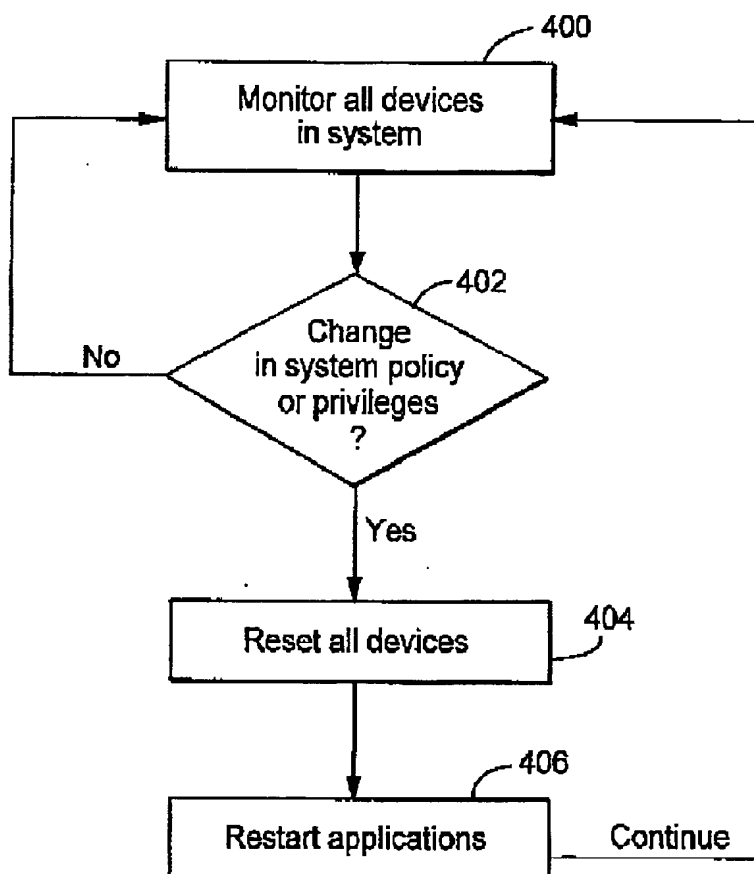
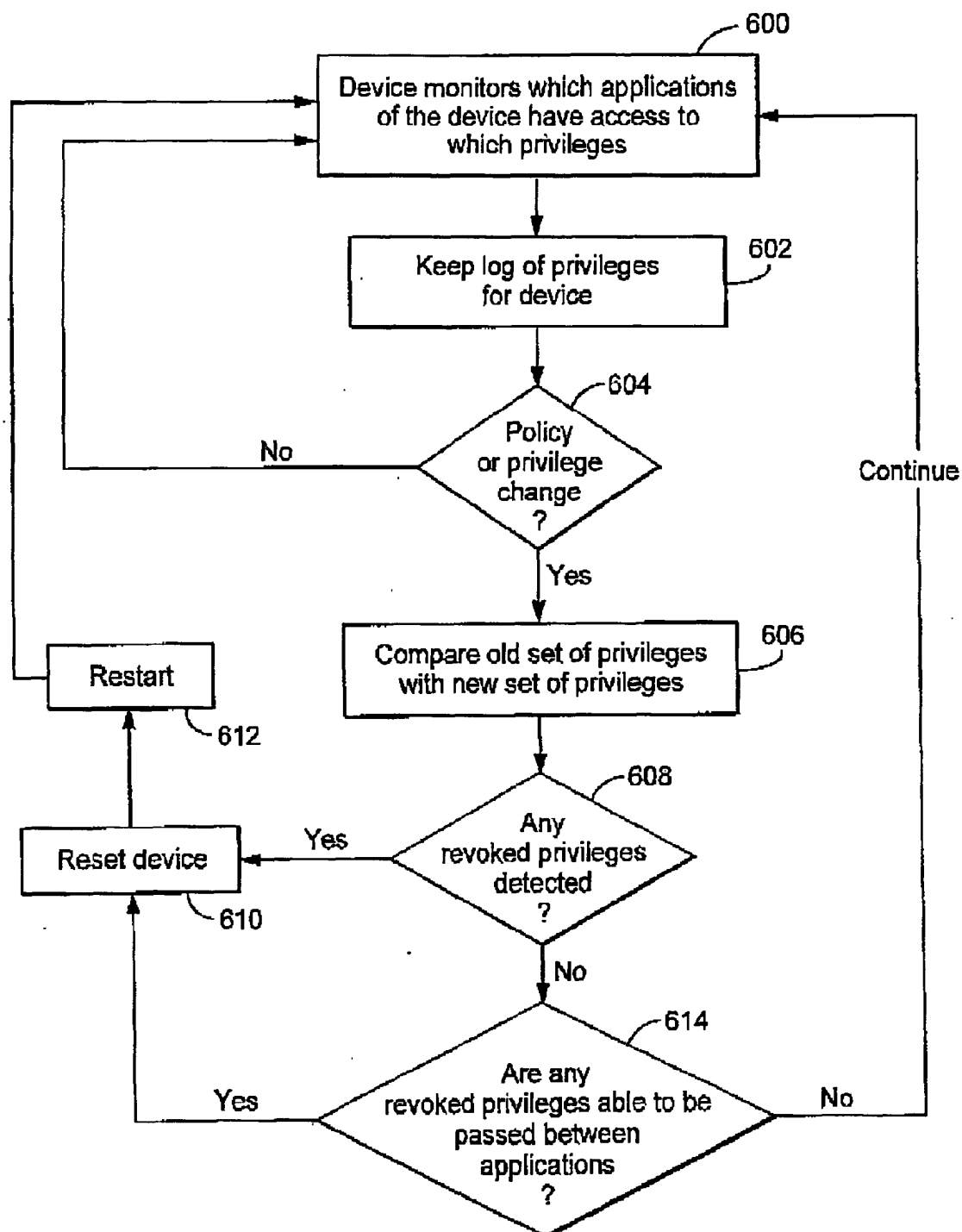


Fig. 2

*Fig. 3*

*Fig. 4*

*Fig. 5*



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 05 25 4068

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	"Using software restriction policies in Windows XP and Windows .NET server to protect against unauthorized software" MICROSOFT WINDOWS XP AND WINDOWS .NET TECHNICAL ARTICLE, January 2002 (2002-01), pages 1-52, XP002959638 * abstract * * page 1 * * page 4 * * pages 39-40, chapter "gpupdate.exe" *	9-15	G06F1/00
X	HANS HEDBOM, STEFAN LINDSKOG, STEFAN AXELSSON, ERLAND JONSSON: "Analysis of the Security of Windows NT" ANALYSIS OF THE SECURITY OF WINDOWS NT, 1 March 1999 (1999-03-01), XP002364916 Chalmers University of Technology, Göteborg, SWEDEN * abstract * * page 34, paragraph 5 - page 35, paragraph 5.2 *	9-15	
A	EP 1 043 648 A (SUN MICROSYSTEMS, INC) 11 October 2000 (2000-10-11) * abstract * * page 3, paragraph 10 * * page 4, paragraph 13 - paragraph 14 * * page 5, paragraph 26 * * page 6, paragraphs 35, 41 * * page 8, paragraph 49 * * page 9, paragraph 58 - paragraph 64 * * page 11, paragraph 85 - page 12, paragraph 88 *	1-22	G06F H04L
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 27 January 2006	Examiner Bichler, M
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

7
EPO FORM 1503 (03.02) (P44C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 05 25 4068

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

27-01-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1043648 A	11-10-2000	US 6615264 B1	02-09-2003

EPC FORM P0459

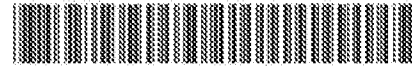
For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 6219694 B [0018]



(11) **EP 1 772 988 A1**

(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 158(3) EPC

(43) Date of publication:
11.04.2007 Bulletin 2007/15

(51) Int. Cl.:
H04L 9/36 (2006.01) H04Q 7/20 (2006.01)

(21) Application number: 05820675.6

(86) International application number:
PCT/CN2005/002254

(22) Date of filing: 20.12.2005

(87) International publication number:
WO 2006/069522 (06.07.2006 Gazette 2006/27)

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI
SK TR

(30) Priority: 28.12.2004 CN 200410103467

(71) Applicant: Huawei Technologies Co., Ltd.
Longgang District,
Shenzhen
Guangdong 518129 (CN)

(72) Inventors:
• ZHENG, Zhibin,
Huawei Administration Building
Guangdong 518129 (CN)

• LIU, Tingyong,
Huawei Administration Building
Guangdong 518129 (CN)
• TU, Weihua,
Huawei Administration Building
Guangdong 518129 (CN)
• HOU, Zhipeng,
Huawei Administration Building
Guangdong 518129 (CN)

(74) Representative: Thun, Clemens
Mitscherlich & Partner
Sonnenstrasse 33
80331 München (DE)

(54) **A METHOD, SYSTEM AND APPARATUS FOR REALIZING THE DATA SERVICE SAFETY OF THE MOBILE COMMUNICATION SYSTEM**

(57) A method for implementing data service security in a mobile communication system includes: obtaining security condition of a user terminal based on security-relevant configuration information reported by the user terminal; determining a security policy for the user terminal based on the security-relevant configuration information of the user terminal and security policy information stored, and sending the security policy determined to a packet service support node and/or the user terminal; implementing, by the packet service support node and/or the user terminal, a control process based on the security policy. The method, system and apparatus provided by the embodiments of the present invention introduce a security mechanism cooperated by the mobile communication network and a user terminal to effectively prevent the mobile communication network against viruses.

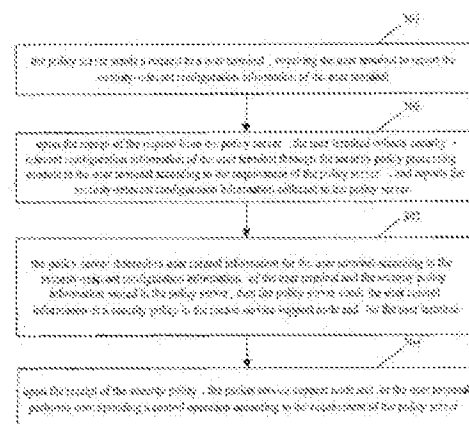


Fig. 3

EP 1 772 988 A1

Description

Field of the invention

[0001] The present invention relates to communication security technologies, and particularly, to a method, a system and an apparatus for implementing data service security in a mobile communication system.

Background of the invention

[0002] Along with applications of data services in mobile communication systems, and particularly with the development of mobile terminals towards intelligence, the mobile terminals are equipped with not only conventional voice communication functions, but also Personal Digital Assistant (PDA) functions, and may provide intelligent operation systems and application software. Moreover, as Personal Computer Memory Card International Association (PCMCIA) is widely applied, more and more users obtain Internet services via mobile networks by inserting the PCMCIA cards into the mobile terminals. Being equipped with WINDOWS operation systems and various kinds of application software, the mobile terminals act more and more like personal computers. Therefore, viruses in fixed networks are also found in the mobile networks.

[0003] In the mobile network, there are two conventional ways to prevent viruses:

1) Install anti-virus software on a terminal side, the terminal scans data to be transmitted and removes possible viruses using the anti-virus software;

2) Install an anti-virus gateway on the mobile network, the anti-virus gateway implements online scan to the data traffic passing the anti-virus gateway and removes the viruses; this method requires high performance for the anti-virus gateway, e.g., in order to scan viruses in short messages, a short message gateway needs virus scan and remove functions.

[0004] It can be seen from the fore-going descriptions that, in conventional ways, anti-virus software is generally installed where the data traffic passes to scan and remove the viruses. However, all types of anti-virus software may only scan and remove known viruses and are not capable of preventing unknown viruses from spreading, thus unknown viruses are still disturbing network traffic.

[0005] Moreover, the impact of the viruses and worms may be brought out by many factors including the version of the operation system, the version of the anti-virus software and the capability of the anti-virus software. For example, greater damages may result from the absence of a certain operation system patch, e.g., the virus worm Blaster damages a system through a bug in the Windows operation system. In fact, before a virus breaks

out, providers of the operation system usually announce a corresponding patch; however, the virus may still spread to a large scope because the patch is not installed in many personal computers in time. In addition, for a terminal in which the anti-virus software has already been installed, the update of the anti-virus software is also very important.

Summary of the invention

[0006] One embodiment of the present invention provides a method for implementing data service security in a mobile communication system, so as to effectively handle and control viruses in the mobile communication system.

[0007] Another embodiment of the present invention provides a system for implementing data service security in a mobile communication system. The system introduces a security mechanism cooperated by the mobile communication network and a user terminal to improve the defense of the mobile communication network against viruses.

[0008] Yet another embodiment of the present invention provides an apparatus for implementing data service security in a mobile communication system, so as to determine, store and distribute security policies.

[0009] According to an embodiment of the present invention, the method for implementing data service security in a mobile communication system includes:

obtaining security-relevant configuration information of a user terminal;

determining a security policy for the user terminal based on the security-relevant configuration information of the user terminal and security policy information stored, and sending the security policy determined to a packet service support node and/or the user terminal;

upon the receipt of the security policy, implementing, by the packet service support node and/or the user terminal, a control process based on the security policy.

[0010] Another embodiment of the present invention provides a system for implementing data service security in a mobile communication system, including:

a packet service support node;

a user terminal, communicates with the packet service support node through the mobile communication network; the system further includes:

a policy service entity, connected to the packet service support node, and configured to obtain security-relevant configuration information of

the user terminal, determine a security policy for the user terminal and distribute the security policy to the packet service support node and/or the user terminal.

[0011] Another embodiment of the present invention provides an apparatus for implementing data service security in a mobile communication system, including:

a security information obtaining module, configured to communicate with a user terminal, obtain security-relevant configuration information of the user terminal and send the security-relevant configuration information obtained to a security policy determination module;

the security policy determination module, configured to determine a security policy based on the security-relevant configuration information of the user terminal and security policy information stored in a security policy storage module and send the security policy determined to a security policy distribution module;

the security policy storage module, configured to store the security policy information;

the security policy distribution module, configured to send the security policy received to a designated network entity.

[0012] The method, system and apparatus for implementing data service security provided by the embodiments of the present invention in a mobile communication system add a policy service entity into the existing mobile communication system. The policy service entity is configured to store security policy information, determine a security policy based on the security-relevant configuration information of the user terminal, and notify the packet service support node on the network side and/or the user terminal to implement the security process. The embodiments of the present invention have the following advantages:

1) the security policy of the user terminal is associated with that on the network side, and a joint security mechanism is provided for the network and the user terminal. Through the protection on both the user terminal and the network side, not only known viruses, but also unknown viruses may be detected and removed, thus full dimensional security is achieved;

2) since security threats always come from the user terminal, the method provided by an embodiment of the present invention determines a security policy based on the security-relevant configuration information reported by the user terminal, therefore implements control on the user terminal. The method

provided by an embodiment of the present invention may implement security control on the headstream, and effectively prevent the security threats from spreading. And, with the cooperation of the network side, the virus may be effectively handled and restricted;

3) with regard to cell phone viruses that tend to be more and more serious in the future, effective security measures may be taken based on the system architecture provided by the embodiments of the present invention to control viruses in the mobile communication network, and further prevent the spreading of cell phone viruses;

4) the embodiments of the present invention may obtain the security condition of the user terminal and determine a security policy according to the security condition of the user terminal, and instructs the packet service support node and/or the user terminal to implement a control process according to the security policy, therefore the embodiments of the present invention may prevent the network from virus infection, especially worm infection;

5) if the packet service support node is a GGSN, the embodiments of the present invention support security control over data packets on both uplink and downlink, thus it is possible to effectively prevent attacks from the mobile network to a public network, and vice versa. Moreover, the implementation of the security policy may be very flexible, i.e., it may be implemented in the GGSN, or implemented in the SGSN or the RNC which is notified to implement the control process by the GGSN;

6) the embodiments of the present invention only need a minor modification or a simple additional protocol to the function modules in the packet service support node, the user terminal and the security gateway to achieve effective security interworking and implement data packets security process. The implementation of the embodiments of the present invention is simple and convenient without increasing hardware cost.

Brief Description of the Drawings

[0013]

Fig. 1 is a schematic structure of a system according to an embodiment of the present invention.

Fig. 2 is a schematic structure of another system according to an embodiment of the present invention.

Fig. 2 is a flow chart of a method for implementing

data service security according to an embodiment of the present invention.

Fig. 4 is a schematic diagram illustrating a structure of the apparatus according to an embodiment of the present invention.

Embodiments of the invention

[0014] The embodiments of the present invention add a policy service entity into the mobile communication network. The policy service entity determines a security policy based on the security-relevant configuration information of a user terminal and notifies a packet service support node on the network side and/or the user terminal to implement a security process according to the determined security policy.

[0015] The policy service entity may be a policy server, a function module embedded in a network entity, or a card. The user terminal may be a mobile intelligent terminal or a portable terminal with card slot. The packet service support node on the network side may be a Serving GPRS Support Node (SGSN), a Gateway GPRS Support Node (GGSN) or a Packet Data Support Node (PDSN).

[0016] As shown in Fig. 1, the system for implementing data service security in the mobile communication system in accordance with an embodiment of the present invention includes a policy service entity, an SGSN and multiple user terminals. The policy service entity is connected to the SGSN directly or through a network, and configured to determine security policies. The policy service entity may interact with the user terminals through the SGSN, obtain the security-relevant configuration information of the user terminals, determine appropriate security policies for different user terminals based on the security-relevant configuration information of the user terminals and the security policy information stored in the policy service entity, and distribute the determined security policies to the user terminals or the SGSN. The policy service entity may store the security policy information issued by a core network device, or directly stores the configured security policy information.

[0017] The policy service entity may be an independent policy server, or a function module in a network entity such as SGSN, or a card equipped with the policy management function and inserted into an SGSN. The user terminal may be the mobile intelligent terminal or the portable terminal with card slot, or any other mobile terminals capable of interacting with the policy service entity to exchange security information.

[0018] To interwork with the policy service entity, the user terminal is equipped with a security policy processing module. The security policy processing module is configured to receive instructions from the policy service entity and perform corresponding operations, e.g., when the policy service entity sends a request to the user terminal requiring security-relevant configuration information

of the user terminal, the security policy processing module collects, upon the receipt of the request, security-relevant configuration information of the user terminal and reports the security-relevant configuration information to the policy service entity. In this way, the policy service entity may obtain, through the security policy processing module, the security-relevant configuration information of the user terminal, including the version information of the operation system of the user terminal, the information of the anti-virus software of the user terminal and the installation condition of the patch.

[0019] The security policy processing module may also actively report the security-relevant configuration information of the user terminal to the policy service entity at a fixed time, or regularly, or upon any change in the security-relevant configuration information of the user terminal. The security policy processing module may be independent software, thus the user terminal communicating with the policy service entity only needs to install the software. The security policy processing module may also store anti-virus software.

[0020] The policy service entity, connected to the SGSN, stores the security-relevant configuration information of the user terminals. After a security protocol negotiation between the policy service entity and the security policy processing module of the user terminal, i.e., after a mutual-trust relationship on security is established between the policy service entity and the security policy processing module of the user terminal, the policy service entity may send a request to the user terminal requiring to collect security-relevant configuration information of the user terminal. The user terminal reports the security-relevant configuration information, e.g., the information of the anti-virus software, installation information of the patch, etc., to the policy service entity.

[0021] In order to enable the SGSN to control the user terminal according to the requirement of the policy service entity, a security policy processing module interworking with the policy service entity and a protocol used for negotiation with the policy service entity are added into the SGSN. In this way, the SGSN may control the user terminal according to the security policy from the policy service entity, and on the other hand, may provide security policy requirement for the policy service entity. The protocol used for the negotiation between the SGSN and the policy service entity includes the mutually agreed interaction method and message format.

[0022] As shown in Fig. 2, a system for implementing data service security in the mobile communication system in accordance with an embodiment of the present invention includes a policy service entity, a GGSN and multiple user terminals as well as an SGSN, an RNC and a Node B. The policy service entity is connected to the GGSN directly or through the network, configured to determine security policies for the user terminals. The policy service entity may interact with the user terminals through the GGSN, and further through the SGSN, the RNC and the Node B, obtain the security-relevant configuration information

formation of the user terminals, determine appropriate security policies for different user terminals based on the security-relevant configuration information of the user terminals and the security policy information stored in the policy service entity, and distribute the determined security policies to the user terminals or the GGSN. The policy service entity may store the security policy information issued by a core network device, or directly stores the configured security policy information.

[0023] The policy service entity may be an independent policy server, or a function module in a network entity such as a GGSN, or a card equipped with the policy management function and inserted into the GGSN. The user terminal may be the mobile intelligent terminal or the portable terminal with card slot, or any other mobile terminals capable of interacting with the policy service entity to exchange security information.

[0024] To interwork with the policy service entity, the user terminal is equipped with a security policy processing module. The security policy processing module is configured to receive instructions from the policy service entity and perform corresponding operations, e.g., when the policy service entity sends a request to the user terminal requiring security-relevant configuration information of the user terminal, the security policy processing module collects, upon the receipt of the request, security-relevant configuration information of the user terminal and reports the security-relevant configuration information to the policy service entity. In this way, the policy service entity may obtain, through the security policy processing module, the security-relevant configuration information of the user terminal, including the version information of the operation system of the user terminal, the information of the anti-virus software of the user terminal and the installation condition of the patch.

[0025] The security policy processing module may also actively report the security-relevant configuration information of the user terminal to the policy service entity at a fixed time, or regularly, or upon any change in the security-relevant configuration information of the user terminal. The security policy processing module may be independent software. The user terminal communicating with the policy service entity only needs to install the software; the security policy processing module may also store anti-virus software.

[0026] The policy service entity interacts with the user terminal through the GGSN, SGSN, RNC and Node B, in which the SGSN, RNC and the Node B transmit the interaction information transparently.

[0027] The policy service entity, which is connected to the GGSN, stores the security-relevant configuration information of the user terminals. After a security protocol negotiation between the policy service entity and the security policy processing module of the user terminal, i.e., after a mutual-trust relationship on security is established between the policy service entity and the security policy processing module of the user terminal, the policy service entity may send a request to the user terminal requiring

to collect security-relevant configuration information. The user terminal reports security-relevant configuration information, e.g., the information of the anti-virus software, installation information of the patch, etc., to the policy service entity.

[0028] In order to enable the GGSN to control the user terminal according to the requirement of the policy service entity, a security policy processing module interworking with the policy service entity and a protocol used for negotiation with the policy service entity are added into the GGSN. In this way, the GGSN may control the user terminal according to the security policy from the policy service entity, and on the other hand, may provide security policy requirement for the policy service entity. The protocol used for the negotiation between the GGSN and the policy service entity includes the mutually agreed interaction method and message format.

[0029] The GGSN is able to resolve the uplink and downlink IP packets in layer 7 and has a redirection function, therefore, the system provided by an embodiment of the present invention may further include one or more security gateways that are configured to implement different security functions or detect different kinds of viruses. The GGSN may redirect the IP packets to the security gateway for further security detection, e.g., redirects the IP packets to an anti-virus gateway. The anti-virus gateway scans the IP packets and removes viruses in the IP packets, and returns the IP packets to the GGSN, and then sends the IP packets to the public network such as the Internet through the GGSN.

[0030] Similarly, the GGSN may also redirect the IP packets from the public network to the security gateway. The security gateway processes the IP packets, e.g., an anti-virus gateway scans the IP packets, removes the viruses in the IP packets, and returns the IP packets to the GGSN. Then the GGSN transmits the IP packets through the SGSN, the RNC and the Node B to the user terminal such as a mobile terminal. To which security gateway the GGSN send the IP packets is decided according to the security policy determined by the policy service entity. For example, provided there are three security gateways in a network, each of them is in charge of IP packets from different IP addresses respectively, the policy service entity may determine that the IP packets with addresses from 10.10.10.0 to 10.10.10.255 shall be redirected to the first security gateway for security detection.

[0031] In the system shown in Fig. 2, after receiving the security policy, instead of executing the security policy, the GGSN may send relevant security policy control information, e.g., deactivate information, to the SGSN or the RNC, the SGSN or the RNC implements corresponding operation. In addition, the policy service entity may also be connected to the SGSN directly to perform unidirectional control, since the SGSN cannot resolve the IP packets, the SGSN may only implement simple security policies, e.g., block the user terminal of a certain IP address.

[0032] Based on the systems shown in Fig. 1 and Fig. 2, the method provided by an embodiment of the present invention is shown in Fig. 3, in which the policy service entity is a policy server, the SGSN and the GGSN are generally referred to packet service support node. The method includes the steps of:

Step 301: the policy server sends a request to a user terminal, requiring the user terminal to report the security-relevant configuration information of the user terminal. The user terminal may be a mobile intelligent terminal or a portable terminal with card slot.

In this step, the request may be initiated by the policy server at any time, and be transmitted to the user terminal through the SGSN transparently. The request includes an indicator indicating the required information, e.g., indicating the user terminal to report the installation information of the patch. The format of the request may be determined through negotiation between the policy server and the user terminal. For example, different fields in the request may represent different types of information required by the policy server.

Step 302: upon the receipt of the request from the policy server, the user terminal collects security-relevant configuration information of the user terminal through the security policy processing module in the user terminal according to the requirement of the policy server, and reports the security-relevant configuration information collected to the policy server.

Step 303: after receiving the security-relevant configuration information of the user terminal, the policy server determines user control information for the user terminal according to the security-relevant configuration information of the user terminal and the security policy information stored in the policy server, then the policy server sends the user control information as a security policy to the packet service support node and/or the user terminal.

The security policy information stored in the policy server includes: information of the patch that should be installed on the user terminal, information of the anti-virus software that should be installed on the user terminal, etc. The packet service support node may be a GGSN, or an SGSN, or a PDSN.

Step 304: upon the receipt of the security policy, the packet service support node and/or the user terminal performs a corresponding control operation according to the requirement of the policy server. For example, if the security policy is to scan for a certain virus in the data from a certain user terminal, the GGSN may send, upon the receipt of the data to or from the IP address of the user terminal, the data to

a designated security gateway for virus scan; or the GGSN transmits the data of the user terminal through a designated security gateway.

[0033] In the system shown in Fig. 1, the policy server sends the security policy to the SGSN, and the SGSN performs corresponding control operation according to the security policy received. In the system shown in Fig. 2, the policy server sends the security policy to the GGSN, the GGSN performs corresponding control operation according to the security policy received or notifies the SGSN to perform corresponding operation, e.g., to block the IP packets from the user terminal with certain IP address.

[0034] The GGSN may also redirect designated uplink and downlink IP packets to a security gateway for corresponding security process, e.g., virus scan. After the security process, the security gateway returns the IP packets to the GGSN for subsequent transmission and process.

[0035] The packet service support node may send a policy request to the policy server, and the policy server executes steps 301 to 304 upon the receipt of the policy request. The user terminal may also initiatively report the security-relevant configuration information of the user terminal to the policy server, and the policy server executes steps 303 and 304 upon the receipt of the security-relevant configuration information. The user terminal may report the security-relevant configuration information regularly, or at a fixed time, or upon any change in the security-relevant configuration information of the user terminal.

[0036] The policy service entity may, in the form of a card, be integrated into the packet service support node, such as the GGSN or the SGSN, to provide corresponding security service.

[0037] In the embodiments of the present invention, through the determination of the security policy by the policy service entity, the security condition of the user terminal may be detected on the network side, and the security threat information or potential threat will be reported to the policy service entity. The policy service entity determines a corresponding security policy for the user terminal through a verification and selection process, and the spread of the threat may be further controlled by the packet service support node.

[0038] Another embodiment of the present invention is described herein, demonstrating an example of patch installation management. Many damages caused by worms, such as worm.Blaster and worm.Sasser are also the result of not installing corresponding patches on the user terminal in time. The method provided by the present invention may prevent the virus from attacking the network.

[0039] In this embodiment, the packet service support node is an SGSN; the policy service entity is a policy server which stores the information of all patches that should be installed and relative information of each patch,

e.g., the importance of each patch. The security-relevant configuration information of the user terminal is the installation information of the patch. In this embodiment, the method includes the steps of:

1) the policy server sends a request to the user terminal M, requiring the user terminal M to return the security-relevant configuration information of the operation system patch of the user terminal M;

2) upon the receipt of the request, the user terminal M obtains the information of the patch that has been installed in the operation system of the user terminal M through the security policy processing module of the user terminal M, and sends the security-relevant configuration information of the operation system patch to the policy server;

3) upon the receipt of the security-relevant configuration information of the operation system patch of the user terminal M, the policy server verifies the operation system patch installation condition of the user terminal M based on the security-relevant configuration information of the operation system patch from the user terminal M and the information stored in the policy server of all patches that should be installed, and finds out that an important patch has not been installed on the user terminal M, e.g., at least four patches, A, B, C and D, should be installed on each user terminal to ensure the basic security of the user terminals, while the user terminal M has only installed A, C and D without installing B;

4) the policy server sends a notification to the user terminal M, informing the user terminal M that a patch has not been installed, e.g., informing the user terminal M that patch B has not been installed; the policy server determines a security policy based on current information obtained, e.g., determines to restrict the bandwidth of the user terminal M and sends a bandwidth restriction message to the SGSN to restrict the bandwidth of the user terminal M;

5) upon the receipt of the bandwidth restriction message, the SGSN applies the bandwidth restriction to the user terminal M, or even blocks the network connection of the user terminal M.

[0040] And the user terminal M may determine whether to install the patch B according to the notification described in step 4).

[0041] In the fore-going example of the patch installation management, if the packet service support node is a GGSN, when the data packets from the user terminal M are transmitted to the GGSN, the GGSN may redirect the data packets received to the security gateway, such as an anti-virus gateway, for corresponding security examination to remove virus, and then the anti-virus gate-

way returns the data packets to the GGSN.

[0042] The policy service entity may be an independent implementing data service security apparatus in the mobile communication system. As shown in Fig. 4, the apparatus includes a security information obtaining module, a security policy determination module, a security policy storage module and a security policy distribution module.

[0043] The security information obtaining module communicates with the user terminal, obtains the security-relevant configuration information of the user terminal through interaction with the user terminal and sends the security-relevant configuration information obtained to the security policy determination module;

the security policy determination module is configured to determine a security policy based on the obtained security-relevant configuration information of the user terminal and the security policy information stored in the security policy storage module, and send the security policy determined to the security policy distribution module for distribution;

the security policy storage module is configured to store security policy information of the user terminals; and the security policy distribution module is configured to send the security policy received to designated network entities, such as a user terminal, SGSN or GGSN.

[0044] The security information obtaining module may also be connected directly to the security policy storage module and store the security-relevant configuration information obtained as security policy information. The security policy storage module may also be connected to an external device such as a core network device and directly obtain and store the security policy information configured by the external device; and the security policy storage module may obtain security policy information configured by a configuration command through a man-machine interface.

[0045] The present invention may be applicable to 2G GPRS system, Enhanced Data rates for GSM Evolution (EDGE) system and 3G Wideband Code Division Multiple Access (WCDMA) system, Time Division-Synchronization Code Division Multiple Access (TD-SCDMA) system and Code Division Multiple Access (CDMA) 2000 system. The fore-going is only the preferred embodiments of the present invention and is not for use in limiting the protection scope thereof.

Claims

1. A method for implementing data service security in a mobile communication system, comprising:

obtaining security-relevant configuration information of a user terminal;

determining a security policy for the user terminal based on the security-relevant configuration information of the user terminal and security pol-

- icy information stored, and sending the security policy determined to a packet service support node and/or the user terminal;
upon the receipt of the security policy, implementing, by the packet service support node and/or the user terminal, a control process based on the security policy.
2. The method of claim 1, wherein the process of obtaining security-relevant configuration information of a user terminal comprises:
- reporting initiatively, by the user terminal, the security-relevant configuration information currently collected of the user terminal.
3. The method of claim 2, wherein the user terminal reports the security-relevant configuration information of the user terminal to the policy service entity at a fixed time, or regularly, or upon any change in the security-relevant configuration information of the user terminal.
4. The method of claim 1, wherein the process of obtaining security-relevant configuration information of a user terminal comprises:
- sending a request to the user terminal, requiring the user terminal to report the security-relevant configuration information;
upon the receipt of the request, collecting, by the user terminal, the security-relevant configuration information of the user terminal based on the request, and reporting the security-relevant configuration information collected.
5. The method of claim 4, further comprising:
- before sending a request to the user terminal requiring the user terminal to report the security-relevant configuration information, sending, by the packet service support node, a policy request; and
upon the receipt of the policy request, sending the request to the user terminal, requiring the user terminal to report the security-relevant configuration information to the user terminal.
6. The method of any one of claims 1 to 5, wherein the security-relevant configuration information of the user terminal comprises at least one of: version information of the operation system of the user terminal, information of anti-virus software of the user terminal and installation condition of a patch.
7. The method of any one of claims 1 to 5, wherein the policy service entity is any one of: an independent policy server, a function module in a network device,
- and a card equipped with a policy management function.
8. The method of any one of claims 1 to 5, wherein the packet service support node is any one of: a Serving GPRS Support Node (SGSN), a Gateway GPRS Support Node (GGSN), and a Packet Data Support Node (PDSN).
9. The method of any one of claims 1 to 5, wherein the user terminal is any one of: a mobile intelligent terminal and a portable terminal with card slot.
10. The method of claim 1, wherein the packet service support node is a GGSN, the process of the packet service support node and/or the user terminal implementing a control process based on the security policy further comprising:
- upon the receipt of the security policy, notifying, by the GGSN, a SGSN or a Radio Network Controller (RNC) to implement the control process based on the security policy.
11. The method of claim 1, wherein the packet service support node is a GGSN, the method further comprising:
- redirecting, by the GGSN, received data packets to a security gateway for security processing; and
returning, by the security gateway, the data packets to the GGSN after the security processing.
12. The method of claim 11, wherein the security gateway is an anti-virus gateway, and the security processing comprises: scanning the received data packets for virus and removing the virus.
13. A system for implementing data service security in a mobile communication system, comprising:
- a packet service support node;
a user terminal, communicating with the packet service support node through the mobile communication network;
a policy service entity, connected to the packet service support node, and configured to obtain security-relevant configuration information of the user terminal, determine a security policy for the user terminal and distribute the security policy to the packet service support node and/or the user terminal;
the user terminal and the packet service support node are respectively equipped with a security policy processing module communicating with the policy service entity, the security policy

processing module is configured to receive an instruction from the policy service entity, implement corresponding process and/or sending of security-relevant configuration information to the policy service entity based on the instruction.

14. The system of claim 13, further comprising:

a security gateway, configured to implement a security process on data packets which are re-directed to the security gateway by the packet service support node.

15. The system of claim 14, wherein the security gateway is an anti-virus gateway.

16. The system of claims 13, 14 or 15, wherein the packet service support node is any one of: a Serving GPRS Support Node (SGSN), a Gateway GPRS Support Node (GGSN), and a Packet Data Support Node (PDSN).

17. The system of claim 13, 14 or 15, wherein the policy service entity is any one of: an independent policy server, a function module in a network device, and a card equipped with a policy management function.

18. The system of any one of claims 13 to 16, wherein the packet service support node is any one of: a Serving GPRS Support Node (SGSN), a Gateway GPRS Support Node (GGSN), and a Packet Data Support Node (PDSN).

19. The system of claim 13, 14 or 15, wherein the user terminal is any one of: a mobile intelligent terminal and a portable terminal with card slot.

20. An apparatus for implementing data service security in a mobile communication system, comprising:

a security information obtaining module, configured to communicate with a user terminal, obtain security-relevant configuration information of the user terminal and send the security-relevant configuration information obtained to a security policy determination module;

the security policy determination module, configured to determine a security policy according to the security-relevant configuration information and security policy information stored in a security policy storage module, and send the security policy determined to a security policy distribution module;

the security policy storage module, configured to store the security policy information;

the security policy distribution module, configured to send the security policy received to a designated network entity.

21. The apparatus of claim 20, wherein the security information obtaining module is further connected to the security policy storage module.

22. The apparatus of claim 20, wherein the security policy storage module is further configured to receive and store security policy information configured by an external device and/or a configuration command.

23. The apparatus of claim 20, 21 or 22, wherein the designated network entity comprises at least one of: a user terminal, a Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN).

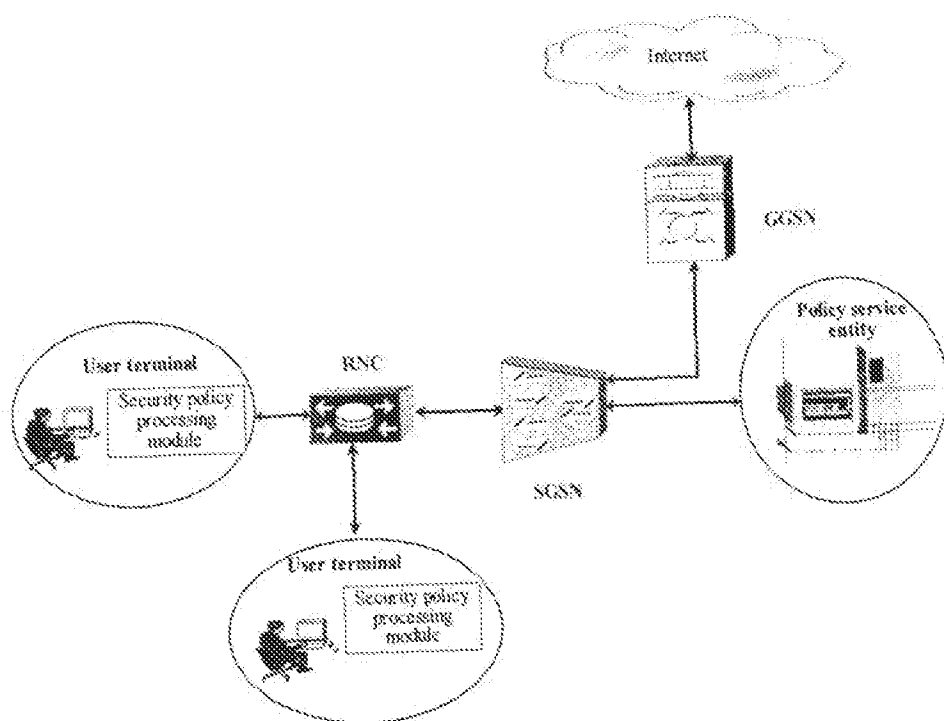


Fig. 1

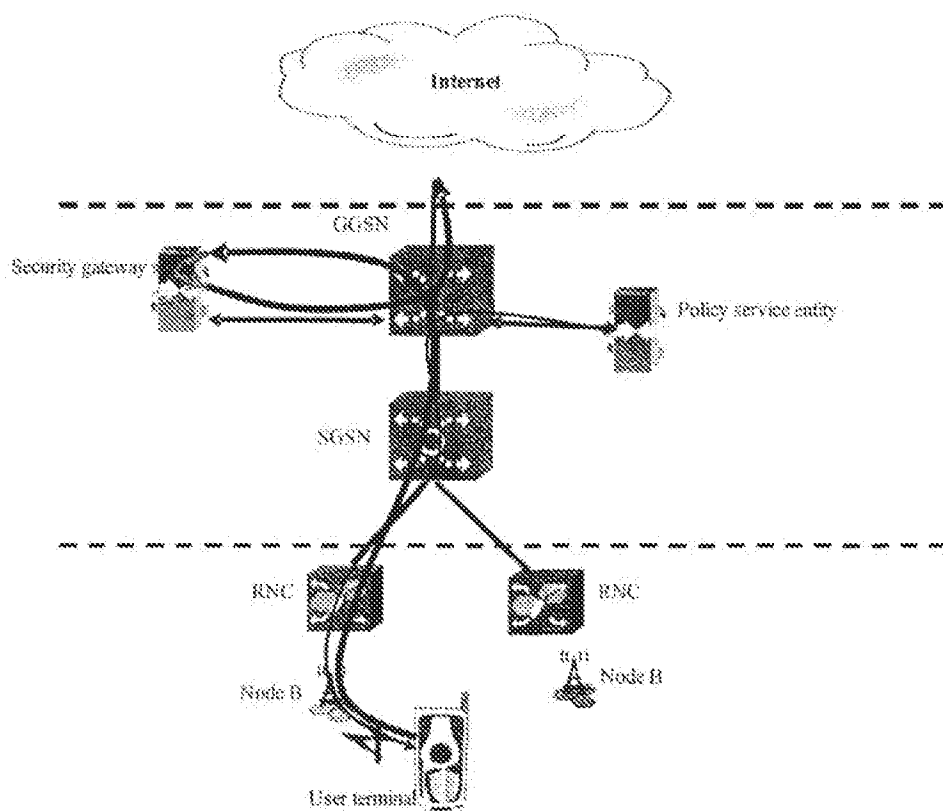


Fig. 2

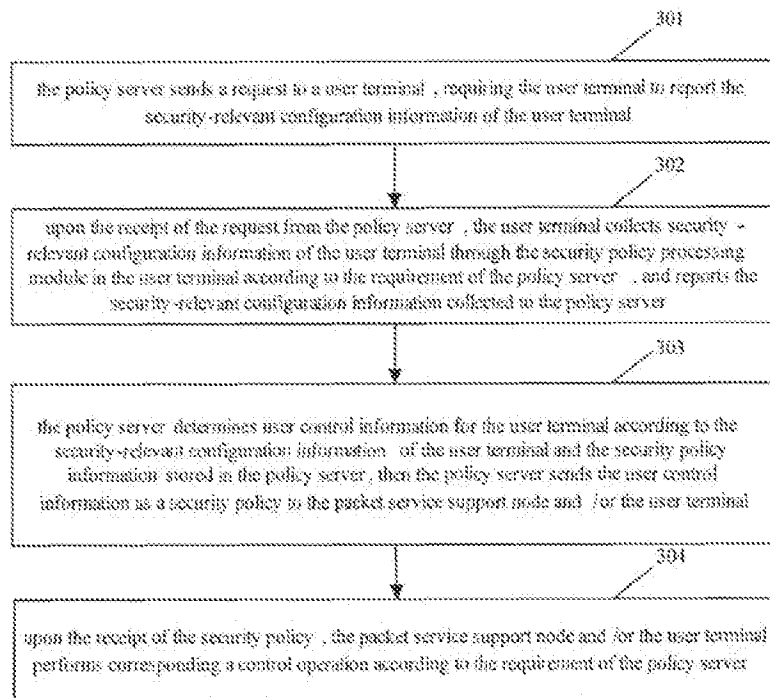


Fig. 3

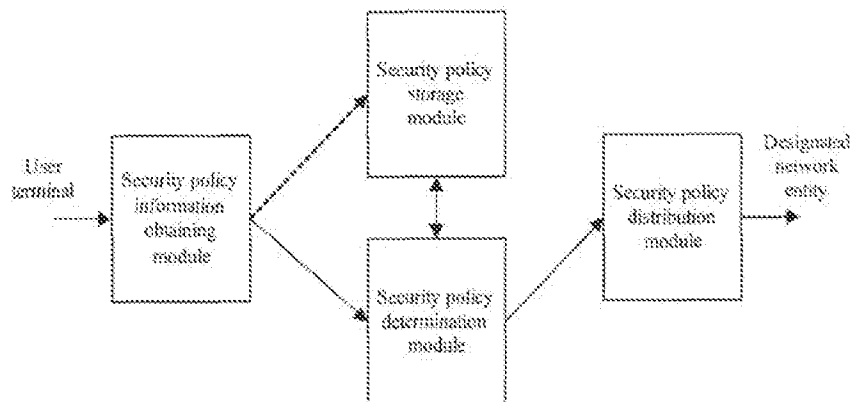


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2005/002254

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, PAJ: safety, security, virus, bug, mobile, cellular, radio, wireless

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP, A2, 1443379 (CURITEL CORP) 4 Aug. 2004 (04.08.2004), the whole document.	1-23
A	EP, A2, 1329790 (NTT DOCOMO INC) 23 Jul. 2003 (23.07.2003), the whole document.	1-23
A	WO, A2, 2004057834 (SENFORCE TECHNOLOGIES INC) 8 Jul. 2004 (08.07.2004), the whole document.	1-23

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"S" document member of the same patent family

Date of the actual completion of the international search

15 Mar. 2006 (15.03.2006)

Date of mailing of the international search report

30 MAR 2006 13 03.2006

Name and mailing address of the ISA/CN
 The State Intellectual Property Office, the P.R.China
 5 Xuezhong Rd., Jinnan Bridge, Haidian District, Beijing, China
 100088
 Facsimile No. 86-10-62019451

Authorized officer

WANG Hongli

Telephone No. (86-10) 62084225

Form PCT/ISA/210 (second sheet) (April 2003)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2005/002254

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
EP1443379A2	04.08.2004	KR2004059328 A	05.07.2004
		US2004127195 A1	01.07.2004
		CN1512798 A	14.07.2004
EP1329790A2	23.07.2003	CN1433243 A	30.07.2003
		US2003154409 A1	14.08.2003
		JP2003216448 A	31.07.2003
WQ2004057834A2	08.07.2004	AU2004299729 A1	14.07.2004
		US2004123153 A	24.06.2004
		US2004123150 A	24.06.2004
		US2005053378 A	10.03.2005

Form PCT/ISA/210 (patent family annex) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2005/002254

CLASSIFICATION OF SUBJECT MATTER

H04L 9/36 (2006.01) i

H04Q 7/20 (2006.01) n

Form PCT/ISA/210 (extra sheet) (April 2005)



(11) **EP 1 978 772 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
08.10.2008 Bulletin 2008/41

(51) Int Cl.:
H04Q 7/38 ^(2006.01) **H04L 29/06** ^(2006.01)

(21) Application number: **07251454.0**

(22) Date of filing: **02.04.2007**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK RS

(71) Applicant: **British Telecommunications Public Limited Company**
London
EC1A 7AJ (GB)

(72) Inventor: **The designation of the inventor has not yet been filed**

(74) Representative: **Sayer, Robert David et al**
BT Group Legal
Intellectual Property Department
PP C5A
BT Centre
81 Newgate Street
London EC1A 7AJ (GB)

(54) **Authentication policy**

(57) A method of managing an authentication policy in a mobile telecommunications device, wherein the mobile telecommunications device comprises a plurality of security module applications, said method comprising the steps of: providing a profile associated with each of the plurality of security module applications, wherein each profile identifies at least one network with which the associated security module application can be used to enable communications; generating an authentication table based on the plurality of profiles provided, wherein said authentication table specifies each of the networks identified in the profiles provided and associates with each of the networks identified an application identifier, wherein each application identifier corresponds to one of the security module applications; and determining, based on the authentication table, one of the plurality of security module applications to use to enable communications with a network identified by the mobile telecommunications device.

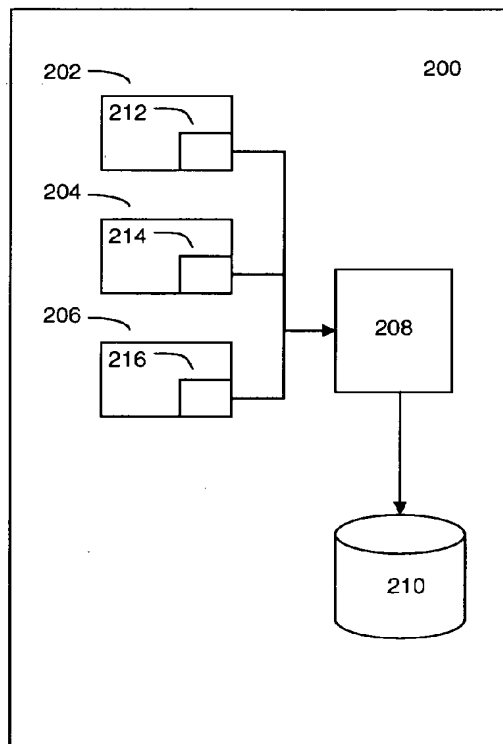


Figure 2

Description

Field of the Invention

[0001] The present invention relates to a method of managing security modules in mobile devices, in particular a method of managing network authentication profiles in multiple security modules for connecting to multiple networks.

Background to the Invention

[0002] Provision of communications services in mobile cellular networks, such as GSM and UMTS, are based upon a key sharing principle, where a secure smart card, a SIM (subscriber identity module), is used in a mobile device to store subscriber details, applications as well as an authentication key. Specifically, the subscriber details are stored in a SIM application resident on the SIM card and include an international mobile subscriber identity (IMSI), an authentication key Ki, as well as various operator secrets and other applications for handling authentication and encryption of communications data.

[0003] The SIM application is thus the core element that enables network identification i.e. it enables network operators to identify and subsequently authenticate a subscriber. In addition to the subscriber details and authentication keys used for identification and authentication, also programmed into the SIM application are the network operator's Mobile Country Code (MCC) and Mobile Network Code (MNC). These provide a reference to the network operator with which the SIM card can be used. Usually, the SIM application has a list of "preferred networks" with which it can connect, listing the MNC associated with each of the "preferred networks". Also commonly found is a list of "barred networks" with lists all the MNCs with which a SIM application should never be used with.

[0004] When the mobile device is switched on, the device scans the MNC list stored on the SIM application and at the same time scans all the GSM frequency bands the device can receive. Any networks operating in the area of the mobile device will be broadcasting their MNC over a broadcast channel. The mobile device determines all the available networks broadcasting in the area and attempts to connect to the MNC highest up on the preferred networks list. This is usually the MNC corresponding to home network of the SIM application i.e. the network belonging to the network operator that issued the SIM card.

[0005] The other MNCs on the preferred network list usually relate to other network operators for use when the subscriber "roams" in a different country for example.

[0006] Whilst a user can usually swap SIM cards in and out of a device to give access to multiple networks, there are no provisions to manage multiple simultaneously active SIM cards in a single device. In particular, existing solutions are based on the fact that there is only

one active SIM in a device at any given time. Furthermore, the SIM functionality provided by a SIM card is actually provided for by the SIM application. In practice, there can also be multiple SIM applications resident on a single card, each capable of providing network access to different networks and supporting distinct applications. These multiple SIM applications, either on a single SIM card or across multiple SIM cards, need to be managed efficiently in order for services to be delivered to the user effectively, in particular in relation to access to different networks.

Summary of the Invention

[0007] It is the aim of embodiments of the present invention to address one or more of the above-stated problems.

[0008] According to a first aspect of the present invention, there is provided a method of managing an authentication policy in a mobile telecommunications device, wherein the mobile telecommunications device comprises a plurality of security module applications, said method comprising the steps of:

- i) providing a profile associated with each of the plurality of security module applications, wherein each profile identifies at least one network with which the associated security module application can be used to enable communications;
- ii) generating an authentication table based on the plurality of profiles provided, wherein said authentication table specifies each of the networks identified in the profiles provided and associates with each of the networks identified an application identifier, wherein each application identifier corresponds to one of the security module applications;
- iii) determining, based on the authentication table, one of the plurality of security module applications to use to enable communications with a network identified by the mobile telecommunications device.

[0009] The security module applications may be subscriber identity module, or SIM applications, and the SIM applications may be located on a SIM card.

[0010] The profiles in the security module applications can identify a list of preferred networks with which the security module application is able to operate. These identified networks are listed by a network type element and a network identifier element. For example, the network type may be GSM, and the network identifier may be the mobile network code (MNC) of the particular GSM network.

[0011] Preferably, the network broadcasts a network identifier and the mobile telecommunications device uses the network identifier to identify the network.

[0012] The profiles may be stored with the associated security module application, and preferably on a SIM card.

[0013] Preferably, the step of generating comprises combining each of the profiles and adding to each network identified in each profile the application identifier corresponding to security module application associated with the profile.

[0014] According to a second aspect of the present invention, there is provided a mobile telecommunications device comprising a plurality of security module applications, wherein each security module application is providing with a profile and each profile identifies at least one network with which the associated security module application can be used to enable communications, said mobile telecommunications device further comprising:

a processor for generating an authentication table based on the plurality of profiles provided, wherein said authentication table specifies each of the networks identified in the profiles provided and associates with each of the networks identified an application identifier, wherein each application identifier corresponds to one of the security module applications; and wherein said mobile device is adapted to determine, based on the authentication table, one of the plurality of security module applications to use to enable communications with a network identified by the mobile telecommunications device.

[0015] As the mobile device has several network connection means allowing connection to several networks at the same time (e.g. GSM, WiFi, Bluetooth), the ability to effectively and conveniently manage such connectivity is very important.

[0016] By having a device that can accept several SIM cards, or more particularly to manage several simultaneously active SIM applications in the device at the same time, authentication and connectivity to different networks at the same time is possible.

[0017] Furthermore, SIM cards and SIM applications from different operators that are potentially competing on the marketplace can co-exist within a single device for the benefit of the user.

[0018] The device can also implement a 'best connected' policy for optimising connectivity so that it is always connected in a manner that is beneficial for the user. Such a policy can be fully automated and does not require any intervention for the user, thus improving usability and delivering true seamless roaming experience.

[0019] Embodiments of the present invention also allow for SIM cards and SIM applications implemented in the device in different formats (e.g. on a standard SIM card, in software only, within some other trusted hardware module, on memory card), thus increasing flexibility of operator's provisioning methods.

Brief Description of the Drawings

[0020] For a better understanding of the present invention reference will now be made by way of example only

to the accompanying drawings, in which:

Figure 1 is a simplified diagram of a SIM card showing two separate SIM applications in an embodiment of the present invention;

Figure 2 is a diagram showing a mobile device and a plurality of SIM applications and their associated profile files in an embodiment of the present invention;

Figure 3 is a table showing the format of an authentication policy in an embodiment of the present invention;

Figure 4 is a network diagram showing an arrangement in which an embodiment of the present invention can be utilised with three different networks.

Description of the Preferred Embodiments

[0021] The present invention is described herein with reference to particular examples. The invention is not, however, limited to such examples.

[0022] Figure 1 shows a SIM card 100 holding two SIM applications, SIM_app_1 102 and SIM_app_2 104. Each SIM application holds separate subscriber details such as an IMSI, authentication key Ki, and other unique parameters. Each SIM application is also provided with an authentication profile file. SIM_app_1 102 includes authentication profile file 106 and SIM_app_2 includes authentication profile 108.

[0023] Each of the authentication profile files list details of the network type and network ID that the corresponding SIM application can be used in. The network type details the type of network the SIM can be used in such as a GSM network, a WiFi network or a Bluetooth network. The network type can be specified by name or preferably by the broadcast frequency or frequency band of the network. The network ID uniquely identifies the specific network within the network type or frequency band. For example, the network ID may be specified by the mobile network code (MNC) if the network type is a GSM network, or the network ID may be a service set identifier (SSID) if the network type is a WiFi network.

[0024] Figure 2 shows a mobile device 200, such as a smart phone, having multiple network access means. The mobile device 200 can access the various communications networks such as GSM mobile networks, WiFi network and also has Bluetooth access. Mobile device 200 also includes two SIM cards. The SIM cards are not shown in the Figure, but the SIM applications that are resident on the SIM cards are shown. In this example, the first SIM card (not shown) holds two SIM applications, which are shown as SIM_A_1 202 and SIM_A_2 204. The first SIM card may be issued by network operator A, and the associated SIM applications are enabled for use with networks controlled by network operator A.

[0025] The other SIM card (not shown) has only one SIM application, SIM_B_1 206. The other SIM card may be issued by network operator B, and the Sim application

therein for use with networks run by network operator B.

[0026] Each SIM application also has a corresponding authentication profile file. SIM_A_1 202 has authentication profile file File_A_1 212, SIM_A_2 204 has authentication profile file File_A_2 214 and SIM_B_1 206 has authentication profile file File_B_1 216. The authentication profile file includes a list of networks that the SIM application can be used with, where the network is specified by a network type field and a network ID field as described in relation to Figure 1 above.

[0027] In this example, File_A_1 212 has entries for one network identified by "GSM 900, MNC 200", where GSM 900 is the network type and MNC 200 is the network ID, and similarly another network identified by "WiFi, SSID 1111". File_A_2 214 has entries for the network "WiFi, SSID 1111". File_B_1 216 has entries for "GSM 1800, MNC 300".

[0028] The mobile device 200 also includes a processor 208 for handling the SIM applications and processing the authentication profile files. When the mobile device 200 is first switched on, the processor detects the presence of the different SIM applications and starts reading the authentication profile files. The processor 208 then takes the details of the networks listed in the authentication profile file and generates an authentication policy table 300 as shown in Figure 3.

[0029] The authentication policy table 300 has a network_type field 302, a network_ID field 304 and a SIM_app field 306. Four entries 308, 310, 312 and 314 are shown in the policy table 300 based on the entries from the authentication profile files collected from the SIM applications by the processor 208. Each entry includes the network type and network_ID as taken from the individual authentication profile files 212, 214 and 216. Also included in each entry is a reference to the SIM application to which the entry corresponds under the SIM_app field 306.

[0030] The authentication policy table 300 is stored locally on the mobile device in data store 210, such as RAM or flash memory, and is used by the mobile device 200 to automatically determine which SIM application to use for a network connection.

[0031] Figure 4 shows a network arrangement 400 including a mobile device 200 loaded with the SIM applications and authentication policy table 300 described above. Figure 4 shows 3 different networks: a GSM network 402, another GSM network 404 and a WiFi network 406. After the mobile device 200 has been activated and generated the authentication policy table 300 as described above, the mobile device starts scanning for the available networks. The mobile device 200 detects GSM network 402, GSM network 404 and WiFi network 406. The mobile device then scans each of these networks further to determine the network type and/or the network ID. In many cases the network type is automatically determined depending on which receiver the mobile device 200 has used to scan for networks e.g. network 402 is detected using a GSM receiver in the mobile device 200

and thus is automatically determined as a GSM network.

[0032] The network ID associated with each network may be broadcasted over a general broadcast channel that can be received by the mobile device 200 or any similar device equipped with a suitable receiver. In this example, the GSM network 402 is identified as having a network ID (in this case a mobile network code MNC) of 200. Similarly, the GSM network 404 is identified as having a network ID of 300. The mobile device 200 also scans the WiFi channels of WiFi network 406 and determines that the network ID, the SSID of the router, is 1111.

[0033] The processor 208 in the mobile device 200 then uses the authentication profile table 300 to determine which SIM application it should use to connect to which network. The processor 208 determines that GSM network 402 with a network ID of 200 can only be connected to using SIM application SIM_A_1 (see 308 of Figure 3) which is associated with the same network type and identifier. The processor 208 also determines that GSM network 404 with a network ID of 200 can only be connected to using SIM application SIM_B_1 (see 310 of Figure 3) which is associated with the same network type and identifier. However, for WiFi network 406 which has a network ID of 1111, either SIM application SIM_A_1 or SIM_A_2 can be used to connect. In such cases, the processor 208 can employ a suitable resolution method, for example giving priority to one of the applications which the user has previously defined as being the preferred application.

[0034] In practice, it may also only be possible to connect to one network of any one type at a time, due to limitations on receivers unless the mobile device 200 includes more than one receiver. So in this example, the mobile device 200 can only connect to one of the GSM networks 402 or 404 at any given time. The determination of which one to connect to can be resolved again by providing a priority to the SIM applications and network IDs. Assuming that each network ID for each SIM application is given a priority, then in the event of any conflict in network type where the device can only connect to one network of a given network type, or if there is a conflict between SIM applications for a given network, then the priority is used to determine which network or SIM application to use in each respective situation. The priorities can be represented in the authentication policy table by the order in which the entries are listed.

[0035] After the mobile device 200 has used the authentication policy table 300 to determine that SIM application SIM_A_1 should be used to connect to the GSM network 402, the mobile device can use the subscriber details, such as the IMSI, stored on SIM_A_1 to register and authenticate with the network 402. The process of authentication will include verification of the SIM application where the network 402 issues a challenge to the authentication key Ki stored at the SIM application. The response generated by the SIM application is checked against a response generated by the network based on a copy of the authentication key Ki stored in the network.

[0036] The authentication profile file associated with each SIM application can be preloaded with the preferred network details when the SIM card is loaded with the SIM applications during manufacture. Furthermore, the authentication profile file can be modified by the network operator over the network to add or delete network details.

[0037] More complex policies that include e.g. a history of connections, presence of other networks, availability of billing information or current time can be deployed as well. Specifically, policies that are used to determine the selection of the network can be remotely updated, independently from the update of authentication profile files.

[0038] In general, it is noted herein that while the above describes examples of the invention, there are several variations and modifications which may be made to the described examples without departing from the scope of the present invention as defined in the appended claims. One skilled in the art will recognise modifications to the described examples.

Claims

1. A method of managing an authentication policy in a mobile telecommunications device, wherein the mobile telecommunications device comprises a plurality of security module applications, said method comprising the steps of:
 - i) providing a profile associated with each of the plurality of security module applications, wherein each profile identifies at least one network with which the associated security module application can be used to enable communications;
 - ii) generating an authentication table based on the plurality of profiles provided, wherein said authentication table specifies each of the networks identified in the profiles provided and associates with each of the networks identified an application identifier, wherein each application identifier corresponds to one of the security module applications;
 - iii) determining, based on the authentication table, one of the plurality of security module applications to use to enable communications with a network identified by the mobile telecommunications device.
2. A method according to claim 1, wherein each network identified in the profiles comprises a network type element and a network identifier element.
3. A method according to claim 1 or claim 2, wherein each security module application is a subscriber identity module application.
4. A method as claimed in any preceding claim, wherein

the mobile telecommunications device uses a network identifier broadcast by the network to identify the network.

5. A method as claimed in any preceding claim, wherein each profile is stored with the associated security module application.
6. A method as claimed in any preceding claim, wherein the step of generating comprises combining each of the profiles and adding to each network identified in each profile the application identifier corresponding to security module application associated with the profile.
7. A method as claimed in any preceding claim wherein the security module application is located on a tamper proof security module.
8. A method as claimed in claim 7, wherein the tamper-proof security module is a subscriber identity module.
9. A mobile telecommunications device comprising a plurality of security module applications, wherein each security module application is providing with a profile and each profile identifies at least one network with which the associated security module application can be used to enable communications, said mobile telecommunications device further comprising:

a processor for generating an authentication table based on the plurality of profiles provided, wherein said authentication table specifies each of the networks identified in the profiles provided and associates with each of the networks identified an application identifier, wherein each application identifier corresponds to one of the security module applications; and wherein said mobile device is adapted to determine, based on the authentication table, one of the plurality of security module applications to use to enable communications with a network identified by the mobile telecommunications device.

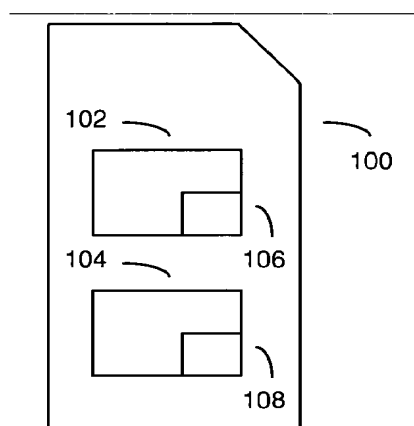


Figure 1

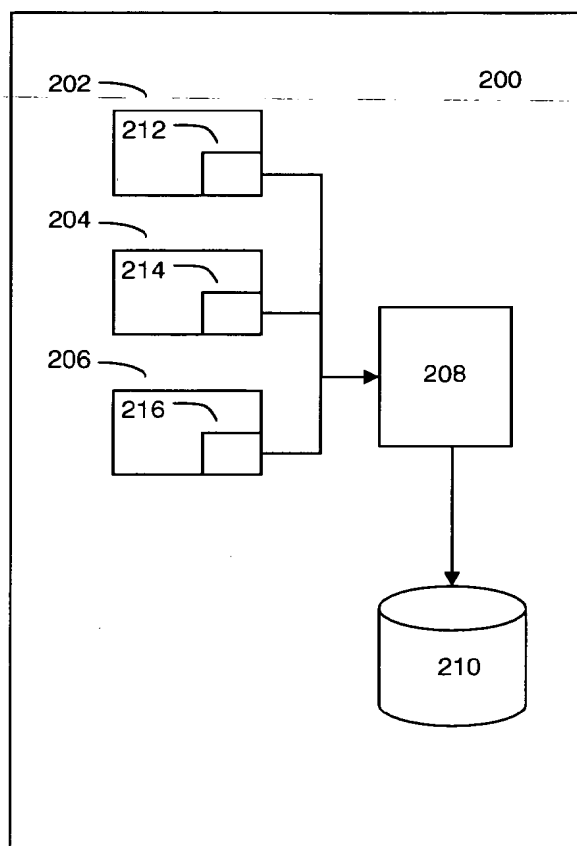


Figure 2

302 304 306

network_type	network_ID	SIM_app
GSM 900	MNC 200	SIM_A_1
GSM 1800	MNC 300	SIM_B_1
WiFi	1111	SIM_A_1
WiFi	1111	SIM_A_2

308
310
312
314

300

Figure 3

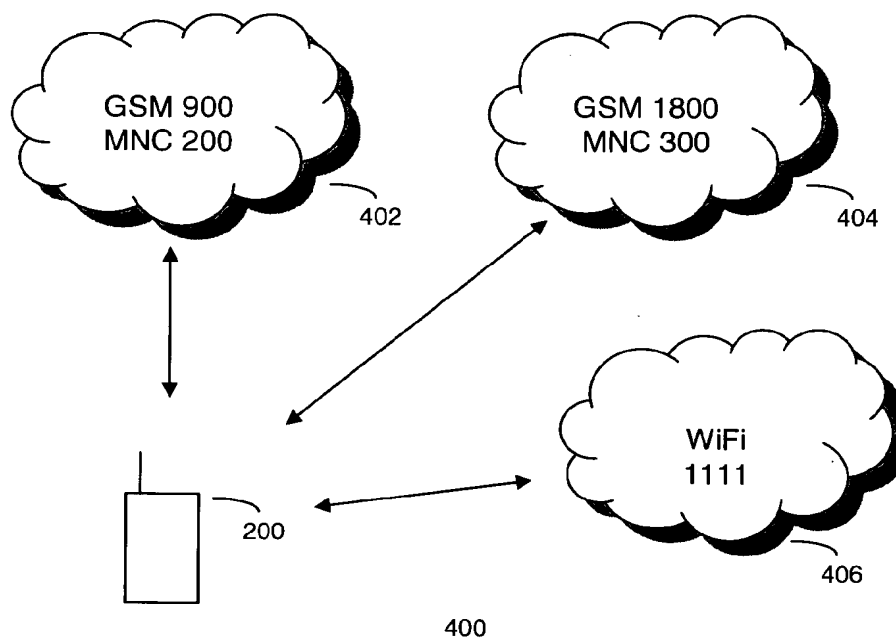


Figure 4



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 25 1454

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	EP 1 513 358 A (RES IN MOTION LTD [CA]) 9 March 2005 (2005-03-09) * abstract * * paragraph [0003] * * paragraph [0008] - paragraph [0009] * * paragraph [0016] - paragraph [0018] * * paragraph [0044] - paragraph [0045] * * paragraph [0047] * * paragraph [0051] - paragraph [0054] * * claims 1-3,8-10 * * figures 4,5,7 *	1-9	INV. H04Q7/38 H04L29/06
X	US 2004/022216 A1 (SHI GUANGMING CARL [US]) 5 February 2004 (2004-02-05) * abstract * * paragraph [0007] - paragraph [0008] * * paragraph [0010] - paragraph [0014] * * paragraph [0024] - paragraph [0026] * * paragraph [0028] - paragraph [0031] * * paragraph [0035] * * paragraph [0040] - paragraph [0041] * * paragraph [0047] - paragraph [0049] * * paragraph [0085] - paragraph [0106] * * figures 1,2,5 *	1-9	TECHNICAL FIELDS SEARCHED (IPC) H04L H04Q
X	WO 03/100647 A (RUSSELL JESSE E [US]) 4 December 2003 (2003-12-04) * abstract * * page 1 - page 6 * * page 9 - page 13 * * page 15 - page 19 * * claims 1,16,25 * * figures 1,2B,2C,2D,2E * ----- -/--	1-9	
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 29 November 2007	Examiner Kopp, Klaus
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

 1
EPO FORM 1503 03/82 (P04C01)



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 25 1454

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	GB 2 395 867 A (ORANGE PERSONAL COMM SERV LTD [GB]; ORANGE SA [FR]) 2 June 2004 (2004-06-02) * abstract * * figure 3 * * page 1, line 13 - line 19 * * page 2, line 8 - line 15 * * page 8, line 14 - page 11, line 3 * -----	1-9	
X	WO 2006/138338 A (QUALCOMM INC [US]; KHANDELWAL DEEPAK [US]; JAIKUMAR SELVARAJ [US]; UCH) 28 December 2006 (2006-12-28) * paragraph [0013] * * paragraph [0017] - paragraph [0018] * * paragraph [0028] - paragraph [0029] * * paragraph [0047] - paragraph [0048] * * paragraph [0053] - paragraph [0056] * * figures 2,5,6A,6B * -----	1-9	
A	DE 101 38 835 A1 (T MOBILE DEUTSCHLAND GMBH [DE]) 27 February 2003 (2003-02-27) * the whole document * -----	1-9	
The present search report has been drawn up for all claims			TECHNICAL FIELDS SEARCHED (IPC)
Place of search Munich		Date of completion of the search 29 November 2007	Examiner Kopp, Klaus
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

 1
EPO FORM 1503 03.92 (F04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 07 25 1454

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

29-11-2007

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1513358 A	09-03-2005	AT 356515 T CA 2478008 A1 DE 60312326 T2 HK 1075996 A1 US 2005113088 A1	15-03-2007 03-03-2005 08-11-2007 14-09-2007 26-05-2005
US 2004022216 A1	05-02-2004	AU 2003254291 A1 CN 1682563 A MX PA05001360 A WO 2004014100 A1	23-02-2004 12-10-2005 27-05-2005 12-02-2004
WO 03100647 A	04-12-2003	AU 2003241592 A1 EP 1540499 A1	12-12-2003 15-06-2005
GB 2395867 A	02-06-2004	AU 2003302358 A1 CN 1717946 A EP 1568243 A1 WO 2004049744 A1 US 2006217153 A1	18-06-2004 04-01-2006 31-08-2005 10-06-2004 28-09-2006
WO 2006138338 A	28-12-2006	US 2006286977 A1	21-12-2006
DE 10138835 A1	27-02-2003	NONE	

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
16 December 1999 (16.12.1999)

PCT

(10) International Publication Number
WO 99/65185 A3(51) International Patent Classification⁶: **H04L 12/14**,
12/56, H04Q 3/00**John** [GB/GB]; Home Farm, Parham, Woodbridge, Suffolk
IP13 9NW (GB). **RIZZO, Michael** [MT/GB]; 12 Dewar
Lane, Kesgrave, Ipswich, Suffolk IP5 2GJ (GB).

(21) International Application Number: PCT/GB99/01773

(22) International Filing Date: 4 June 1999 (04.06.1999)

(74) Agent: **EVERSHED, Michael**; BT Group Legal Services,
Intellectual Property Dept., 8th floor, Holborn Centre, 120
Holborn, London EC1N 2TE (GB).

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

9812161.9	5 June 1998 (05.06.1998)	GB
98309609.0	24 November 1998 (24.11.1998)	EP
9825723.1	24 November 1998 (24.11.1998)	GB
9902052.1	29 January 1999 (29.01.1999)	GB
9902648.6	5 February 1999 (05.02.1999)	GB

(81) Designated States (*national*): AE, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE,
ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP,
KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD,
MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD,
SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ,
VN, YU, ZA, ZW.(71) Applicant (*for all designated States except US*): **BRITISH
TELECOMMUNICATIONS PUBLIC LIMITED
COMPANY** [GB/GB]; 81 Newgate Street, London EC1A
7AJ (GB).(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM,
AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT,
BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,
NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA,
GN, GW, ML, MR, NE, SN, TD, TG).

(72) Inventors; and

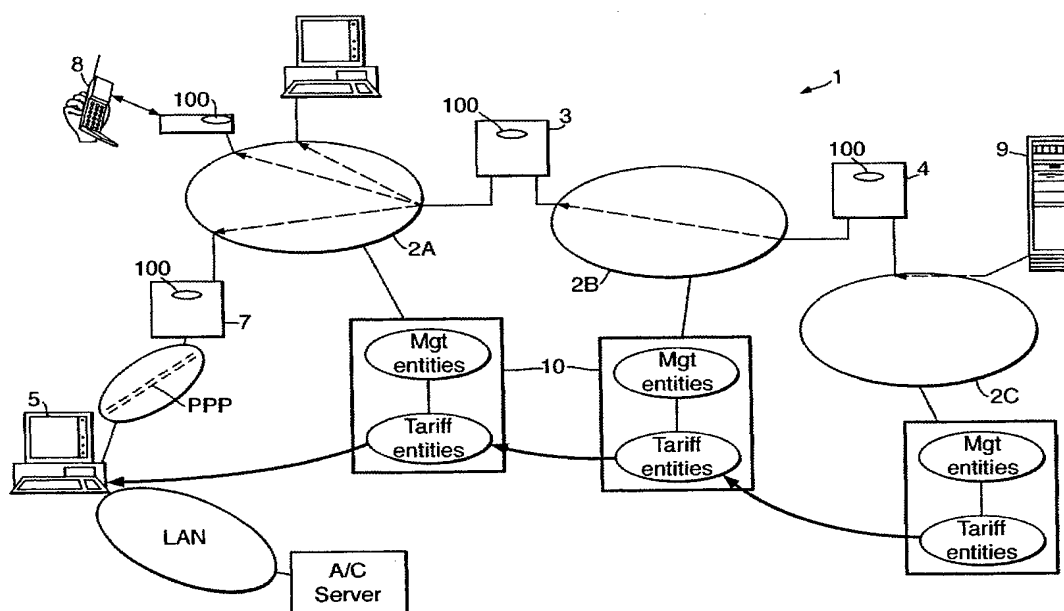
Published:

(75) Inventors/Applicants (*for US only*): **BRISCOE, Robert**,

— With international search report.

[Continued on next page]

(54) Title: COMMUNICATIONS NETWORK WITH TARIFF BASED ON NETWORK LOAD



(57) Abstract: In a communications network, loading of network resources is detected locally at a customer terminal, and a tariff for network usage is varied automatically depending on the usage.



(88) Date of publication of the international search report:
3 May 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 99/01773

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04L12/14 H04L12/56 H04Q3/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L H04Q H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SIETMANN R: "TARIFMODELLE GEGEN STAUS AUF DER INFOBAHN" FUNKSCHAU, vol. 71, no. 8, 3 April 1998 (1998-04-03), pages 28-30, XP000779238	1,14-16
A	page 28, left-hand column, line 1 -right-hand column, line 40 --- -/--	2,4,11, 17

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *Z* document member of the same patent family

Date of the actual completion of the international search

18 October 1999

Date of mailing of the international search report

25/10/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5810 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Lievens, K

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 99/01773

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MURPHY J ET AL: "DISTRIBUTED PRICING FOR EMBEDDED ATM NETWORKS" FUNDAMENTAL ROLE OF TELETRAFFIC IN THE EVOLUTION OF TELECOMMUNICATION NETWORKS, PROCEEDINGS OF THE 14TH. INTERNATIONAL TELETRAFFIC CONGRESS - ITC 1 JUAN-LEES-PINS, JUNE 6 - 10, 1994, no. 1B, 6 June 1994 (1994-06-06), pages 1053-1063, XP000593354 LABETOULLE J;ROBERTS J W (EDS) ISBN: 0-444-82031-0	1,2, 14-16
Y A	page 1054, line 17 -page 1055, line 10 page 1057, line 6-14 page 1060, line 9 -page 1061, line 15	3-6,11 7-9,12, 13,17
Y	B. KALTENMORGEN, R. KLEINWILLINGHÖFER-KOPP: "Verkehrskontrolle in ATM-Netzen" DER FERNMELDE INGENIEUR, vol. 46, no. 1, January 1992 (1992-01), pages 1-33, XP000407119 page 6, line 21-29	3
Y	ESTRIN D ET AL: "DESIGN CONSIDERATIONS FOR USAGE ACCOUNTING AND FEEDBACK IN INTERNETWORKS" COMPUTER COMMUNICATIONS REVIEW, vol. 20, no. 5, 1 October 1990 (1990-10-01), pages 56-66, XP000167877 ISSN: 0146-4833 page 60, left-hand column, line 40-52 page 64, right-hand column, line 13-32	4-6,11
A	MACKIE-MASON J K ET AL: "PRICING CONGESTIBLE NETWORK RESOURCES" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, vol. 13, no. 7, 1 September 1995 (1995-09-01), pages 1141-1149, XP000577206 page 1141, left-hand column, line 1 -page 1145, left-hand column, line 6	1,2, 14-16

-/--

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 99/01773

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MURPHY L ET AL: "FEEDBACK AND EFFICIENCY IN ATM NETWORKS" 1996 IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS (ICC), CONVERGING TECHNOLOGIES FOR TOMORROW'S APPLICATIONS DALLAS, JUNE 23 - 27, 1996, vol. 2, 23 June 1996 (1996-06-23), pages 1045-1049, XP000625931 INSTITUTE OF ELECTRICAL & ELECTRONICS ENGINEERS page 1045, right-hand column, line 37 -page 1047, right-hand column, line 42 ---	1,14-16
A	HIDANO F: "A PRACTICAL AND ECONOMICAL APPROACH TO RESOURCE ALLOCATION" 1997 IEEE 47TH. VEHICULAR TECHNOLOGY CONFERENCE, PHOENIX, MAY 4 - 7, 1997, vol. 3, no. CONF. 47, 18 November 1996 (1996-11-18), pages 1107-1113, XP000741599 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS page 1109, right-hand column, line 25 -page 1110, left-hand column, line 17 ---	1,14-16
A	DAVID CLARK: "A model for cost allocation and pricing in the Internet" MIT WORKSHOP ON INTERNET ECONOMICS, March 1995 (1995-03), XP002102708 http://www.press.umich.edu/jep/works/ClarkModel.html cited in the application page 2, line 11-33 page 8, line 15 -page 10, line 31 page 15, line 21 -page 16, line 15 ---	1,14-16
A	WO 98 02828 A (BELLSOUTH CORP) 22 January 1998 (1998-01-22) abstract page 6, line 4 -page 13, line 8 page 14, line 8 -page 15, line 2 page 19, line 17 -page 21, line 16 page 23, line 26 -page 25, line 8 page 27, line 18 -page 30, line 6 page 32, line 17 -page 33, line 1 figures 2,3 ----- -/--	9

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 99/01773

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>WO 97 05749 A (WULKAN ITZHAK ;BARAK GIDEON (IL); CALL MANAGE LTD (IL)) 13 February 1997 (1997-02-13) abstract page 1, line 9-29 page 5, line 15 -page 7, line 30 page 11, line 13-28 page 22, line 12 -page 23, line 30 page 25, line 26 -page 26, line 32 figures 7-9,11</p> <p style="text-align: center;">-----</p>	9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/GB 99/01773

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9802828 A	22-01-1998	AU 3660997 A CA 2259367 A EP 0913050 A	09-02-1998 22-01-1998 06-05-1999
WO 9705749 A	13-02-1997	US 5764741 A US 5799072 A AU 705826 B AU 6368396 A CA 2227569 A EP 0865706 A US 5862203 A	09-06-1998 25-08-1998 03-06-1999 26-02-1997 13-02-1997 23-09-1998 19-01-1999



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 12/00	A2	(11) International Publication Number: WO 99/65185 (43) International Publication Date: 16 December 1999 (16.12.99)		
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top; padding: 5px;"> (21) International Application Number: PCT/GB99/01773 (22) International Filing Date: 4 June 1999 (04.06.99) (30) Priority Data: <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 60%;"> 9812161.9 5 June 1998 (05.06.98) 98309609.0 24 November 1998 (24.11.98) 9825723.1 24 November 1998 (24.11.98) 9902052.1 29 January 1999 (29.01.99) 9902648.6 5 February 1999 (05.02.99) </div> <div style="width: 35%; text-align: right;"> GB EP GB GB GB </div> </div> (71) Applicant (for all designated States except US): BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB). (72) Inventors; and (75) Inventors/Applicants (for US only): BRISCOE, Robert, John [GB/GB]; Home Farm, Parham, Woodbridge, Suffolk IP13 9NW (GB). RIZZO, Michael [MT/GB]; 12 Dewar Lane, Kesgrave, Ipswich, Suffolk IP5 2GJ (GB). (74) Agent: EVERSLED, Michael; BT Group Legal Services, Intellectual Property Dept., 8th floor, Holborn Centre, 120 Holborn, London EC1N 2TE (GB). </td> <td style="width: 50%; vertical-align: top; padding: 5px;"> (81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>Without international search report and to be republished upon receipt of that report.</i> </td> </tr> </table>			(21) International Application Number: PCT/GB99/01773 (22) International Filing Date: 4 June 1999 (04.06.99) (30) Priority Data: <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 60%;"> 9812161.9 5 June 1998 (05.06.98) 98309609.0 24 November 1998 (24.11.98) 9825723.1 24 November 1998 (24.11.98) 9902052.1 29 January 1999 (29.01.99) 9902648.6 5 February 1999 (05.02.99) </div> <div style="width: 35%; text-align: right;"> GB EP GB GB GB </div> </div> (71) Applicant (for all designated States except US): BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB). (72) Inventors; and (75) Inventors/Applicants (for US only): BRISCOE, Robert, John [GB/GB]; Home Farm, Parham, Woodbridge, Suffolk IP13 9NW (GB). RIZZO, Michael [MT/GB]; 12 Dewar Lane, Kesgrave, Ipswich, Suffolk IP5 2GJ (GB). (74) Agent: EVERSLED, Michael; BT Group Legal Services, Intellectual Property Dept., 8th floor, Holborn Centre, 120 Holborn, London EC1N 2TE (GB).	(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>Without international search report and to be republished upon receipt of that report.</i>
(21) International Application Number: PCT/GB99/01773 (22) International Filing Date: 4 June 1999 (04.06.99) (30) Priority Data: <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 60%;"> 9812161.9 5 June 1998 (05.06.98) 98309609.0 24 November 1998 (24.11.98) 9825723.1 24 November 1998 (24.11.98) 9902052.1 29 January 1999 (29.01.99) 9902648.6 5 February 1999 (05.02.99) </div> <div style="width: 35%; text-align: right;"> GB EP GB GB GB </div> </div> (71) Applicant (for all designated States except US): BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB). (72) Inventors; and (75) Inventors/Applicants (for US only): BRISCOE, Robert, John [GB/GB]; Home Farm, Parham, Woodbridge, Suffolk IP13 9NW (GB). RIZZO, Michael [MT/GB]; 12 Dewar Lane, Kesgrave, Ipswich, Suffolk IP5 2GJ (GB). (74) Agent: EVERSLED, Michael; BT Group Legal Services, Intellectual Property Dept., 8th floor, Holborn Centre, 120 Holborn, London EC1N 2TE (GB).	(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>Without international search report and to be republished upon receipt of that report.</i>			
(54) Title: COMMUNICATIONS NETWORK				
(57) Abstract <p>In a communications network, loading of network resources is detected locally at a customer terminal, and a tariff for network usage is varied automatically depending on the usage.</p>				

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

Communications Network**BACKGROUND TO THE INVENTION**

The present invention relates to a communications network, and in particular
5 to charging mechanisms in such a network. It includes aspects of the inventions
disclosed and claimed in the present applicant's co-pending British patent application
no. 9812161.9 filed 5 June 1998 (applicant's ref: A25547) and the contents of that
earlier application are incorporated herein by reference.

In conventional communications networks, such as national PSTNs (public
10 switched telephone networks), a significant proportion of the network resources are
devoted to metering and billing network usage. Studies have estimated these
resources as consuming as much as 6% of the revenue of a telecommunications
company. The Internet, by contrast, does not in general incorporate metering and
billing mechanisms for individual customers. The absence of the network
15 infrastructure required to support metering and billing reduces the operational costs
of the Internet compared to conventional telephony networks, and has facilitated the
rapid expansion of the Internet. However, the absence of appropriate billing
mechanisms has significant disadvantages in terms of the characteristics of the
traffic carried by the Internet: it encourages profligate use of network resources, and
20 diminishes the incentive for investment in network infrastructure to support new
applications requiring, e.g., guaranteed quality of service (QoS).

SUMMARY OF THE INVENTION

According to a first aspect of the present invention, there is provided a
25 method of operating a communications network, including automatically varying,
depending on network loading as detected at a customer terminal, a tariff for
network usage by the customer terminal.

In this document references to varying a tariff encompass changing a price,
e.g. as a function of a congestion parameter. The structure of the tariff may be
30 unchanged.

The present invention provides an approach to charging for network usage
which involves little or no network overheads, and which moreover is able to reflect
local variations in network loading. This is achieved by detecting a measure of

network loading at the customer terminal. This measure will reflect those resources being used by the customer terminal at a particular time. For example, in a federated data network comprising a number of sub-domains, such as the Internet, a customer terminal in one subdomain may attempt to access a server in another subdomain at a time when there is overloading of a router somewhere in the path from the customer terminal to the server. Then, even if average loading of the network as a whole is low, the loading as perceived by the customer terminal is high, and a tariff for use of the network by the customer terminal is increased to reflect the scarcity of the relevant network resources. Similarly other terminals attempting to access data via the same router will also perceive the network loading as being high, and will also have their tariffs increased accordingly. With an appropriately steep rise in tariff, at least some customer terminals will then choose to abandon or defer their attempts to use the network resource in question, thereby relieving the loading of the router.

This aspect of the invention may be used in systems in which the end user is merely informed of the price and accounting and billing is carried out by the network provider, also in systems where the end user measures their usage and supplies this information to the network provider, and also in systems where the end user both measures their usage and calculates the payment due to the network provider.

The method may include detecting at the customer terminal a network performance parameter which depends on network loading, and varying the tariff depending on the network performance parameter. When the network is a packet network, then the network performance parameter may be the number of packets lost in transmission between a data source and the customer terminal. This approach has the advantage that it is suitable for implementation using existing congestion control mechanisms in packet networks. For example, in the Internet, routers respond to congestion by dropping packets, and a customer terminal using TCP (Transport Control Protocol) detects packet loss and controls a congestion window at the terminal accordingly. The present invention may use the detected packet loss to trigger an increase in the tariff applicable to the terminal. This may be accompanied by the signalling of congestion by the receiving terminal to the data source.

In an alternative and preferred approach, when congestion is detected within the network an explicit congestion signal may be generated and transmitted to the customer terminal, and the receipt of the explicit congestion signal at the customer

terminal may then trigger the increase in the tariff. This approach has the advantage that an appropriate congestion signal may be generated in advance of significant degradation in network performance occurring, making it easier to maintain a required quality of service. Preferably the explicit congestion signal is carried with a data
5 packet on the communications network. Preferably a router in the network writes an explicit congestion signal in a packet when congestion is detected at the router.

As a further alternative, the congestion notification signal may be a source quench signal generated at the router and transmitted back to the data source.

Preferably there is a non-linear relationship between the increase in tariff and
10 the detected network loading. Preferably the method includes making a first relatively smaller increase in the tariff when congestion is first detected, and making at least one further, relatively larger increase, if the congestion persists. This behaviour may be pre-programmed into the tariff algorithm. In this way oscillatory behaviour of the network can be avoided, while ensuring that a sufficient increase is made to have a
15 desired impact on the demand for network resources.

Preferably the method includes programming a decision agent at the customer terminal with user-determined price criteria, and comparing a price calculated using the tariff with the said price criteria. For example, the decision agent might be programmed to proceed with data communications as long as a per-
20 packet charge is zero or is less than a predetermined threshold. Then if congestion causes the charge to rise above that threshold, the data communication is interrupted and the decision agent modifies the operation of the customer terminal. For example the decision agent may slow down communications once the cost threshold is exceeded. The user may then choose to continue with the communication, or may
25 elect to abandon the attempt to access data from a particular source. The decision agent may be programmed with rules which relate to an overall price for multiple simultaneous transmissions and which accord different weights to different respective applications.

Preferably the method includes distributing a tariff algorithm via the
30 communications network to a plurality of terminals and calculating at each terminal using the tariff a charge for network usage by the terminal. In this case preferably the method includes steps, carried out by a network operator, of intermittently

sampling traffic between a customer terminal and the network, and as part of the sampling recording network loading affecting the customer terminal;

for the sampled traffic comparing a charge calculated by the customer terminal and an expected charge and detecting thereby any discrepancy.

5 The step of recording network loading may involve, for example, recording packet drops, or explicit congestion notification (ECN) bits or source quench messages.

The invention also encompasses a network operating by a method in accordance with the first aspect of the invention, and customer terminals, network
10 routers and other network nodes for use in such a network.

DESCRIPTION OF DRAWINGS

Systems embodying the present invention will now be described in further detail, by way of example only, with reference to the accompanying drawings, in
15 which:

Figure 1 is a schematic showing a network embodying the invention;

Figures 2a and 2b are graphs showing tariff functions;

Figure 3 shows the format of a differential service byte;

Figure 4 is a schematic showing the component objects of a charging
20 architecture for use with the network of Figure 1;

Figure 5 shows data passed between the accounting objects of Figure 4;

Figure 6 is a schematic showing protocol stacks on a customer terminal and in the network domain;

Figure 7 is a graph showing the variation of tariff with time;

25 Figures 8a to 8e are class diagrams for software implementing accounting and measurement objects;

Figure 9 is a diagram showing a graphic user interface (GUI) for use with the objects of figures 8a to 8e;

Figure 10 is a class diagram for software implementing tariff objects; and

30 Figure 11 is a diagram showing an alternative embodiment.

DESCRIPTION OF EXAMPLES

As shown in Figure 1, a communications network 1 includes a number of network sub-domains 2A-C. The network sub-domains may be under the control of different operators who may not trust each other. The network subdomains are interconnected by gateway routers 3, 4. In the present example the communications network is the Internet and supports both unicast and multicast Internet Protocol (IP) and associated protocols. A customer terminal 5 is connected via a public switched telephony network (PSTN) 6 and an access router 7 to a subdomain 2A. A single blocking test is applied to traffic at this point of access. The gateway routers 3,4, and access router 7 may be commercially available devices such as CISCO series 7500 routers and CISCO series AS5800 universal access server respectively. Other customer terminals are connected to the network, including a Java-enabled mobile terminal 8 and a data server 9. The customer terminal 5 may be connected via a LAN to an accounting server. The accounting server may include an accounting object as described below that receives measurement data from the customer terminal.

In addition to the local tariff variation mechanism that is described below, the network also uses network-based control of a number of tariff bands. A network management platform 10 is connected to each subdomain. Each network management platform may comprise, for example, a computing system comprising a SPARC workstation running UNIX (Solaris) together with network management applications. The network management platform 10 hosts management entities and tariff entities. The network management platform communicates with agents 100 in managed devices connected to the respective subdomain, for example using SNMP (simple network management protocol). The management platforms monitors the overall loading of network resources in the respective subdomains, and, as will be further described below, adjust the tariffs for network use accordingly. The Net management platform (NMP) instructs the agent to monitor the device and report aggregated results at regular intervals back to the NMP, so the NMP can monitor the combination of all reports.

Tariff data is communicated to peer tariff entities in other subdomains and also to the customer terminals. The tariff data is multicast using, for example Distance Vector Multicast Routing Protocol (DVMRP) or Protocol Independent Multicast (PIM) dense mode. The tariff data channels are announced and monitored

using protocols based on SDP (Session Description Protocol), SAP (Session Announcement Protocol) Charging is carried out on a "pay and display" model. Each customer terminal monitors its own network usage, for example by counting the number of packets it sends or receives across the network interface and the quantity
5 of data (in bytes) in those packets. It calculates, using a tariff received via the network, the payment due to the network operator, and makes a corresponding payment into an account at the network operator. The network operator polices the use made by customers of the terminal by intermittently sampling traffic to or from a particular customer and comparing the use made and the use paid for.

10 The tariffs supplied to the customer terminals are divided into bands of different volatilities. The tariffs are varied under the control of the network operators to reflect the overall loading of the network. That is to say, if network loading becomes high, then the tariffs may be increased to reflect the scarcity of network resources.

15 A service provider may offer different products defined by different service level agreements, and/or by different price volatilities. For example product A might offer best-effort service at a fixed price while another product B might offer best-effort service at a variable price. A service provider may adjust product prices on the basis of the following parameters: the price the service provider pays to its wholesale
20 provider: competitors' prices; current resource utilisation; relevant demand for different products. In response to changes in these parameters, tariff adjustments may be effected in one of three ways. Firstly, a tariff may adjust prices on the basis of local observations of network loading, without necessitating explicit communication from the provider. This approach, which is described in further detail
25 below, needs to be built into the tariff at the outset, and is limited to those price variations which are dependent exclusively on local observations. Secondly, the provider may tune a tariff by adjusting some of its parameters. This kind of adjustment is required when the decision is dependent on parameters which cannot be observed directly by the customer, e.g., variation in the wholesale price of
30 network resources. Thirdly, the provider may completely replace a tariff. This is required when the existing tariff cannot accommodate the changes that are required.

The first of the tariff changes described above is necessarily carried out automatically. The second type of change may be performed manually, or by an

agent that issues adjustments automatically in response to observations made by the service provider system. The third type of change is likely to be performed manually, as replacement of a new tariff will in general require an element of design requiring human input. However, it is possible that an agent might be employed to

5 automatically switch tariffs for a product on the basis of a set of specified rules.

This section describes a prototype that we implemented to demonstrate the tariff subsystem outlined above. Features of the design include:

- using mobile code to represent tariffs and associated user interface components;
- use of a repeated multicast announcement protocol to communicate tariffs and
- 10 tariff adjustments efficiently;
- using dynamic class loading and reflection in order to receive and tune tariffs.

The prototype consists of a library of general-purpose Java classes and two specific applications, namely:

- a provider system which allows the provider to introduce, replace, and tune tariffs
- 15 for a number of products;
- a customer system that enables customer to keep track of the charges being applied for the products they are using.

The provider system services multiple instances of the customer system running on different hosts in a multicast-enabled network. A multicast announcement protocol is

20 used to communicate tariff changes from the provider system to customer systems.

In order to maximise flexibility with respect to the definition of tariffs, we chose to represent tariffs using Java classes. This technique is also used to supply user interface components to customers to support visualisation of the behaviour of a tariff.

25 The `Tariff` interface acts as the base class for all tariffs. This defines a single operation `get GUI()` which returns as a Java SWING component that can be incorporated into the customer's GUI (graphical user interface). This GUI component enables the customer to visualise the behaviour of the tariff using techniques appropriate to the tariff.

30 Subclasses of the `Tariff` interface establish a set of tariff types, each of which is associated with a different set of measurement and input parameters. These parameters are identified by listing them in the signature of the `getCharge()` method. For example, the interface `RSVPTariff` defines `getCharge()` as

receiving an RSVP TSPEC, allowing for the definition of tariffs that compute price on the basis of the characteristics of an RSVP reservation. On the other hand, the interface PacketCountTariff defines getCharge () as receiving measurements of packets in, packets out, and current congestion (typically measured as a function of packet drop), allowing for the definition of tariffs that are dependent on packet counts and sensitive to congestion. Other tariffs may be added as new forms of usage-measurement emerge.

Tariffs are defined by providing implementations of the various tariff interfaces described above. For example, the tariff PacketCountLinear implements PacketCountTariff to compute charges in proportion to packet counts. Another tariff CongestionSensitiveLinear works on a similar basis, but adds a penalty charge if the customer does not stay within a specified traffic limit in the presence of congestion.

In addition to the tariff interface implementation, a tariff may make use of other 'helper' classes to assist in its operation, as well as one or more user interface component classes for customer visualisation purposes. A provider-side user interface may also be required in order to enable the provider to make tariff adjustments.

A complete tariff description consists of a set of Java classes, some of which are destined for the customer system and others which are intended for use by the provider system. The customer-side classes are bundled into a Java archive (JAR) file to facilitate processing by the provider system.

In order to deploy a new tariff, the provider system first loads the tariff classes which it requires into its execution environment. It then loads the customer-side bundle, serialises it, signs it with a private key, and uses an announcement protocol to distribute it to customer systems. The use of a signature makes it possible for customers to verify that received tariffs are authentic.

Upon receiving the bundle, each customer system verifies the signature (using the public key matching the provider's private key), and at the activation time specified in the announcement protocol headers which may be significantly later, e.g. hours or days, unpacks the bundle, and loads the classes into its execution environment using a purpose-built dynamic class loader. An instance of the received tariff class is created and installed in place of the previous tariff. If the tariff has a

user interface component (obtained by calling the tariff object's `getGUI ()` method), then it replaces the user interface of the previous tariff. The change in user interface serves to notify the user that the tariff has changed.

Tariff adjustment involves the remote invocation of an operation which is
5 specific to the tariff currently in force. This means that a customer system cannot know the signature of this operation in advance of receiving the tariff i.e. the operation will not be listed in any of the tariff interfaces known to the customer system.

In order to get around this problem, use is made of the "reflection" feature
10 supported by Java. In order to disseminate a tariff adjustment, the provider creates an instance of an `Invocation` object, which stores the name of the operation to be called, together with the parameters that are to be supplied to it. This object is then serialised, signed, and announced using the announcement protocol. When an adjustment is receive and verified by a customer system, the `Invocation` object is
15 de-serialised and applied to the current tariff by using reflection to invoke the described operation.

In order to simplify the announcement protocol, adjustments are required to be idempotent and complete. Idempotency guarantees that a tariff will not be adversely affected if an adjustment is applied more than once. Completeness implies
20 that an adjustment determines the entire parameter set of a tariff object, so that an adjustment completely removed the effects of any previously applied adjustments.

The customer system may apply a tariff by repeatedly invoking the `getCharge()` operation supported by that tariff every second, and adding the returned value to the cumulative charge. The parameters supplied to `getCharge`
25 `()` depend on the kind of tariff currently in force. For example, if the tariff is an implementation of `PacketCountTariff`, then measurements of inbound packets, outbound packets and congestion over the past second are required. However, if the tariff is an implementation of `RsvpTariff`, then only a `TSPEC` describing the current reservation is required. This implies that a customer system can only subscribe to a
30 product if it can supply the parameters require by the tariff associated with hat product.

Each invocation of the `getCharge ()` method also results in an update to the tariff-specific user interface. For example, in the `CongestionSensitiveLinear` tariff, the usage parameters supplied to `getCharge ()` are used to update the graphical displays of traffic and congestion.

5 The announcement protocol is used to communicate serialised tariffs and adjustments from a provider system to multiple customer systems. The number of customer systems is assumed to be large, and a repeated multicast solution is adopted.

Each product supported by a provider is assigned a multicast channel for
10 announcement purposes. Customer systems listen to the channels corresponding to the products that they are using. In the current implementation, it is assumed that each customer system has knowledge of well-known multicast addresses for the products it is interested in.

For each product channel, the provider repeatedly announces the current
15 tariff and the most recent adjustment made to it (if any). Each announcement carries a version number, which is incremented each time the announcement is changed. Customer systems only process announcements when a version number change is detected. If a new customer joins a channel, it waits until it receives a tariff before processing any adjustment announcements. Furthermore, an adjustment is only
20 applied if its announcement version is greater than that of the current tariff, thereby ensuring that a missed tariff announcement does not result in the application of a subsequent adjustment to an old tariff.

While centralised monitoring and control of tariffs by the network management platform is effective to respond to global changes in the loading of the
25 network, it is difficult to handle localised congestion in this way. It is difficult to cause a price rise signal to be multicast in such a way that the signal is only received by those attempting to communicate packets through the point of congestion. This would require a separate multicast transmission for each element in the Internet, e.g. a multicast for every different queue on every interface of every router. Alternatively
30 some aggregation of price rises triggered by local resource loading might be used. This however would mean that price rise signals were sent to users who were not making use of the congested resource. This in turn would make it necessary for the

price rise signal to be damped, reducing the ability of the price rise to reduce the demand on the congested resource.

To overcome these difficulties, the tariff algorithms installed on the customer terminals are arranged to respond automatically to congestion in a network resource being used by the terminal. Each algorithm includes a function which varies the price for network usage in dependence upon the detected congestion level. This function may be integrated in the main tariff algorithm, or, as in the example described here may be a separate algorithm used to calculate a premium to be added to a price calculated in accordance with the main tariff algorithm.

The main tariff algorithm calculates a price P as a function of a number of quality parameters, Q_1, Q_2, Q_3 where, for example, Q_1 is a specified latency for packets communicated across the interface between the customer terminal and the network, Q_2 is the reserved bandwidth for the transmission, Q_3 is a specified level of reliability corresponding to a maximum permissible level of packet loss.

The price P is then given by:

$$P = f(Q_1, Q_2, Q_3, \dots)$$

An example of the pricing function in terms of one of the quality parameters Q is shown schematically in Figure 2a.

The congestion tariff algorithm calculates a premium ΔP which is a function of one or more congestion parameters C :

$$\Delta P = f(C_1, C_2, \dots)$$

The congestion parameters provide a measure of the loading of the resources which a customer terminal is making use of at any given time. In the present example the ratio of packets lost to packets received is used as the congestion parameter. This parameter is readily calculated, for example in the case of packets using TCP (transport control protocol), or RTP (real time protocol) over UDP (user datagram protocol), since such packets include a sequence number. Figure 2b shows one example of the function for generating the premium. In this case, the premium increases as an approximately exponential function of the congestion, so that at low congestion levels a small premium is charged, while if congestion increases still further, then at higher levels of congestion the premium increases sharply.

In an alternative implementation, an explicit congestion signal is added by any congested router within the network to packets transmitted to the customer

terminal. Whether congestion is signalled explicitly or implicitly by packet drop, the price algorithm might not directly charge for congestion indication. Instead, it may charge if the customer terminal does not halve the congestion window in response to a congestion indication. Halving the congestion window halves the rate of transmission which is the standard response to congestion indication used in TCP and other compatible congestion control protocols. The change in transmission rate can be measured by the network provider as well as at the customer terminal, although this places a heavy load on router processing resources. If the provider is merely sampling certain customers to audit their own measurements, this results in an acceptable load.

Although only a single main tariff and premium are described here, in practice different subdomains, and different service providers associated with each subdomain, may each have a different pricing structure, with different main and premium tariffs. However, there is across all the subdomains a common relationship between network loading levels and congestion signalling.

The operation of this second implementation will now be described in the context of a network operating using a differentiated service as described in the Internet Engineering Task Force draft "Differentiated Services Operational Model and Definitions" and in the paper by David D Clark (MIT), "A Model for Cost Allocation and Pricing in the Internet", presented at MIT Workshop on Internet Economics, Mar 1995, URL:<http://www.press.umich.edu/jep/works/ClarkModel.html>. In a network implementing differentiated services, nodes are arranged to discriminate between packets to provide different levels of service. This capability might be used, for example, to accord delay-sensitive data, such as data generated by an IP telephony client, a higher priority compared to other data, such as email data. At the network edge, for example at a client terminal running the IP telephony client, bits in a TOS (type of service) octet contained within each packet header are set to indicate the appropriate service level. Those bits are used by routers within the network to determine how the relevant packets should be handled.

The TOS octet when used in this way is termed the DS (differential service) byte. The format of the differential service byte is shown in Figure 3. Bit zero, labelled "IN" indicates whether the packet is inside or outside a defined profile. Bits 1 to 5 labelled "PHB" define a "per-hop-behaviour" that is they indicate how, for

example, a router should handle the packet, e.g. by according it lower or higher priority. Bits 6 to 7, in this particular form of the DS byte, are used for explicit congestion notification (ECN). One of these bits is set to indicate whether the routers in the path of the packet are capable of setting the ECN field, and the other
 5 bit is used as a flag which is set (by ECN capable routers) when congestion, or loading which would potentially lead to congestion, occurs. Random Early Detection (RED) algorithms are currently implemented in routers. These algorithms measure average queue length within the packet buffers of a router. An exponential moving average is calculated. When that average queue length exceeds a predetermined
 10 threshold, then the router signals that congestion is occurring. Conventionally this signalling has been done simply by dropping a packet. However, in the context of an ECN scheme, the router, instead of dropping a packet, sets an ECN bit in a packet header to indicate that congestion is occurring. This is done probabilistically: that is, some only of the packets passing through the router are marked. The probability of
 15 a packet being marked increases with the average queue size. In the rare case that the queue increases to a length where the router buffers are full, then packets are dropped, rather than an ECN bit being set. In this case ECN bits are set for all the remaining packets.

In operation, if the client terminal 5 is accessing a data source on the server
 20 9, congestion may occur, for example, at router 4 which links network sub-domains 2B and 2C. RED-like algorithms in the router 4 detect that the queue lengths in the router buffers, as calculated using the exponential moving average, exceed a predetermined threshold. Accordingly some of the packets from the server 9 en route to the client terminal have the ECN bit of the DS byte set by the router 9 to
 25 mark the fact that congestion is occurring. At the client terminal, the DS byte in the headers of incoming packets is read. A moving average of the number of packets containing an ECN bit which is marked is calculated. This average then provides the congestion parameter C_1 which is used to calculate the premium:

$$\Delta P = f(C_1).$$

30 The total price to the user P_{TOT} is then calculated by adding together the prices determined by main tariff algorithm and by the premium algorithm:

$$P_{TOT} = P + \Delta P.$$

This total price is passed to a cost decision agent running on the client terminal. This cost decision agent is programmed with user defined rules. These might state, for example, that the cost decision agent should authorise the system to proceed with a connection as long as the total cost averaged over a certain time period falls below a
5 predetermined threshold, e.g. of £0.01 per minute, and that the cost decision agent should suspend a connection and alert the user if the cost rises above that threshold. Alternatively, as previously noted, the cost decision agent may handle several applications simultaneously, and may be programmed to slow down one of the applications as the premium for using a data source accessed by that application
10 increases.

For some customers in some circumstances, the variability of the tariff for network usage may pose problems. For example, a customer might wish to schedule a multicast audio-video conference with, say, twenty participants and with the customer intending to pay the network usage costs for all of the participants. The
15 conference will be scheduled a day or more in advance, but since the tariff is variable over time, at the point when the conference is scheduled, the customer will not know the cost which will be incurred. The preferred implementation of the present invention overcomes this problem for the customer, and also provides an additional revenue source for the network operator. This is achieved by applying a further tariff
20 which defines a premium for price stability for a given customer terminal, the value of the premium increasing as the required duration of the period of stability increases. In the example referred to above, the customer scheduling a conference one day in advance refers to the current tariff to determine the present cost of the network resources required, including any congestion premium currently applicable, and then
25 refers to the further tariff to determine the premium for maintaining the cost at its present value for a period of one day. Then if the user decides to make use of the fixed tariff a message is sent from the user to the network operator. The message identifies the data flows in question, for example by specifying the IP addresses and the service levels for the audio and video data flows between the participants,
30 together with the current time at which the user is contracting for a fixed period, and the required duration of the fixed period and also an identifying code for the message. Alternatively, the message with these details may be tracked with an appropriate cryptographic function (e.g. MD5), and the hash value only communicated initially to

the provider, and subsequently used to verify account data. Subsequently, for the duration of the specified period, in this case one day, the user applies the fixed tariff. In systems where the users themselves are responsible for generating accounting data and calculating the applicable charge for network usage, then the user calculates
5 the charge using the fixed tariff and returns the accounting data to the network operator together with the identifying code for the fixed tariff contract.

This aspect of the invention is not only applicable to systems where tariff variation is carried out locally in response to the detection of congestion, but may also be used in systems where, for example, the only variation is imposed by the
10 network operator.

The tariff for the stability premium may be distributed by multicasting from tariff entities in network operator platforms to the customer terminals in the same manner as described previously for the other tariffs discussed above. As with those other tariffs, different tariffs and optionally different periods of stability might apply
15 to different service levels. In a scenario such as that discussed in the preceding paragraph, then different service levels might be used for different elements of the audio and video data streams required for the multicast conference.

Figure 2c shows a possible for the stability premium tariff. This tariff may be embodied in a Java function multicast to the users. Curve C is communicated to the
20 customer terminal as another subsidiary algorithm that contributes to the main tariff algorithm. The customer may choose a period of price stability and calculate the premium above the spot price that his will require using curve C. Curve B is an example of the stable price chosen in a particular case. Once the period of stability expires a new one can be bought at the premium over the spot price at that time. To
25 buy a period of price stability, the customer must announce the period required and the range of addresses for which it applies to her provider. It may be required for one address (e.g. for the duration of an Internet phone call to a single person) or for a range of addresses (e.g. for a video conference). Certain risk-averse customers might request stable pricing for all addresses all the time.

30 For ease of description, the preceding sections have treated in isolation the local variations in tariff in response to congestion. In practice, this mechanism will in general be combined with other responses to congestion, and with other sources of variation in the tariff. Also, a decision to proceed with a transmission despite

congestion will in general require the consent of parties at both ends of the transmission. Considering the entire system of the data source, network and routers and the data receiver, the implementation of an increase in tariff (also termed here a "fine") in response to locally detected congestion occurs as a last resort. Other

5 responses are implemented first, in the following numerical order:

- 1.the network re-routes around congestion
- 2.the network borrows capacity from lower levels of service (lower in the context of the relevant dimension(s) of QoS) including the best effort service
- 3.the network introduces extra capacity (possibly automatically)
- 10 4.the end-system establishes that the congestion is on the shared network and not just on the access links or end systems
- 5.the end-system sets QoS requirements to a "higher" level (if cheaper than the fine for ignoring congestion at the current level)
- 6.the end-system decides it is essential to ignore the congestion, given the fine for
- 15 doing
- so might be quite high
- 7.both (all) end-systems agree to ignore the congestion.

Typically, it is at step 4 that an ECN signal is generated. Steps 1 to 3 precede the generation of this signal and steps 5 to 7 follow the generation of the

20 ECN signal.

The last step prior to proceeding with a connection and paying the premium for doing so is establishing agreement by both parties. Accordingly, when the customer terminal detects congestion, either through receiving explicit congestion notification, or through detection of a relevant parameter such as packet loss, the

25 customer terminal signals this fact back to the or each other end system. In the present example therefore, the client terminal 5 signals to the data server 9 that congestion is occurring. The data server is programmed with rules, which as at the customer may be implemented as an agent, which determine the response to such a signal. For example, the server may refuse service in these conditions. As

30 described previously with respect to Figure 1, in the present example tariffs are multicast through the network from network operators to the customer terminals, and charging is carried out using a "pay and display" process. Figures 4a and 4b shows the objects used to implement the charging architecture in this case. Figure 4a

shows the higher level objects and 4b shows the component objects used in a software implementation of the architecture of Figure 4b. In Figure 4a, objects on the client terminal are shown in the half of the Figure labelled "customer" and objects on the access router 7 and the corresponding network sub-domain are shown in the half of the Figure labelled "edge network". The objects on the customer terminal include a session control object S, a customer business rules object B_c , a customer pricing object Pr_c , a QoS manager Q, a customer accounting object Act_c and a customer measurement object M_c . The business rules object B_c receives information on those aspects of the session which involve liability for payment and receives current pricing data from the pricing object Pr_c . The customer business object makes decisions, under the customer's policy control on which chargeable services are utilised, and how much of the chargeable services are utilised. These decisions are fed to the QoS manager Q, which decides which mechanisms are used to achieve the requirements. The QoS manager then controls the customer measurement object M_c to determine which aspects of traffic and service to measure and which aspects to ignore. The measurement object then records the selected aspects of the traffic, for example counting the number of packets received by the customer terminal and the QoS levels for those packets. These data together with the current tariffs, including any premium for congestion, are then used by the customer terminal to determine the charge payable to the network operator. The measurement object M_c is also programmed with instructions which determine the frequency with which it passes data to the customer accounting object Act_c . The customer accounting object Act_c passes payments to an accounting object Act_p in the network provider's domain.

The accounting objects on the customer terminal may be implemented using a small encrypted flat-file database. On the network provider's side, the equivalent objects may be implemented using a larger database that is scaleable to handle e.g., tens of thousands of customer accounts. An object request broker (ORB) is used for communication between the customer-side objects and the network-side objects, implemented using commercially available tools such as ORBIX (TradeMark) from Iona Technologies plc.

On the network provider's side, that is to say within the subdomain to which the customer terminal is connected, the customer's traffic is measured by a version of M, denoted M_p , but only on a sampling basis determined by the policing function,

Po. That is to say, the network operator samples the customer's traffic only intermittently. Po controls where in the network measurements are made in order to capture all of any particular customer's traffic. A bulk measurement function, M_b , is responsible for reporting aggregate traffic levels, as reflected in the moving average of the router queue lengths, to the pricing object, Pr_p . Bulk measurements would typically be collected from across the provider's domain to a centralised pricing function (which would be replicated for reliability). Pr_p sets prices taking into account the business rules from the network provider's business object, B_p , as well as the current traffic levels reported by M_b and pricing from neighbouring providers (see below). The policing function, Po, compares sample measurements from M_p with accounting messages received at Act_p as a result of the customers own measurements. If it establishes that the accounts are insufficient it might restrict service at the access control gateway, Acs , or initiate some other punishment. Encapsulated within the accounting object another policing object checks the accounts match the payments within the contracted time for payment. Finally, the identity mapping function, I , provides a mapping between a customer's identity (account, digital signature, etc.) and their current network address (typically allocated by the ISP, whether unicast or multicast).

Figure 5 shows the data which are passed between the accounting objects. In this example the account data comprises: account identity; bill record identity; service type identifier; source address; destination address; tariff identity; time; period (i.e. the period covered by the bill record); units; cost; and currency. In addition, the payment data comprises the amount of money and the currency of payment.

Figure 6 shows the measurement region within protocol stacks on the customer terminal and in the network domain. Ideally there would be two measurement points within this region, one trusted by the customer and one trusted by the network, for example at the two points referenced (a) in the Figure. For ease of implementation, a single measurement point (b) trusted by both parties may be used. This might be implemented, for example within a secure module such as a cryptographic card on the client terminal. As an alternative, measurements may be made at different points with some possibility of discrepancies between measurements. On the network the practical measurement point is at the first

access device(s) that, for each customer, inspects network layer headers (c)(IP in this case). ISPs should not measure any deeper into their network (d) because their access network and systems will introduce delays and losses.

For an individual customer (e.g. on dial-up access), a practical point at which
5 to measure would also be alongside the network layer but in their end-system's stack (e). Ideally these measurement points would be lower in each stack to be closer to the interface between the two parties and less likely to be affected by contention in the stack. However, measuring at the link layer (f-f) would be inappropriate because only some chargeable parameters set at the network layer will ever be
10 reflected in link layer frames; network level multicast, end-end latency requirements etc. may never be visible at the link layer. Also, link layer headers would need to be ignored when measuring packet sizes for bandwidth calculations to avoid apparent discrepancies where different link technologies are chained together.

In the reception direction (up the stack) this choice of measurement points
15 implies that the lower layers must be dimensioned (buffer sizes, interrupt and thread scheduling priorities) to cope with the most stringent QoS requirements of higher layers. As frames are taken off the physical media, the machine must be able to pass data up the stack without any chance that usage-charged data gets discarded (e.g. due to buffer overflow caused by interrupt contention) before it gets to the network
20 layer. It is at the network layer where the ISP's service is to be measured and where it is most convenient for QoS requirements to control correct differential treatment of the various flows as they are passed further up the stack (on end-systems) or forwarded (on routers).

The measurement objects described above may be implemented using, with
25 appropriate modifications, publicly available network metering software such as Nevil Brownlee's NeTraMet system. This is a software meter which conforms to the IETF internet accounting architecture described in RFC 2063 and RFC 2064. The meter builds up, using "packet sniffing", packet and byte counts for traffic flows, which are defined by their end-point addresses. Although generally, Addresses can be ethernet
30 addresses, protocol addresses (IP, DECnet, EtherTalk, IPX or CLNS) or 'transport' addresses (IP port numbers, etc), or any combination of these, in the present implementation IP addresses only are used. The traffic flows to be observed are specified by a set of rules, which are downloaded to NeTraMet by a 'manager'

program. Traffic flow data is collected via SNMP (Simple Network Management Protocol) from a 'collector' program.

Figure 7 shows how the main tariff determined by the network operator varies in time. In the Figure, curve A is the spot price calculated to reflect the loading of the network at any instant. Curve B is one of a number of different tariff bands. Different tariff bands have different volatilities, and the customer pays a premium for bands offering greater stability. Tariffs are communicated to the customer terminals using a hierarchy of channels carried by the network. An initial contract between a customer and a service provider a single channel address that might typically hold new announcements distributed some months apart (e.g. for contract variations or for new services specifying which second level channel to listen to for tariffs or for downloading new code to handle new tariff structures). The second level channels might deliver updates hours apart which simply announce the addresses of third level channels for the most volatile information. These third level channels may carry updates at intervals of less than a second. Prices for many services may be carried on one channel. For greatest efficiency, this one channel may be split into several channels at times of highest volatility, and re-aggregated into a single channel in more stable periods.

Tables 1 to 7 below list Java source code used to implement two different tariffs. The code of table 1 establishes the operations used for communication between a customer system and a tariff algorithm downloaded by the customer system. Table 2 shows a linear tariff algorithm, in which the tariff depends on the total of the packets sent and packets received by the customer together with a congestion parameter. Table 3 shows the code for generating the customer display in this case. Table 4 shows the code used to display the tariff at the network operator's server. Table 5 shows an exponential tariff algorithm. Table 6 generates the customer display and Table 7 the operator display for the exponential tariff algorithm. By downloading Java code to generate the user interface, that interface can be tailored to the requirements of the particular tariff, and can be adapted as the tariff changes.

Although the examples so far described have been in the context of federated packet data networks, such as the Internet, many aspects of the invention can also be used with advantage in other types of network, such as in a circuit-

switched PSTN (public switched telephony network). Figure 11 shows an example of the invention applied in this context. In this network, customer terminals 81, which are in this example so-called intelligent phones, that is telephones incorporating a microprocessor and a data interface, are connected via local exchanges 82 and trunk exchanges 3 to the telephony networks. The trunk exchanges 83 are connected via a common channel SS7 (signalling system number 7) signalling network to a service control point 85 that is responsible for the execution of advanced call control functions. The service control point 85 is also connected to an operational support server 86 that is responsible for billing operations, and that, in this example, controls the setting of tariffs for the network. The OSS server and customer terminals include tariff entities (TE). The fixed PSTN network is also interconnected via a gateway 87 to a cellular GSM network 88. Base Stations BS in the cellular network communicate signals to intelligent mobile phones 89. In operation, network tariffs are distributed to customer terminals via the PSTN network and via the GSM network. Conveniently, the tariff may again take the form of Java functions which are executed on processors in the customer terminals. The Java functions may be streamed as Internet packets. In one implementation, these Internet packets may be distributed via the PSTN networks and GSM networks themselves. For example, the packets may be encapsulated and transported to the trunk exchanges using the MTP (message transport part) transport layer and may be communicated onwards to the customer terminals using out-of-band signalling. Alternatively, a separate data connection may be established between the OSS server and the customer terminals via the public internet. As in the examples above, the network operator monitors the loading of resources within the network and may transmit signals to the tariff entities in the customer terminals to change the tariff to reflect the scarceness or otherwise of relevant resources. Customer terminals may themselves monitor network loading and automatically generate variations in the tariffs. Usage of network resources may be measured locally by the customer terminals instead of conventional billing carried out within the network. The network operator may police the measurement of usage data by carrying out sampling, as described previously.

Table 1

```
5      // Generated by Together
      package com.bt.jungle.lsma.charging.pricing;

      import com.sun.java.swing,JComponent;

10     /**This establishes the operations used for
      communication between the customer system
      and the downloaded algorithm.
      @author Mike Rizzo*/
      public interface Tariff {
15     Jcomponenet getGUI( );
      Float getPrice (int pkin, int pkout, int cng);
```

Table 2

```

package algorithms.linear;

5    import com.sun.java.swing.JComponent;
    import com.sun.java.swing.JTextField;

    import com.bt.jungle.lsma.charging.pricing.Tariff ;

10   public class LinearAlgorithm implements Tariff {
        private float rate;
        private LinearAlgorithnDisplay display;
        public LinearAlgorithm ( ) {
            display = new LinearAlgorithmDisplay ( );
15         setRate (new Float(1));
        }
        public float getPrice (int pkin, int pkout, int cng) {
            return (pkin + pkout + cng) * rate;
        }
20     public JComponent getGUI( ) { return display; }
        public void setRate (Float f) {
            rate = f.floatValue( ) ;
            display.setRate (rate) ;
        }
25     }

```

Table 3

```

// Generated by Together

5    package algorithms.linear;

    import com.sun.java.swing.JPanel;
    import com.sun.java.swing.JTextField;
    import com.sun.java.swing.Box;
10   import com.sun.java.swing.JLabel;

    public class LinearAlgorithmDisplay extends JPanel {
        private JTextField tfRate = new JTextField (4);
        public LinearAlgorithmDisplay ( ) {

15             Box vbox = Box.createVerticalBox ( ) ;

                Box hbox = Box.createHorizontalBox ( ) ;
                hbox.add (Box.createHorizontalGlue ( ) ) ;
20             hbox.add (new JLabel ("Rate:"));
                hbox.add (Box.createHorizontalGlue( ));
                hbox.add (tfRate);
                tfRate.setEditable (false);
                hbox.add (Box.createHorizontalGlue( ))
25             vbox.add (hbox);

                add (vbox());
            }
        public void setRate (float f) {
30             tfRate.setText (String.valueOf (f));
        }
    }

```

Table 4

```

// Generated by Together
package algorithms.linear;

5
import com.sun.java.swing.*;
import java.awt.event.*;

import com.bt.jungle.lsma.charging.pricing.provider.*;
10
import com.bt.jungle.util.*;

public class LinearAlgorithmGUI extends JPanel {
    private JTextField tfRate - new JTextField ( );
    private TuningMessageListener tuningMessageListener;
15
    private final static String DEFAULT_RATE = "1.0";
    public LinearAlgorithmGUI (TuningMessageListener tml) {
        tuningMessageListener = tml;
        tfRate.setText (DEFAULT_RATE);

    Box vbox = Box.createVerticalBox( );

    Box hbox = Box.createHorizontalBox ( );
    hbox.add (new JLabel ("Rate:"));
    hbox.add (Box.createHorizontalGlue( ));
25
    hbox.add (tfRate);
    hbox.add (Box.createHorizontalGlue( ));
    hbox.add (hbox);

    JButton bTransmit = new JButton ("Transmit");
30
    bTransmit.addActionListener (
        new ActionListener ( ) {
            public void actionPerformed (ActionEvent e) {
                transmit ( ) ;
            }
        }
35
    );
    hbox = Box.createHorizontalBox( );
    hbox.add. (Box.createHorizontalGlue( ));
    hbox.add (bTransmit);
40
    hbox.add (Box.createHorizontalGlue( ));
    vbox.add (hbox);

    add (vbox);
}
45
void transmit ( ) {
    try {
        Float f = new Float (tfRate.getText( ));
        Object args [ ] = new Object [1];
        Args [0] = f;
50
        TuningMessageListener.notify(

```

26

```
                    new Invocation ("SetRate", args)
                );
            }
5      catch (Exception e) {
                e.printStackTrace ( );
            }
        }
    }
```

Table 5

```

package algorithms.exp;

5      import com.sun.java.swing.JComponent;
      import com.sun.java.swing.JTextField;

      import com.sun.java.isma.charging.pricing.Tariff;

10     public class ExpAlgorithm implements tariff {
          private float min;
          private float base;
          private float divisor;
          private ExpAlgorithmDisplay display( );
15     public ExpAlgorithm( ) {
          display = new ExpAlgorithmDisplay ( );
          setMin (new Float (1));
          setBase (new Float (2));
          setDivisor (new Float (10));
20     }
          public float getPrice (int pkin, int pkout, int cng) {
          return min + (float)math.pow (base,(pkin + pkout + cng)/divisor);
          }
          public JComponent getGUI( ) {return display; }
25     public void setMin (Float f) {
          min = f.floatValue( );
          display.setMin(min);
          }
          public void setBase (Float f) {
30     base = f.floatValue( );
          display.setBase(base);
          }
          public void set Divisor (Float f) {
          base = f.floatValue( );
35     display.setBase (divisor);
          }
      }

```


Table 6

```

// Generated by Together

5  package algorithms.exp;

import java.awt.GridLayout;
import com.sun.java.swing.JPanel;
import com.sun.java.swing.JTextField;
10 import com.sun.java.swing.Box;
import com.sun.java.swing.JLabel;

public class ExpAlgorithmDisplay extends JPanel {
    private JLabel tfDisplay = new JLabel ( );
15     private float min, base, div;

    public ExpAlgorithmDisplay ( ) {

        add (tfDisplay);
20         //         tfDisplay.setEditable (false);
        updateDisplay ( );
    }
    private void updateDisplay ( ) {
        tfDisplay.setText ("price = " + min + " + " + base +
25  " ^((pkin+pkout+cng)/" + div +")");
    }
    public void setMin (float f) {
        min = f;
        updateDisplay ( );
30    }
    public void setBase (float f) {
        base = f;
        updateDisplay ( );

35    public void setDivisor (float f) {
        div = f;
        updateDisplay ( );
    }
}

```

Table 7

```

// Generated by Together

5    package algorithms.exp;

    import java.awt.GridLayout;
    import com.sun.java.swing.*;
    import java.awt.event.*;

10   import com.bt.jungle.Isma.charging.pricing.provider.*;
    import com.bt.jungle.util.*;

    public class ExpAlgorithmGUI extends JPanel {
15       private JTextField tfMin = new JTextField ( );
       private JTextField tfBase = new JTextField ( );
       private JTextField tfDivisor = new JTextField ( );

       private TuningMessageListener tuningMessageListener;
20       private final static String DEFAULT_MIN = "1.0";
       private final static String DEFAULT_BASE = "2.0";
       private final static String DEFAULT_DIV = "10.0";

       public ExpAlgorithmGUI (TuningMessageListener tml) {
25           tuningMessageListener = tml;
           tfMin.setText (DEFAULT_MIN);
           tfBase.setText (DEFAULT_BASE);
           tfDivisor.setText (DEFAULT_DIV);

30           Box vbox = Box.createVerticalBox ( );

           vbox.add (new JLabel ("price = min + pow (base,
(pkin + pkout + cng)/divisor)"));

35           vbox.add (Box.createVerticalGlue ( ));

           JPanel panel = new JPanel (new GridLayout (3,2));
           panel.add (new JLabel ("Minimum"));
           panel.add (tfMin);
40           tfMin.addActionListener (
               new ActionListener ( ) {
                   public void actionPerformed (ActionEvent e) {
                       transmit ("setMin", tfMin);
                   }
               }
45       );
       panel.add (new JLabel ("Base"));
       panel.add (tfBase);
       tfBase.addActionListener (
50           new ActionListener ( ) {

```

30

```

        public void actionPerformed (ActionEvent e) {
            transmit ("setBase", tfBase);
        }
    }
};
5   panel.add (new JLabel ("Divisor"));
    panel.add (tfDivisor);
    tfDivisor.addActionListener (
        new ActionListener ( ) {
10      public void actionPerformed (ActionEvent e) {
            transmit ("setDivisor", tfDivisor);
        }
    }
);
15   vbox.add (panel);

    add (vbox)
}
void transmit (String m, JTextField tf) {
20   try {
        Float f = new Float (tf.getText ( ));
        Object args [ ] = new Object [1];
        args [0] = f;
        tuningMessageListener.notify(
25      new Invocation (m, args)
        );
    }
    catch (Exception e) {
30      e.printStackTrace ( );
    }
}
}

```

CLAIMS

1. A method of operating a communications network, including automatically varying, depending on network loading as detected at a customer terminal, a tariff for
5 network usage by the customer terminal.
2. A method according to claim 1, including detecting at the customer terminal a network performance parameter which depends on network loading, and varying the tariff depending on the network performance parameter.
- 10 3 A method according to claim 2, in which the network is a packet network and the network performance parameter is the number of packets lost in transmission between a data source and the customer terminal.
- 15 4. A method according to claim 1, including detecting a congestion signal at the customer terminal and varying the tariff in response to the congestion signal.
5. A method according to claim 4, including reading a congestion signal at the customer terminal from a data packet received at the customer terminal.
- 20 6. A method according to claim 4 or 5, including generating a congestion signal at a router in the network in response to the detection of congestion at the router.
7. A method according to any one of the preceding claims, including making a first
25 relatively smaller increase in the tariff when congestion is first detected, and making at least one further, relatively larger increase, if the congestion persists
8. A method according to any one of the preceding claims, including programming a decision agent at the customer terminal with user-determined price criteria, and
30 comparing a price calculated using the tariff with the said price criteria.
9. A method according to any one of the preceding claims, including distributing a tariff algorithm via the communications network to a plurality of terminals and

calculating at each terminal, using the tariff, a charge for network usage by the terminal.

10. A method according to claim 9, further comprising steps, carried out by the
5 network operator, of:

intermittently sampling traffic between a customer terminal and the network,
and as part of the sampling recording network loading affecting the customer
terminal; and

for the sampled traffic comparing a charge calculated by the customer
10 terminal and an expected charge and detecting thereby any discrepancy.

11. A method according to any one of the preceding claims, in which when the
customer terminal detects congestion in data transmitted to the customer terminal
from a data source via the network, the customer terminal returns a congestion
15 notification signal to the data source.

12. A method according to any one of the preceding claims, including at a customer
terminal, selecting a period of time for which the tariff is to be fixed and paying a
premium depending on the duration of the said period.

20

13. A method of operating a communications network including applying to
customer terminals a tariff for network usage, varying the tariff with time; at a
customer terminal, selecting a period of time for which the tariff is to be fixed; and
paying a premium depending on the duration of the said period.

25

14. A communications network including :

means for detecting network loading locally at a customer terminal; and

means responsive to the said means for detecting arranged automatically to
vary a tariff for network usage by the customer terminal.

30

15. A customer terminal for use in a communications network, the customer
terminal including:

means for detecting loading of a network to which, in use, the customer terminal is connected;

means responsive to the said means for detecting and arranged automatically to vary a tariff for network usage by the customer terminal.

5

14. A customer terminal for use in a communications network, the customer terminal including one or more processors arranged to carry out the following steps in sequence:

detecting loading of resources in a network to which the customer terminal is
10 connected; and

automatically varying in dependence on the detected loading a tariff for network usage by the customer terminal.

15. A method according to any one of claims 1 to 13, in which the tariff is
15 varied only if the terminal fails to reduce its output in response to detected congestion.

Fig.2a.

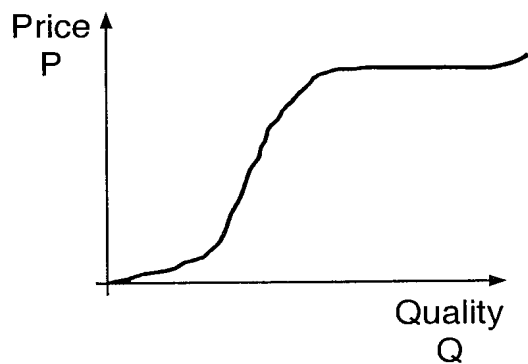


Fig.2b.

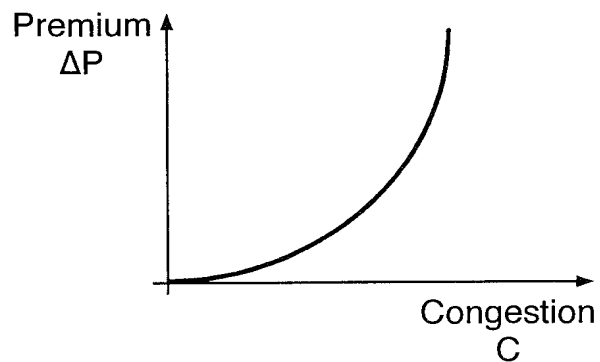


Fig.3.

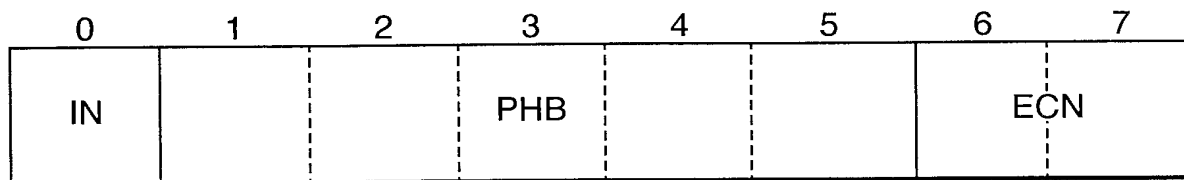


Fig.2c.

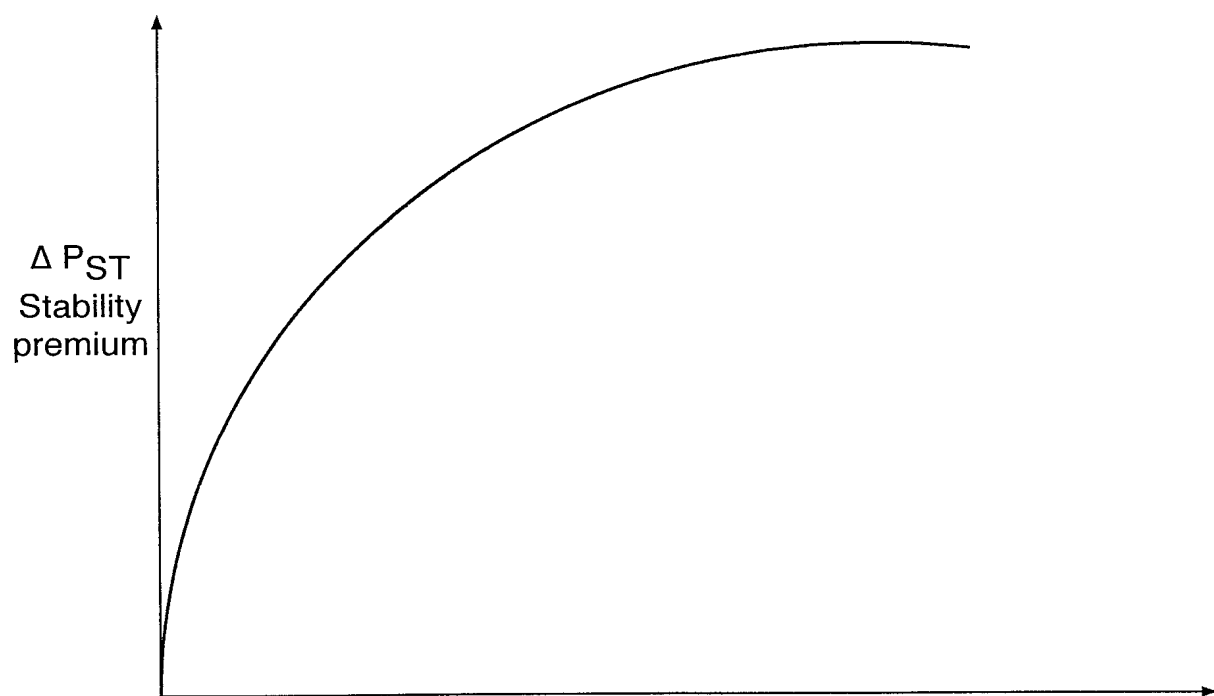


Fig.4a.

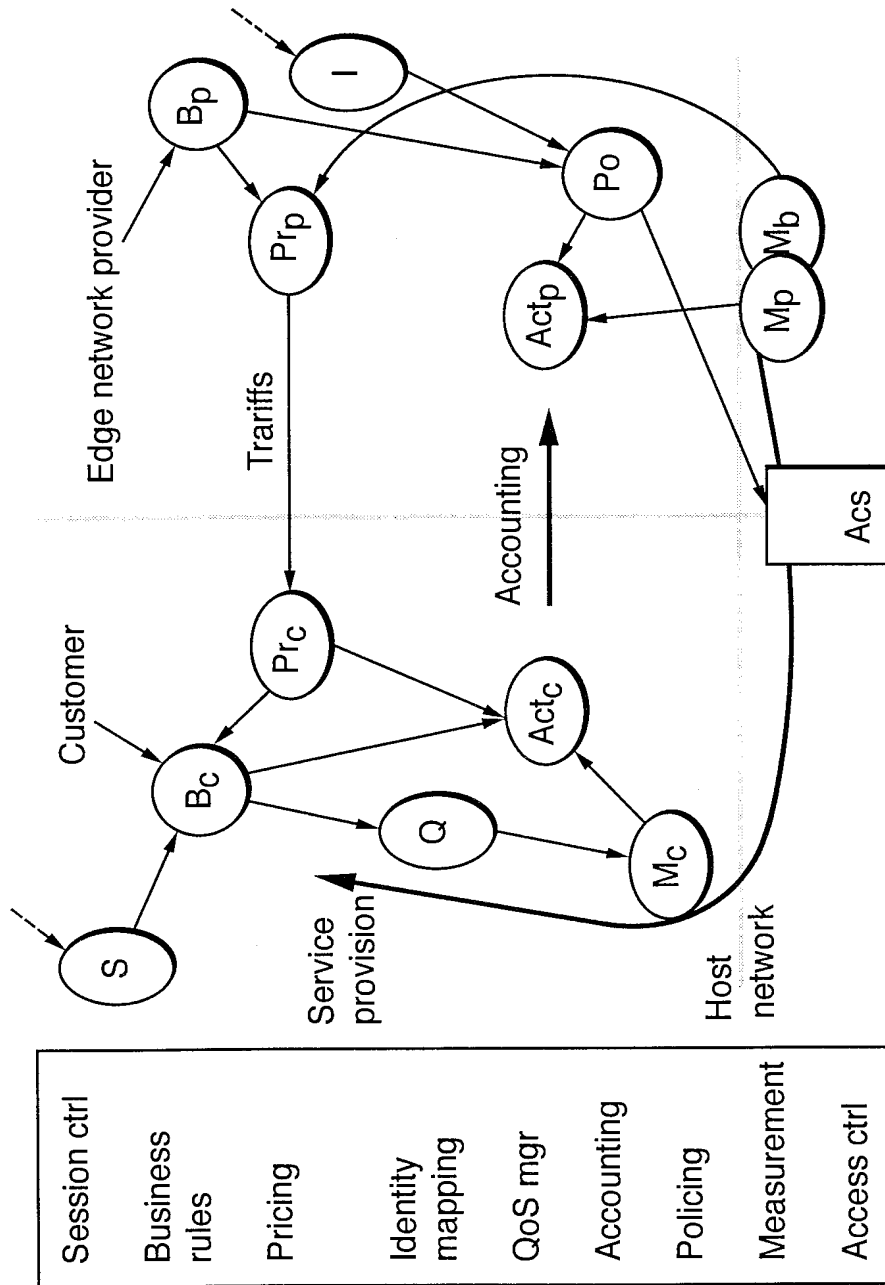


Fig.4b.

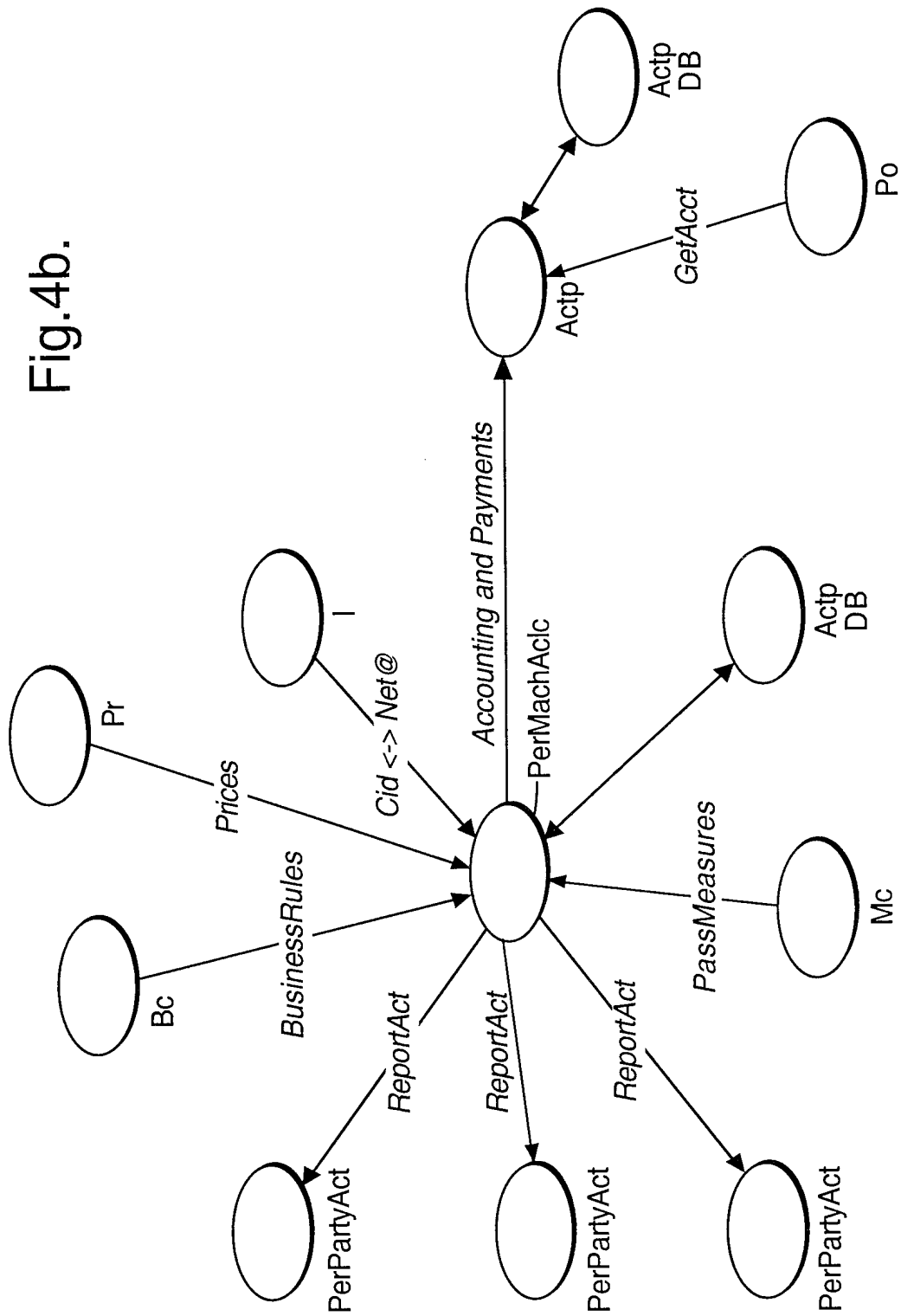


Fig.5a.

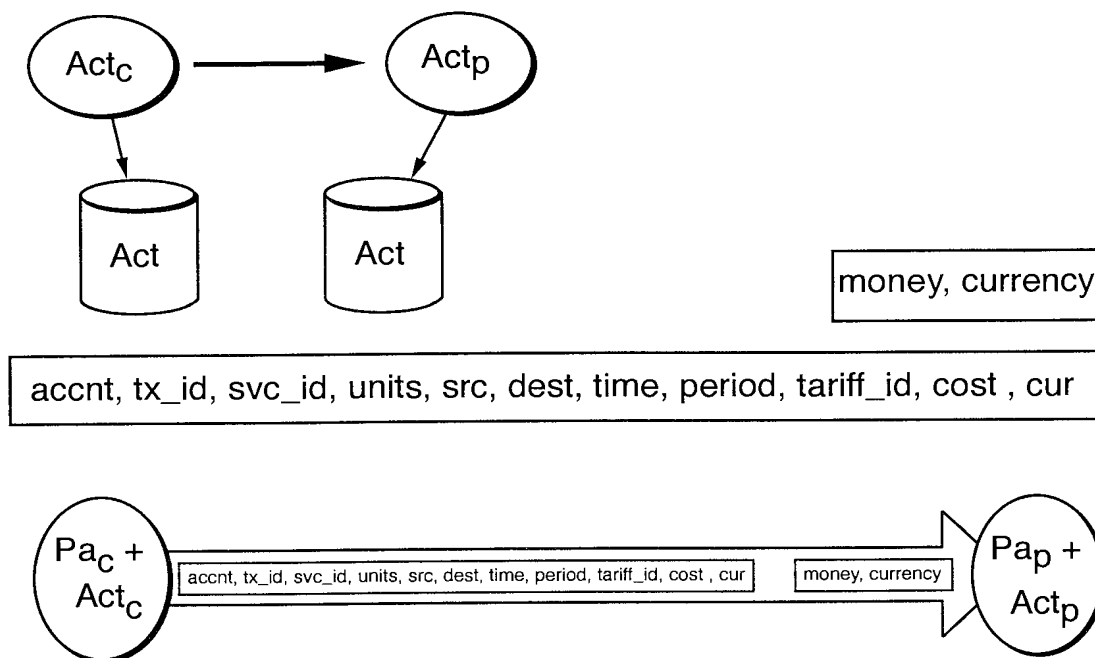


Fig.5b.

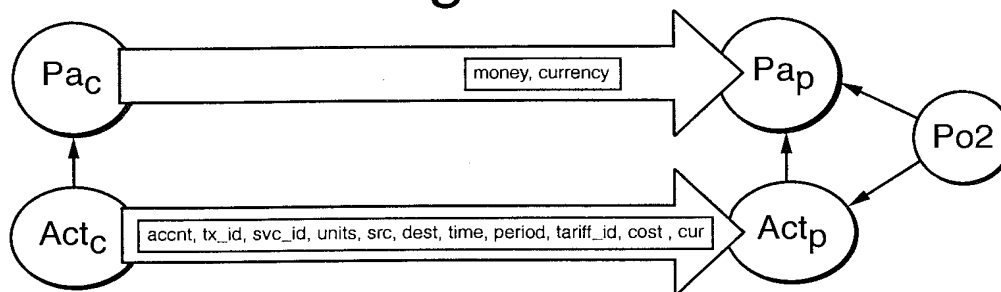


Fig.6.

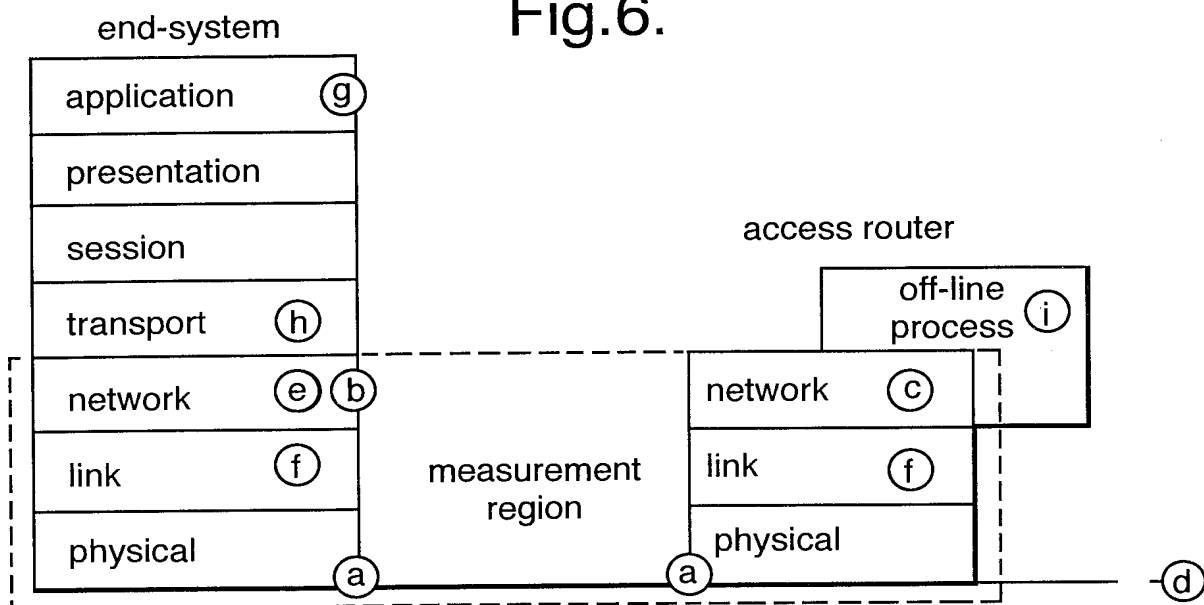


Fig.7.

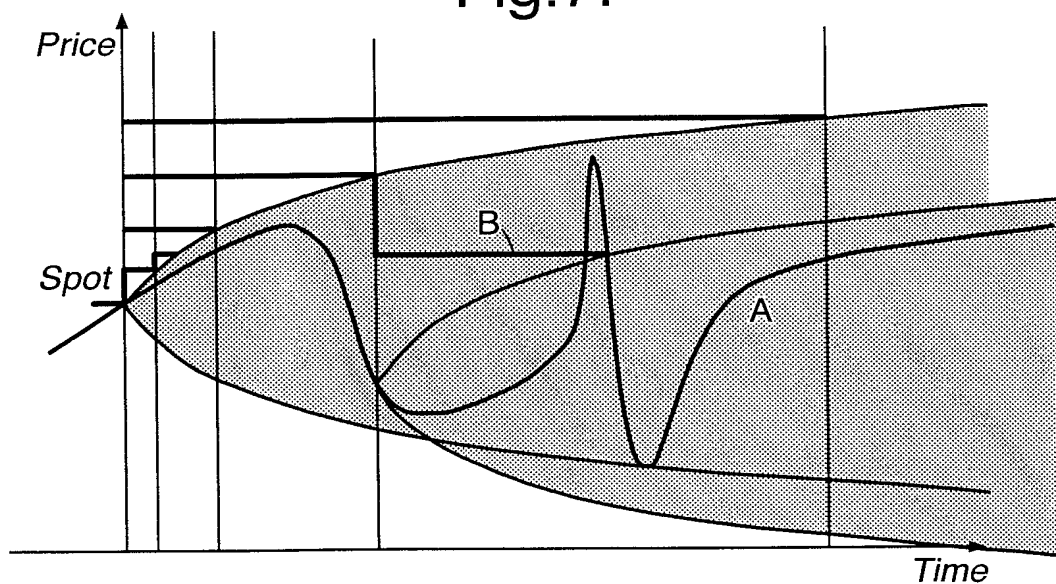


Fig. 8a.

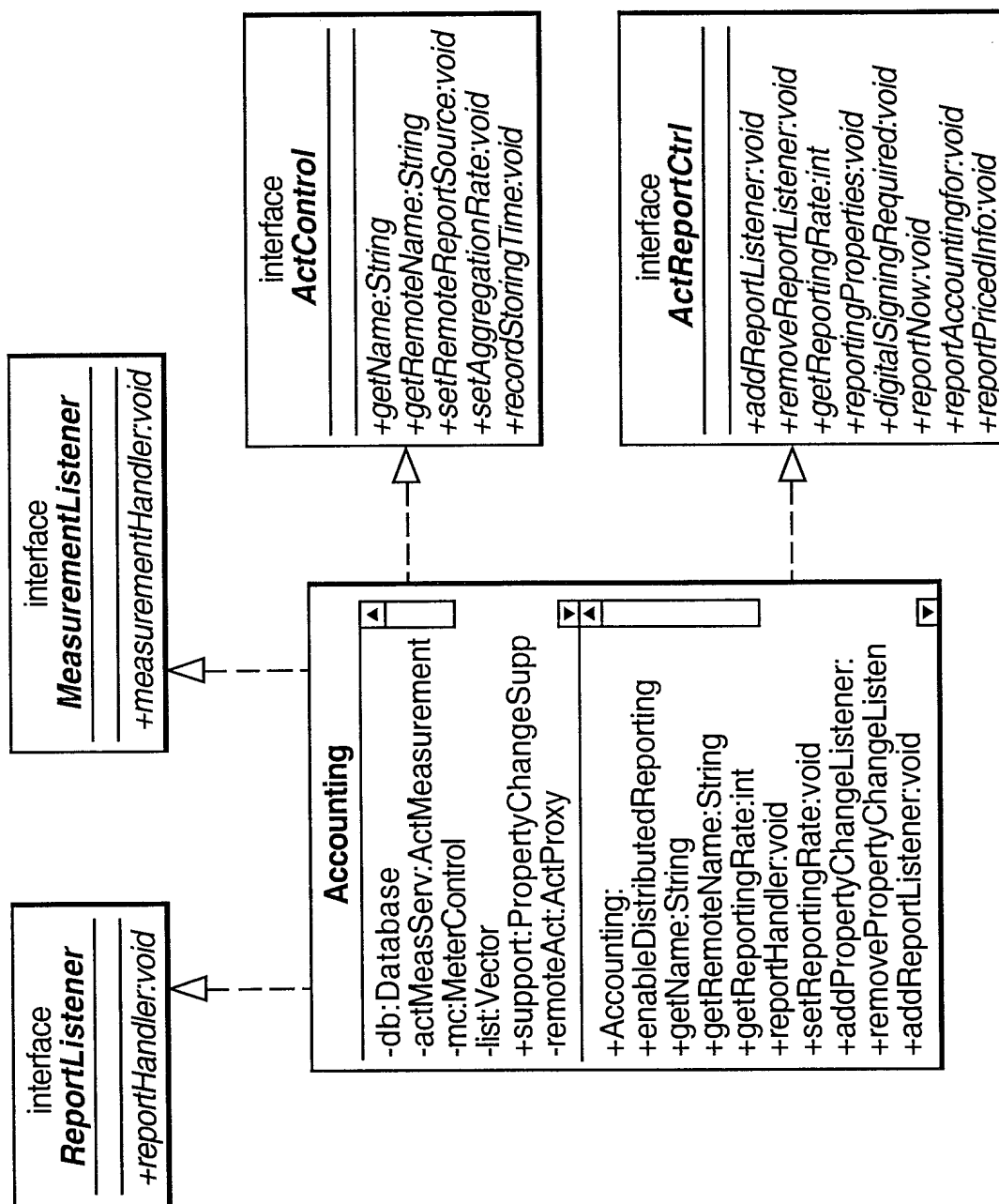


Fig.8b.

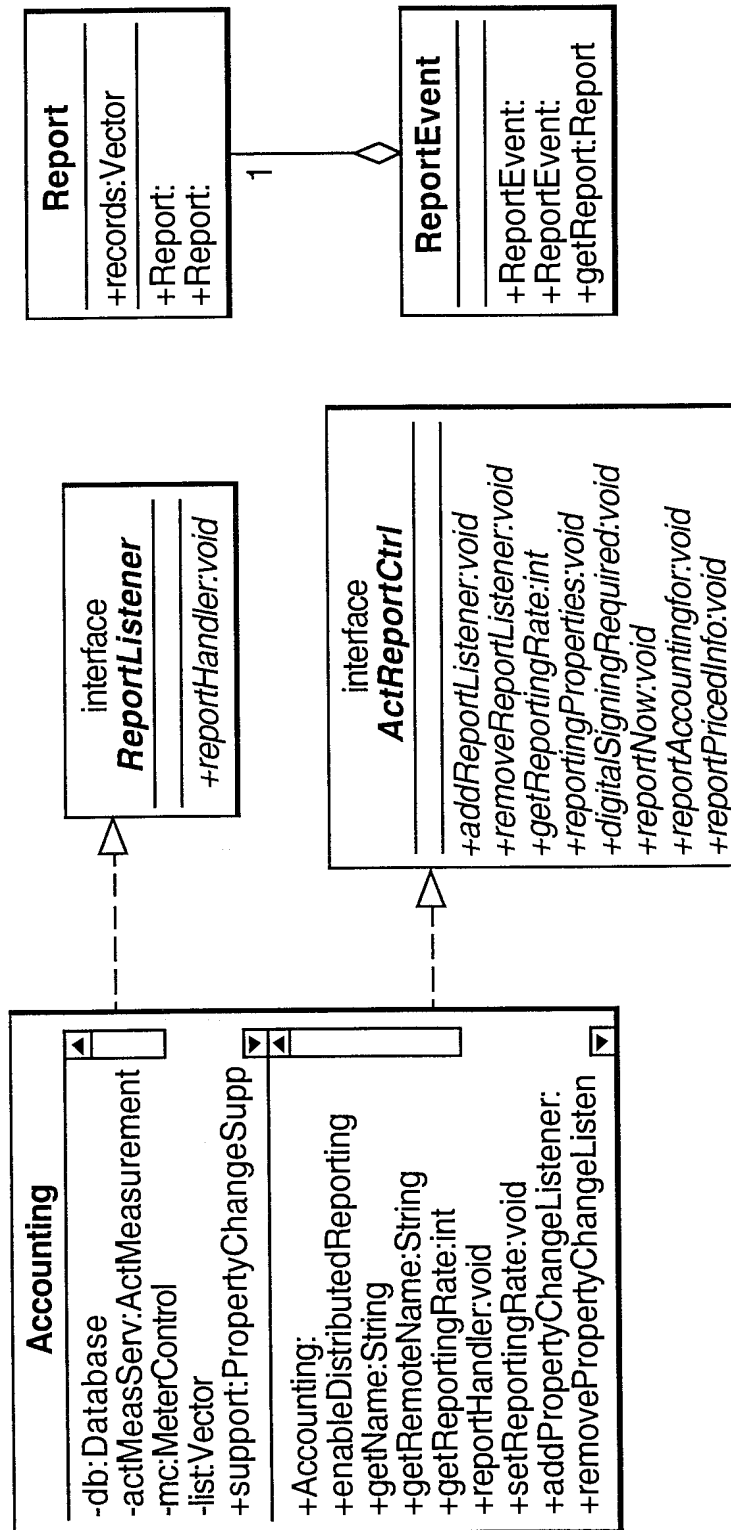


Fig.8c.

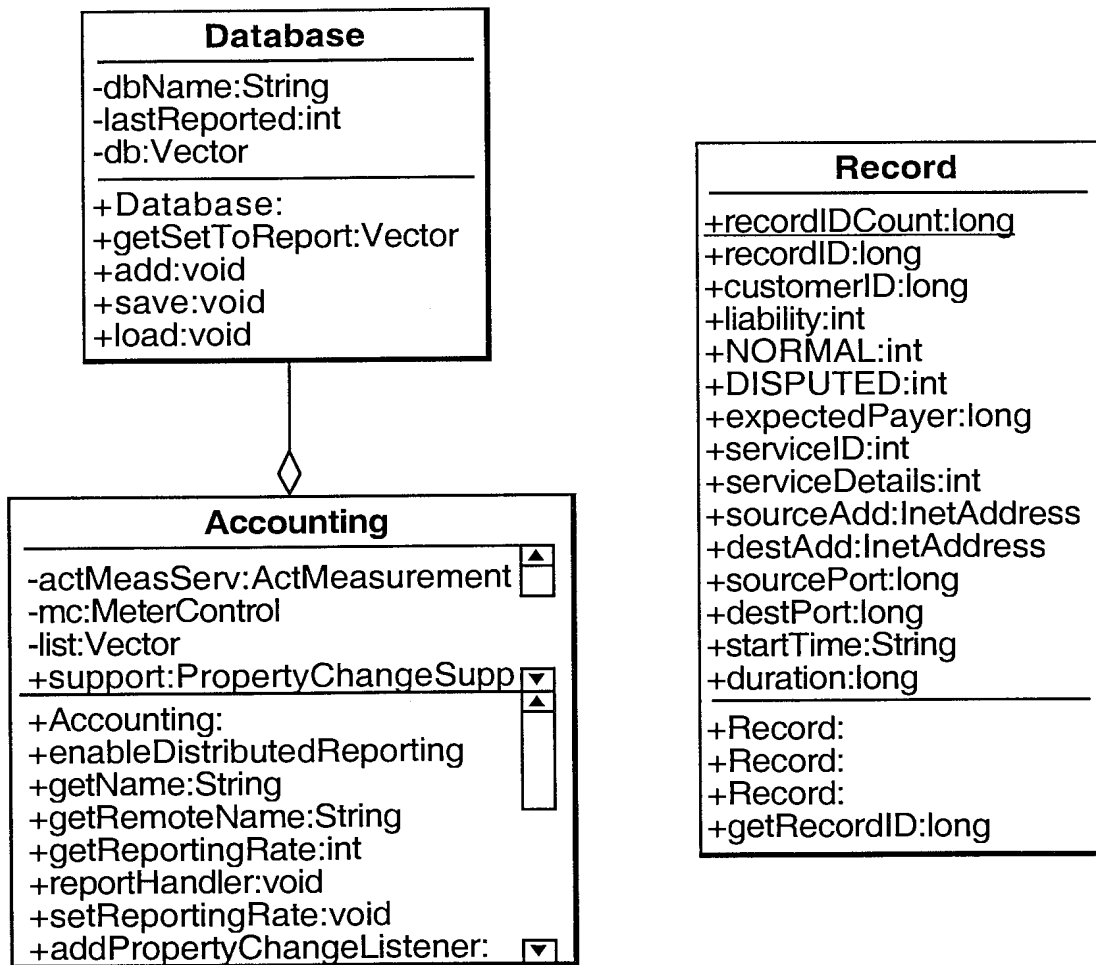


Fig.8d.

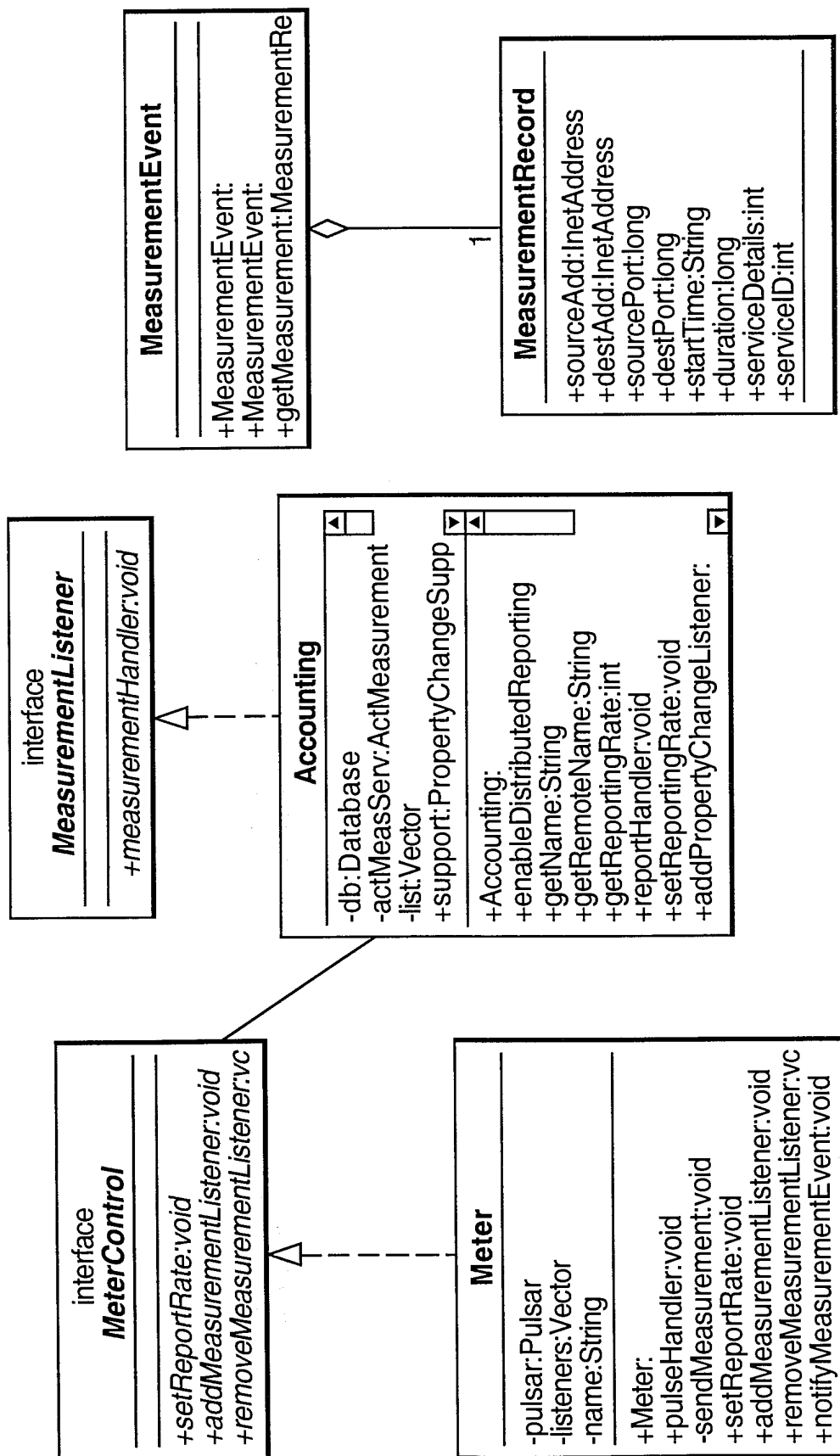


Fig.8e.

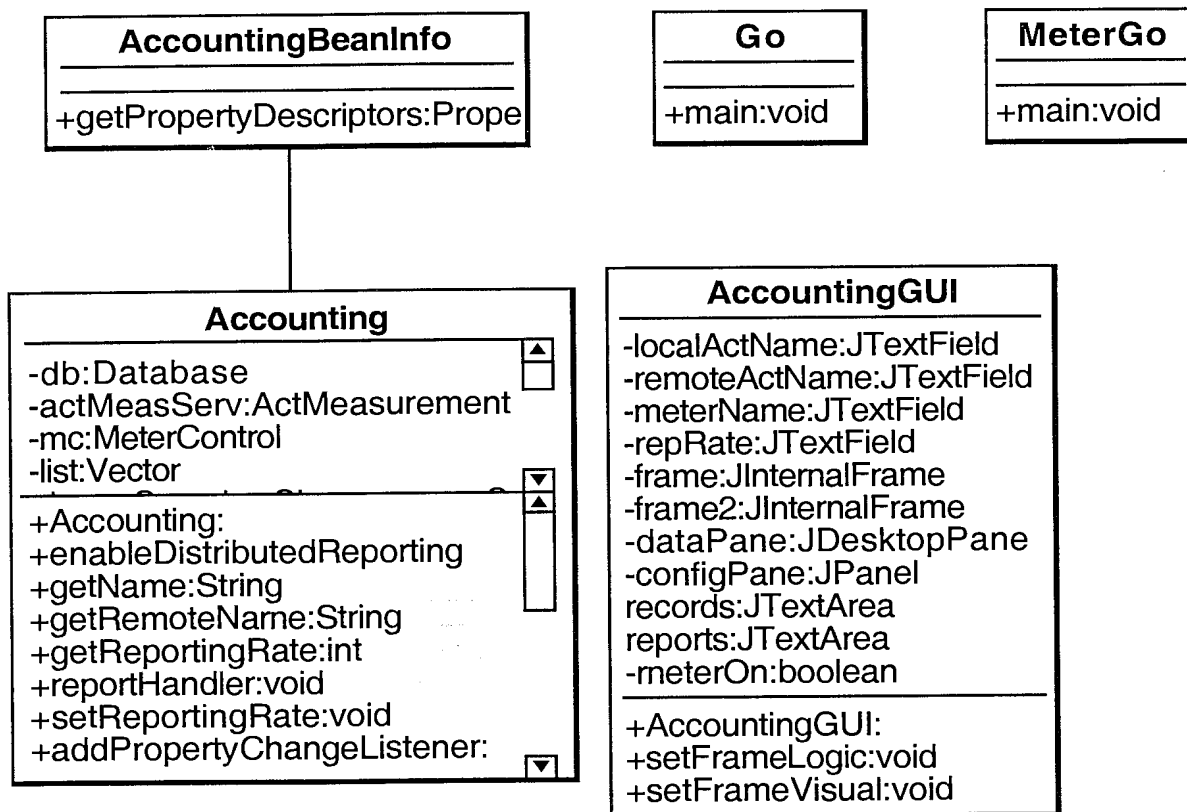


Fig.9.

BTInternet Internet Accounting Control Platform	
Local Platform ID	BTInternet
Local Meter ID	local
Local Reporting Rate	1000
Reporting Source	<input type="text"/> <input type="button" value="Add"/> <input type="button" value="Remove"/>
Demon	<input type="button" value="Report NOW!"/>
MCI	Required Reporting Rate
BTInternet	<input type="text" value="2000"/>
	Reporting Phase
	<input type="text"/>
	☐ Reporting priced data
	Security
	☐ Encryption required
	☐ Digital signing Required
	<input type="button" value="Update"/>

Fig.10.

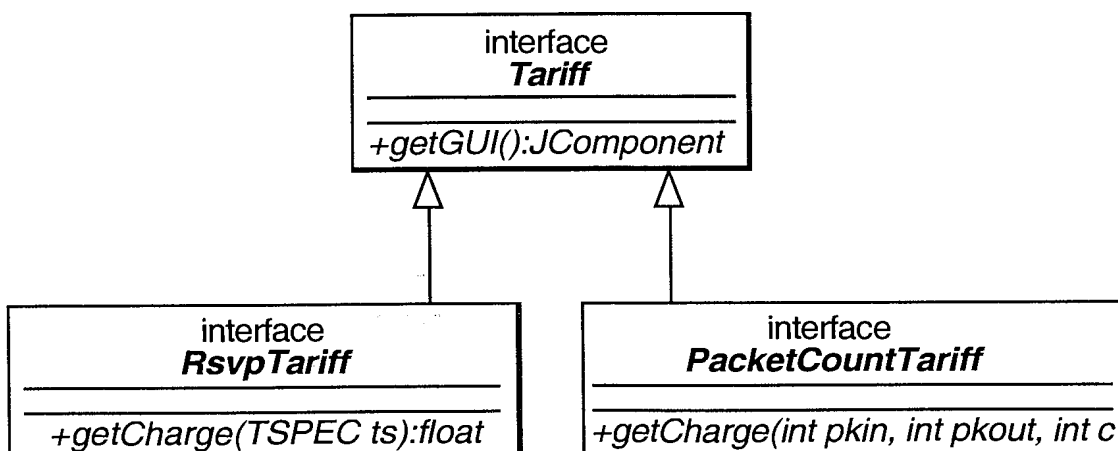
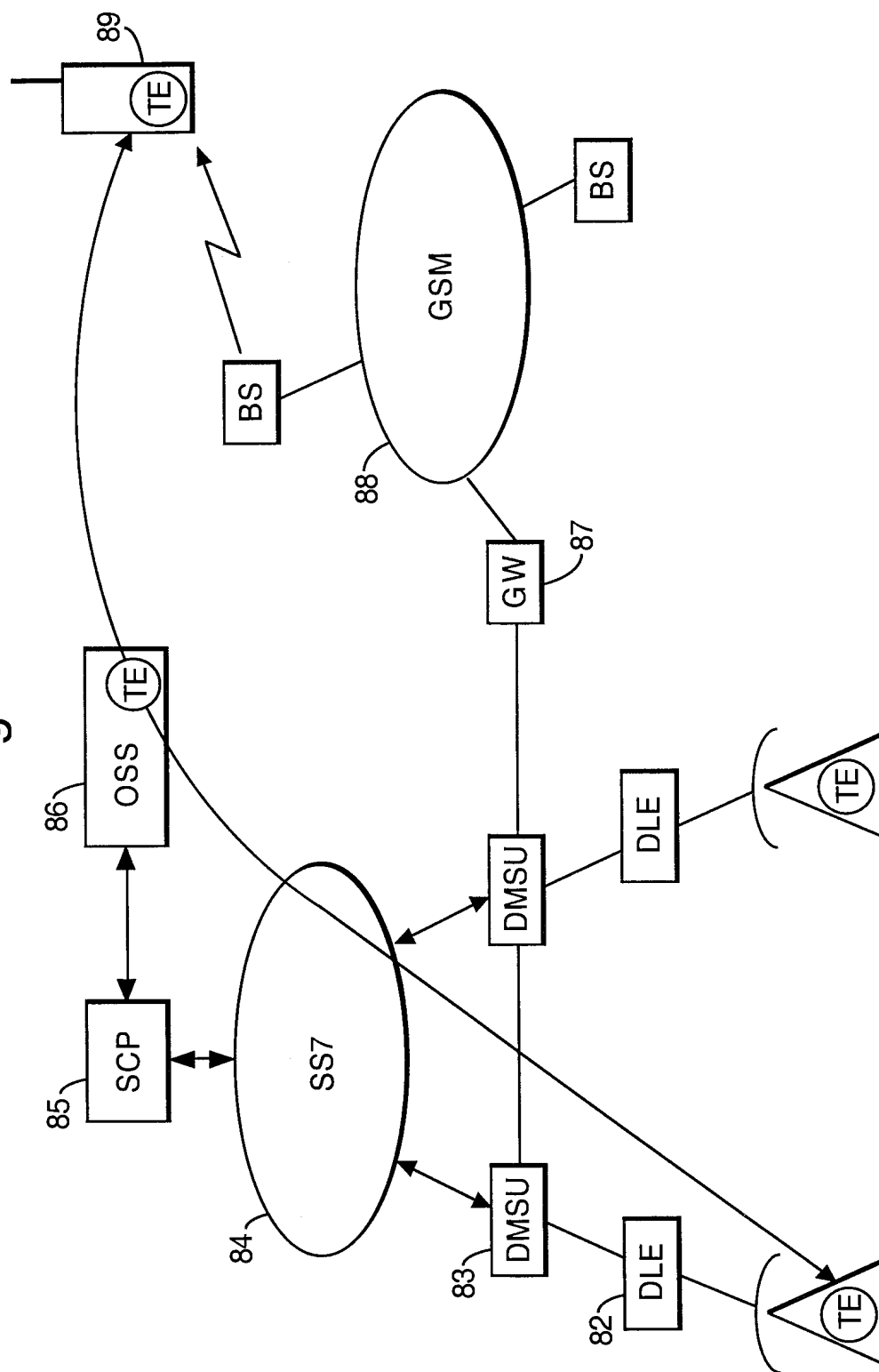


Fig.11.



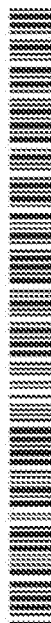
(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
20 February 2003 (20.02.2003)

PCT

(10) International Publication Number
WO 03/014891 A2

- (51) International Patent Classification: G06F 1/00
- (21) International Application Number: PCT/US02/23226
- (22) International Filing Date: 19 July 2002 (19.07.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/309,862 3 August 2001 (03.08.2001) US
09/992,310 19 November 2001 (19.11.2001) US
- (71) Applicant: THE BOEING COMPANY [US/US]; P.O. Box 3707, M/S 13-08, Seattle, WA 98124-2207 (US).
- (72) Inventor: ROCKWELL, Lawrence, L.; 8018-146th Avenue NE, Redmond, WA 98052 (US).
- (74) Agent: GALBRAITH, Ann, K.; The Boeing Company, P.O. Box 3707, M/S 13-08, Seattle, WA 98124-2207 (US).
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, EG, KZ, MD, RU, TJ, TM), European patent (AE, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Published:**
— without international search report and to be republished upon receipt of that report.
- For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*



WO 03/014891 A2

(54) Title: AN AIRBORNE SECURITY MANAGER

(57) **Abstract:** An airborne security management system is provided for monitoring security activities in a mobile network platform. The airborne security management system includes a mobile network that is interconnected via an unreliable communication link to a terrestrial-based network security management system; an intrusion detection system connected to the mobile network and operable to detect a security intrusion event whose origination is associated with the mobile network; and a mobile security manager adapted to receive the security intrusion events from the intrusion detection system. The mobile security manager is operable to transmit a message indicative of the security intrusion event to the network security management system and to perform security response activities in response to security commands received from the network security management system. The mobile security manager is further operable to command security response activities on the mobile network platform, when the mobile network platform is not connected with network security management system.

AN AIRBORNE SECURITY MANAGER

[0001] This application claims priority under 35 U.S.C. §119(e) to United States Provisional Application No. 60/309,862 filed on August 3, 2001, and entitled "An Airborne Security Manager" the specification and drawings of which are hereby expressly incorporated by reference.

TECHNICAL FIELD

5 [0002] The present invention relates generally to an airborne security management system for monitoring security activities in a mobile network platform, and more particularly to an autonomous airborne security manager for responding to detected security intrusion events when the mobile network platform is or is not in communication with a terrestrial-based network security
10 management system.

BACKGROUND OF THE INVENTION

[0003] Broadband data and video services, on which our society and economy have grown to depend, have heretofore generally not been readily available to users onboard mobile network platforms such as aircraft, ships, trains,
15 automobiles, etc. While the technology exists to deliver such services to most forms of mobile network platforms, past solutions have been generally quite expensive, with low data rates and/or available to only very limited markets of government/military users and some high-end maritime markets (i.e., cruise ships).

[0004] Previously developed systems which have attempted to provide data and video services to mobile network platforms have done so with only limited success. One major obstacle has been the high cost of access to such broadband data and video services. Another problem is the limited capacity of previously developed systems, which is insufficient for mobile network platforms carrying dozens, or even hundreds, of passengers who each may be simultaneously requesting different channels of programming or different data services. Furthermore, presently existing systems are generally not readily scalable to address the demands of the traveling public.

10 [0005] Of particular interest, presently existing systems also have not comprehensively addressed security issues relating to the mobile network platform. Therefore, it is desirable to provide a network security architecture for monitoring, reporting and responding to onboard security activities in a mobile network platform. It is envisioned that such a network security architecture should
15 be designed to (a) secure computing resources to which passengers may have access on the mobile platform; (b) communicate reliably with terrestrial-based system components over an unreliable communication link; (c) provide a policy mediated response to detected security intrusion events occurring on the mobile platform; and (d) scale the management of the system to hundreds or thousands
20 of mobile platforms.

SUMMARY OF THE INVENTION

[0006] In accordance with the present invention, an airborne security management system is provided for monitoring security activities in a mobile network platform. The security management system includes a mobile network
5 network platform. The security management system includes a mobile network that is interconnected via an unreliable communication link to a terrestrial-based network security management system; an intrusion detection system connected to the mobile network and operable to detect a security intrusion event whose origination is associated with the mobile network; and a mobile security manager
10 adapted to receive the security intrusion events from the intrusion detection system. The mobile security manager is operable to transmit a message indicative of the security intrusion event to the network security management system and to perform security response activities in response to security commands received from the network security management system. The mobile
15 security manager is further operable to command security response activities on the mobile network platform, when the mobile network platform is not connected with network security management system.

20

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The various advantages of the present invention will become apparent to one skilled in the art by reading the following specification and subjoined claims and by referencing the following drawings in which:

[0008] Figure 1 is a block diagram depicting a network security

architecture for a mobile network platform in accordance with the present invention;

[0009] Figures 2A and 2B are state machine diagrams illustrating a security policy for a given user access point on the mobile network platform in accordance with the present invention;

[0010] , Figure 3 is a diagram of an exemplary data structure for implementing the security policies of the present invention;

[0011] Figure 4 is a diagram depicting the primary software components of the network security architecture of the present invention;

10 [0012] Figure 5 is a block diagram depicting the functional software modules which comprise the airborne security manager in accordance with the present invention;

[0013] Figure 6 is a block diagram depicting the functional components implementing the terrestrial control and data storage functions of a terrestrial-based network security system in accordance with the present invention;

[0014] Figure 7 is an exemplary aircraft browser window used to implement the monitoring and manual control functions of a terrestrial-based network security system in accordance with the present invention; and

[0015] Figure 8 is an exemplary aircraft status window used to
20 implement the monitoring and manual control functions of a terrestrial-based network security system in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0016] Figure 1 illustrates a network security architecture 10 for

monitoring security activities in an unattended mobile network platform 12. The primary purpose of the network security architecture 10 is to monitor, record, report and respond to security-relevant events associated with the mobile network platform 12. In a preferred embodiment, the network security architecture 10 supports a mobile network platform residing in an aircraft. The mobile network platform 12 is in turn interconnected via one or more unreliable wireless communication links 14 to a terrestrial-based communication system 16, including a terrestrial-based network security management system 18. While the following description is provide with reference to an airborne application, it is readily understood that the broad aspects of the network security architecture are applicable to mobile network platforms which may reside in passenger buses, cruise ships, etc.

[0017] It is envisioned that the mobile network platform 12 provides aircraft passengers a suite of broadband two-way data and video communication services. The infrastructure allows information to be transferred to and from the aircraft at high enough data rates to support a variety of services. To do so, the mobile network platform 12 is primarily comprised of four subsystems: an antenna subsystem 22, a receive and transmit subsystem (RTS) 24, a control subsystem 26, and a cabin distribution subsystem 28. Each of these four subsystems will be further described below.

[0018] The antenna subsystem 22 provides two-way broadband data connectivity and direct broadcast television reception capability to the aircraft. Although the invention is not limited thereto, the antenna subsystem 22 is generally designed to provide this connectivity during cruise conditions (limited roll

and pitch angles) of the aircraft. Connectivity with the aircraft is most commonly achieved via a K band Fixed Satellite Service (FSS) satellite, a Broadcast Satellite Service (BSS) satellites, and/or a direct broadcast television service (DBS) satellite.

5 **[0019]** For illustration purposes, additional description is provided for the processing associated with Ku band satellite broadcast signals. The antenna subsystem 22 may receive and/or transmit Ku band satellite broadcast signals. The antenna system 22 down-converts an incoming Ku-band signal, amplifies, and outputs the L-band signals to the RTS 24. The antenna system may also
10 provide a broadband downlink capability. In this case, the antenna system 22 receives an L-band data signal from an on-aircraft modem, up-converts this signal, amplifies it and then broadcasts as a Ku band signal to selected satellite transponders.

[0020] The receive and transmit subsystem (RTS) 24 operates in
15 receive and transmit modes. In receive mode, the RTS 24 may receive rebroadcast video signals, rebroadcast audio signals and/or IP data embedded in an L-band carrier. The RTS 24 in turn demodulates, de-spreads, decodes, and routes the received signals to the cabin distribution subsystem 28. In transmit mode, the RTS 24 sends IP data modulated into an L-band signal. The RTS 24
20 encodes, spreads, and modulates the signal the IP data it receives from the cabin distribution subsystem 28.

[0021] The control subsystem 26 controls the operation of the mobile security platform 12 and each of its four subsystems. Of particular interest, the control subsystem 26 includes one or more intrusion detection subsystems 32 and

an airborne security manager 34. An intrusion detection subsystem 32 is operable to detect security intrusion activities which may occur on or in relation to the mobile network platform. To do so, an intrusion detection subsystem 32 inspects all of the data packets entering a computing device on which it is hosted and, upon detection of a security intrusion activity, transmits a security intrusion event to the airborne security manager 34. As will be apparent to one skilled in the art, the intrusion detection subsystem 32 may be implemented using one of many commercially available software products.

[0022] The airborne security manager 34 is responsible for enforcing security policy for an aircraft. Because communication with the aircraft may be sporadic, the airborne security manager 34 must provide the capability to act autonomously when responding to security intrusion events. When a security intrusion event is detected, the airborne security manager 34 responds appropriately in accordance with a customizable security policy. Thus, the airborne security manager 34 is adapted to receive security intrusion events from any of the intrusion detection subsystems and operable to implement a security response. Exemplary responses may include warnings one or more passengers on the aircraft, alerting terrestrial-based security administrators, and/or disconnecting a passenger's network access.

[0023] The cabin distribution subsystem (CDS) 28 provides network connectivity through a plurality of user access points to the passengers of the aircraft. In a preferred embodiment, the cabin distribution system may be composed of either a series of 802.3 Ethernet switches or 802.11X wireless access points. It should be noted that the current 802.11B standard only allows

for a shared secret between all users of a wireless access point and thus is not suitable for providing the desired level of communication privacy in the passenger cabin. In contrast, next generation wireless standards, such as 802.11X ("X" denotes a revision of 802.11 beyond "B") will support "channelized" or individual user level encryption. It is envisioned that such wireless standards are within the scope of the present invention.

[0024] Each user access point preferably has the properties of a managed layer 3 switch. First, each user access point must enforce the association of IP address and MAC address with a particular port. This requirement is applicable to either a wired and wireless cabin environment. A second requirement for each user access point is to accept a command to shut off its access port. In the case of a wireless access device, a communication channel consisting of a particular frequency, time division or sub-frame substitutes for the physical access port. A third requirement for each user access point is to preclude passengers from eavesdropping or receiving Ethernet packets not directly addressed to them. In a wired cabin distribution system, this can be accomplished through the use of a switched Ethernet architecture. In a wireless cabin distribution system, this can be accomplished through the use of "channel level encryption" specific to a particular user.

[0025] The design of a security policy mechanism is the most fundamental element of the network security architecture 10. In accordance with the present invention, it is envisioned that the security policy will be designed within the following design constraints. First, the security policy mechanism should map different security intrusion events to different responses. It should be

appreciated that the severity of response is based on the danger of the detected activities. Second, the automated response policy has to be enforced at all times (subject to over-ride conditions), regardless of whether airborne to terrestrial communications are available or not. If the automated responses are disabled
5 during periods of connectivity, the connectivity might fail before a security administrator has a chance to take action in which case the system reverts to the automated policy in effect prior to the override. The security administrator can retract the response if they desire. Third, the policy mechanism has to arbitrate between automated responses from the airborne security manager and manual
10 commands received from terrestrial-based security administrators. If the automated system mistakenly blocks a passenger's network address, and the terrestrial administrator overrides that action, the security policy mechanism needs to know about that action and not try to enforce the block.

[0026] State machines are a flexible, yet intuitively appealing,
15 mechanism for modeling complex behaviors. Therefore, state-machines have been chosen to represent the security policies of the present invention. Figures 2A and 2B illustrates basic UML state machines which model the security policy associated with an user access point in the mobile network platform.

[0027] In Figure 2A, each user access point can be in one of three
20 defined states. By default, all user access points begin in a normal state 42. A security intrusion event of any kind will result in a transition to either a suspected state 44 or a disconnected state 46 for the applicable user access point. Each transition is in the form of "event/response" where events are the external triggers that cause the state transition and responses are external actions that the system

initiates when making the transition. For instance, a low or medium priority event
48 occurring in a normal state will cause the system to log the event and/or
attempt to provide a warning to the passenger connected at that user access
point. The user access point then transitions to the suspected state as shown in

5 Figure 2A.

State machine models may be enhanced to incorporate manual controls.
Specific manual control commands enable a terrestrial-based security
administrator to explicitly disable or enable a user access point from the ground.
By adding a state that indicates that the user access point is under manual control
10 ensures that the automated responses do not override the manual control
command received from the security administrator. Therefore, it is envisioned that
each state machine may provide an autoreponse disable state 50 as shown in
Figure 2B. Transitions to and from the autoreponse disable state are
commanded by a terrestrially-based security administrator. While in the
15 autoreponse disable state, the administrator can initiate any one of various
predefined security responses. In the event connectivity is lost between the
administrator and the aircraft, the state machine model reverts to the normal state
or the previous state depending on configuration settings.

State machines models are also used to represent each of the host servers
20 or other types of computing devices which reside on the mobile security platform.
In this way, a server that is under attack may respond differently than a user
access point. It is also envisioned that each of the state machines can be tied
together through synthetic event generation, such that when a server is under
attack, the user access points may employ a different security policy that is less

tolerant of suspicious behavior.

[0028] Each state machine can be represented by a data structure 51 as depicted in Figure 3. The data structure includes a current state 52, a possible security event 54, a resulting state 56 and a possible response 58. In this way, 5 each state can be cross-referenced against possible events to produce a resulting state and a list of possible actions. Possible events may include (but are not limited to) a security intrusion event having high priority, a security intrusion event having medium priority, a security intrusion event having a low priority, a reset event, a timer expiration event, a communication link up event, a communication 10 link down event and one or more custom events for supporting manual control commands from the security administrator. Possible responses may include (but are not limited to) setting a timer, installing a filter, resetting a filter, alerting control panel, alerting terrestrial-based security administrator, disconnecting user access point, issuing a passenger warning, and one or more predefined customer 15 responses. One skilled in the art will readily recognize from such discussion how to implement a security policy mechanism in accordance with the present invention.

[0029] Referring to Figure 4, the overall network security architecture 10 may be logically decomposed into five major components. The five major 20 components are airborne policy enforcement 62, air-ground communication 64, terrestrial control and data storage 66, terrestrial monitoring and manual control 68, and terrestrial policy editing and assignment 70. Each of these logical components are also mapped to their physical location within the network security architecture 10 as shown in Figure 4.

[0030] The airborne policy enforcement component 62 is provided by the airborne security manager 34. The primary responsibilities of the airborne security manager include (but are not limited to) managing and monitoring intrusion detection sensors, monitoring other airborne event sources, responding to security events in accordance with the applicable security policy, monitoring the airborne intrusion detection sensors, configuring static network traffic filters at user access points, executing any manual overrides commands from the terrestrial-based network security management system, installing new security policies received from the terrestrial-based network security management system, and reporting events and status of interest to the terrestrial-based network security management system. As will be apparent to one skilled in the art, the airborne security manager 34 is comprised of one or more software applications residing on one or more server(s) on each aircraft. A configuration of redundant airborne security managers provide for fail over in the event of a hardware or software failure.

[0031] With reference to Figure 5, the airborne security manager 34 is further comprised of five functional modules: an event response module 72, an onboard status module 74, a policy manager 76, a persistent storage manager 78, and a communication manager 80. The event response module 72 is responsible for receiving events, interpreting the active security policy, and triggering the appropriate actions in response to each event. It should be appreciated that this module is adapted to handle events other than security intrusion events received from the intrusion detection subsystems.

[0032] In conjunction with the onboard status module 74, the event

response module interprets and executes the state machine representing the active security policy. For instance, upon arrival of a security intrusion event, the event response module determines whether the event is associated with an individual passenger connection, an individual host server, or the airborne security manager as a whole. This module then retrieves the current state of that passenger connection, host server, or airborne security manager from the onboard status module 74 and performs the actions associated with that state and event in accordance with the active security policy. Exemplary actions may include issuing new events, making state transitions, modifying network filters, disabling passenger connections, and/or queuing messages for transmission to the terrestrial-based network security management system.

[0033] The onboard status module 74 maintains the current state of each individual passenger connection, each host server, and of the airborne security manager as a whole for the purpose of directing the state machine event response. The onboard status module 74 also tracks the status of intrusion detection sensors (e.g., signature file, operational/inactive status, sensor configuration) as well as collects status information from the other onboard modules.

[0034] The policy manager 76 is responsible for reacting to commands from the terrestrial-based network security system regarding security policy loading and activation. The policy manager also serves as a repository for configuration information relating to the airborne security manager, including, for instance, general communications parameters that determine frequency of status reports and event reporting.

[0035] The persistent storage manager 78 manages the overall data storage requirements for the onboard network security architecture. Data residing in persistent storage generally falls into one of three categories: (1) communications queue (i.e., messages to be transmitted to the terrestrial-based security management system), (2) onboard status (i.e., per-passenger connection, per-host, and system-wide data requirements), and (3) security policies. The persistent storage manager may rely on various well known, lightweight mechanisms for data storage.

[0036] Referring to Figure 4, the terrestrial control and data storage (C&DS) component 66 is provided by the terrestrial-based network security management system 16. The control and data storage functions include (but are not limited to) storing all event data in persistent storage, tracking the desired and last known configurations for each aircraft, supporting multiple security management consoles having multiple windows, notifying open console windows of any data changes that affect the window contents, providing an interface for effecting manual overrides in security policy, offering a reporting interface for reviewing stored data, and controlling access to all stored data. This component may be implemented using Java-based applications residing on one or more terrestrial servers which constitute the network security management system 16.

[0037] A more detailed description of the terrestrial control and data storage component 66 is provided with reference to Figure 6. This terrestrial component will maintain one aircraft object 90 for each aircraft associated with the security architecture. The aircraft object 90 maintains all state information for a given aircraft as well as keeps track of the last reported and the desired state of

the airborne security manager 34 residing on the given aircraft. The aircraft object 90 is a dynamic object, such that its state is maintained in dynamic memory and can be reconstructed from event histories, if necessary. Any activity that could alter the state of the airborne security manager 34 is performed by invoking a method of the aircraft object. Each method represents an event and is logged in an appropriate event log. In addition, these methods are all synchronized, ensuring that only one thread can be effecting state changes at any given time. In order to eliminate the possibility of deadlock, none of these event operations will block on communication or issue events to other aircraft.

10 **[0038]** The aircraft object 90 uses a communication subsystem 100 to exchange information with the airborne security manager 34. The aircraft object 90 issues commands and requests for status reports as well as receives events and status reports. Until an appropriate event or status report is received, any command is considered pending. This does not mean that the command has not yet executed – it may not have been executed, or it may have been and the acknowledging status report has simply not yet been received. Due to this gap in knowledge about what is actually taking place onboard the aircraft, the aircraft object 90 must carefully differentiate between the last known status and the desired status.

20 **[0039]** The aircraft object 90 is the controller in a Model-View-Controller architecture as is well known in the art. In this paradigm, the model is the data stored in a database, and the views are the various user interfaces being used to display information about the aircraft. The aircraft object is responsible for updating all of the views any time the model changes. In order to enforce this, all

changes to the model must be performed by the aircraft object and the aircraft object must keep track of those user interfaces that could be affected by the change.

[0040] The aircraft object 90 also maintains a collection of host objects
5 92 and passenger connection objects 94. The host objects 92 are used to represent the state of each onboard host server that the airborne security manager 34 is responsible for. The passenger connection objects 94 represent the individual passenger connections to the onboard network.

[0041] The terrestrial control and data storage component 66 also
10 includes a single aircraft container object 96. It is envisioned that this object may be implemented as a collection class, such as a hash table. Under this approach, aircraft objects will be created by the aircraft container 96 for every aircraft in the system. By routing incoming communication through the aircraft container 96, we ensure that the communication subsystem 100 will be able to deliver incoming
15 messages to the appropriate aircraft object. In addition, the container concept may be used to facilitate the manner in which aircraft objects are created. For instance, aircraft objects may be created only as they are needed. When an incoming message is received, the aircraft container 96 locates the applicable aircraft object. If the aircraft object is not present in memory, the aircraft container
20 can create the object. Likewise, aircraft objects that are no longer being actively monitored could be deleted until they are needed again.

[0042] The terrestrial control and data storage component 66 will also maintain event histories for each of the aircraft in a central database 98. The database 98 will maintain a record of all the events reported by an aircraft in the

system. In addition, it will maintain a record of all of the commands performed by terrestrial-based security administrator. The former represents the last known state of each aircraft; whereas the latter represents the desired stated of each aircraft. The choice of the term "last known" reflects the time delay between events occurring on board the aircraft which might not have been reflected on the ground.

[0043] Security policy files are also stored within the database 98. As a configuration option, in order to maintain a history of old policies, the policy tables may be append-only. The primary policy table will maintain a mapping of names and version numbers to a series of smaller policy elements. The communication subsystem 100 interfaces with the database 98 in order to retrieve security policy files and update the policy files onboard the aircraft.

[0044] A policy manager 99 will be responsible for any changes to policy files. This object is necessary because policy is the only thing that is not associated with a single aircraft. The policy manager 99 will ensure that any changes to policy files are properly versioned. It will also be responsible for delivering updated policy to one or more aircraft.

[0045] Returning to Figure 4, the terrestrial monitoring and manual control component 68 and the terrestrial policy editing and assignment component 70 also reside at the terrestrial-based network security management system 12. The monitoring and manual control component functions include (but are not limited to) monitoring the state and activities of a group of aircraft and selecting an individual aircraft for closing examination, monitoring the state and activities of a single aircraft and selecting an individual server or passenger connection for

closer examination, monitoring the state and activities of a single airborne server, manually controlling a single airborne server, monitoring the state and activities of a single airborne passenger connection, and manually controlling a single airborne passenger connection. This component may be implemented using a Java-based user interface running on one or more terrestrial servers.

[0046] To support the monitoring and manual control functions, the user interface includes a number of windows that may be monitored by a human network security administrator. For instance, an aircraft browser allows groups of aircraft to be navigated and aggregate/summary information displayed as shown in Figure 7. However, this window does not show the status of the communication link. In order to display such status information, the user can select a specific aircraft from the aircraft browser, thereby navigating to an aircraft status window. An exemplary aircraft status window is shown in Figure 8. The aircraft status window enables the user to view all data relevant to a specific aircraft in a single tree structure view 102. In addition, all logged events and commands are displayed in a lower log panel 104. The tabs 106 along the top of the window permit navigation to other panels which in turn focus on a different specific element associated with the aircraft. For instance, the seat panel 108 will provide status information, log detail, and manual controls for a specific seat. Other exemplary windows used to support the monitoring and manual control functions may include (but is not limited to) a passenger connection status window that focuses on displaying information for a single passenger connection, an onboard host status window that focuses on displaying information on a specific host computing device residing on the aircraft, and an events log window that displays

event information for a given group, aircraft, passenger connection or host device.

It is envisioned that the above-described windows are merely representative of some of the functionality and appearance that be used to implement the monitoring and manual control functions of the present invention.

5 **[0047]** In addition to monitoring and manual control, services for editing security policy files and distributing security policy updates also reside at the terrestrial-based network security management system 16. The policy editing and application functions include (but are not limited to) editing sensor configuration files, retrieving intrusion detection signature file updates from the applicable
10 vendor website, editing response policy state machines and parameters, editing static security configurations, combining sensor files, signature files, response policies, and static configuration into specific security policies, providing version control over security policy updates, browsing the aircraft in the system by last known policy and desired policy, and distributing a new policy to a selected group
15 of aircraft. The editing of security policy is not intended to be a routine daily activity. For this reason, policy editing and application functions are treated as a separate, distinct logical component from the other functions administered through the user interface running on the terrestrial servers.

[0048] The air-ground communication component 64 is responsible for
20 communication between the airborne security manager and the terrestrial servers. Thus, this component is distributed across these two physical locations. The air-ground communication functions include (but are not limited to) providing non-blocking communications, retrying transmissions until reliable delivery is achieved, queuing up messages during periods of non-connectivity, handling communication

session authentication, utilizing cryptographic integrity checks to protect against tampering and replay, optimizing away redundant or superseded messages where possible, utilizing available bandwidth according to message priorities, minimizing bandwidth consumption, and delivering security policy updates to aircrafts.

- 5 Logically isolating the communications component helps protect the design of the airborne security manager and the terrestrial servers from unnecessary complexity arising from sporadic connectivity.

[0049] The foregoing discussion discloses and describes preferred embodiments of the invention. One skilled in the art will readily recognize from
10 such discussion, and from the accompanying drawings and claims, that changes and modifications can be made to the invention without departing from the true spirit and fair scope of the invention as defined in the following claims.

What is claimed is:

1. A network security architecture for monitoring security activities in a mobile network platform, comprising

a mobile network residing on the mobile network platform, the mobile network being interconnected via an unreliable communication link to a terrestrial-based network security management system;

an intrusion detection system connected to the mobile network and residing on the mobile network platform, the intrusion detection system operable to detect a security intrusion event that is associated with the mobile network; and

a mobile security manager residing on the mobile network platform and adapted to receive the security intrusion events from the intrusion detection system, the mobile security manager is further operable to perform security response activities in response to the security intrusion events, when the mobile network platform is not connected with network security management system.

2. The network security architecture of Claim 1 wherein the mobile security manager is operable perform security response activities in accordance with a security policy resident on the mobile network platform.

3. The network security architecture of Claim 2 wherein the security policy is defined as a plurality of predefined security intrusion events and a

corresponding security response for each of said plurality of security intrusion events.

4. The network security architecture of Claim 2 wherein the security
5 policy is defined by a data structure having a current operational state element, a possible security intrusion event element, a resulting operational state element, and a security response element.

5. The network security architecture of Claim 1 wherein the mobile
10 network includes a plurality of user access points, such that the security intrusion event is associated with one of the plurality of user access points and the security response is directed to said one of the plurality of user access points.

6. The network security architecture of Claim 5 wherein the security
15 response is selected from the group consisting of logging the security intrusion event received from the intrusion detection system, providing a warning message to at least one of said user access points, providing an alert message to a terrestrial-based network security management system, installing a network traffic blocking filter at one of said user access points, and disconnecting one of said
20 user access points from the mobile network.

7. The network security architecture of Claim 5 wherein the mobile security manager maintains an indicator of the current operational state for each

of the plurality of user access points, such that the security response directed to said one of the plurality of user access points is in part based on the operational state of said one of the plurality of user access points.

5 8. The network security architecture of Claim 7 wherein the current operational state for any given user access point is selected from the group consisting of a normal state, a suspected state, and a disconnect state.

 9. The network security architecture of Claim 7 wherein the mobile
10 security manager is further operable to identify the current operational state for said one of the plurality of user access points and perform security response activities based in part on the identified operational state and the security intrusion event received from the intrusion detection system.

15 10. The network security architecture of Claim 9 wherein the mobile security manager is further operable to modify the current operational state for said one of the plurality of user access points in accordance with the security policy.

20 11. The network security architecture of Claim 1 wherein the mobile security manager is operable to transmit a message indicative of the security intrusion event to the network security management system and to perform security response activities in response to security commands received from the

network security management system.

12. A method for monitoring security activities associated with a network residing in a mobile network platform, the mobile network platform being
5 interconnected via an unreliable communication link to a terrestrial-based network security management system, comprising:

detecting a security intrusion event whose origination is associated with the network residing on the mobile network platform;

providing a mobile security manager residing on the mobile network
10 platform, where the mobile security manager is adapted to receive the security intrusion event; and

performing a security response activity in response to the detected security intrusion event, when the mobile network platform is not connected with the network security management system.

15

13. The method of Claim 12 wherein the step of performing a security response activity further comprises applying the security response activity in accordance with a security policy, where the security policy is defined as a plurality
20 of predefined security intrusion events and a corresponding security response for each of said plurality of security intrusion events.

14. The method of Claim 12 further comprising the steps of applying the security response activity in accordance with a security policy, where the security policy is defined by a data structure having a current operational state element, a possible security intrusion event element, a resulting operational state element,
5 and a security response element.

15. The method of Claim 12 wherein the network includes a plurality of user access points, such that the security intrusion event is associated with one of the plurality of user access points and the security response is directed to said one
10 of the plurality of user access points.

16. The method of Claim 15 wherein the security response activity is selected from the group consisting of logging the security intrusion event, providing a warning message to at least one of the user access points, providing
15 an alert message to a terrestrial-based network security management system, installing a network traffic blocking filter at one of the user access points, and disconnecting one of the user access points from the network.

17. The method of Claim 15 further comprising the steps of maintaining
20 an indicator of the current operational state for each of the plurality of user access points and performing a security response activity in response to the detected security intrusion event, where the security response activity is in part based on the operational state of said one of the plurality of user access points.

18. The method of Claim 17 wherein the current operational state for any given user access point is selected from the group consisting of a normal state, a suspected state, and a disconnect state.

5

19. An airborne security system for monitoring security activities associated with a network residing on an aircraft, the aircraft being interconnected via an unreliable communication link to a terrestrial-based network security management system, comprising:

10 an intrusion detection system connected to the network and operable to detect a security intrusion event that is associated with network; and

 an airborne security manager connected to the network and adapted to receive the security intrusion event from the intrusion detection system, 15 the security manager is further operable to perform security response activities in accordance with a security policy, when the aircraft is not connected with the network security management system.

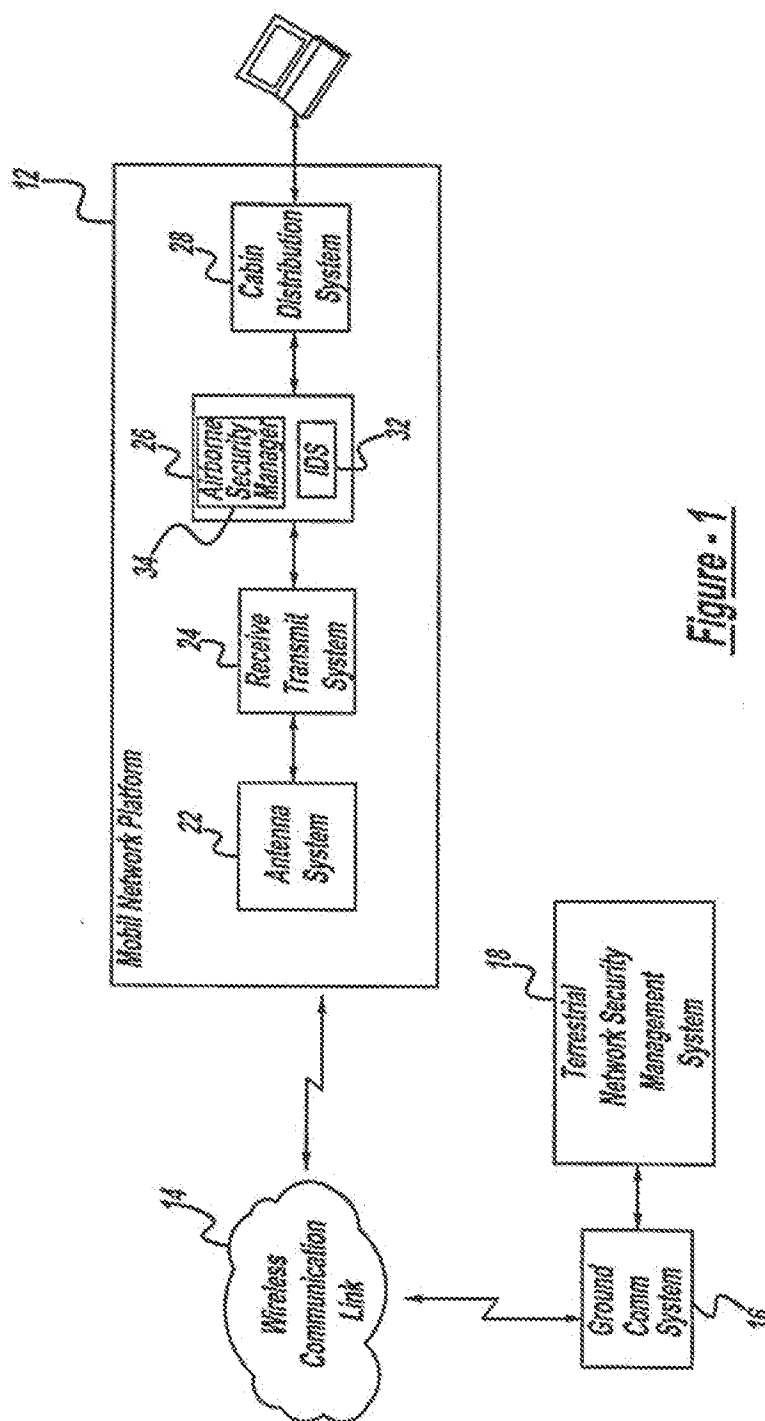


Figure - 1

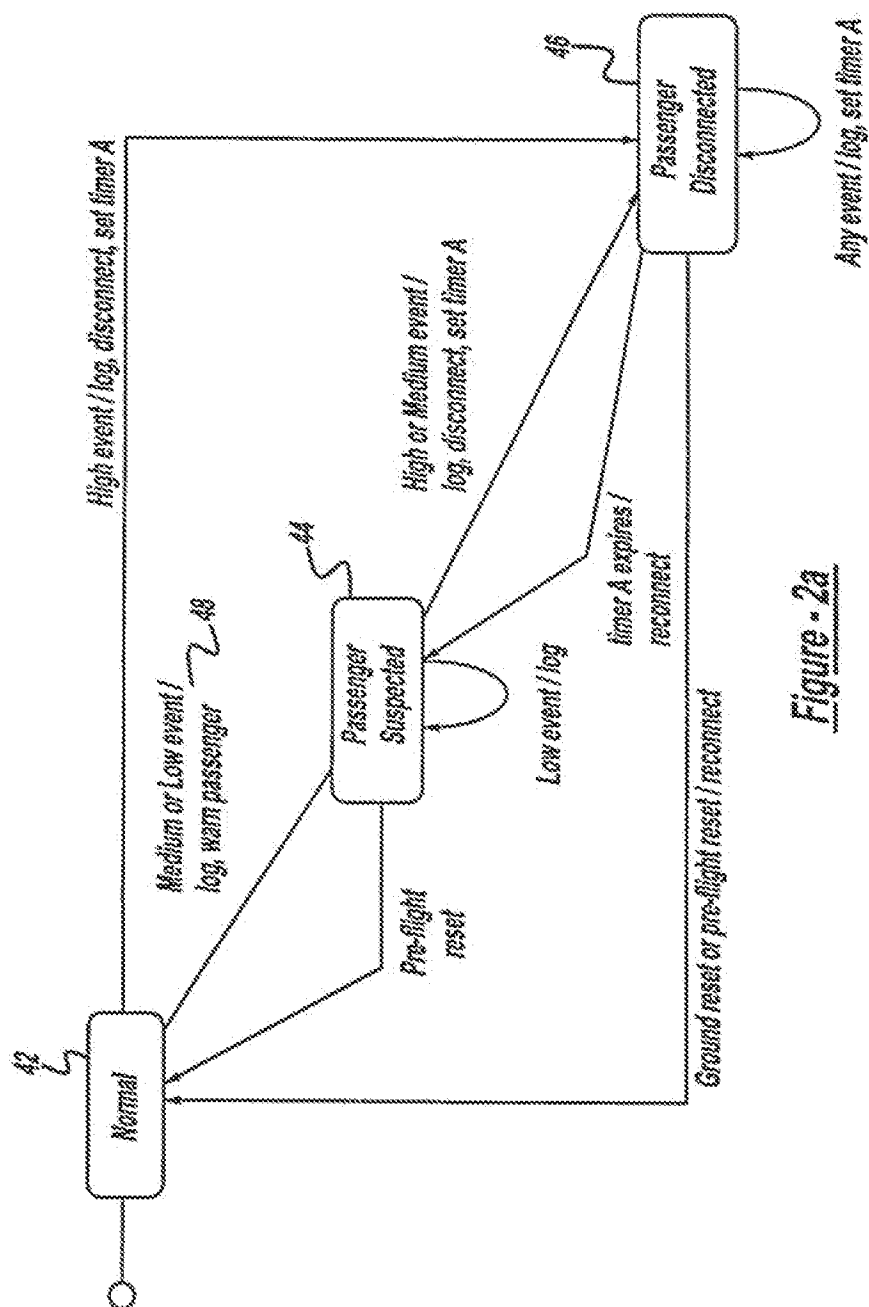


Figure - 2a

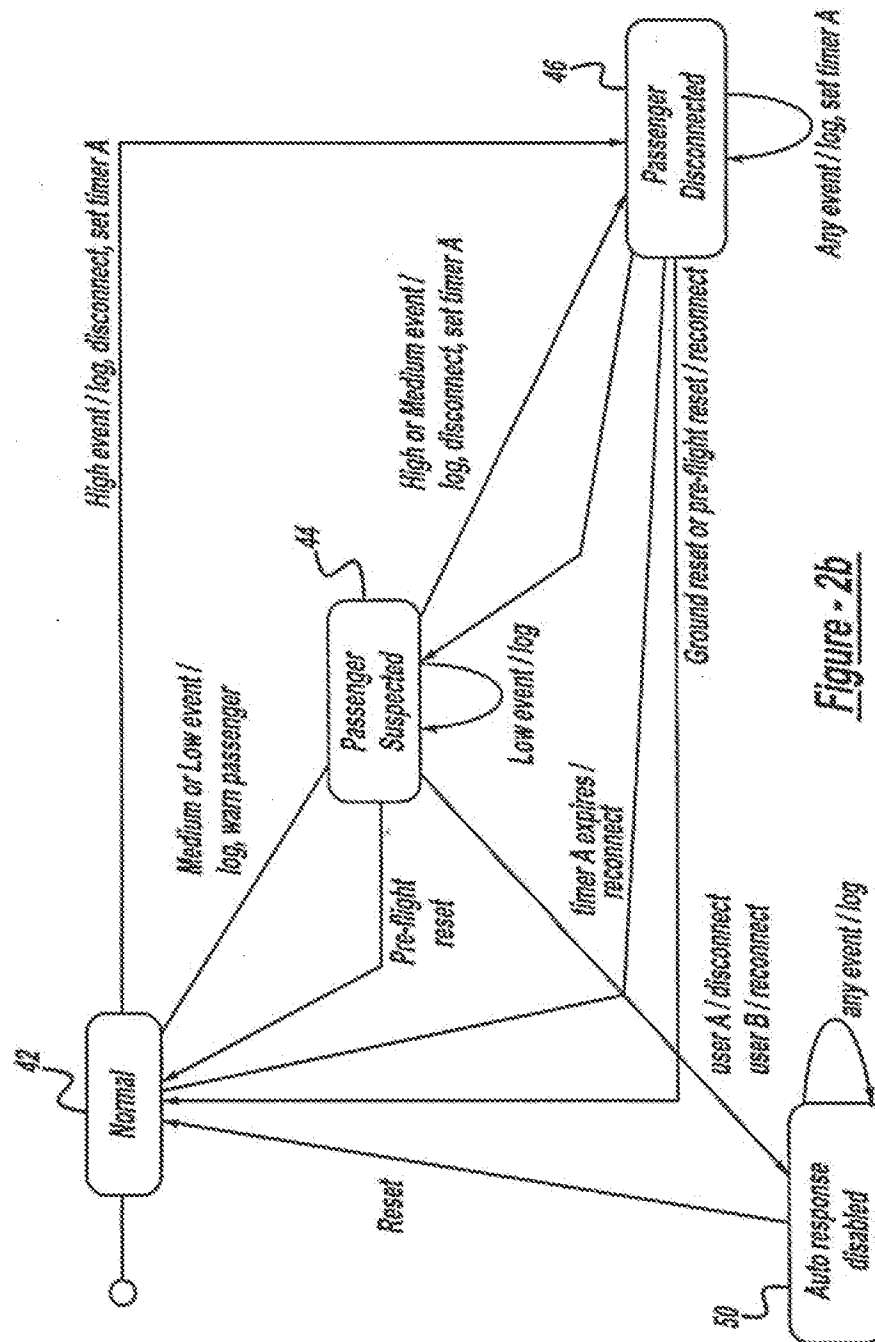


Figure - 2b

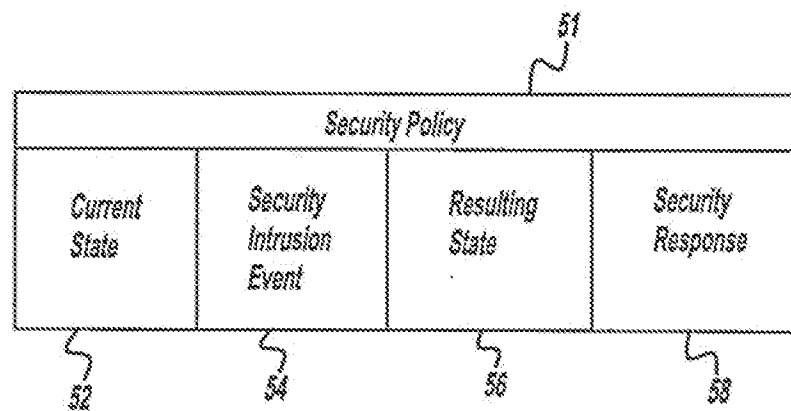


Figure - 3

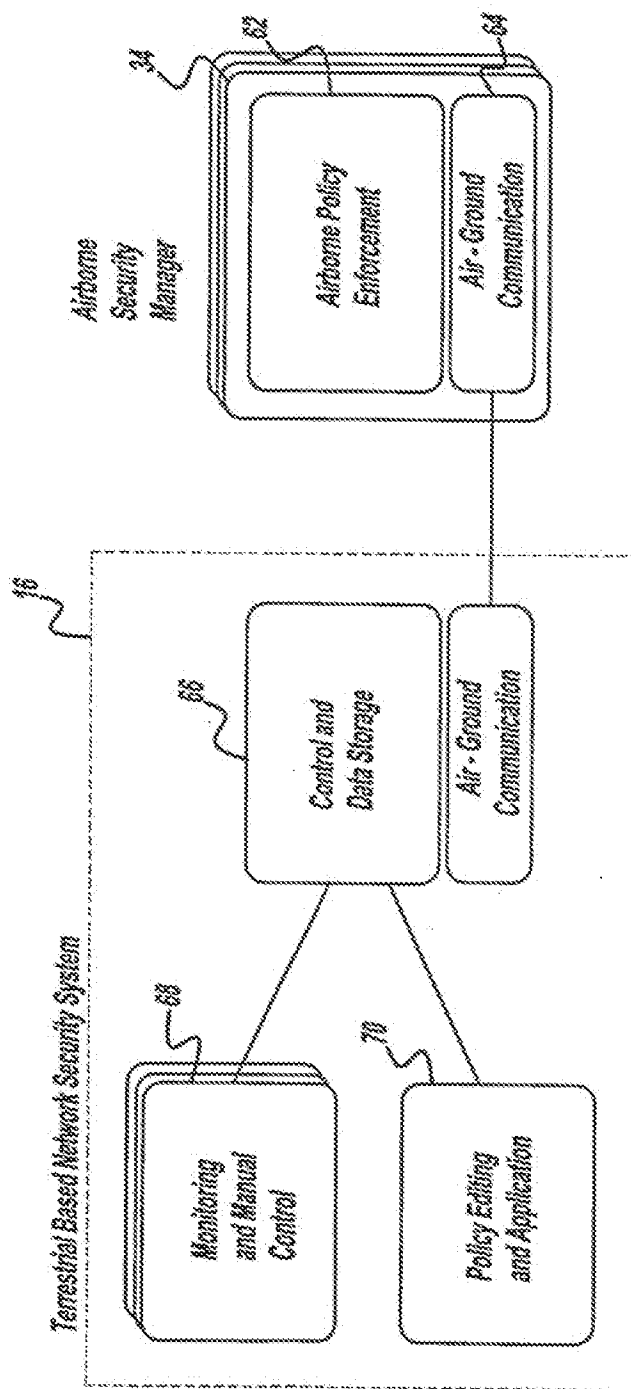


Figure - 4

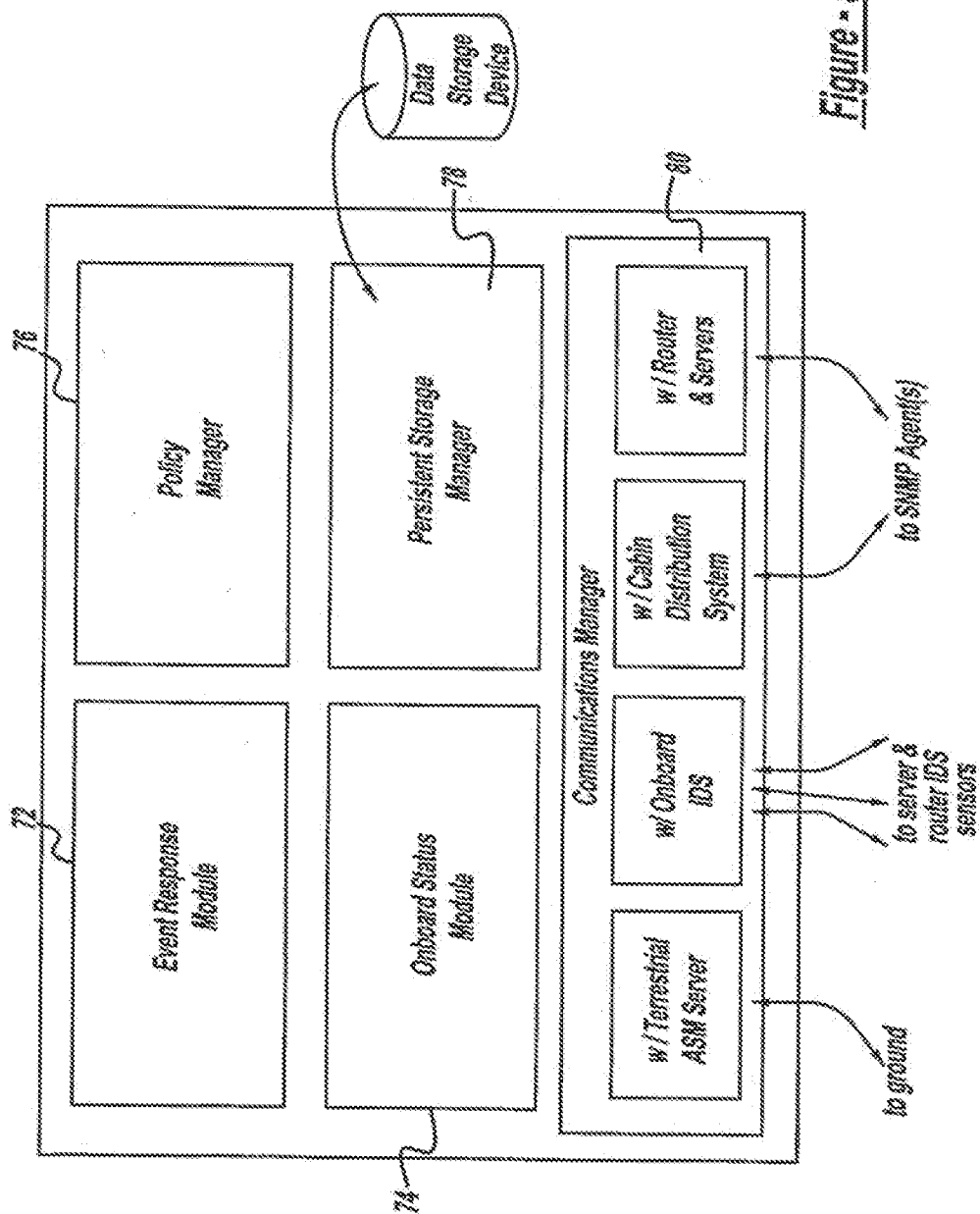


Figure - 5

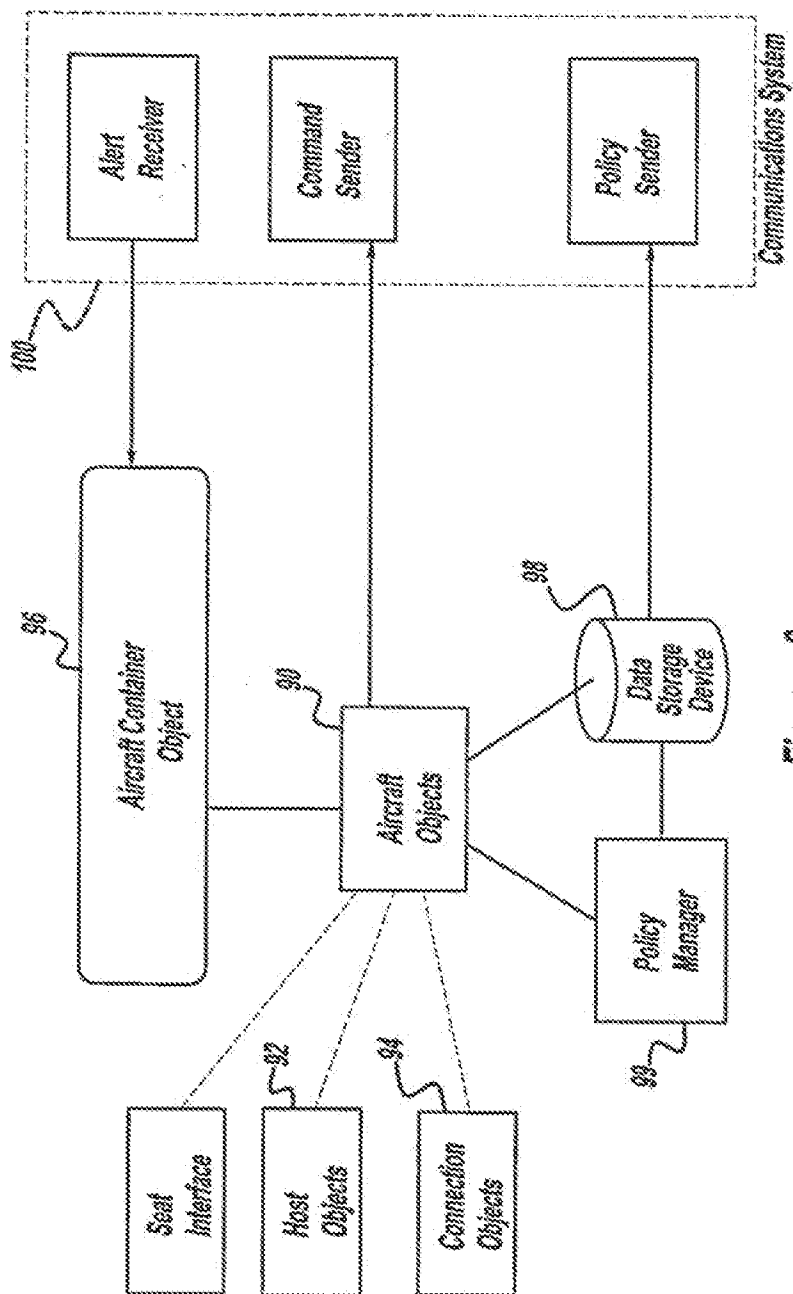


Figure - 6

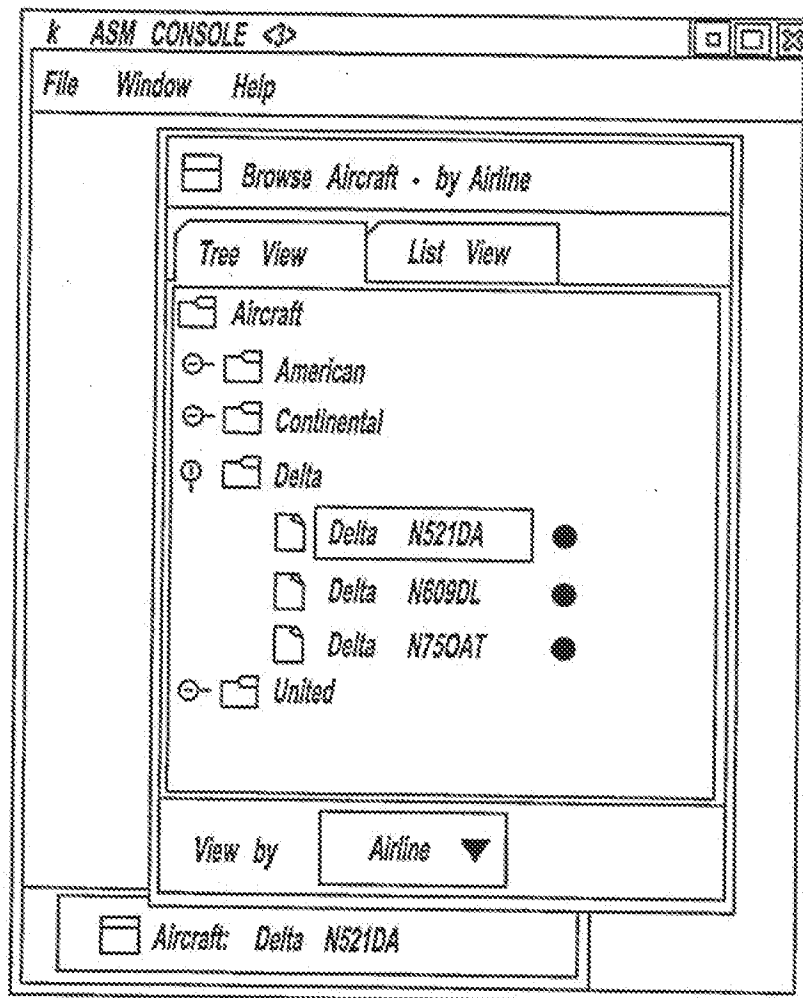
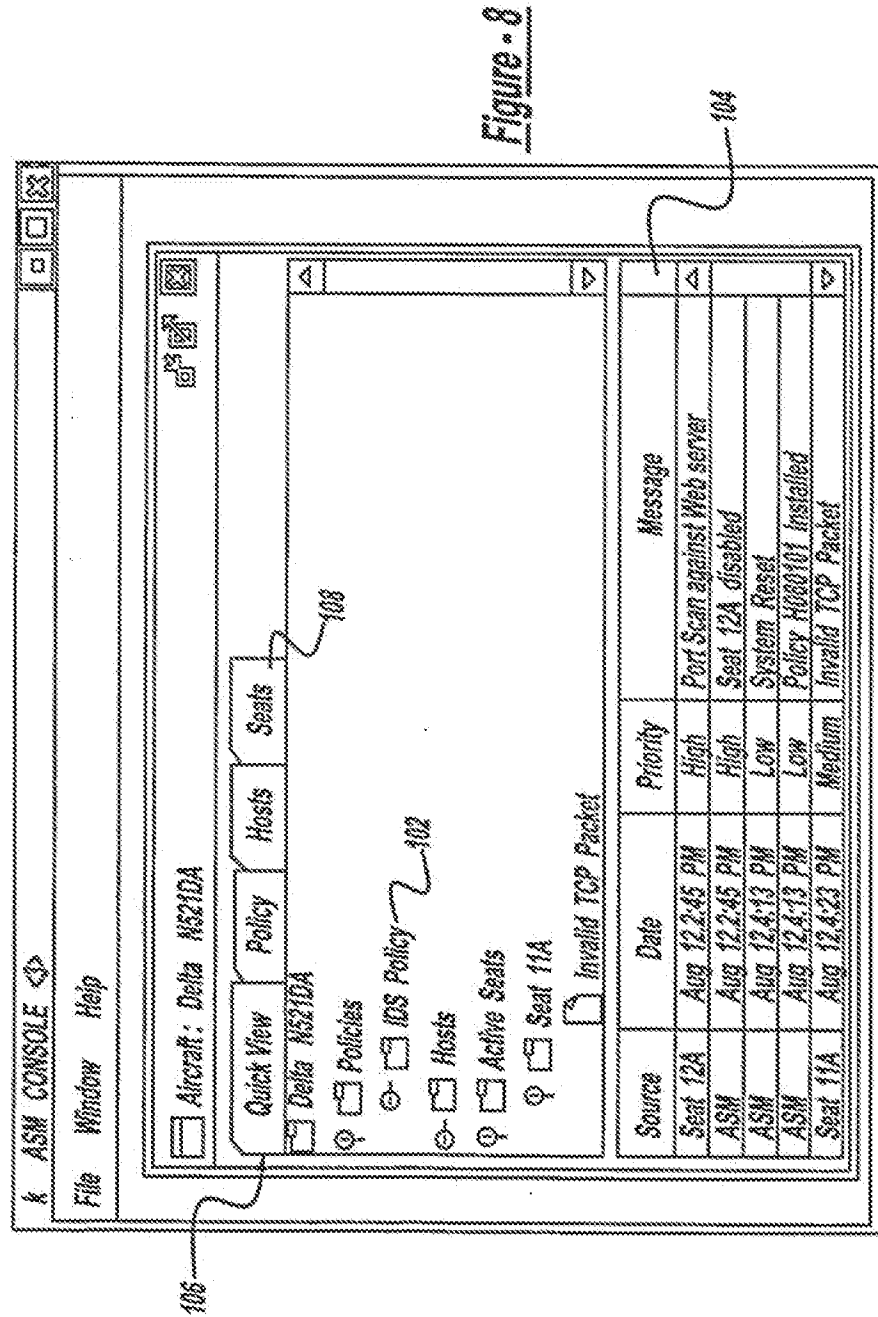


Figure - 7



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
17 July 2003 (17.07.2003)

PCT

(10) International Publication Number
WO 03/058880 A1(51) International Patent Classification⁷: H04L 9/32,
G07F 7/08[SE/SE]; John Ericssonsgatan 16, S-652 22 Karlstad (SE).
KÄWE, Rolf [SE/SE]; Lingonstigen 7, S-654 68 Karlstad
(SE).

(21) International Application Number: PCT/SE02/02424

(22) International Filing Date:
20 December 2002 (20.12.2002)(74) Agent: SVENSSON, Peder; Telia Research AB, Vitsands-
gatan 9, S-123 86 Farsta (SE).

(25) Filing Language: English

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,
SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN,
YU, ZA, ZM, ZW.

(26) Publication Language: English

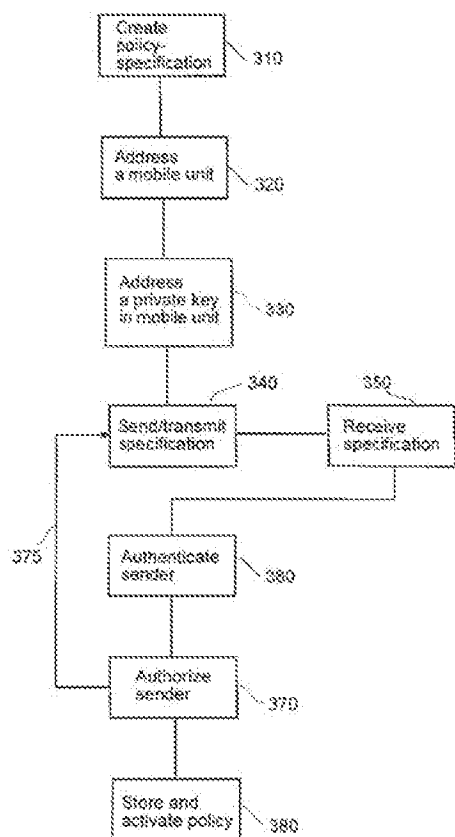
(30) Priority Data:
0208061-0 10 January 2002 (10.01.2002) SE(71) Applicant (*for all designated States except US*): **TELIA
AB** (publ) [SE/SE]; Mälbackagatan 11, S-123 86 Farsta
(SE).(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, EG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,

(72) Inventors: and

(75) Inventors/Applicants (*for US only*): **ERIKSSON, Jonas**

[Continued on next page]

(54) Title: METHOD AT ACCESS RIGHT CONTROL WITHIN MOBILE COMMUNICATION



(57) Abstract: The present invention related to a method in a mobile radio communication system with mobile units and connected service providers who provide services over said communication system, where the access from a mobile terminal of a service in a service provider requires a password. The method includes the steps to: - from a service provider, or by him/her appointed certificate authority, electronically transmit/send a password policy to a mobile unit, - in a mobile unit electronically receive said policy and handle and create/configure password connected/associated with said service provider according to rules specified in, the from the service provider or by him/her appointed certificate authority, said policy. The method also includes that the mobile unit or a specific gateway authenticates and authorizes the transmitter/sender of the policy in order to prevent illegal utilization of the possibility to change a policy.

WO 03/058880 A1



ES, FI, FR, GB, GR, IE, IT, LI, MC, NL, PT, SE, SI, SK,
TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

----- with international search report

METHOD AT ACCESS RIGHT CONTROL WITHIN MOBILE COMMUNICATION

TECHNICAL FIELD

5 The present invention relates to the field access right control within mobile communication systems.

PRIOR ART

There is a number of connections/situations within a mobile
10 radio communication system with mobile units and connected units which provide services over said communication systems, where the access from a mobile terminal of a service at such a service provider requires a password for access right control/check in a mobile unit for access to
15 different functions, data files or for use of encryption keys. These passwords frequently can be changed by the user. Usually there is a need for certain restrictions regarding among other things configuration and validity for these passwords.

20

In the patent document WO 01/35685 a system to deliver a PIN-code (PIN = Personal Identification Number) to a mobile terminal by means of an SMS-message (SMS = Short Message Service) is described. The system makes it possible that a
25 SIM-card (SIM = Subscriber Identity Module) is equipped with a PIN-code after the card having been delivered to customer.

In the patent document US 6,202,157 a system to distribute
30 and execute a policy for password in a network for data communication is described.

In the patent document US 4,924,514 a device for handling of encryption keys is described. Control vectors control
35 the handling of the keys at which the cryptographic facility is given possibility to change its policy.

The invention is among other things based on the knowledge of the inventors about that there usually is a need to put a policy into practice about which codes that can be selected. In order to today apply a policy for password, which is connected to local functions in the mobile unit, is required that this policy is entered into the mobile unit or additional units, for instance a smart card at, or just before, distribution of these units.

Both mobile operators and banks are interested in, and are working on, solutions where a user shall be authenticated (be identified to have declared/stated identity) and by his/her mobile unit create digital signatures which cannot be rejected. Typically the mobile unit consists of a mobile telephone with one or more so called smart cards. The mobile unit (or usually a smart card in the mobile unit) in its turn contains one or more private keys, which can be used for authentication and to create "non-rejection" only when a CA (Certificate Authority) has issued certificate which verifies that a specific user holds these private keys.

The use of the private keys are all but always protected by a password, which users often have possibility to change or select themselves. CA has in many cases points of view on which rules that shall apply for which passwords a user is allowed to select. CA then has what is generally called a password policy. The password policy can for instance apply to rules regarding length, allowed characters and updating intervals. Such a policy only has been possible to apply to the cases where it already at the issuing of the card has been made clear which CA that shall issue the certificate connected/associated to the keys on the card. In the mobile case, the smart card often will be distributed to the user before anyone knows what CA that shall issue the certificate connected/associated to pair of keys on the

card; so the method of entering/applying CA's password policy on the card before it is distributed to the user is not applicable.

5 SUMMARY OF THE INVENTION

The aim of the invention is to provide a method to electronically distribute a password policy over a mobile communication system to a mobile unit so that said policy directly can start being applied in the mobile unit or an
10 additional unit. The invention consequently includes a method within a mobile radio communication system with mobile units and connected service providers who provide services over said communication system, where the access from a mobile terminal of a service at a service provider
15 requires a password. The method includes the steps to:
- from a service provider, or by him/her appointed certificate authority, electronically transmit a password policy to a mobile unit;
- in a mobile unit electronically receive said policy and
20 handle and draw up/configure passwords associated with/to said service provider according to rules specified in the from the service provider or by him/her appointed certificate authority, said issued/transmitted policy.
The method also includes that the mobile unit or a specific
25 gateway authenticates and authorizes the sender of the policy in order to prevent illegal utilization of the possibility to change a policy.

BRIEF DESCRIPTION OF THE DRAWINGS

30 The invention will be described more in detail in the following, with references to enclosed drawings, in which:
Figure 1 shows an administration route/path according to one embodiment of the invention for PIN-policy.
Figure 2 shows an administration route/path for PIN-policy
35 according to another embodiment of the invention; and

Figure 3 shows a flow chart for a method according to the invention.

Figure 4A and 4B show schematically the location/placing of authentication and authorization units according to two
5 embodiments of the invention.

DESCRIPTION OF PREFERRED EMBODIMENTS

One embodiment of the invention relates to a method to distribute a password in form of a PIN-policy for
10 cryptographic keys in mobile units "over the air", that is via the communication system in which the unit is intended to operate. The keys are in the typical case held/kept in a device/smart card in the mobile unit which cannot be juggled with, but it is not necessary. The cryptographic
15 keys are in the typical case private keys in asymmetric pair of keys. The cryptographic keys, or the unit in which these are generated, have been distributed to the user already before it is known which party that will issue certificate which associates/connects the user to a certain
20 pair of keys.

When a CA shall issue a certificate, the user is linked/associated to a private key in usual way via an "over the air proof of possession"-procedure. Before, after
25 or during this procedure CA distributes its PIN-policy via the cellular mobile communication system to the mobile unit which holds/contains the private key. An application in the mobile unit attends to that the PIN-policy comes into force, and forces the user to select a PIN-code according
30 to the policy for utilization of the certified key. In Figure 1 the flow is illustrated:

1. CA 101 has decided to distribute its PIN-policy to a certain mobile unit.
- 35 2. CA addresses the PIN-policy to a certain mobile unit and a certain private key in the mobile unit 115 and

transmits/sends this to a gateway 105 for the purpose.
This gateway 105 authenticates CA 101 and decides
whether CA 101 is entitled to distribute a PIN-policy
to the mobile unit 115 (authorization). Said gateway
105 is preferably arranged at the operator of the
mobile communication system.

3. Gateway 105 sends/transmits the PIN-policy further
over the mobile communication network 110.
4. The mobile unit 115 receives the PIN-policy, secures
that it is coming from the mobile operator's gateway
105, and activates the policy for key in question. If
the user since before has a PIN-code which does not
fulfil the policy, he/she is requested to select a new
PIN-code according to the policy.
5. Alternatively, when the user changes PIN-code next
time, it has to fulfill the requirements in the PIN-
policy.

Step 1 is preferably preceded by an inquiry from the
client/user to CA about issuing of a client certificate.
A password policy preferably includes rules about, in the
general case:

- number of characters/symbols(min., max.)
- prohibited characters/symbols
- prohibited combination of characters/symbols
- intervals for how often change of password has to be
done (for instance the number of times a password is
allowed to be used).

The policy of course can be general for all users, but
also "personalized", for instance include controls of
that a certain user does not utilizes his/her personal
code number as PIN etc.

In one embodiment a PIN-policy consists of a data
structure which is interpreted by an application for the
purpose which has been arranged in the mobile unit. In

another embodiment a PIN-policy is realized as an executable application which is transmitted to the mobile unit. In the first case it is conceivable that a plurality of PIN-policies can be active at the same time, but some mechanism to solve conflicting policies, if any, then is needed.

The mobile unit 115 then preferably includes one or more integrated or removable smart cards or any other form of device which is protected against manipulations. The invention of course is applicable also in the cases when the private key is not stored in a device which is protected against manipulation, but in any other way in the mobile unit.

In one embodiment the specific gateway which is mentioned in step 2 does not exist, compare Figure 2. Instead CA 201 transmits its policy via a general traffic gateway for the mobile communication network (GGSN for GPRS/UMTS) 210, without mechanisms for authentication and authorization of CA 201. In this embodiment mechanisms for authentication and authorization are instead implemented in the mobile unit 215

In Figure 3 the method steps corresponding to the distribution path in Figure 1 and Figure 2 are shown. CA creates 310 a policy specification, and addresses 320 a mobile unit and addresses 330 a private key within said mobile unit. Further, the specification is transmitted 340 over the mobile network, possibly via a specific gateway as has been mentioned above. The specification is received 350 and the transmitter/sender is authenticated 360, respective, whenever applicable, authorized 370. Depending on the number of units between CA and mobile unit which need own authentication and authorization, the steps to transmit 340, receive 350, authenticate 360 and

authorize 370 are repeated 375. Finally, the policy is stored and activated in the mobile station.

Of course in alternative embodiments other parties than
5 CA can load down a PIN-policy. Particularly in one embodiment the operator of the mobile communication service is capable of loading down his/her PIN-policy to the mobile units in his/her network.

10 PIN-policy for other purposes than unlocking/use of private keys of course also can be distributed to the mobile unit according to the invention. For instance PIN-codes and passwords for:

- use of symmetrical keys
- 15 - write/read rights to/of data files
- GSM
- execution of applications
- etc.

20 In the case there are more than one CA (we call these A respective B) which certifies the same key, the following method is an embodiment of the invention:

- Both A and B can load down its policy to the mobile unit. Both policy from CA A and a policy from CA B are
25 put into practice each time PIN is changed. This requires a mechanism in the mobile unit to solve conflicting demands.
- Both A and B sends/transmits its policy to the operator of the mobile communication network. The
30 operator creates a "summing up" of these rules and decides about which policy that finally is transmitted to the mobile unit.
- Both A and B can load down its policy to the mobile unit. Separate PINs are used for the same key
35 depending on which of his/her certificates the user wants to refer to. Policy from CA A applies when the

user refers to his/her certificate from CA A, and policy from CA B applies when the user refers to his/her certificate from CA B.

3 In Figure 4 A and B are shown how units for authentication and authorization have been arranged in preferred embodiments. Fig. 4A shows an authentication unit 402 and an authorization unit 404 arranged in gateway 105. Figure 4B shows an authentication unit 402 and an authorization
10 unit 404 arranged in a mobile unit 115.

Of course there is in most cases a reliable transport mechanism required to transmit a PIN-policy from CA, or other provider/issuer of the policy, to the mobile unit.

15 There are several methods to realize this, but this is out of the scope of the invention.

The scope of protection is only limited by the following patent claims.

20

PATENT CLAIMS

1. A method in a mobile radio communication system with mobile units and connected service providers who provide services over said communication system, where the access via a specific mobile terminal of a specific service at a specific service provider requires a password, characterized in that said method includes the steps to
- 10 - from a service provider, or by him/her appointed certificate authority electronically transmit a password policy to a mobile unit
 - in a mobile unit, electronically receive said policy and handle and create/configure password in connection with said service provider according to rules specified in,
 - 15 from the service provider or by him/her appointed certificate authority, said transmitted/send policy.
2. A method as claimed in patent claim 1, characterized in the following steps:
- 20 - creation of a password policy specification at a service provider or by him/her appointed certificate authority (CA)
 - production/deriving of the address to a mobile unit,
 - 25 - production/deriving of the address to a private key in said mobile unit,
 - transmission/sending of the specification,
 - reception of the specification,
 - authentication of CA,
 - 30 - authorization of CA,
 - storing of a policy which corresponds to the specification, and
 - activation of said policy.

3. A method as claimed in patent claim 1,
c h a r a c t e r i z e d in that it includes the following
steps.

- creation of a password policy specification at a CA,
- 5 - production/deriving of the address to a mobile unit,
- production/deriving of the address to a private key in
said mobile unit,
- distribution of the policy specification to a gateway
for downloading of policy,
- 10 - authentication of CA in said gateway,
- authorization of CA in said gateway,
- distribution of the specification from gateway to mobile
unit over a mobile communication network,
- reception of the specification,
- 15 - ensuring that the specification is emanating from
approved gateway,
- storing of a policy which corresponds to the
specification, and
- activation of said policy.

20

4. A method as claimed in patent claim 3,
c h a r a c t e r i z e d in that it further includes the
step:

- forcing the user to immediately change password to one
25 which fulfils the new policy.

5. A method as claimed in patent claim 3,
c h a r a c t e r i z e d in that it further includes the
step:

- 30 - awaiting to insert/apply the policy until the user
changes password next time.

6. A method as claimed in any of the patent claims 1-5,
c h a r a c t e r i z e d in that said password is a PIN-
35 code.

7. A mobile radio communication system with mobile units and connected service providers who provide services over said communication system, where the access via a specific mobile terminal of a specific service at a specific service provider requires a password, characterized in that said system includes means to, from a service provider, transmit/send a policy specification for password to a mobile unit.
8. A mobile communication system as claimed in patent claim 7, characterized in that said system includes means to in a mobile unit receive a policy specification for password.
9. A mobile communication system as claimed in patent claim 8, characterized in that in said system means has been arranged for authentication of a policy sender/transmitter.
10. A mobile communication system as claimed in patent claim 8, characterized in that in said system means has been arranged for authorization of a policy sender/transmitter.
11. A mobile communication system as claimed in patent claim 7, characterized in that a gateway including means for authentication and authorization of a policy-sender/transmitter has been arranged to connect a CA to the mobile communication system, and to authorize and authenticate said CA.
12. A mobile communication system as claimed in patent claim 9 or 10, characterized in that means for authorization of a policy-transmitter/sender has been arranged in a mobile unit.

13. A mobile communication system as claimed in any of the patent claims 7-12, characterized in that said policy specification is arranged in form of a data structure.

5

14. A mobile communication system as claimed in any of the patent claims 7-12, characterized in that said policy specification is arranged in form of an executable application.

10

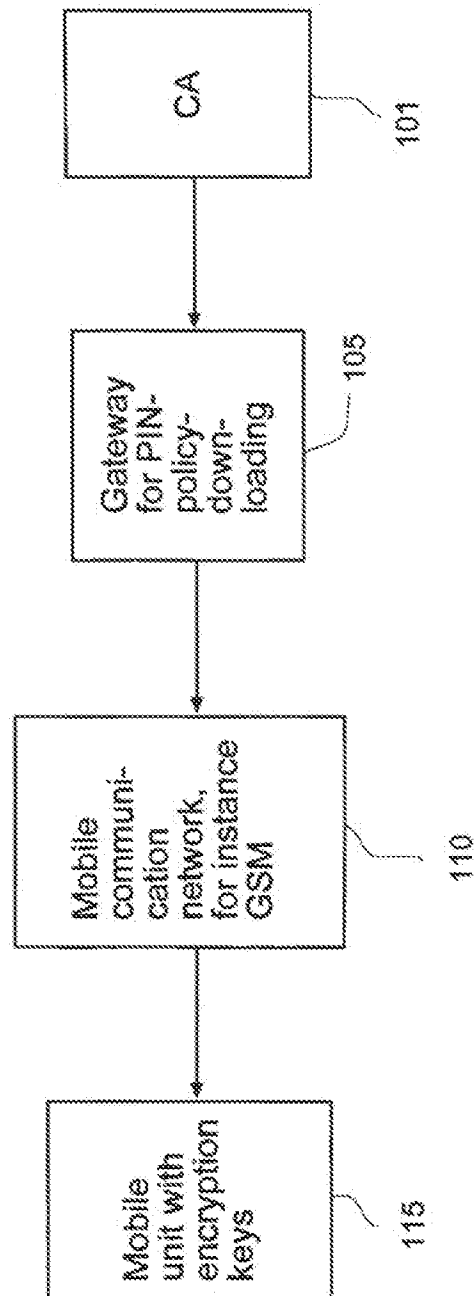


Figure 1

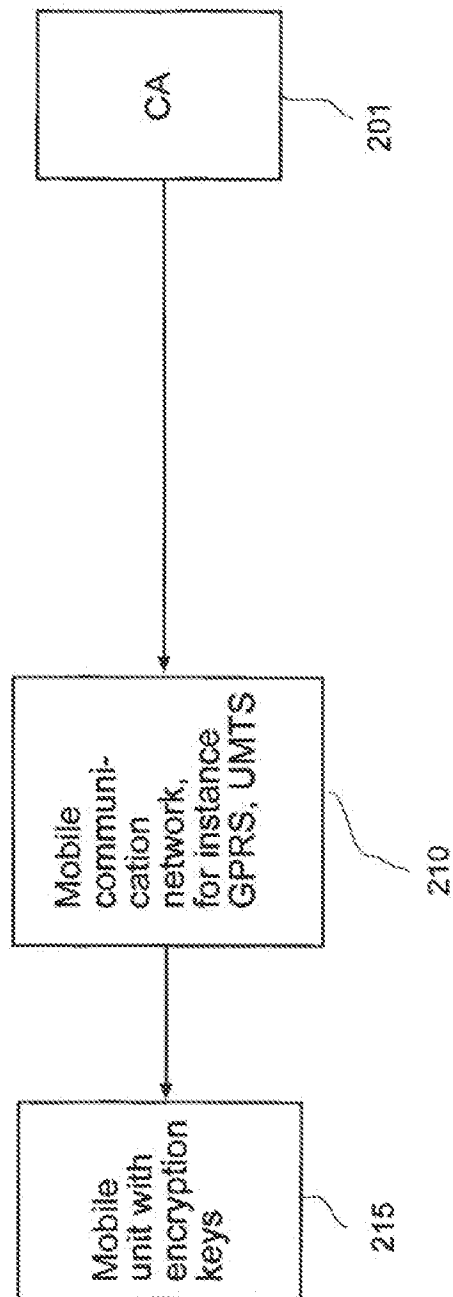


Figure 2

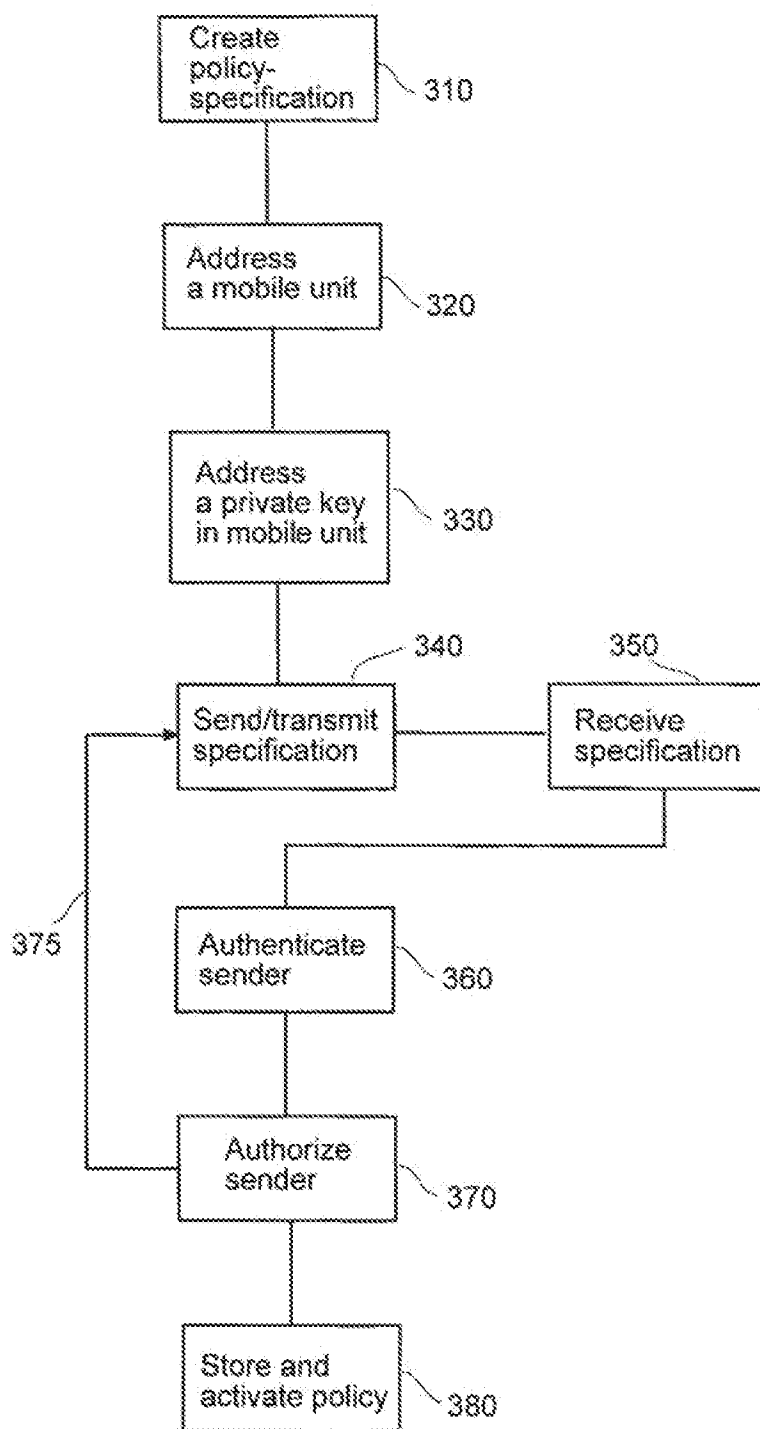


Figure 3

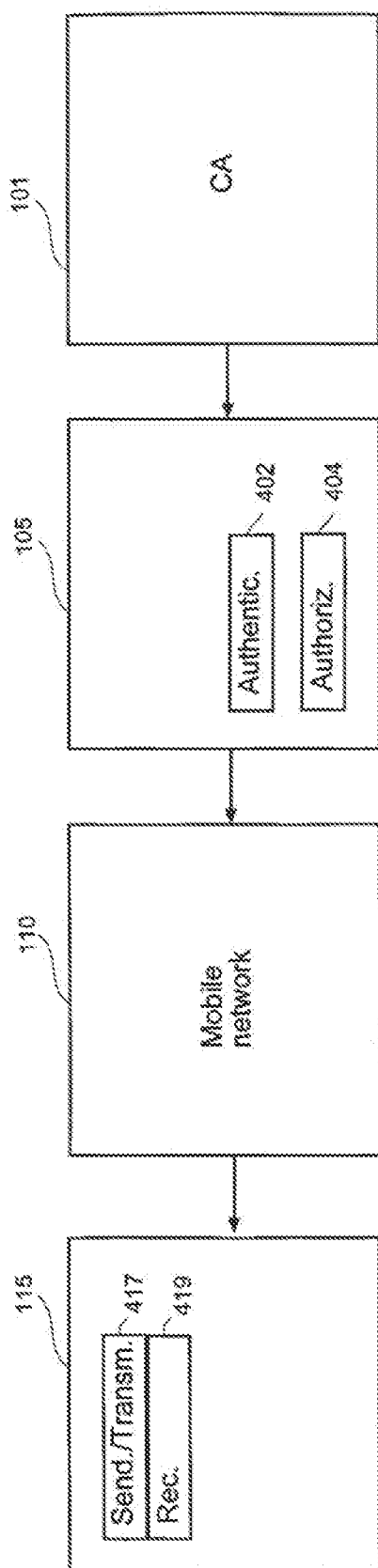


Figure 4A

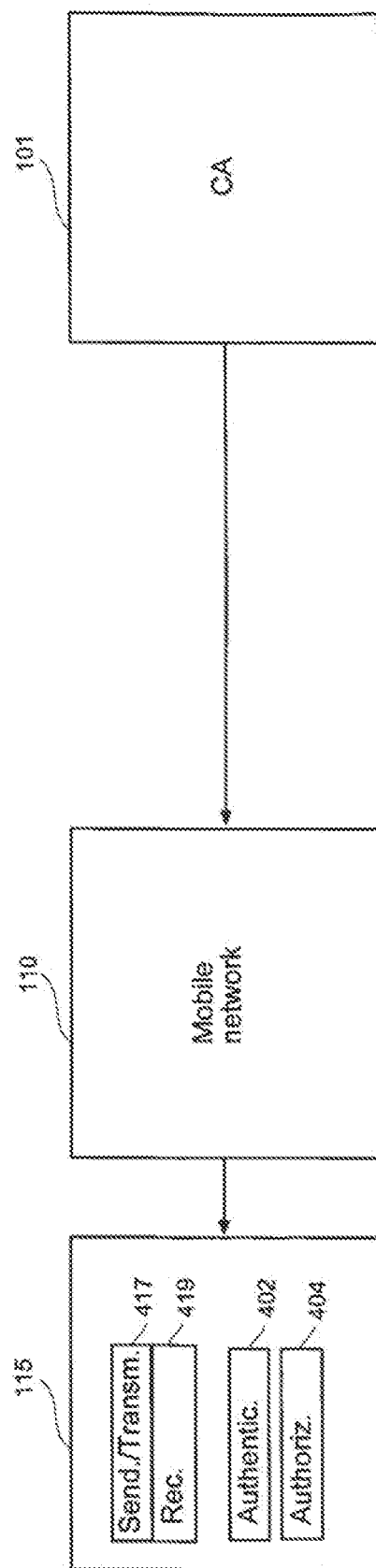


Figure 4B

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 02/02424

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32, G07F 7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6202157 B1 (BROWNLIN, M. ET AL), 13 March 2001 (13.03.01), abstract, cited in the application ---	1-14
A	WO 0135685 A1 (MOBILIX A/S), 17 May 2001 (17.05.01), abstract, cited in the application ---	1-14
A	US 5944824 A (HE, J.), 31 August 1999 (31.08.99), claim 1 ---	1-14
A	US 4924514 A (MATYAS, S.M. ET AL), 8 May 1990 (08.05.90), cited in the application ---	1-14

☒ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

7 April 2003

Date of mailing of the international search report

09-04-2003

Name and mailing address of the ISA/

Swedish Patent Office

Box 5055, S-102 42 STOCKHOLM

Facsimile No. +46 8 666 02 86

Authorized officer

Rune Bengtsson/mj

Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 02/02424

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0354771 A2 (INTERNATIONAL BUSINESS MACHINES CORPORATION), 14 February 1990 (14.02.90), abstract -- -----	1-14

INTERNATIONAL SEARCH REPORT

Information on patent family members

28/02/03

International application No.

PCT/SE 02/02424

Patent document cited in search report			Publication date	Patent family member(s)		Publication date
US	6202157	B1	13/03/01	NONE		
WO	0135685	A1	17/05/01	AU	1269001 A	06/06/01
				BR	0015445 A	05/11/02
				DK	160899 A	10/05/01
				EP	1228653 A	07/08/02
US	5944824	A	31/08/99	NONE		
US	4924514	A	08/05/90	CA	1313411 A	02/02/93
				DE	68922884 D,T	30/11/95
				DE	68926005 D,T	17/10/96
				EP	0354771 A,B	14/02/90
				EP	0356065 A,B	28/02/90
				JP	2105192 A	17/04/90
				JP	2107722 C	06/11/96
				JP	8023736 B	06/03/96
EP	0354771	A2	14/02/90	CA	1317677 A	11/05/93
				DE	68922884 D,T	30/11/95
				DE	68926005 D,T	17/10/96
				DE	68926076 D,T	14/11/96
				DE	68926200 D,T	17/10/96
				EP	0354770 A,B	14/02/90
				EP	0354774 A,B	14/02/90
				EP	0356065 A,B	28/02/90
				JP	2099984 A	11/04/90
				JP	2105990 C	06/11/96
				JP	8020848 B	04/03/96
				US	4941176 A	10/07/90
				CA	1313411 A	02/02/93
				JP	2105192 A	17/04/90
				JP	2107722 C	06/11/96
				JP	8023736 B	06/03/96
				US	4924514 A	08/05/90

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
1 April 2004 (01.04.2004)

PCT

(10) International Publication Number
WO 2004/028070 A1

(51) International Patent Classification⁷: H04L 9/00, 9/32

(US): GORDON, Ian, R.; 32 Melgund Avenue, Ottawa, Ontario K1S 2S2 (CA).

(21) International Application Number:

PCT/US2003/029347

(74) Agents: TOLER, LARSON & ABEL, LLP, ET AL., et al.; 5000 Plaza on the Lake, Suite 265, Austin, TX 78746 (US).

(22) International Filing Date:

19 September 2003 (19.09.2003)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

10/252,212	23 September 2002 (23.09.2002)	US
10/252,225	23 September 2002 (23.09.2002)	US
10/252,213	23 September 2002 (23.09.2002)	US
10/252,211	23 September 2002 (23.09.2002)	US

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TL, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, OW, ML, MK, NE, SN, TD, TO).

(71) Applicant: CREDANT TECHNOLOGIES, INC. [USA/US]; Suite 1010, 15305 Dallas Parkway, Addison, TX 75001 (US).

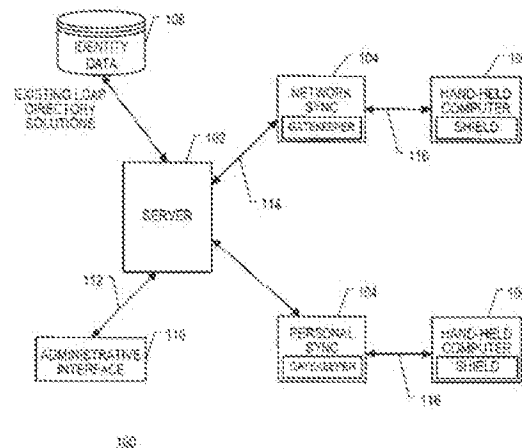
(72) Inventors: MANN, Dwayne, R.; 401 Del Rio Court, Allen, TX 75013 (US); HEARD, Robert, W.; 3321 Wolfe Court, Plano, TX 75025 (US); BURCHETT, Christopher, D.; 1019 Sir Lancelot Circle, Lewisville, TX 75056

Published:

— with international search report

[Continued on next page]

(54) Title: SERVER, COMPUTER MEMORY, AND METHOD TO SUPPORT SECURITY POLICY MAINTENANCE AND DISTRIBUTION



(57) Abstract: In a particular embodiment, a server module deployed on a server (102) is disclosed. The server module is connected to a wireless network access node (104). The server module includes a database (108) containing user information for multiple wireless devices (106). Each element in the database (108) is attributable to at least one authorized wireless device (106) and contains at least one type of data file from the following group: (i) wireless connectivity permissions, (ii) authorized wireless device identification, and (iii) authorized network access node information. In another embodiment, a method of enforcing security policies at a mobile computing device (106) is provided. The method includes receiving a policy at the mobile computing device (106) and enforcing the policy at the mobile computing device (106) by disallowing a user of the mobile computing device (106) from engaging in the use precluded by the use limitation. The policy includes at least one device use limitation.



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SERVER, COMPUTER MEMORY, AND METHOD TO SUPPORT SECURITY POLICY MAINTENANCE AND DISTRIBUTION

5

BACKGROUND

Field of the Invention

10 The present application relates to systems and methods of distributing and enforcing security policies.

Description of the Related Art

15 The use of mobile devices, such as personal digital assistants (PDAs), in corporate environments is projected to grow significantly over the next 3-5 years. These smart devices are increasing in diversity and capability as well as number. These devices offer a unique blend of lightweight mobility, convenience and functionality providing an instant-on access to information such as email, calendar, address book and other documents. Many enterprises are developing or have deployed special applications for mobile devices that transform the platform into a mission critical tool and repository for sensitive corporate data.

20 As a result, mobile devices have become indispensable tools for business communications. The use of these devices is expected to grow rapidly according to industry experts.

25 The prevalence and power of mobile computing devices and the increasing availability of wireless connectivity represents a paradigm shift in how people will use computers and access data. The current use and diversity of these devices are impacting the integrity of corporate IT infrastructures in many ways. These devices connect to the corporate network in multiple, unsecured and difficult to monitor transient ways. Cradles are used to 'synch' the devices to laptops or desktops using serial or USB lines. Modems and wired or wireless networks are used. Cell phones are converging with PDAs to provide

- 2 -

a new generation of devices that may access corporate data in an expanding network of advanced cellular access points. Finally, since these devices have significant storage, computing power and operate in a connected and disconnected mode, security management and control of these devices remains an important challenge.

5 Mobile devices provide an "open door" into the enterprise, especially if lost or stolen. A variety of sensitive information may reside on these devices including passwords and access codes for most corporate databases, network files and applications. These pocket-size devices have become the "password sticky note" of the 21st century. In a wireless "always-on" world, these devices can enter and exit numerous unknown and ad hoc
10 networks in a single day. At industry tradeshows, cyber-cafes or industry networking environments, corporate data is especially exposed to unauthorized access.

 These devices have become large walking repositories for business confidential information. Mobile professionals frequently synch or copy proprietary corporate information from laptops, such as financial results, launch plans, personnel information,
15 client records or application specific information. The large memory capacity of mobile devices and the plummeting price of after market memory cards make it more likely that users will store additional information on their devices.

 The emerging corporate use and capabilities of these devices make unique challenges for an enterprise scale mobile security solution. Because mobile devices often
20 operate in a disconnected mode, on-device policy enforcement is required.

 The number of mobile devices entering the enterprise and the complexity of the security requirements is placing an increased demand on the enterprises ability to manage and enforce corporate security on mobile devices. Many information technology (IT) departments do not know how many non-company issued devices are currently being used
25 by employees. They have no tools to restrict these devices from accessing corporate data. Simply put, current IT departments are not equipped to respond to the emerging computing standard of the mobile device.

 Accordingly, there is a need for an improved system and method of handing security policies with respect to mobile devices.

- 3 -

SUMMARY

In a particular embodiment, a server module deployed on a server that is connected to a wireless network access node is disclosed. The server module includes a database containing user information for multiple wireless devices. Each element in the database is attributable to at least one authorized wireless device and contains at least one type of data file from the following group: (i) wireless connectivity permissions, (ii) authorized wireless device identification, and (iii) authorized network access node information.

In another embodiment, a computer memory is disclosed. The computer memory includes a plurality of operating keys for use in connection with security features of a mobile computing device and a root key. The root key is to encrypt the plurality of operating keys.

In another embodiment, a method of enforcing security policies at a mobile computing device is provided. The method includes receiving a policy at the mobile computing device and enforcing the policy at the mobile computing device by disallowing a user of the mobile computing device from engaging in the use precluded by the use limitation. The policy includes at least one device use limitation.

In another embodiment, a security method is provided. The security method includes receiving a password from a user of a mobile computing device; deriving a security code from the password by applying a non-linear function; and encrypting the security code using the password as an encryption key.

In another embodiment, a method of selectively providing a mobile computing device with access to a software application on a server is provided. The method includes receiving a request to access the software application from the mobile computing device and determining whether to grant access to the software application by checking whether the mobile computing device has an installed security program.

In a further embodiment, a method of updating policies and key materials is provided. The method includes providing a shared encryption key that is shared by a server and a client module; encrypting data on the client using the shared encryption key; authenticating a user of a mobile computing device by receiving a password, where the client is resident at the mobile computing device; decrypting the shared key using the

- 4 -

password; using the shared key to decrypt updated policies and key materials; and replacing policies and key materials at the mobile computing device with the updated and decrypted policies and key materials.

BRIEF DESCRIPTION OF THE DRAWINGS

5 FIG. 1 is a block diagram of an embodiment of a system for use in providing security policy distribution and mobile device management.

 FIG. 2 is a block diagram of an embodiment of a server within the system of FIG. 1.

 FIG. 3 is a general diagram that illustrates software layers within the server of FIG. 2.

10 FIG. 4 is an illustrative screen shot of an administrative user interface for use with the server of FIG. 2.

 FIG. 5 is a block diagram that illustrates functional elements within the gatekeeper of FIG. 1.

 FIG. 6 is block diagram that illustrates elements within the shield application of the
15 system of FIG. 1.

 FIG. 7 is a flow chart that illustrates installation of the shield security application onto mobile devices.

 FIG. 8 is a flow chart that illustrates a method of updating policy information and distributing the updated policy information to a mobile device.

20 FIG. 9 is a flow chart that illustrates another method of updating policy information and distributing the updated policy information to a mobile device.

 FIG. 10 is a diagram that illustrates key materials and specific key field formats for use with encryption of policy information.

 The use of the same reference symbols in different drawings indicates similar or
25 identical items.

DETAILED DESCRIPTION OF THE DRAWINGS

Referring to FIG. 1, a system 100 for use in enterprise security management is disclosed. The system 100 includes a server 102, a gatekeeper 104, and a client device module 106. The client device module 106 that is used to provide security functionality is also referred to as a shield. The system 100 is a comprehensive enterprise security management software platform for diverse mobile operating systems, applications and devices. The system 100 enables an organization to secure and manage mobile devices easily and cost effectively. The server 102 integrates with existing security policy management systems and allows administrators to centrally create new mobile security policies by extending existing security policies and to distribute them to a diverse population of mobile devices. The server 102 and gatekeeper 104 work together to automatically and securely push these security policies to a specified mobile device. The shield 106 is a trusted computing environment on the mobile device that enacts and enforces the distributed security policies, controls access to the mobile device, and provides data security.

The server 102 may be implemented as a web-based application server that provides central creation and management of mobile security policies. The server 102 is preferably implemented with portability, scalability and maintainability in mind using industry standards such as Java, XML and other advanced web technologies. To provide easy control and accessibility, an administrative interface to the server 102 is provided through a secure browser interface allowing the simple delegation of responsibilities and access by any workstation or PC on a local network connected to the server 102.

A consolidated LDAP directory (CLD) technique may be used to integrate the server 102 with existing enterprise security infrastructure, such as an existing identity database 108. Existing policy and identity management systems are integrated through a real-time interface to directory resources. A layer in the server 102 provides a consolidated view of the external LDAP services and extends these services through policy inheritance and overriding. As a result, existing identity directories, such as directory 108, can be used without copying data and without changing the data schemas of the existing enterprise security systems.

- 6 -

The data passed to the gatekeeper 104 and subsequent mobile devices 106 is derived from security role and is protected through a combination of secure socket layer (SSL) and data encryption. Mobile security policies are formed using the administration interface 110, which is coupled to the server 102 via interface 112, to set and extend policies in a consolidated directory (e.g., LDAP). Once policies are set, a policy package is generated for each user within a role, encrypted with the specific users' encryption key, and forwarded to the gatekeeper 104 for installation on the target mobile device 106. Policy package encryption forms a main pillar of system security. Additionally, SSL communication is used for added privacy and authentication between the server 102 and the gatekeeper 104 over the secure interface 114. The system 100 is designed for robust security management to provide many advanced security features including: centralized management of disconnected devices, automatic versioning and distribution of policies, role-based policy creation and management, seamless integration with existing role repositories and security infrastructure, delegated security management, separation of administrative duties, automatic retrieval of device audit logs, consolidation, alerting and reporting, and mobile device management.

The gatekeeper 104 may be implemented as a security management software agent that forms a virtual security layer on existing, third party synchronization systems, such as HotSync, ActiveSync, and ScoutSync. A function of the gatekeeper 104 is to receive policy packages from the server 102 and install the packages on target mobile devices 106. The gatekeeper 104 operates in two modes to support local and network synchronization. In local mode, the gatekeeper 104 executable operates on desktop and laptop computers forming a security layer on top of personal synchronization tools. In network mode, the gatekeeper 104 executable operates on an enterprise server and forms a security layer on top of a network synchronization application. When the gatekeeper 104 is deployed, mobile devices 106, such as personal digital assistants (PDAs), are required to authenticate and to request permission to synchronize before the third party data synchronization tool is allowed to launch. Additionally, the gatekeeper 104 provides for automatic installation of the mobile shield on specified PDAs, application configuration, update and patch management, mobile device configuration management, monitoring, management, and control access to synchronization application, and distribution of device policies, permissions and configurations.

- 7 -

The mobile device application, i.e., shield, 106, may be implemented as a trusted computing environment operating as a software layer on top of the mobile device operating system. Security policies are received from the gatekeeper 104 using a two-way authentication process. The policies are used by agent software at the mobile device to
5 encrypt data, and to monitor and control device access, device peripherals, and device software and hardware operations. The mobile device trusted environment approach provides many security features, including: on-device policy enforcement whether connected or disconnected, mandatory access control, data encryption with secure recovery, mandatory synchronization authentication, controlled application access and use, control
10 over hardware ports – infrared (IR), compact flash (CF), universal serial bus (USB), secure digital (SD), multiple profiles – personal and business, and secure audit logs. Sample devices that may accept shield software include personal devices made by Palm, Handspring, Sony, Compaq iPaq, and the HP Jornada 500 series.

To summarize, all three major components of the system 100 interoperate
15 substantially seamlessly and transparently to the user to enable a secure mobile environment without materially detracting from the user's experience. The server 102 virtually consolidates external LDAP identity and policy data to integrate to existing security infrastructure. The administrative tools on the server 102 allow policy packages to be automatically formed and distributed to each mobile device 106. The gatekeeper 104
20 monitors synchronization and installs the shield software and policy packages on targeted devices. Finally, the shield forms a trusted computing environment by forming a security layer on the mobile operating system to enforce the policies originating from the server 102. The complete system 100 forms a comprehensive, enterprise scale mobile security management system.

25 The system 100 includes components that integrate to external systems. To support a large customer base, multiple platforms are supported for each component. The following sample list identifies illustrative devices and software platforms for integration. At the server 102, the windows2000 operating system, an LDAP of MS Active Directory System (ADS), Critical Path, or iPlanet flat files, and the Explorer version 5.0+ browser. At the
30 gatekeeper 104, compatible operating systems include Win98, WinNT 4.0, Win2000, WinXP, compatible data synchronization software includes HotSync, ActiveSync version 3.1+, server operating system of Win2000, and the network synchronization of ScoutSync

- 8 -

version 3.5+. For the shield, the supported operating systems include PocketPC 2000, PocketPC 2002, and device OS version 3.5+.

5 The server 102 is constructed using enterprise scale server technology, such as federated webservices to provide scalability servers and portability of functions, model-view-controller (MVC) web interface techniques to provide maintainability and speed, and consolidated LDAP Directory (CLD) technology to provide compatibility and reduce installation and administrative costs in existing security infrastructures.

10 The server 102 architecture is integrated through a web service paradigm, as illustrated in FIG. 2. This paradigm is an industry recognized best practice for developing and integrating enterprise web applications. The web service paradigm is a loosely coupled architecture of processes that is flexible, allows additional functions, and allows replacement of servers as well as increased scale through load balancing and additional servers.

15 The core of the web services approach is in the ability to expose or advertise services through a consolidating interface. Referring to FIG 2 many of the key functions of the server 102 such as access control, audit log and security policy management are implemented as individual Java "applications" and advertised or exposed to the internal local area network (LAN) as services. These "applications" operate as web services. Each service can be run as a process or thread on a shared server, on separate servers or in combinations on fewer servers. Scalability and load balancing is achieved by running multiple threads of a service on a single server or on a cluster of servers. Maintenance is simplified by supporting the ability to move services between servers and to replace servers dynamically.

25 The federating web service in FIG. 2 is a proxy type of service that consolidates the internally advertised services and provides the corresponding service to an external user through a hyper-text transfer protocol (HTTP) interface. The federated web service consolidates internal services by proxying the functionality to external users. The location of the services is specified in a service table or configuration file formatted with eXtensible markup language (XML). Service management is an advantage to the federated services approach. Only a single URL needs to be maintained to provide service to a scalable cluster of servers and services. The federating service has the ability to route application calls

- 9 -

dynamically to perform load balancing. Scalability of the federating service is achieved using multiple federating service servers and standard load balancing routers such as Cisco's LocalDirector router.

5 The federating services and external users may be integrated through industry standard scripting protocols XML (eXtensible Markup Language) and SOAP (Simple Object Access Protocol). XML is a markup language similar to HTML for web pages, while SOAP is composed with structures or sentences written in XML. With web services, XML is the alphabet that represents data while SOAP is the grammar that defines the service call similar to a remote function call. Specifically, XML provides a tagged markup
10 language that allows portable data representation between services. SOAP is an industry standard structure of XML tags that define calling sequences, parameter structures and result variables. These protocols are supported over the ubiquitous HTTP communication channels of the web.

As a result, XML/SOAP allows an external application, such as the gatekeeper 104,
15 to request a service as a single federated web service URL, to proxy the result to the actual web service and to provide the result back to the gatekeeper 104. Privacy and authentication of the gatekeeper 104 can be achieved using SSL services by using the standard HTTPS protocol in place of HTTP.

The administrator interface 112 is provided through use of a lightweight HTTP or
20 web interface. Benefits of this configuration includes wide availability of access from anywhere in the LAN, secure usage through SSL protocol, as well as simple delegation of responsibilities and separation of duties through authentication and access control.

The server 102 uses the industry recognized best practice of MVC programming model to implement the graphical user interfaces (GUI) of the administrator console. Model
25 View Controller (MVC) is similar to web service in that it is a method of providing remote function calls. MVC leverages the federating web service to manage resources. However, MVC provides an additional capability to graphically represent the results of the service to provide a web page representation and a GUI.

MVC is the modern evolution of CGI for calling functions from web pages. The
30 CGI approach used a myriad of printf() calls to return HTTP data back to the browser for

- 10 -

display. Servlets are a server side Java application that perform a specific task and that do not have GUI capabilities. The servlets were used to manage flow while JSP managed the HTML formatting. The MVC model separates servlets into logic (or model) servlets and control servlets resulting in the acronym MVC.

5 The server 102 uses MVC to implement the GUI. A view component is used to format and represent GUI to the browser. JSP and HTML are used to implement the view component. A controller component is used to consolidate, delegate and manage control flow and may be implemented with a Java servlet controller using HTTPS with the federated web service. Finally, the controller delegates work to an appropriate model within
10 the server 102. The model may be implemented as a servlet in Java. The models are used to control setting of policies, accessing roles stored in the LDAP and forming policy packages for distribution. The entire GUI including operation and logic is controlled and managed by the MVC framework. The framework is quickly implemented, and is easily modified, expanded and maintained.

15 Simplifying and lowering the total cost of ownership of the mobile security management system is a goal in the design of system 100. A challenge and cost of installation is integration with existing identity data management systems. LDAP is data directory structure that is commonly used to store identity information and security policies to support authentication and authorization systems. It is understandable that customers
20 want to reuse existing LDAP repositories after investing the time and effort to create an LDAP role-based policy system and populate the system with every user in the company. Furthermore, customers may desire future security systems to use the existing LDAP repositories without compromising the integrity of the system by modifying any database schemas.

25 The server 102 uses a consolidated LDAP directory (CLD) technology to address this integration challenge. The server 102 uses a layering approach and places a virtual layer above external and internal LDAP systems to provide a federated view of LDAP repositories. FIG. 3 illustrates this approach.

30 The federation works with three layers. The bottom layer 302 is an adapter layer that is specific to a data store format and converts the store representation to a portable format. The middle layer 304 is a core directory engine that performs on-the-fly mapping to

- 11 -

transform top-level client requests into the context of each repository and results into federated representations. The top level 306 is a front-end listener that converts the directory engine results into proper LDAP format. The result is a powerful method for integrating disparate customer identity data stores into a unified view for simplified server
5 installations.

An access control service provides authentication for administrator logins and for gatekeeper 104 communications. This service interfaces to the LDAP repository of identities and permissions to provide control for system and data access. Administrators are authenticated through a login screen presented by a browser with JSP. The JSP requests
10 authentication with the user name and password through the servlet interface of the federated service. The request is proxied to the access control service for completion. The authentication may be performed with LDAP version 3 operations through the CLD and may alternatively be performed using private key encryption type authentication systems.

The gatekeeper 104 is authenticated using SSL server certificates and realm
15 authentication. An SSL connection is created to provide communications between the server 102 and gatekeeper 104. Initially, the server 102 is authenticated to the gatekeeper 104 through SSL certificate authentication. Next, an SSL channel is constructed for privacy. Finally, a name/password pair (per realm authentication) is passed to through the federated service to the access control service for authentication. Successful match of name
20 and password provides authentication of the gatekeeper 104 to the server 102.

A policy service provides management of the role-based policies as well as creation of the policy files. The policy management service is provided to the administration console and allows definition of the policy values for both roles (or groups) and individual users. Once the policies have been defined for a population of users, the administrator can select to
25 publish the policies. The publication process is the act of forming the secure policy files and automatically pushing the policy files out to the individual shield application 106. An example screen shot of the policy management service is shown in FIG. 4.

The system 100 provides a key management service that generates and archives password keys for encryption operations in the shield 106. Symmetric encryption keys are
30 generated using techniques such as industry standard X9.17. Symmetric keys are used to protect data on the mobile device. These data encryption keys are generated uniquely for

- 12 -

each mobile device and are stored on both the server 102 and the shield 106 to enable data protection while allowing secure data recovery with administrator intervention.

Asymmetric or public/private key pairs are created with the elliptical curve cryptography (ECC) key algorithm and are used to encrypt policy files and audit log files. Separate key
5 pairs are generated for each device and individually for the policy files and the audit logs. The key pairs are stored on the server 102 for secure data recovery through administrator intervention. The private audit log key is stored on the shield 106 to encrypt audit log information to support transference off of the device. The public policy file key is stored on
10 the shield 106 to allow the software to authenticate and extract the policy items from the encrypted policy files. The opposite keys are used on the server 102 to decrypt audit log files and to encrypt policy files in support of the device.

A policy file is a collection of policy items combined into a single data package and formatted with XML. The policy file is transferred from the server 102 to the mobile device for security configuration and enforcement. The policy file is actually a number of files;
15 one main index file and another for each category of policies defined. Each category file contains a series of policies that define the permissions and behavior of the shield 106. Three items define each policy: category, key and value name. A key may have zero or more name/value pairs associated with it.

The server 102 encodes the policy file with ECC asymmetric encryption and
20 transfers the file to the mobile device. The key pair corresponding to the policy management of an individual mobile device is created and managed by the server 102. The private key is stored on the server 102 and used to encrypt the policy file. The public key is stored on the mobile device by the shield application 106. The policy file is transferred to the mobile device during synchronization, after authentication is performed. The public key
25 stored in the shield is used to open the policy file. The public key is passed to the shield application in a secure manner. This method of policy file management provides private transfer to specific shield deployments, provides policy authentication and management, and is tamper resistant to enable consistent policy enforcement.

Policy data falls into the following categories: I/O, storage, applications, and
30 authentication.

- 13 -

The following tables specify sample types of policy data:

Permission Policies

Name	ID (Category)	Value	Type	ReadOnly	Affects
IR_Enable	I/O	True/False	Boolean	True	Palm: Exchange Manager, IR Library CE:
TCP/IP_Enable	I/O	True/False	Boolean	True	Palm: Network, INet Library CE:
NetBios_Enable	I/O	True/False	Boolean	True	Palm: N/A CE:
SyncAuthenticated_Required	I/O	True/False	Boolean	True	Palm: CE:
VolumeMount_Enable	Storage	True/False	Boolean	True	Palm: DB, VFS Manager (File system mounting) CE:
DateBook_Enable	Applications	True/False	Boolean	True	Palm: DateBook CE: Calendar
AddressBook_Enable	Applications	True/False	Boolean	True	Palm: AddressBook CE: Contacts
Todo_Enable	Applications	True/False	Boolean	True	Palm: Todo CE: Tasks
Memo_Enable	Applications	True/False	Boolean	True	Palm: Memo CE: Notes
Expense_Enable	Applications	True/False	Boolean	True	Palm: Expense CE: Money
Mail_Enable	Applications	True/False	Boolean	True	Palm: Mail CE: Inbox
Prefs_Enable	Applications	True/False	Boolean	True	Palm: Prefs CE: Settings
Security_Enable	Applications	True/False	Boolean	True	Palm: Security CE: N/A
FileExplorer_Enable	Applications	True/False	Boolean	True	Palm: N/A CE: File Explorer
InternetExplorer_Enable	Applications	True/False	Boolean	True	Palm: N/A CE: Internet Explorer
PocketWord_Enable	Applications	True/False	Boolean	True	Palm: N/A CE: Pocket Word
PocketExcel_Enable	Applications	True/False	Boolean	True	Palm: N/A CE: Pocket Excel
WindowsMedia_Enable	Applications	True/False	Boolean	True	Palm: N/A CE: Windows Media
Reader_Enable	Applications	True/False	Boolean	True	Palm: N/A CE: MS Reader

- 14 -

Rule Policies

Name	ID (Category)	Value	Type	ReadOnly	Description
PINEnable	Authentication	True/False	Boolean	True	Whether to include PIN authentication in the password hierarchy
PasswordEnable	Authentication	True/False	Boolean	True	Whether to include Password authentication in the password hierarchy
PassPhraseEnable	Authentication	True/False	Boolean	True	Whether to include Pass Phrase authentication in the password hierarchy
ManAuthEnable	Authentication	True/False	Boolean	True	Whether to include PIN authentication in the password hierarchy
PasswordNumChars	Authentication	8-16 characters	Number	True	
PasswordAlphasRequired	Authentication	True/False	Boolean	True	
PasswordNumericRequired	Authentication	True/False	Boolean	True	
PasswordSpecialRequired	Authentication	True/False	Boolean	True	
PasswordUpperCaseRequired	Authentication	True/False	Boolean	True	
PassPhraseNumChars	Authentication	16-32 characters	Number	True	
NumPINAttempts	Authentication	1-4	Number	True	
NumPasswordAttempts	Authentication	1-4	Number	True	
NumPassPhraseAttempts	Authentication	1-4	Number	True	
NumManAuthAttempts	Authentication	1-4	Number	True	
UserSessionTimeout	Authentication	1-120 minutes	Number	True	Inactive time till user must re-authenticate
PowerOffTimeoutEnable	Authentication	True/False	Boolean	True	Requires user to re-authenticate after device has been turned off
AuthDataExpires	Authentication	1-365 days	Number	True	Time till user must reset authentication information

- 5 The system 100 also provides a logging service. Each event defined in the logging service has a corresponding registered policy. This will enable the administrator to control which events are written to the audit logs.

A log file is a record of events that is generated by the shield software 106. The shield 106 initially stores the file locally. During synchronization, the log file is automatically transferred through the gatekeeper 104 to the server 102. After synchronization, the shield 106 initializes a new file. The server 102 automatically appends
5 the new log to the previous synchronized logs to form a consolidated log. Server access to the log is provided through an open database connectivity (ODBC) interface to allow custom or third party reporting tools to be used.

The log files are locally protected against tampering with elliptical curve algorithm asymmetric encryption. The key pair corresponding to the on-device audit logs of an
10 individual mobile device is created and managed by the server 102. The public key is stored on the server and used to open the audit log after synchronization. The private key is stored on the mobile device by the shield application 106 and is used to add new event records to the event log. An initial value or seed is transferred from the server 102 to the mobile device in a secure mode during synchronization. This seed is updated through the
15 encryption process as records are added to the audit log. This forms an encryption thread through the event recording process. Additionally, a time stamp from the server is used to initialize the file. The initial time stamp combined with periodic time events in the file allows monitoring of the mobile device clock to prevent time tampering. This method of on-device audit logging provides a secure and private audit log that is easily maintained by
20 the server, detects gaps in time and in logging sequence, and is tamper resistant to provide a robust, on-device monitoring system.

Referring to FIG. 5, an illustrative functional diagram for the gatekeeper 104 is disclosed. The gatekeeper 104 includes a persistence network 502, a server interface 504, a client interface 506, an encryption module 508, an audit module 510, a synchronization
25 plug-in module 512, and an authentication module 514. The gatekeeper 104 communicates with the server 102 using HTTPS and XML over the interface 114 and communicates with the mobile device 106 via the synchronization interface 116, such as with SKID3 and XML.

Referring to FIG. 6, an illustrative block diagram for the shield application 106 on a representative mobile device is shown. The shield application 106 includes a
30 communication module 602, a storage area 604, a user interface 606, encryption module 608, audit and log module 610, policy rule engine 612, and system interface 614.

- 16 -

The communication module 602 communicates with external systems such as the gatekeeper. The communication module receives application data, personal information data (PIM), new key materials and policy data from the gatekeeper 104. The application data and PIM data are stored in the general device storage 604. This general storage may be encrypted by the encryption module 608. The new key materials are decrypted by the encryption module 608 and stored in the key data store in 608. The policy data is decrypted by the encryption module 608 and stored in the rules engine store 612.

The user interface module 606 communicates with the device user to authenticate the user and unlock the device. The user interface may retrieve any of a plurality of data such as PIN (personal identification number), password, answer to a question or response to a challenge. Authentication is tested by decrypting data in the encryption module 608 with the retrieved data. Upon successful decryption, authentication is approved. A similar authentication test can be hashing the retrieved information and comparing the information with data stored in the encryption module 608. The user interface 606 also displays alerts such as sync in progress or device is locked.

The audit log module 610 stores system event data, such as successful or unsuccessful authentication attempts, in the encrypted log store of 610. The events are encrypted by the encryption module 608 and transferred to the gatekeeper 104 by the communications module 602.

The rules engine 612 provides authorization based on the policy data in its store. The policies are retrieved from the communications module 602 during connectivity to the gatekeeper 104 and enforces the policies at all times whether connected or disconnected. The policy data is retrieved from the gatekeeper 104 by the communications module 602 in an encrypted form. The encryption module 608 decrypts the data prior to storage on the policy data store in 612. The rules engine receives authorization requests from a plurality of modules and responds with authorization based on the policies stored within. The policy engine can signal the user interface 606 to lock the device if a user action is denied or an unauthorized event occurs.

The rules engine 612 can enforce which devices to which the communications module 602 can communicate. The policy database may contain a list of devices that can be communicated with, a list of devices that cannot be communicated with or a list of keys

- 17 -

stored in the encryption module 608 with which can be used to authenticate devices. If an external device is included in the list of approved devices to communicate with, the rules engine 612 grants authorization to the communication module 602 to communicate with the external device. If an external device is included in the list of disapproved devices to communicate with, the rules engine denies authorization to the communications module 602 to communicate with the external device. If a plurality of keys is listed in the policy database, then the rules engine can request the encryption module 608 to perform a challenge response with an external device to determine authentication. If the authentication is successful, the rules engine 612 may grant authorization to the communications module 602 to communicate with the external device. Otherwise, the rules engine may deny authorization to the communications module 602 to communicate with an external device.

The rules engine 612 and user interface 606 can enforce a personal or business mode. The user interface 606 can authenticate a user in either personal mode or business mode. The mode is determined from the data retrieved from the user interface indicating which mode the user requests. The rules engine authorizes what actions can be performed in each mode. Additionally, the rules engine can authorize which data items in the general data store 604 can be displayed by the user interface 606, can be accessed by a plurality of modules, or can be transferred by the communications module 602.

The system interface 614 communicates using intercepted events with an external event handler, such as OS event handler 630 and communicates, by intercepting system calls, with external operating systems, such as OS 632. The system interface 614 authorizes system calls and events by intercepting the system calls and events, requesting authorization from the policy engine 612, and granting or denying the system calls or events.

Referring to FIG. 7, a method of distributing security software from the server 102 to a mobile computing device is illustrated. First, gatekeeper software 104, including network scripts, policies, and key materials, is installed from the server 102 to a desktop computer, or other suitable gatekeeper platform, at 702. When the mobile computing device connects to the gatekeeper 104 during a data synchronization event, the shield software application 106, i.e., security software for the mobile computing device, is installed from the gatekeeper 104 to the mobile computing device, at 704. The gatekeeper 104 requests a one-

- 18 -

time use password from the server 102, at 706. The server 102 emails the one-time use password to the user of the mobile computing device, at 708. The mobile computing device user can then use the one-time password to complete installation of the security shield application.

5 At this point, the root key for the key pack is decrypted using the one-time password, allowing access for the user to enter a new password, a personal identification number (PIN), and a password phrase, and optionally other user identification information, such as the user's mothers maiden name or pet name, at 710. The root key is then encrypted using each of the above user information entries, including the new password, the PIN, the phrase,
10 and the user's answers to key questions, at 712. The above process of having a mobile computing device user initiate security operations may be accomplished using user interface software, such as by providing prompting screens to facilitate entry of the user information.

 Referring to FIG. 8, a method for distributing a new or modified security policy information to a mobile device is illustrated. At 802, a policy change or a new policy is
15 added by an administrator connected to the server 102 and the server 102, in response to the administrator request, creates a new policy package. The policy package contains the new or modified policy. To distribute the new policy package to the mobile computing device, the server 102 authenticates a connection with the gatekeeper 104 and upon successful authentication, sends the policy package to the gatekeeper 104, at 804.

20 The authentication between the device and gatekeeper may be implemented using a mutual challenge-response algorithm that uses a shared key as a shared secret for determining authentication. The process is a two step challenge-response that may begin with either the device or the gatekeeper. Consider an example where the device initiates the challenge. A random number is calculated by the device and sent to the gatekeeper as a
25 challenge. The gatekeeper and the device compute the expected answer in parallel and in private. The answer can be calculated by any one way function of the shared key and challenge value. For example, the key can be appended to the challenge and input to a hashing algorithm such as MD5 for calculation of a message digest. The gatekeeper responds to the device by returning the computed response. If the response matches the
30 expected answer, the first step or phase of the mutual challenge response is completed successfully and the gatekeeper calculates a random number for the return challenge. The

- 19 -

next step repeats the first step but in reverse roles. The gatekeeper challenges the device with the random number. Each computes the expected response privately. The device returns the calculated value as the response. If the values match, then the second phase is passed. If either phase fails, then the entire process is failed. Both steps must pass in order
5 to be successful.

The gatekeeper 104 receives the policy package and waits for the next data synchronization communication with the mobile computing device, at 806. When the mobile computing device initiates data synchronization, at 808, the gatekeeper 104 authenticates the mobile computing device. The gatekeeper 104, upon successful
10 authentication of the mobile computing device, pushes the policy package to the mobile computing device, at 810. The mobile computing device then decrypts the policies and activates the new or modified security policies, at 812. If authentication of either the gatekeeper 104, from the server 102, or the mobile computing device from the gatekeeper 104 fails, then the updated policy package is not distributed and the administrator may be
15 notified.

Referring to FIG. 9, a method where a mobile computing device requests policy updates is shown. In this method, the mobile computing device initiates synchronization with the gatekeeper 104, at 902. The connections between the mobile computing device and the gatekeeper 104 and between the gatekeeper 104 and the server 102 is authenticated, at
20 904. After successful authentication, the gatekeeper 104 checks the server 102 for new policies, at 906. The server 102 creates a policy package based on new and modified policies and sends the policy package to the gatekeeper 104, at 908. The gatekeeper 104 installs the new and/or modified policies onto the mobile computing device, at 910. At the mobile computing device, the security application (i.e., the shield application 106) decrypts
25 the policy package and activates the new or modified policies on the mobile computing device, at 912.

Referring to FIG. 10, the key materials and the use of the key materials to provide for security applications is illustrated. A sample key 1002 with a plurality of fields, including the software field 1004, the date field 1006, the owner field 1008, the length field
30 1010, the key ID 1012, and a cyclic redundancy check field 1014 is shown. Also shown is a root key 1016. The root key 1016 is encrypted using a user's PIN 1018, password 1020,

- 20 -

phrase 1022, and challenge 1024 (i.e., answer to key questions). The root key 1016 is then used to encrypt a set of operating keys 1036 referred to as a key ring. The operating keys 1036 include a data key 1038, a policy key 1040, a log key 1042, a gatekeeper authentication element 1044, an updating key 1046, and a heartbeat log key 1048. The data
5 key 1038 is linked to unlock data storage 1054 within the mobile computing device. The policy key 1040 is used to access policies 1050 and the log key 1042 is used to access log files 1052 that track historical mobile device user activities.

The log key is the public key used with a public key encryption algorithm to encrypt data into the event log that tracks historical mobile device user activities.

10 The gatekeeper authentication key is used by the device in a challenge-response algorithm to prove its identity with the gatekeeper. The key is used as a shared secret to compute the response to a challenge. The update key is used to decrypt new keys sent by the server to the device as replacements to any of the plurality of keys. The heartbeat key is used similar to the gatekeeper authentication key for authenticating between the device and
15 the server. The challenge and response between the device and server is used as a heartbeat to monitor the device.

Also illustrated, is the policy package that includes the policy pack 1056, encrypted using the policy key, and a key material pack 1058 that has been encrypted using the root key 1016. The policy package may be pushed from the server 102, via the gatekeeper 104,
20 to the mobile computing device 106 or may be pulled from the mobile computing device from the server 102, via the gatekeeper 104. Methods for distributing the policy package were described above with respect to FIGs. 8 and 9.

The above disclosed subject matter is to be considered illustrative and the appended claims are intended to cover all such modifications and other embodiments which fall within
25 the true spirit and scope of the present invention. Thus, to the maximum extent allowed by law, the scope of the present invention is to be determined by the broadest permissible interpretation of the following claims and their equivalents, and shall not be restricted or limited by the foregoing detailed description.

- 21 -

WHAT IS CLAIMED IS

1. A server module deployed on a server that is connected to a wireless network access node, comprising:
 - a database containing user information for multiple wireless devices, each element in the database attributable to at least one authorized wireless device and containing at least one type of data file from the group consisting of: (i) wireless connectivity permissions, (ii) authorized wireless device identification, and (iii) authorized network access node information.
2. A computer memory comprising:
 - a plurality of operating keys for use in connection with security features of a mobile computing device; and
 - a root key, the root key to encrypt the plurality of operating keys.
3. A method of enforcing security policies at a mobile computing device, the method comprising:
 - receiving a policy at the mobile computing device, the policy including at least one device use limitation;
 - enforcing the policy at the mobile computing device by disallowing a user of the mobile computing device from engaging in the use precluded by the use limitation.
4. A security method comprising:
 - receiving a password from a user of a mobile computing device;
 - deriving a security code from the password by applying a non-linear function; and
 - encrypting the security code using the password as an encryption key.

- 22 -

5. A method of selectively providing a mobile computing device with access to a software application on a server, the method comprising:
receiving a request to access the software application from the mobile computing device;
5 determining whether to grant access to the software application by checking whether the mobile computing device has an installed security program.
6. A method of updating policies and key materials, the method comprising:
providing a shared encryption key that is shared by a server and a client module;
encrypting data on the client using the shared encryption key;
10 authenticating a user of a mobile computing device by receiving a password, the client resident at the mobile computing device;
decrypting the shared key using the password;
using the shared key to decrypt updated policies and key materials; and
replacing policies and key materials at the mobile computing device with the
15 updated and decrypted policies and key materials.
7. A wireless security system, comprising:
a client module deployed on a wireless device;
a network module selectively coupled to the client module during synchronization;
and
20 a server module coupled to the network module,
wherein the client module is adapted to authenticate use of a wireless computing device independent of the network module and the server module.

- 23 -

8. A method of installing a security software application from a network module to a mobile computing device, the method comprising:

- 5 providing a network module, the network module including security policies and key material, the security policies and key material communicated to the network module from a server;
- when the mobile device is synchronizing with the network module, initiating installation of a security software program onto the mobile security device;
- requesting a one-time password;
- receiving the one-time password at the mobile computing device; and
- 10 using the one-time password to decrypt a root key associated with the key materials.

9. A method of distributing security policy information from a server to a mobile computing device, the method comprising:

- authenticating a connection between the server and a gatekeeper;
- sending a policy package to the gatekeeper;
- 15 initiating data synchronization between the mobile computing device and the gatekeeper;
- authenticating the mobile computing device; and
- sending the policy package from the gatekeeper to the mobile computing device.

10. A client module deployed on a wireless device, comprising:

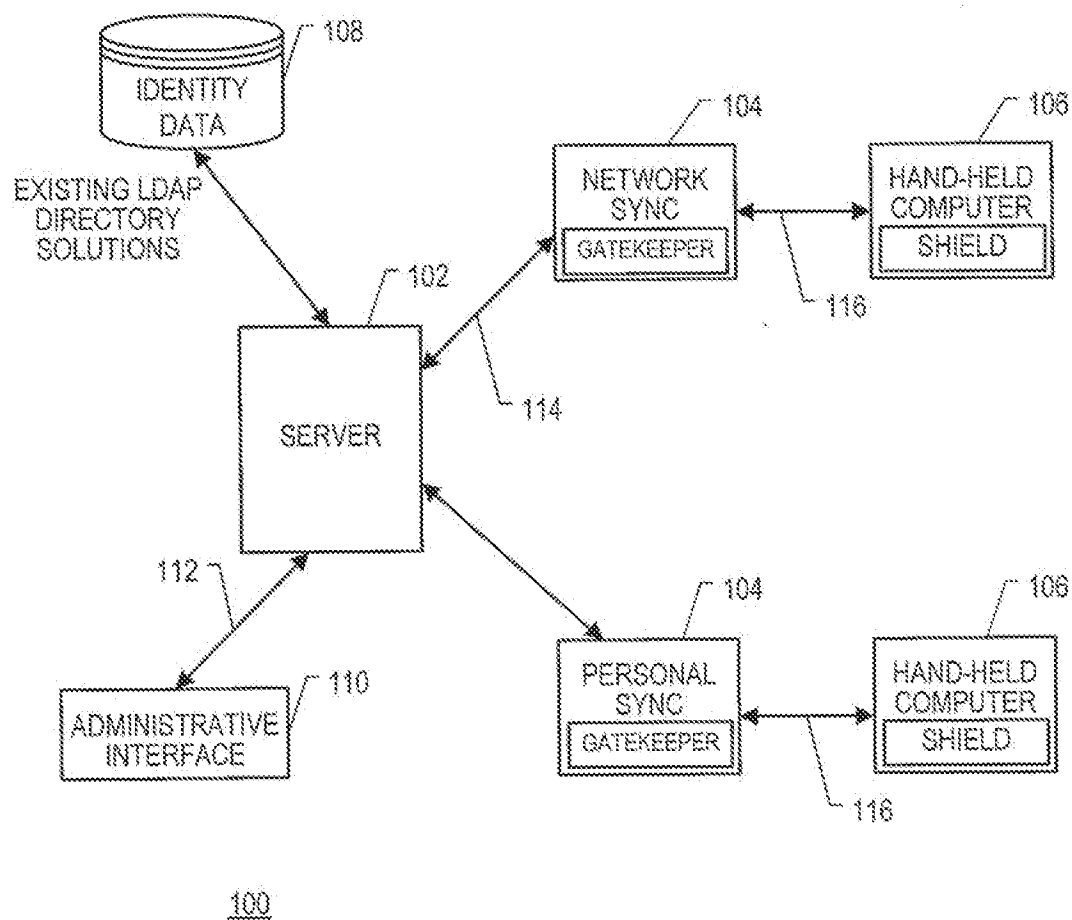
- 20 a policy database including a list of authorized devices to which the wireless device may communicate.

11. A client module deployed on a wireless device, comprising:

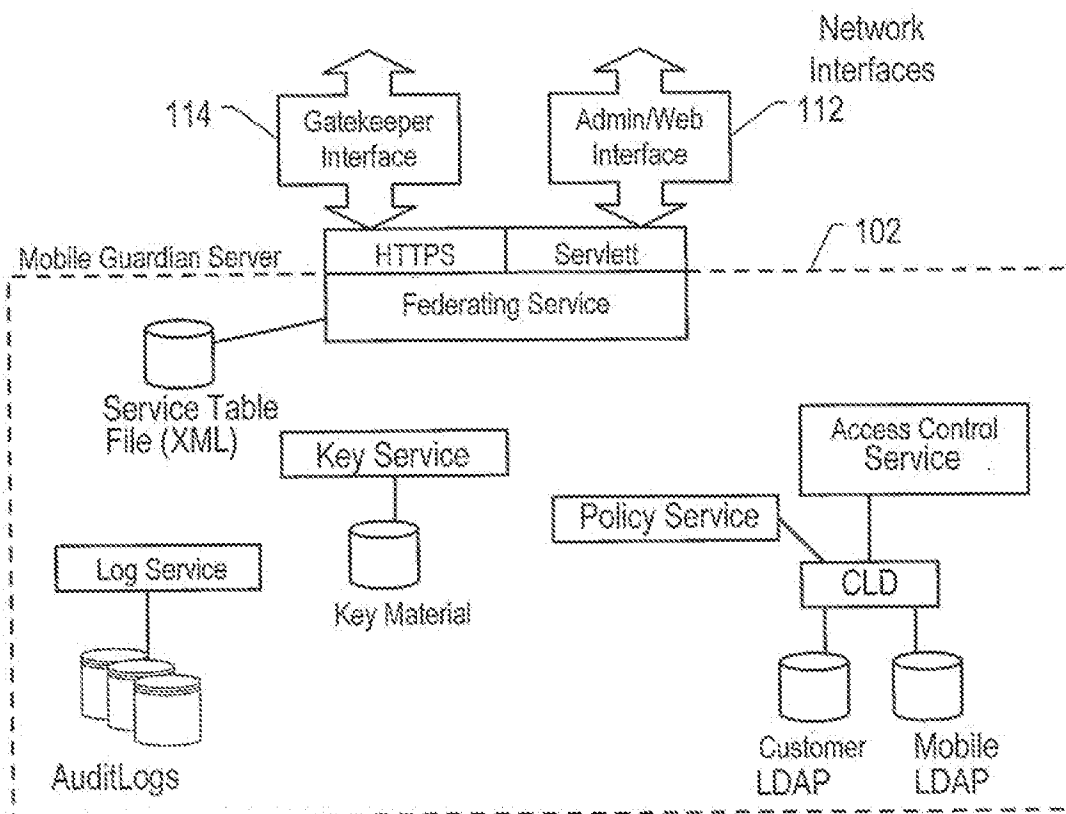
- a policy database containing at least two user profiles on the wireless device.

12. A client module deployed on a wireless device, comprising:
a policy database including rules related to wireless connectivity permissions; and
an intelligent agent for enforcing the policy database rules.
13. A client module deployed on a wireless device, comprising:
5 a policy database; and
an agent responsive to the policy database, the agent configured to monitor
unauthorized use of the wireless device.
14. A client module deployed on a wireless device, comprising:
a policy database including at least one type of data file from the group consisting
10 of: (i) multiple profile data, (ii) connectivity permissions, (iii) authorized
wireless device identification, and (iv) authorized network access node
information;
an intelligent agent for enforcing rules of the policy database; and
an activity log containing wireless connectivity history information.
15. A network module deployed at a wireless network access node, comprising:
a policy database including a list of authorized wireless mobile devices; and
an agent for enforcing rules of the policy database.

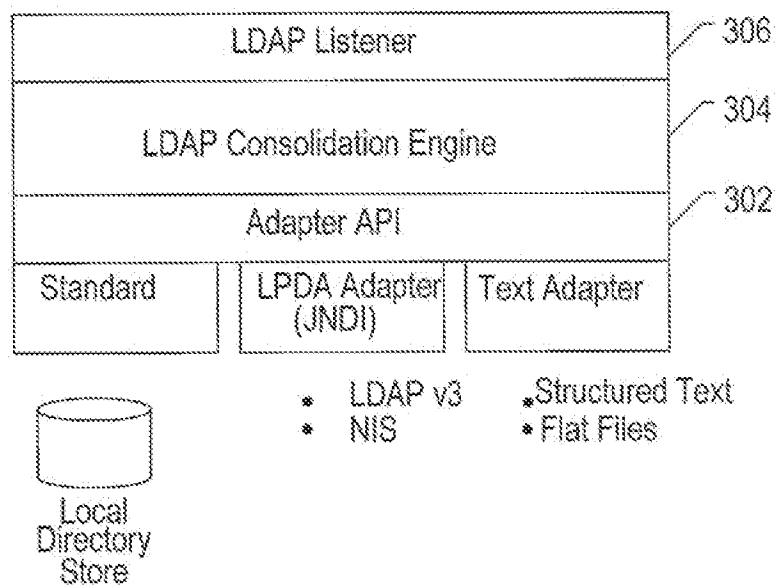
1/10

**FIG. 1**

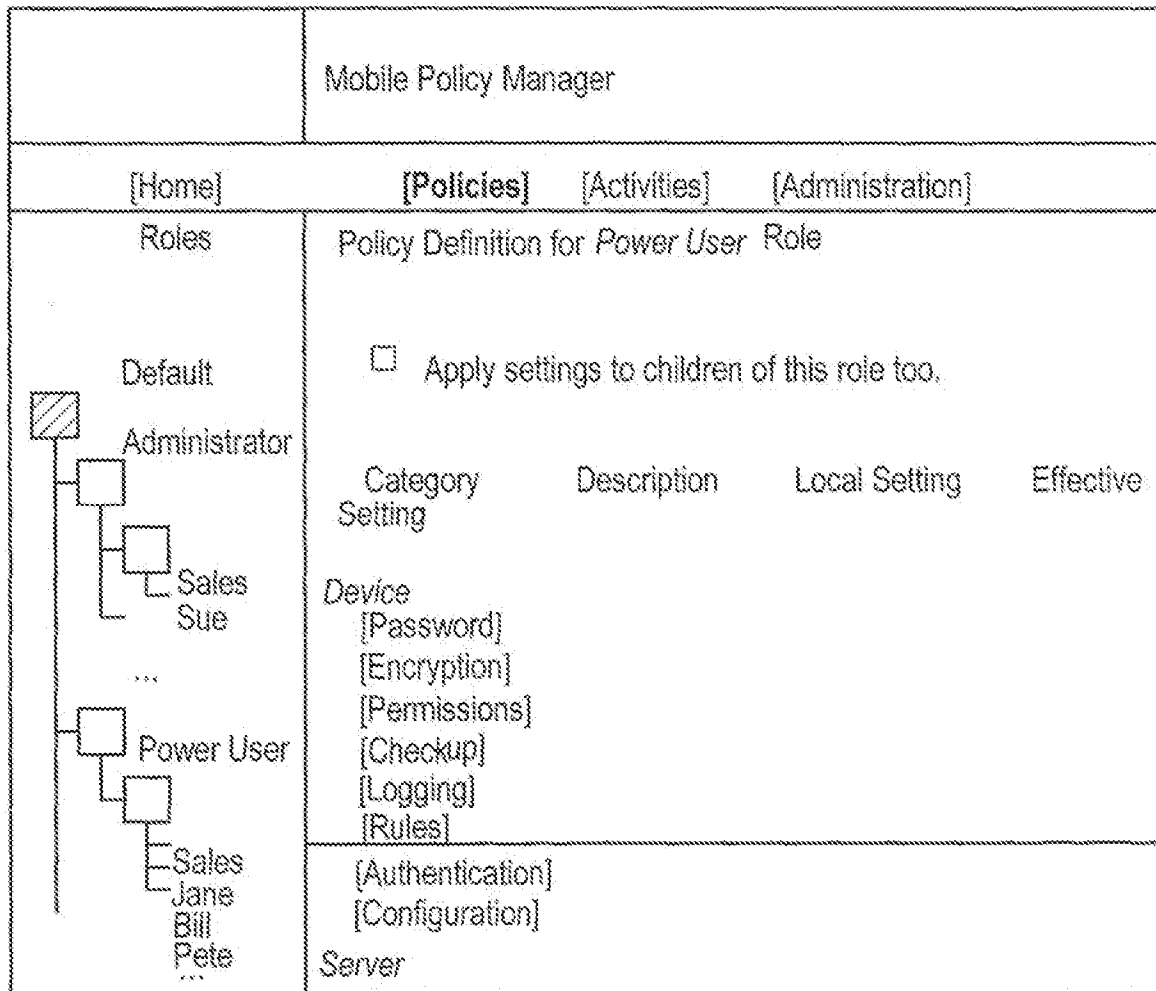
2/10

**FIG. 2**

3/10

**FIG. 3**

4/10

**FIG. 4**

5/10

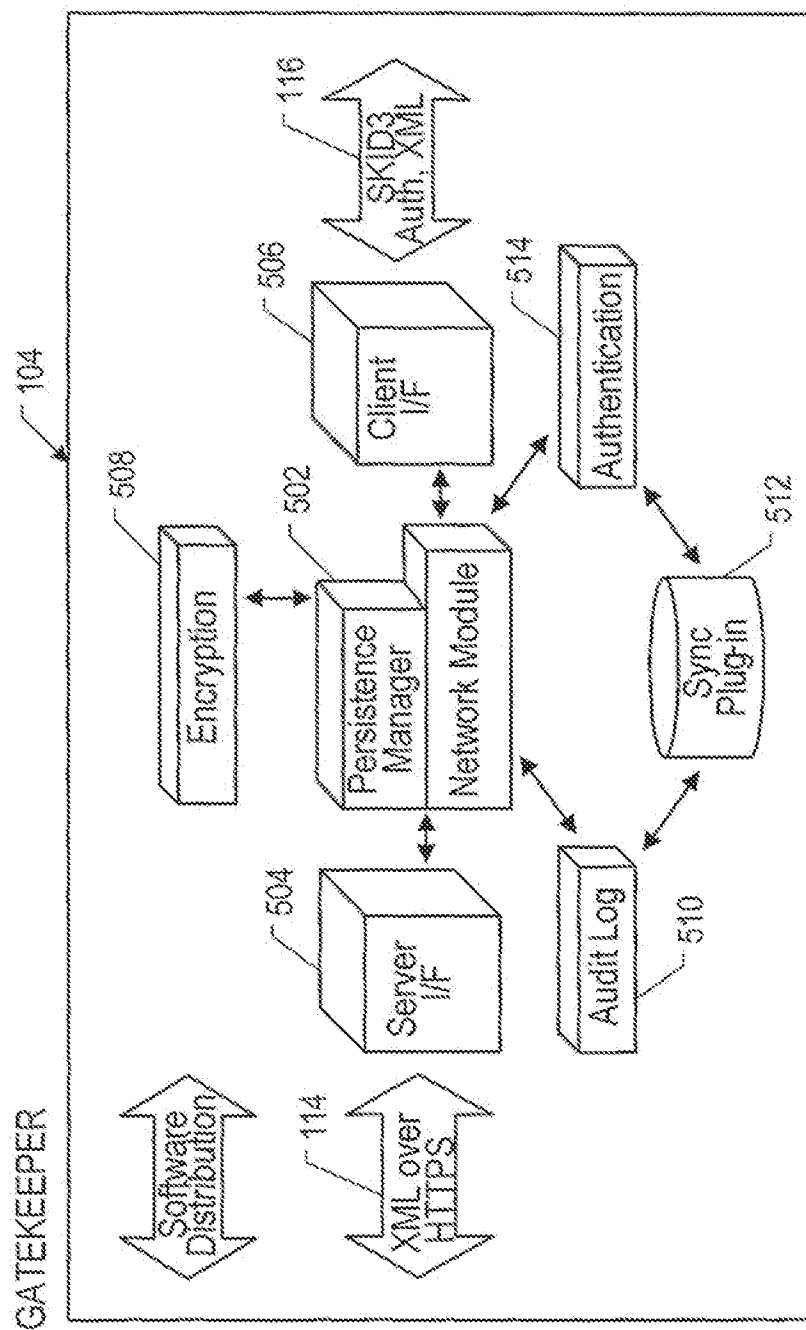
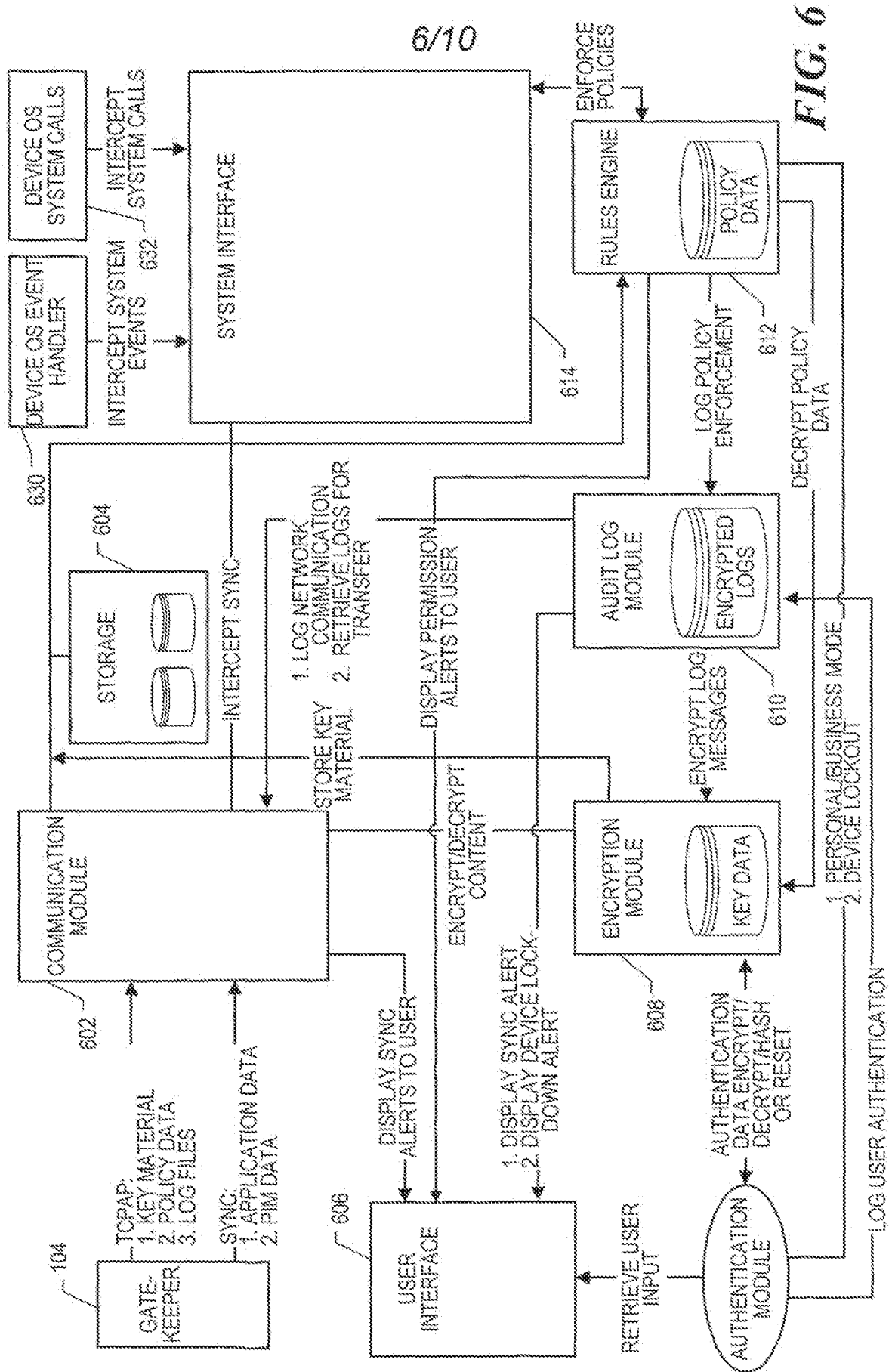
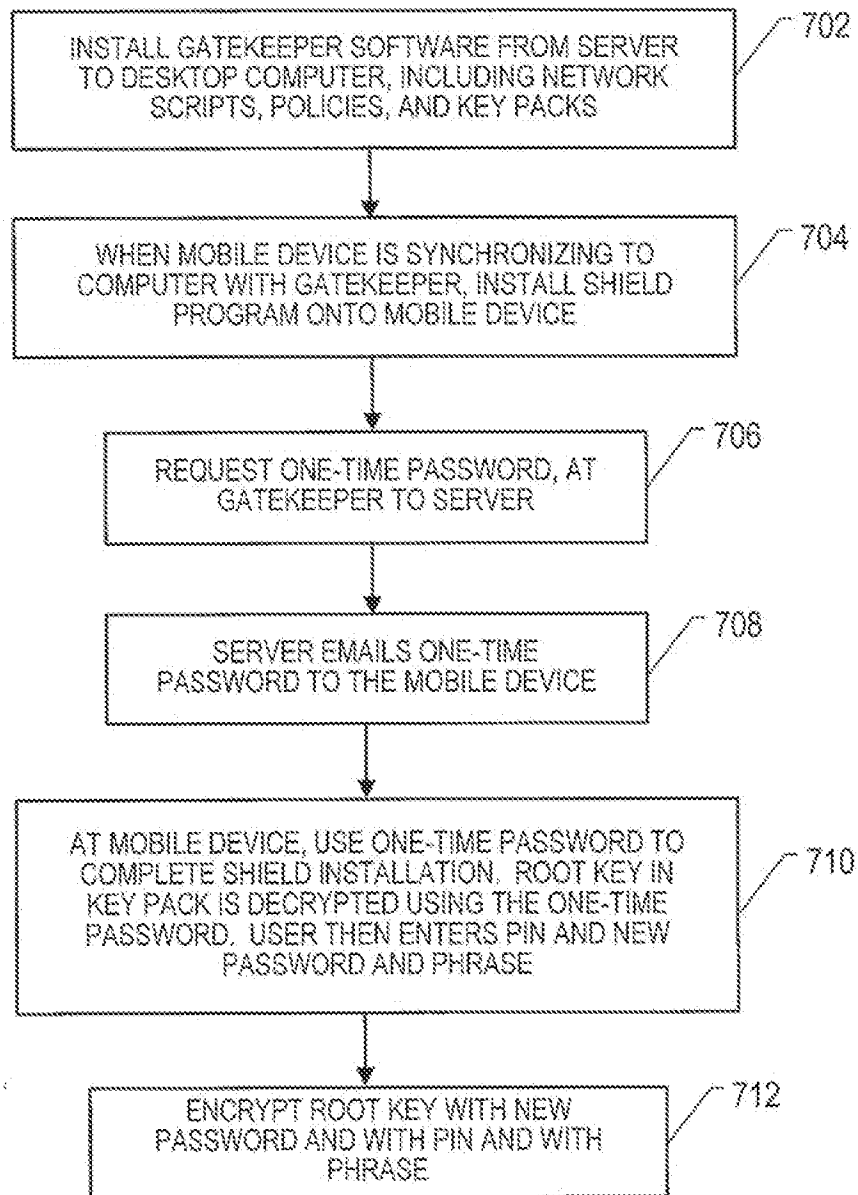


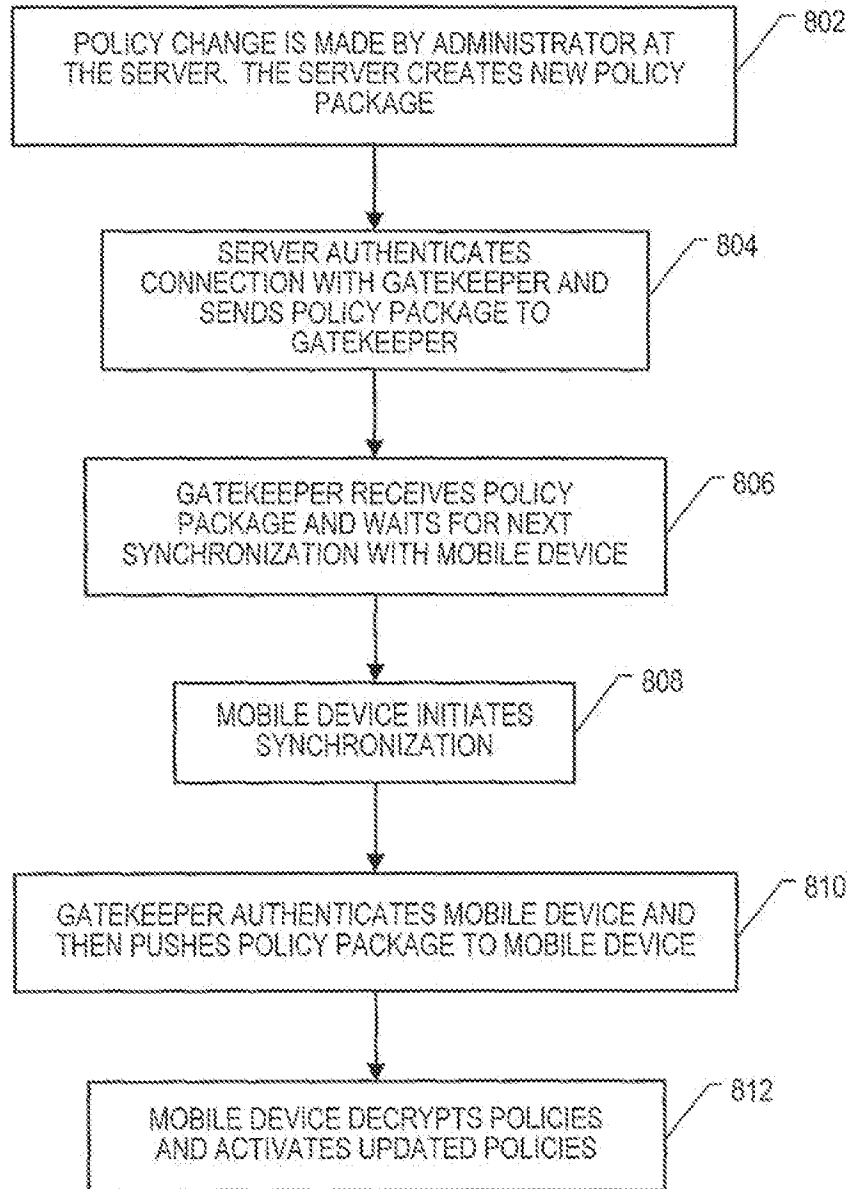
FIG. 5



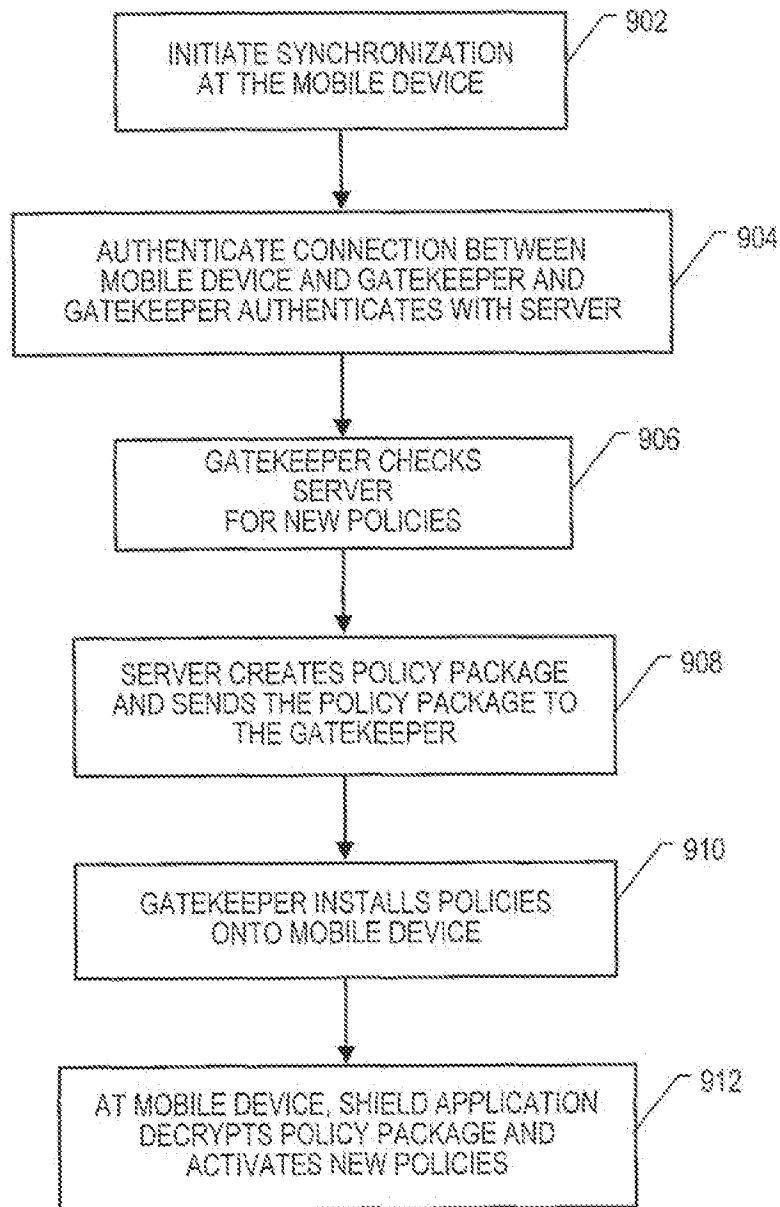
7/10

**FIG. 7**

8/10

**FIG. 8**

9/10

**FIG. 9**

10/10

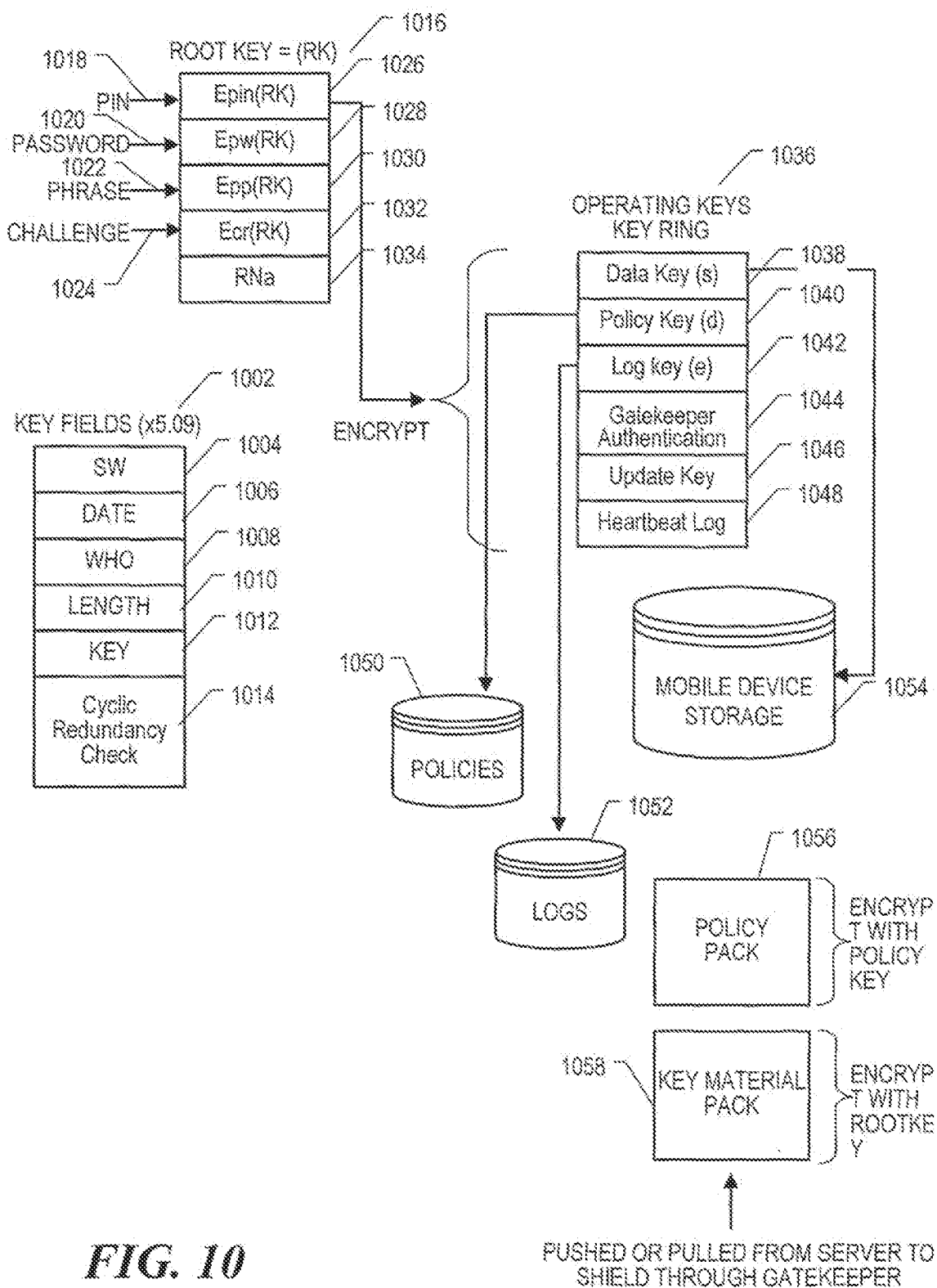


FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/29347

A. CLASSIFICATION OF SUBJECT MATTER

IPC(Cl) : H04L 9/00, 9/32

US CL : 713/150, 200-202; 380/255, 270, 277, 278, 279, 281, 283, 284

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/150, 200-202; 380/255, 270, 277, 278, 279, 281, 283, 284

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,236,892 B1 (VEERASAMY et al) 22 May 2001, see abstract, col. 2, lines 4-36, col. 5, lines 14-40, col. 8, lines 19-53, col. 9, lines 23-46, col. 11, lines 5-11	1,3,5,9-15
X	US 5,850,444 A (RUNE) 15 December 1998, see abstract, col. 3, lines 12-50, col. 4, lines 16-38, col. 5, lines 54-61	2,8
X	US 6,178,506 B1 (QUICK, JR.) 23 January 2001, see col. 2, lines 46-60, col. 4, line 45- col. 5, line 8, col. 6, lines 11-40	4,6

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

04 December 2003 (04.12.2003)

Date of mailing of the international search report
23 DEC 2003

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Facsimile No. (703)305-3230

Authorized official

Nyaz Shmida
Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US03/29347

Continuation of B. FIELDS SEARCHED Item 3:

BRS TEXT SEARCH (files: USPAT, DERWENT, JPO, EPO, IBM TDB, US PGFUB)

search terms: wireless, cell, cellular, policy, net, key, encrypt, encrypting, password, authentic, authenticate, authentication, authenticating, authenticated, authorize, authorizing, authorization, authorized

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
10 September 2004 (10.09.2004)

PCT

(10) International Publication Number
WO 2004/077797 A2

(51) International Patent Classification⁷: **H04M**
(21) International Application Number:
PCT/US2004/006252
(22) International Filing Date: 23 February 2004 (23.02.2004)
(25) Filing Language: English
(26) Publication Language: English
(30) Priority Data:
606449,907 25 February 2003 (25.02.2003) US

(71) Applicant (for all designated States except US): **BOSTON COMMUNICATIONS GROUP, INC.** [US/US]; 100 Sylvan Road, Suite 100, Woburn, MA 01801 (US).

(72) Inventors: **ERSKINE, Thomas**, 15 Summit Road, Marblehead, MA 01845 (US); **SONBERG, Kenneth, W.**, 6 Greyhinch Road, Andover, MA 01810 (US); **RUDISILL, Luther**, 6804 Poon Drive, Parker, TX 75002 (US).

(74) Agents: **LEBOVICI, Victor, B.** et al.; Weingarten, Schurigin, Gagnebin & Lebovici, LLP, Ten Post Office Square, Boston, MA 02109 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GR, GU, HD, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NL, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, EG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), GAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TO).

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GR, GU, HD, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NL, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, EG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), GAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designation US

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: **METHOD AND SYSTEM FOR PROVIDING SUPERVISORY CONTROL OVER WIRELESS PHONE USAGE**

(57) Abstract: A system for controlling wireless phone usage enables a supervisor to establish user profiles for supervised users of wireless phones across a range of parameters which are stored in a user profile database. Such parameters may include one or more locations at which use of the wireless phone is restricted or permitted. In addition, restrictions on phone use may be provided based upon total phone usage within a specified control period, time periods, dates or days of the week during which phone use is restricted or permitted. One or more lists including numbers that are always-accessible may be provided and one or more lists including numbers that are never-accessible may also be provided. In the event a call does not satisfy predefined criteria, the call is blocked. Predetermined messages may be played to the called or calling party as applicable when a call is blocked. Boolean combinations of restrictions and permissive use criteria for the wireless phone may be specified to provide for flexibility when establishing use criteria for the wireless phone.

WO 2004/077797 A2

TITLE OF THE INVENTION
METHOD AND SYSTEM FOR PROVIDING SUPERVISORY
CONTROL OVER WIRELESS PHONE USAGE

5 CROSS REFERENCE TO RELATED APPLICATIONS

This application claims priority under 35 USC §119(e) to provisional application serial number 60/449,907, entitled "METHOD AND SYSTEM FOR EXERCISING SUPERVISORY CONTROL OVER WIRELESS PHONE USAGE", filed February 25, 2003.

10

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR
DEVELOPMENT

N/A

15

BACKGROUND OF THE INVENTION

The present invention generally relates to wireless communication systems and more specifically to a method and system for providing supervisory control over wireless phone usage.

20

Wireless phones are widely used in this country. Wireless phone service providers typically allow a wireless phone subscriber to place calls at any time. For reasons of safety and convenience, more and more parents are inclined to have their children of school age carry wireless phones to make it easier for their children to contact them and vice versa. It has also been observed, however, that many children that are provided wireless phones tend to spend inordinate amounts of time on calls to friends during the school day and late into the evenings, and that the availability of wireless phones can present a distraction during the school day. Presently available wireless phone systems provide no way to adequately

25

30

provide supervisory control of wireless phone usage by others, e.g. children.

Accordingly, it would be desirable to have a method and system by which supervisory control may be exercised over wireless phone usage. It would further be desirable to be able to establish a user profile for wireless phone service on a user by user basis without intervention by the telephone service provider. Moreover, it would be desirable to be able to have the ability to allow a supervisor to modify the user profile as circumstances warrant without requiring human intervention by the telephone service provider so as to allow a supervisor to readily change the nature of the wireless service available to supervised individuals.

BRIEF SUMMARY OF THE INVENTION

In accordance with the present invention, a method and system for exercising supervisory control over wireless phone usage is disclosed. The disclosed system allows a Supervisor, such as a parent or manager, to establish individual profiles for supervised Users of respective wireless phones across a range of parameters. For example, a parent may establish user profiles for each child that is to be provided a wireless phone. The user profiles allow the use of the respective phones by the child subject to controls on incoming and/or outgoing calls as specified by the Supervisor. For example, the disclosed system allows the Supervisor to limit the total phone usage time within a specified control period, such as a week or a month, to a predetermined number of minutes and, to prevent incoming or outgoing calls during specified periods, such as school hours, except from predetermined numbers (always accessible numbers) specified by the Supervisor. Restrictions on phone usage may also be defined with regard to incoming or outgoing calls while the phone is at or near defined geographic

locations. For example, calls may be blocked while the phone is within the grounds of a school attended by the user. Additionally, a location restriction may be employed in conjunction with other restrictions on phone use and capabilities described herein. For example, calls may be restricted if the wireless phone is at a prescribed geographic location and the time is within a time period specified by the Supervisor. More specifically, the decision whether to block or permit a call may be made as a Boolean function of any of the applicable restrictive or permissive criteria applicable to phone usage herein described. The location of the wireless phone may be obtained using cell sector identifiers alone or in combination with signal strength information, a global positioning system receiver disposed within the wireless phone or any other suitable technique for resolving the geographic location of the wireless phone.

In one embodiment, calls to predetermined numbers specified by the Supervisor, and time spent on calls from one or more numbers specified by the Supervisor, are not counted toward the total number of minutes permitted during the specified control period.

When a supervised user attempts to make a call during a period in which use is prohibited, a message may be played to the user indicating that the call will not go through at the specified time. Similarly, when a call is placed to a supervised user during a period in which wireless phone usage is prohibited, an audible message may be played to the calling party indicating that the phone is not accessible at the present time.

The Supervisor may also specify telephone numbers within the user profile that are never permitted to be connected to the respective user's phone, and the system will prevent calls from such numbers from being connected to the respective

wireless phone. Additionally, the system may prevent the wireless phone from being used to call predetermined numbers specified by the Supervisor. The numbers telephone that cannot be called from the supervised phone and the telephone numbers of phones from which communications are blocked are referred to
5 herein as never-accessible numbers.

If voicemail capability is enabled for the respective user's phone, voicemail messages from callers other than always-accessible callers may optionally be blocked during
10 periods when phone use is restricted.

Certain numbers, namely the always accessible numbers, may be identified within the user profile and callers from these numbers may always access the supervised wireless phone or voicemail should the phone not be answered, even during a prohibited use period. For example, a parent's home number or
15 wireless phone number may be included in the profile so that the parent is always able to reach the child's phone. In the event the child or wireless phone user is not available when a call from such a number comes in, the call may be forwarded to voicemail if voicemail is enabled for that user. An incoming
20 call to a supervised phone is analyzed to determine if the calling number is one of the numbers on the list of always-accessible numbers. If the calling number is not one of the numbers on the always-accessible list, the call will not go through during a prohibited use period. However, a caller is
25 provided the ability to access the supervised wireless phone upon dialing of a security code referred to herein as a cut-through code. Thus, the Supervisor, (or an individual having knowledge of the cut-through code) may access the supervised
30 wireless phone when calling from a number other than one of the always-accessible numbers via the use of the cut-through code.

The user profiles are maintained within a database that may be modified at any time by the Supervisor. More

specifically, the Supervisor can log in over a global communications network, or other network that permits remote access, and can change usage limits in real time, change, add, delete numbers that are always or never accessible to/by a particular supervised wireless phone, change restricted use times, and make all other permitted changes to the respective user profiles. To assure that changes to the respective user profiles managed by the Supervisor may be made only by the Supervisor, a security code is required to be entered and verified before permitting changes to be made to the managed user profiles under the respective Supervisor's control. The presently described supervisory functions may operate independent of billing controls such as real-time pre-paid billing controls, or post-paid billing systems, that may also be applicable to the respective supervised phone, although the information defining the restrictions on phone use may be stored in a separate database or a common database with billing parameters. Alternatively, the presently described functionality may be provided as an overlay to pre-paid billing controls or other call billing and control systems and may be configured to share resources with such other systems while exercising call control independently of such other systems. The presently described supervisory system may employ one or more servers that operate independent of servers that provide billing functionality, or alternatively, the presently described supervisory system may share server resources while exercising control independent of restrictions pertaining to billing functions.

Other aspects, features and advantages of the presently disclosed system for exercising supervisory control over wireless phone usage will be apparent from the Detailed Description of the Invention that follows.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

The invention will be more fully understood by reference to the following detailed description of the invention in conjunction with the drawings, of which:

5 Fig. 1 is a block diagram depicting a system operative in accordance with the present invention;

Fig. 2 is another block diagram depicting a system operative in accordance with the present invention;

10 Fig. 3 is a flow chart depicting the processing of incoming calls;

Fig. 4 is a flow chart depicting the processing of incoming calls;

Fig. 5 is a flow chart depicting the processing of outgoing calls; and

15 Fig. 6 is a flow chart depicting the processing of outgoing calls.

DETAILED DESCRIPTION OF THE INVENTION

20 U.S. provisional patent application serial number 60/449,907, entitled "METHOD AND SYSTEM FOR EXERCISING SUPERVISORY CONTROL OVER WIRELESS PHONE USAGE", filed February 25, 2003, is hereby incorporated herein by reference.

In accordance with the present invention, a system and method for providing Supervisory control over wireless phone usage is disclosed. Referring to Fig. 1, a Supervisor S1 10, such as a parent or manager, is provided the ability to define a user profile for each of one or more users, such as children or employees. The user profile includes parameters and information that are used to manage phone usage. For example, 25 the user profile may specify the total number of minutes the supervised phone may be used during a specified control period, the time of day and/or day of week when incoming and/or outgoing calls are prohibited, telephone numbers for numbers 30

that are never accessible, and telephone numbers that are always accessible via the respective supervised phone, among other controlled characteristics.

Referring to Fig. 1, each wireless phone, shown for purposes of illustration as P1 12 and P2 14, may communicate with a wireless switch 16. For purposes of explanation, the wireless switch 16 in the illustrative embodiment may be a switch that is associated with a respective home serving system. The wireless switch 16 is communicably coupled to a Mobile Services Switching Center (MSC) 18 within a Service Switching Point SSP 1 20, which, in turn, is communicably coupled with the presently disclosed Supervisory Control System 22 via a telecommunications network 25 which typically includes a plurality of Signal Transfer Points (STPs) 26a, 26b, 26c, 26d, as known in the art.

The Supervisory Control System 22 includes a Service Control Point (SCP) 24 that communicates with the telecommunications network 25 and performs SS7 signaling, a Service Data Point (SDP) 30 that includes a User Profile Database 32 for storing a user profile associated with each supervised wireless phone subscribed to the presently disclosed service, and Business Logic 34 that serves as an intelligent interface between the SCP 24 and the User Profile Database 32. The Business Logic 34 typically comprises a computer that executes software to provide the supervisory processes herein described. The Supervisory Control System 22 further includes a Web-Server 36 that permits accounts to be established in the User Profile Database 32 and updated by Supervisor S1 10 as subsequently discussed. The Supervisory Control System 22 in the illustrated embodiment also includes a co-located Intelligent Peripheral or VRU 38 that is operative to play audible scripts in response to controls issued by the SDP 30. The VRU 38 may alternatively be located geographically

proximate to the respective SSP 20 as is known in the art. The SCP 24, Web-Server 36, SDP 30 and VRU 38 in the illustrated embodiment are communicably coupled via a local area network (LAN) 40, such as an Ethernet or any other suitable network. The SCP 24 employs SS7 signaling over the telecommunications network 25 and the SDP 30 executes control software to implement the supervisory control functions herein described.

The Supervisor S1 10, operating through a PC, mobile phone or other Internet enabled access point 42 equipped with a suitable browser or micro-browser, may access the Web-Server 36 via the Internet 28 or another suitable network to establish and modify user profiles for the respective Users U1 44, U2 46.

Control and operation of the presently disclosed Supervisory Control System 22 falls within several areas of functionality, which are listed below:

1. Supervisory Control System service subscription and provisioning.
2. User profile configuration
3. Event control

These functional capabilities are discussed in greater detail below.

1. Supervisory Control System Service Subscription and Provisioning

Further with reference to Fig. 1, the Supervisor S1 10 may create an Supervisory Control System account by accessing the Web-Server 36 within the Supervisory Control System 22 via the Access point 42 or alternatively, by calling a service representative who enters the applicable account information. A supervisory account identifier is associated with the respective Supervisory Control System account and stored in the

User Profile Database 32. Account setup includes the following three functions:

1. provisioning the Supervisory Control System account within the wireless network;
- 5 2. provisioning the Supervisory Control System account within the billing system so that appropriate charges will be applied with respect to each wireless supervised phone; and
3. establishing applicable Supervisory Control System parameters for each supervised wireless phone.

10 More specifically, when creating a Supervisory Control System account via a graphical user interface provided through the Web-Server 36, the Supervisor S1 10 may employ a browser resident on the access point 42 to access Web pages served by the Web-Server 36 within the Supervisory Control System 22 or
15 alternatively, the Supervisor S1 10 may place a voice call to a service representative who enters applicable Supervisory Control System account information.

When creating a Supervisory Control System account via the Internet, the Web-Server 36 is accessed via a domain-name
20 associated with a carrier and linked to the respective Web-Server 36. The interface provided by the Web-Server 36 guides the Supervisor S1 10 through the necessary steps to establish a Supervisory Control System account via one or more interface screens served by the Web-Server 36. Any suitable format for
25 interface screens may be used as is appropriate for a given implementation, so long as the interface allows the Supervisor S1 10 to establish a Supervisory Control System account and to enter User Profile data applicable to one or more supervised phones.

30 After accessing the Web-Server 36, the Supervisor S1 10 may log in via the access point 42 using a conventional login registration process. During this login process, the Supervisor S1 10 typically provides a user name and an email

address. In response, the Web-Server 36 emails a pass code to the specified email address. The Supervisor S1 10 then enters the pass code into an interface screen served by the Web-Server 36 to confirm that the Supervisory Control System account is associated with the proper individual. The supervisory account identifier is associated with the Supervisory Control System account established by the Supervisor.

2. User Profile Configuration

Following the creation of a Supervisory Control System account as described above, the phones to be supervised through the account, are identified to the SSP 1 20 so that a determination can be made whether calls relating to such phones should be processed by the Supervisory Control System 22. Accordingly, the Supervisor S1 10 is requested by the Web-Server 36 to enter a logical phone identifier (which is referred to herein as a Mobile Station Identifier (MSID)) and the Electronic Serial Number (ESN) for each wireless phone in the Supervisory Control System account. The specific Mobile Station Identifier employed may vary from system to system. For example, the MSID may be a Mobile Directory Number (MDN), a Mobile Identification Number (MIN), an International Mobile Subscriber Identity (IMSI) or a Mobile Subscriber International Services Directory Number (MSISDN) or any other suitable phone identifier. In the illustrative example, the MSID and the ESN for wireless phones P1 12 and P2 14 shown in Fig. 1, that are to be supervised by the respective Supervisor S1 10, are associated with the Supervisory Control System account. The Supervisor S1 10 also associates the name of each user with the applicable identifier(s) for the respective wireless phones. For example, in the illustrative configuration shown in Fig. 1, the Supervisor S1 10 would enter the name of User 1 U1 44 in association with wireless phone P1 12, and the name of User 2

U2 in association with wireless phone P2 14. An MSID is used to identify the wireless phone during call processing. As indicated above, the MSID used may vary from system to system and additionally at different points within a given system.

5 Information and parameters defining restrictions or permissive conditions for each supervised user's phone are stored in the User Profile Database 32. The parameters are employed to control the use of the respective wireless phone or to establish conditions that define when alert or warning
10 messages should be provided with respect to the usage of the supervised phone.

Following the association of the applicable identifier(s) with the respective users, the Web-Server 36 steps the Supervisor S1 10 through a configuration sequence for each user
15 having a phone to be supervised through the Supervisory Control System account. During this process, the Web-Server 36 presents the terms and conditions applicable to the service and requests that the Supervisor S1 10 accept the terms and agree to payment of a predetermined monthly fee for each wireless phone that is
20 subject to control of the Supervisory Control System 22.

The Supervisor S1 10 also enters user profile data to be stored within the User Profile Database 32. The user profile data specifies how the respective wireless phone may be used and characteristics associated with such usage. The user
25 profile data may impose restrictions on the use of a phone associated with the user profile data or, alternatively, may specify that warnings and/or alerts regarding phone usage are to be provided to the User or Supervisor S1 10 without restricting phone use. Such warnings or alerts may indicate
30 that usage restrictions are in effect or provide alerts that pertain to the amount of phone usage.

The user profile data described below corresponds to the data that may be entered for a single user. It should be

recognized that the same process is repeated for each user specified by the Supervisor S1 10 within the Supervisory Control System account.

By way of example, and not limitation, the Supervisor S1 10 enters the following information from the access point 42 via a browser interface in response to prompts by the Web-Server 36.

3. Event Control

10

3a. Overall Usage Limits

The Supervisor S1 10 may optionally specify an overall usage limit for a respective user. The overall usage limit specifies the number of minutes that the wireless phone associated with that user may be used within a predetermined control period, such as a week, a month or any other suitable interval. For example, the predetermined control period may correspond to a weekly or monthly period specified by the Supervisor S1 10, a billing period, or a calendar month, and may be revised from time to time by the Supervisor S1 10 via the Web-Server 36 interface or through a service representative who updates the User Profile Database 32. Once the user of a supervised phone uses a number of minutes equal to the overall usage limit allotted for the control period, no further incoming or outgoing calls are permitted until the next control period, except for calls to or from always-accessible numbers as discussed below. If the usage limit is set to 0 minutes, the phone will only be usable for calls to/from always-accessible numbers that are defined by the Supervisor S1 10. As an exception to the restrictions discussed in the preceding two sentences, in the case of an incoming call that is placed to a restricted phone using a valid cut-through code as described below, the call is connected and in one embodiment, the call

time associated with such a call is not assessed against the user's usage limit.

In one embodiment, the time on calls to or from the always-accessible numbers are not applied against the overall usage limit. For example, it may be desirable for a child to be able to call or be called by a parent without exhaustion of the overall usage limit established by the parent. In such event, the Supervisor (parent) may establish a usage limit and calls made to or from the parent are not applied against the overall usage limit.

3b. Warning Messages and Tones

Even if the Supervisor S1 10 does not establish an overall usage limit for a respective user, the Supervisor S1 10 may optionally enter an indication in the user profile information that warnings or alerts regarding phone usage should be provided to the user or supervisor after one or more usage thresholds are reached. For example, the Supervisor may specify in the User Profile Database 32 that usage alerts are to be provided after a predetermined number of minutes and at subsequent intervals. The Supervisory Control System 22 maintains a value reflective of the cumulative usage of the wireless device within the control period. From time to time the Supervisory Control System 22 determines whether the cumulative usage of the wireless device has reached the interval value specified by the Supervisor at which usage alerts are to be provided. During a call, such usage alert may, for example, be provided to the user in the form of a predetermined tone. Pre-call or post-call audible warning messages to a subscribed user may be injected as an audible script as discussed herein via the VRU 38 or alternatively as text messages via a data bearer service to advise the user of the alert condition.

Additionally, alerts may be generated and forwarded to the Supervisor regarding the usage of the supervised phone at periodic usage intervals. More specifically, the Supervisor may specify a usage interval at which alerts are to be generated and store a value corresponding to the usage interval in the User Profile Database in association with an identifier of the supervised wireless phone. The Supervisory Control System 22 may then determine when the cumulative usage of the wireless device within a control period equals the usage interval specified by the Supervisor or is an integral multiple of the time interval specified by the Supervisor. An alert message may be generated and forwarded to the Supervisor when the cumulative usage of the wireless phone equals the time interval specified by the Supervisor or is an integral multiple of the specified time interval or at any times specified by the Supervisor. The alert may be forwarded to the Supervisor as an audible script, by a text messaging service or alternatively, via email delivery. When forwarding an alert to the Supervisor as an audible script, the message may be communicated to a telephone number specified by the Supervisor and stored in the User Profile Database 32 in association with an identifier for the wireless phone. When forwarding an alert message to the Supervisor as a text message, the text message may be forwarded to the Supervisor at a telephone number specified by the Supervisor and stored in the User Profile Database 32 in association with the wireless phone identifier. When forwarding the alert message to an email address, the message may be forwarded to an email address specified by the Supervisor and stored in the User Profile Database 32 in association with the wireless phone identifier. The alert message may also be communicated to the Supervisory account by the Web Server 36 and accessed by the Supervisor either at the Access Point 42 or via a personal computer, mobile phone, or

personal digital assistant (PDA) having access to the Web Server 36. At the beginning of each control period (e.g. each month) the value maintained by the Supervisory Control System 22 pertaining to the cumulative usage of the wireless phone may be reset to reflect no usage of the wireless phone within the new control period.

The above-described alerts may be forwarded to the Supervisor and/or User with or without the imposition of restrictions on the use of the supervised phone.

3c. Permitted/Non-Permitted Usage Periods

Within the user profile data, the Supervisor S1 10 may specify time periods during which general phone use is permitted or not permitted. Whether an embodiment of the disclosed system provides for the specification of prohibited usage times or permitted usage times is a matter of design choice.

By way of example, and with reference to Fig. 1, within the user profile data, the Supervisor S1 10 may specify that User U1 44, who for purposes of illustration is assumed to be a young child, is not permitted to use the supervised wireless phone P1 12 for general usage calls other than between 4pm and 8pm on weekdays and between 9am and 8pm on weekends and holidays.

If the overall general usage limit for the specified control period is set to 0 minutes for a particular supervised phone, the system permits calls only to and from always accessible numbers and additionally, calls to the supervised phone using a valid cut-through code as discussed below.

3d. Location Controls

Also within the user profile data, the Supervisor S1 10 may specify one or more geographic locations or geographic

areas within which general phone use is permitted or not permitted. Whether an embodiment of the disclosed system provides for the specification of prohibited usage locations or geographic areas, or permitted usage locations or geographic areas, is a matter of design choice. The Supervisor may specify the geographic location as a street address and a converter or conversion service, as known in the art, may be employed to resolve the street address into a set of coordinates in a predetermined coordinate system. For example, the street address specified by the Supervisor may be stored in the User Profile Database 32 and converted into latitude and longitude coordinates prior to use. Following conversion of the street address into coordinates represented within the specified coordinate system, the coordinates may be stored within the User Profile Database so that the conversion need not be performed each time a call to or from the respective wireless device is made.

The location of the phone is generated using a global positioning system, cell sector identifiers or any other suitable technique for generating coordinates defining the location of the phone. More specifically, cell sector identifiers may be employed to resolve the geographic location of the wireless phone. The function of determining the geographic location of a wireless phone is performed via the use of a location server 57, also known as a location service broker. Such services are commercially available. One company that offers location service broker services is Apertio Limited, Kingswood, Bristol, United Kingdom and such services are described at www.invergence.co.uk. More specifically, the location service broker is operative to convert cell sector identifiers into a coordinate system such as latitude and longitude for subsequent use.

Alternatively, location information regarding the current location of the supervised wireless phone P1 12 may be obtained through the use of a GPS (Global Positioning System) receiver disposed within the wireless phone.

5 After determination of the geographic location of the phone, the location of the wireless phone is compared to the geographic location specified in the User Profile Database 32 to determine if a call should proceed. More specifically, the Supervisor may specify a distance between the location
10 specified in the User Profile Database and the location of the wireless phone within which the location of the wireless phone is deemed to correspond to the location specified by Supervisor. If the location of the wireless phone corresponds to at least one location specified by the Supervisor within the
15 User Profile Database 32, the call may be permitted to be completed or the connection of the call may be prevented based upon the parameters specified by the Supervisor in the User Profile Database 32 in the event of such a correspondence. By way of example, and with reference to Fig. 1, within the user
20 profile data, the Supervisor S1 10 may specify that User U1 44, who for purposes of illustration is assumed to be a young child, is not permitted to use the supervised wireless phone P1 12 for general usage calls when the phone is generally within the geographic area defined by the school grounds of User U1
25 44.

Any appropriate technique for definition of such a restricted area may be used. For example, an indication of a restricted address, combined with the radius of the area to be considered restricted around that address, may be entered by
30 the Supervisor S1 10 into the user profile data to provide the restricted area definition.

The present system may be embodied to allow the definition of restricted or permitted phone use locations for incoming calls, outgoing calls, or both.

5 1. Use of Cell Sector Identifiers

The Supervisory Control System 22, in one embodiment, obtains cell sector identifiers and uses the cell sector identifiers alone or in combination with associated signal strength information to obtain the location coordinates of the wireless phone. More specifically, the wireless phone has access to the received radio signal transmission strength at the mobile station radio transceiver (P1, P2). A processor on the wireless phone may execute a script or application that enables the wireless phone to calculate, extract and transmit signal strength measurements to the network via a non-
10 displayable SMS message or via any other suitable protocol. The signal strength data is coupled with the cell sector identifier information and the location area code that may be obtained from the home location register (HLR) 56. The signal strength and cell sector identifier information may then be
20 forwarded to the location server 57 to calculate coordinates of the mobile station. The location server 57 may generate coordinates using the cell sector identifiers alone or in combination with the signal strength information to resolve the wireless phone coordinates with greater accuracy. In
25 particular, the Supervisory Control System 22 communicates the cell sector identifiers and optionally the signal strength information to the commercially available service provider, such as the location server 57, to map cell sector identifiers and signal strength data into coordinates that identify the
30 location of the wireless phone. The location server may also be employed to map street address or address information entered in the Profile Database by the Supervisor into

coordinates that are returned to the Supervisory Control System 22.

It should be recognized that the mapping of street address information to latitude and longitude information may also be performed by the Supervisory Control System 22. In the
5 circumstance in which the mapping is performed by the Supervisory Control System 22, the Supervisory Control System 22 would include the location server 57 functionality.

The Supervisory Control System may include a program that
10 inspects the HLR 56 at specific time intervals, obtains or derives the latitude and longitude of the supervised phone at each such time, and arithmetically derives a speed of the supervised phone based upon the location information and the time interval. A speed threshold may be stored by the
15 Supervisor in the User Profile Database 32. If the speed threshold is exceeded, a program within the Supervisory Control System may take such actions as are specified by the Supervisor. For example, the Supervisory Control System may be programmed to forward to the Supervisor S1 10 an audible
20 message communicated to a telephone number specified by the Supervisor, a text message via a data bearer service (such as SMS messaging), or an email message that includes an alert that the respective supervised phone has been detected as having exceeded the specified speed threshold. Additionally, the
25 Supervisory Control System may be programmed to communicate a notice to the Supervisor S1 10 via the Web Server 36 that is posted in association with the Supervisory account and accessible by the Supervisor. Moreover, the Supervisory Control System 22 may be programmed to prevent further incoming
30 or outgoing calls or to terminate any call in progress at the time of the detection of the excessive speed condition.

In the event of an outgoing call by a supervised phone, the network inspects the HLR and identifies the telephone as

one being managed by the Supervisory Control System 22. This determination may be made based upon the telephone number of the calling party or any other suitable phone identifier. In response to the determination that the phone associated with the respective phone identifier is managed by the Supervisory Control System 22, the network passes call control to the Supervisory Control System 22. The Supervisory Control System 22 looks up the user profile in the User Profile Database 32 for the calling party. Upon ascertaining that there is a location restriction on phone use, the Supervisory Control System 22 sends an inquiry to the HLR to ascertain the location of the calling party. The HLR returns to the Supervisory Control System 22 the cell sector identifier associated with the calling party. In one embodiment, the Supervisory Control System 22 obtains coordinates of the wireless phone using the location server 57 and determines whether the coordinates of the wireless phone correspond to the coordinates corresponding to the address entered into the User Profile Database by the Supervisor.

In another embodiment, the Supervisory Control System 22 compares the cell sector identifier associated with the calling party with the locations identified in the User Profile Database 32. More specifically, using a location server, the addresses entered by the Supervisor are mapped into cell sector identifiers. If the cell sector identifier of the calling party's phone corresponds to a restricted cell sector identifier identified in the User Profile Database 32, the Supervisory Control System 22 provides appropriate signaling to the control network to prevent the call from being connected. It should be appreciated that if the cell sector identifier of the calling phone is forwarded to the Supervisory Control System 22 along with the request for service by the Supervisory Control System

22 a subsequent request for the cell sector identifier can be avoided.

When a call is placed to a supervised phone, the network inspects the HLR and identifies the supervised phone as one that is managed by the Supervisory Control System 32. In response to this determination, call control is passed to the Supervisory Control System 22. The Supervisory Control System 22 looks up the user profile in the User Profile Database 32 for the called party. Upon ascertaining that there is a location restriction on phone use, the Supervisory Control System 22 sends an inquiry to the HLR to ascertain the location of the called party. The HLR returns to the Supervisory Control System 22 the cell sector identifier(s) associated with the called party and optionally signal strength information associated with each of the cell sector identifiers as discussed above. The Supervisory Control System 22 then compares the location of the wireless phone to the location specified in the User Profile Database 32. This comparison may involve a comparison of coordinates after resolving the cell sector identifier data into coordinates or alternatively a comparison of cell sector identifiers to determine if the wireless phone is at a location that corresponds to a location specified by the Supervisor in the User Profile Database 32. The Supervisory Control System 22 provides appropriate signaling to the control network to either permit the call to be connected or to prevent the call from being connected based upon the result of the comparison. It should be noted that if the cell sector identifier of the wireless phone is forwarded to the Supervisory Control System 22 along with the request for service by the Supervisory Control System 22 a subsequent request for the cell sector identifier can be avoided.

ii. Use of GPS Coordinates

Alternatively, GPS coordinates may be employed to provide restrictions on phone use for a supervised phone. As discussed above, the Supervisor S1 10 enters into the User Profile Database 32 a physical address or the identification of a location at which the phone use is restricted or permitted, as applicable. The physical address, street address or identification entered into the User Profile Database 32 by the Supervisor S1 10 is converted into coordinates. More specifically, a converter accepts input information in the form entered by the Supervisor and converts such information into coordinates defining the location of the wireless phone. In the instant example, it is assumed that the Supervisor has entered into the User Profile Database 32 an address at which the use of the supervised phone is restricted.

The Supervisory Control System 22 accesses the location server 57 to obtain the geographic coordinates (latitude, longitude description) corresponding to the restricted/permitted use location specified by the Supervisor as an address. The geographic area in which the use of the wireless phone is restricted may be represented by a set of coordinates defining boundaries, as a mathematical description, as a set of coordinates and a radius defining a circular area, or any other suitable way of describing the geographic area within which the phone use is restricted or permitted. While the presently illustrated embodiment utilizes latitude and longitude coordinates to identify the geographic area of interest, any other suitable coordinate system may be employed. The Supervisory Control System 22 stores the coordinates or mathematical description defining the geographic location in which the use of the wireless phone is restricted.

In one embodiment, the location of the wireless phone is deemed to be at the location specified in the User Profile

Database, if the coordinates of the wireless phone are within a specified distance of the coordinates corresponding to an address specified in the User Profile Database 32. The specified distance may be input by the Supervisor S1 10 and
5 stored in the User Profile Database 32 or a default distance may be specified which may be modified by the Supervisor S1 10.

In response to an outgoing call from a managed phone, the HLR associated with the wireless phone identifies the phone as one that is serviced by the Supervisory Control System 22 and
10 passes control to the Supervisory Control System 22. The Supervisory Control System 22 inspects the User Profile Database 32 and identifies the calling phone as one that has one or more restrictions involving locations of use. The Supervisory Control System initiates a network query to obtain
15 GPS coordinates of the handset which are provided by a GPS receiver contained within the wireless phone. The network query may comprise a query of the wireless phone or any other network element having access to the GPS coordinates of the wireless phone. In response to the network query, the GPS
20 coordinates of the supervised phone are returned to the Supervisory Control System 22.

The coordinates of the wireless phone are then compared by the Supervisory Control System 22 to the restricted area as specified within the User Profile Database 32 to determine to
25 the wireless phone coordinates are within a restricted area. If the coordinates of the wireless phone are within the restricted area, the Supervisory Control System 22 prevents the call from being connected.

Additionally, the Supervisory Control System 22 may
30 include a program that permits the wireless phone or the network to be queried to ascertain the physical location of the phone in response to the receipt of a control code such as "*" or any other suitable control code entered on the keypad of the

wireless phone by the supervised user. Alternatively, the Supervisory Control System 22 may initiate a query to ascertain the location of the supervised phone in response to an inquiry initiated by the Supervisor S1 10. Additionally, the Supervisor
5 may initiate a query to ascertain the location of the wireless phone for one of the supervised Users. The request from the Supervisor may be communicated to the Supervisory Control System 22 from the Supervisor's phone, from the Access Point 42 via the Web Server 36 or via any other communication path.
10 Location information responsive to a request initiated either by the supervised user or the Supervisor may be communicated to the Supervisor audibly via a script played by the VRU 38 to the Supervised User's phone, via text messaging or via email. Prior to communication of the location of the wireless phone to
15 the Supervisor S1 10, a conversion of the wireless phone coordinate data to an address may be performed and address information may be conveyed to the Supervisor instead of coordinate data.

In the circumstance of an incoming call to a supervised
20 phone, a determination is made whether the call may be completed as discussed above.

It should be recognized that if the coordinates of the supervised phone are provided along with the request for service by the Supervisory Control System 22, the network query
25 can be avoided.

iii. Combinations of Restrictions or Permissive Use

The location information obtained via a GPS receiver disposed in the wireless phone, or a system that resolves the
30 wireless phone location using cell sector identifiers, may be employed in conjunction with other restrictions and/or permissions to determine whether a call placed to or from the wireless phone should be connected. For example, Boolean

functions of restrictions and/or permissions described herein and the location information may be generated to determine whether a call should be connected or blocked. More specifically, a location restriction may be employed in conjunction with a time period restriction to prevent the wireless phone from being used for normal calls while a child is at school and during the normal school hours of 9am to 3pm. Thus, the child could make and receive calls while at school before and after the normal school day or while away from the school. Similarly, location restrictions may be employed in conjunction with one or more lists of always accessible numbers and/or one or more lists of never accessible numbers to allow or disallow calls to/from specific numbers based upon the location of the supervised wireless phone and the telephone numbers on the lists of always accessible numbers and/or never accessible numbers as applicable. Finally, a determination may be made by the Supervisory Control System 22 whether to complete or block a call based upon a combination of one or more of the wireless phone location, always accessible or never accessible numbers, date, day or the week and/or a permitted or restricted time period.

While the restrictions and/or permissions regarding phone usage are entered by the Supervisor S1 10 into the User Profile Database 32 for the respective wireless phone, information representative of the location information stored in the User Profile Database may be downloaded from the User Profile Database 32 to a first memory region within the wireless phone and a determination may be made within the wireless phone whether to connect a call dialed by the wireless phone user based upon a comparison of the downloaded information to location information generated within the wireless phone. Such a determination may be made using a processor within the wireless phone that executes a software program stored in a

second memory region within the phone. The first and second memory regions may be within the same physical memory or different physical memories within the wireless phone. For example, if a supervisor has entered into the respective User Profile Database 32 a restriction on phone use that indicates that the wireless phone may not be used when a student is at school between 9am and 3pm, a determination may be made by the processor within the wireless phone whether the phone is at the restricted location and whether the current time is within the specified time period, in which event the call may be blocked. By making such a determination within the wireless phone rather than at the Supervisory Control System 22, unnecessary network traffic is avoided. It should be recognized that the location information stored within the User Profile Database 32 may comprise conventional street address information which may be converted to latitude and longitude coordinates prior to communication to the wireless phone. Thus, a comparison of the latitude and longitude coordinates corresponding to the street address entered by the Supervisor S1 10 may be made with respect to the latitude and longitude coordinates obtained from a GPS receiver disposed within the wireless phone and a determination may be made that the wireless phone is at the address specified by the Supervisor if a distance between a location specified by the latitude and longitude associated with the street address and a location specified by the latitude and longitude obtained from a GPS receiver within the wireless phone is less than a predetermined threshold distance. If the wireless phone is determined to be at the address specified in the User Profile Database 32, the call may be terminated or connected as specified by applicable rules maintained within the User Profile Database 32.

3e. Cut-Through Capability

A Supervisor or other individual that desires to call a supervised user's phone (assuming the phone is on and not otherwise in use), may always reach the user's phone provided that a cut-through code has been established for the respective Supervisor or entered by the Supervisor. More specifically, in one embodiment, in response to prompting by the Web-Server 36, the Supervisor S1 10 may provide a cut-through code that is typically defined as being between n and m numerical characters in length. For example a numeric code between 4 and 6 characters in length may be employed. The cut-through code allows the Supervisor S1 10 to access one or more of the supervised phone(s) during hours or under circumstances in which phone usage is restricted and when the Supervisor S1 10 is not located at an always-accessible number. The cut-through code is communicated from the access point 42 to the web server 36 via the communications network 28. The web server communicates the cut-through code over a data path to the User Profile Database 32 for storage. The data path may include a computer that forms a component of the business logic 34 and that writes the cut-through code to the User Profile Database 32.

In one embodiment, as a default, the cut-through code is assigned based upon the Supervisor's user name that is communicated from the access point to the User Profile Database 32. For example if the Supervisor's user name is "abodef" the cut-through code would be "222333" which represent the number keys on a typical phone keypad that correspond to the letters in the username. If the username were "222333", the cut-through code would be "222333". By way of further example, if the username were "abc444", the cut-through code would be "222444". If the username were more than six characters in length, the cut-through code may be truncated at a

predetermined number of characters, such as at six characters. By using the username as the default cut-through code, the necessity to have the Supervisor input this code is avoided. The Supervisor may be permitted to modify the default cut-through code to specify a different cut-through code to provide
5 higher security.

The Supervisor may also convey the cut-through code to an administrator orally and the administrator may input the cut-through code to the Supervisory Control System 32.

10 When a Supervisor having knowledge of the cut-through code calls a supervised phone at a time when the use of the phone is subject to a restriction on use, a message is played to the calling party (the Supervisor) that indicates that the called phone is not accessible. If the Supervisor successfully
15 enters the cut-through code before a predetermined time interval expires, the call is allowed to proceed. If the cut-through code is not entered within the predetermined time interval, the call is blocked. If the call is allowed to proceed, a control message of a first type is forwarded to the
20 control network to signal that the call should be connected. If the call is not to be connected, a control message of a second type is forwarded to the control network to prevent the call from being connected.

The "cut-through" capability may be tested during the
25 user profile data setup. At such time, the Supervisor S1 10 may have physical possession of the phones controlled under the Supervisory Control System account before the phones have been distributed to their users. More specifically, in response to prompting from the Web-Server 36, the Supervisor S1 10 powers
30 on the respective user's phone, which is subject to at least one use restriction, and attempts to call it. When the Supervisor S1 10 hears a prompt advising that the phone is not presently reachable, the Supervisor S1 10 enters the previously

selected cut-through code. If the cut-through capability is functioning properly, the respective user's phone rings as a result of the entry of the cut-through code.

5 3f. Always-Accessible Numbers

10 In response to a prompt from the Web-Server 36, the Supervisor S1 10 may optionally enter a first list of telephone numbers that may always be called by the respective user and a second list of numbers that may always call the respective
15 user's phone number assuming the wireless phone is powered on and reachable within the wireless network. These lists may be provided as separate lists or alternatively, may be aggregated as a single list. Optionally, the Supervisor S1 10 may enter or associate within the user profile data short codes that
20 correspond to the always-accessible numbers so that one or more of the always-accessible numbers can be rapidly called in an emergency situation without the need for a user to remember the numbers.

20 3g. Never-Accessible Numbers

 In response to a prompt from the Web-Server 36, the Supervisor S1 10 may optionally enter a list comprising one or more telephone numbers or telephone number prefixes that the user of an associated phone should never be able to call and a
25 list of telephone numbers or telephone number prefixes that should never be able to call the supervised user's phone. These lists may be entered as separate lists or alternatively may be aggregated as a single list.

30 3h. Saving of User Profile Data

 When the Supervisor S1 10 initiates the saving of the user profile data, that data is associated with the respective user. If the Supervisor S1 10 exits the setup routine without

saving the user profile data, the respective wireless number is provisioned within the Supervisory Control System 22 for unrestricted use.

5 3i. Setup of Additional Users

 The Web-Server 36 may prompt the Supervisor S1 10 to determine whether he/she desires to utilize the same user profile data for the next user that needs to be configured. The Supervisor S1 10 may apply the previously entered user
10 profile data for the setup of the next user or alternatively, establish a new user profile for the next user. Moreover, as further discussed below, user profiles may be defined and modified on a user group basis. Under such circumstances, the disclosed system enables the Supervisor S1 10 to define a set
15 of user profile parameters that apply to a group of phones and associated users. The control parameters for the group can subsequently be modified and members of the group added or deleted.

20 4. Supervisory Control System Operation

4a. Supervisory Control System Operation for Incoming Calls to a User

 Operation and signaling for the Supervisory Control
25 System 22 with respect to a telephone call that is placed to a user is described below with respect to the devices in Fig. 1 and the steps shown in Fig. 3.

 The following example describes an exemplary call from a calling party U5 52 from a telephone P5 50 to a called party U2
30 46 at a supervised wireless phone P2 14. It is assumed for purposes of the present discussion that Supervisor S1 10 established a user profile applicable to phone P2 14 at a prior time and that the user profile for the phone P2 14 prohibits

general phone usage during school hours from 8:00am to 4:00pm weekdays.

5 The call placed by caller U5 52 from phone P5 50 is received at an associated Signal Switching Point (SSP 2) 54 as depicted at step 80 of Fig. 3. The Signal Switching Point (SSP 2) 54 accesses the Dialed Number Identification Service (DNIS) which includes the dialed telephone number for the call. From the DNIS, the SSP identifies the service provider for the dialed phone number and routes the call to the applicable
10 service provider. In the instant example, the call is routed to SSP 1 20 which is within the home serving system for the wireless phone P2 14.

The SSP 1 20 within the home serving system for the called number extracts a MSID from the DNIS. The SSP 1 20
15 performs a lookup within the Home Location Register (HLR) 56 using the extracted identifier to obtain the HLR record for the respective called wireless phone P2. The HLR record includes data that instructs the respective Signal Switching Point (SSP 1) 20 what to do next. If the HLR record indicates that the
20 Supervisory Control System 22 should be accessed in the event of calls to the respective called party, the Supervisory Control System 22 is signaled. If the HLR 56 does not indicate that the Supervisory Control System 22 should be accessed, the call is connected subject to any other restrictions and
25 protocols that may be applicable.

In the instant example, the HLR record includes information that instructs the SSP 1 to signal the Supervisory Control System 22 that an incoming call is pending. More specifically, as depicted at step 82 of Fig. 3, the respective
30 SSP (SSP 1) 20 signals the SCP 24 within the Supervisory Control System 22 that an incoming call is pending for a called party having a specified MSID. The Service Data Point (SDP) 30 within the Supervisory Control System 22 performs a lookup

within the User Profile Database 32, as depicted at step 84 of Fig. 3 to ascertain whether the MSID corresponds to a user profile within the User Profile Database. If as a consequence of the lookup, it is determined that the MSID corresponds to an MSID within the User Profile Database 32, the Business Logic 34 executes a software program as shown at step 86 of Fig. 3 to determine how the call should be handled. As a result of the Business Logic 34 processing, the SCP 24 may be instructed to initiate SS7 signaling and a VRU such as VRU 38 may be instructed to play an audible script to a supervised phone or a calling party. More specifically, if the MSID of the called party corresponds to the MSID of a phone within the User Profile Database 32, the Business Logic 34 within the SDP 30 accesses the relevant data within the applicable records of the User Profile Database 32, current conditions, such as time, date, calling number, and called number and determines what action should be taken. Exemplary Supervisory Control System processing under the control of the Business Logic 34 is described below with reference to Fig. 4.

As depicted at step 90 of Fig. 4, the Business Logic 34 determines at step 90 of Fig. 4 whether the calling number corresponds to an always-accessible telephone number that can always be put through to the supervised phone P2 14. If the calling number corresponds to a telephone number that is specified in the User Profile Database 32 as being an always-accessible number that can always access phone P2 14, the SCP 24 within the Supervisory Control System 22 signals the SSP 1 20 associated with the phone P2 14 (in the instant example SSP 1 20) to allow the call to be connected to the phone P2 14 as indicated at step 92. In response, the call is routed through the MSC 18 in SSP 1 20 to P2 14 to establish the desired connection between P5 52 and the supervised wireless phone P2 14.

IF the Business Logic 34 determines, as depicted at step 90, that the calling number does not correspond to a number that can always access the respective phone P2 14, the Business Logic 34 next determines whether the calling number corresponds to a number that is identified within the User Profile Database 32 as never being permitted to access the phone P2 14 as depicted at step 93 of Fig. 4. If the Business Logic 34 determines that the calling number is on the list of never-accessible numbers as depicted at step 93, the Business Logic 34, in conjunction with the SCP 24 may cause a connection in the form of a T1 link or any other suitable communication link to be established between the Intelligent Peripheral or Voice Response Unit (VRU) 38 and the MSC 18. The MSC 18 then couples the VRU 38 through to the calling party. An audible message specified by the Business Logic 34 is played to the calling party by the VRU 38 to indicate that the called party is not accessible as depicted at step 94. The SCP 24 then causes the T1 connection between the VRU 38 and the MSC 18 to be torn down and the SCP 24 signals the Signal Switching Point SSP 1 20 to disconnect the call from the calling party.

If the Business Logic 34 determines that the number of the calling party does not correspond to an always-accessible number or a never-accessible number, as depicted at step 96, the Business Logic determines whether the present time is within a period during which general phone usage is prohibited, e.g. between 8:00am and 4:00pm on a weekday in the instant example. If the present time is within a prohibited period, the Business Logic 34 causes a connection to be established between the VRU 38 and the calling phone P5 50 and causes the VRU 38 to play a message indicating that the called phone is not accessible at the present time as shown at step 97 of Fig. 4. If a cut-through code is entered within a predetermined time period as depicted in step 98, the Business Logic 34

verifies the cut-through code and the SCP 24 signals the MSC 18 to connect the calling party to the supervised phone P2 14 as shown in step 102 by forwarding a control message of a first type. If the proper cut-through code is not entered within the predetermined time period, the Business Logic 34 causes the SCP 24 to initiate SS7 signaling via a control message of a second type that causes the T1 connection between the VRU 38 and the MSC 18 to be broken and the call to be released as depicted in step 104.

10 If the Business Logic 34 determines that the present time is not within a time period specified within the respective user profile as a period during which general phone usage is prohibited per step 96, the Business Logic 34 determines whether a limit has been established for the number of minutes
15 the phone may be used within a control period and whether the number of allotted minutes for the applicable control period have been exhausted as depicted at step 100. If the total number of allocated minutes for the control period have been exhausted, the Business Logic 34 in conjunction with the SCP 24
20 causes a connection to be made between the VRU 38 and the calling party via the MSC 18, and causes a message to be played by the VRU 38 indicating that the called party is not accessible as shown at step 97 of Fig. 4. If a proper cut-through code is entered within a specified time period, the
25 Business Logic 34 causes a control message of a first type to be forwarded to the MSC 18 to signal the MSC 18 that the call should be connected. If the predetermined time period has expired without entry of a proper cut-through code, the Business Logic 34, in conjunction with the SCP 24, causes the
30 connection between the VRU 38 and the MSC 18 to be torn down. The Business Logic 34 also initiates signaling of the MSC 18 via a control message of a second type that indicates that the call should not be completed.

If the Business Logic 34 determines that the allocated minutes for the control period for the called party have not been exhausted, the Business Logic 34 next determines whether the calling party has called the supervised user's phone when the phone happens to be at a geographic location at which the use of the phone is restricted as depicted in step 106. If it is determined in step 106 that the called phone is not at a location at which the use of the phone is restricted, the Business Logic 34 initiates signaling of the MSC 18 to cause the call from the calling party to the supervised user's phone P2 to be connected as depicted at step 108.

If the incoming call is placed to the supervised phone at a time when the supervised phone is at a location at which the use of the phone is restricted, a message may be played to the calling party advising that the called phone is not accessible as discussed above with respect to step 97. If a proper cut-through code is not entered within the predetermined time period, the Business Logic 34 initiates signaling of the MSC 18 to prevent the call from being connected as shown in step 104. Alternatively, if the calling party enters the applicable cut-through code as depicted in step 98, the Business Logic initiates signaling of the MSC 18 to instruct the MSC 18 to connect the call as shown in step 102.

It should be recognized that the order of the above steps may be varied and/or selected types of restrictions may be omitted, without departing from the presently disclosed invention and that the present invention involves the functions that are provided rather than the particular order in which such functions are realized. Additionally, the tests applied by the Business Logic 34 may be tests framed in the context of permissive use of the supervised phone rather than in terms of restrictions on use of the supervised phone. By way of example, the User Profile Database 32 in one embodiment includes

parameters that define time intervals during which calls are permitted and/or locations at which calls are permitted. The Business Logic 34 in such embodiment is operative to test the current time to determine if the current time is within a time period during which use of the phone is permitted and/or test the current location to determine if the phone is at a location at which use of the phone is permitted. The Business Logic 34 initiates appropriate signaling to the MSC 18 depending upon the outcome of the comparisons.

Appropriate signaling between the MSC 18 and the Business Logic 34 via the SCP 24 is maintained to update the call usage information so that the number of minutes used by the supervised user within the respective control period does not exceed the total number of minutes allotted for general phone usage within the control period. Thus, the SCP 24, in response to a command from the Business Logic 34 may signal the home serving system MSC 18 to release a call upon a determination that the total minute allotment for the control period has been exhausted or allow the respective call to complete as discussed below. Prior to causing a call to be released due to the exhaustion of the total allotted minutes within the applicable control period, the Supervisory Control System 22 may cause a tone to be injected into the ongoing call between the calling party and the supervised phone to indicate to the respective subscribed user that the call is to be released after a predetermined period. This function may be initiated by the SCP 24, the Business Logic 34, or a combination of both depending upon the design partitioning in a given system. The warning tone may be played by the VRU 38 or injected via any other suitable device.

In an alternative embodiment, even if the total number of minutes used by a supervised user within a control period is exceeded during the pendency of a call, the Supervisory Control

System 22 permits the call to continue to its completion by the parties. Subsequent general usage calls are blocked until a new control period commences or until modification of the usage controls within the User Profile Database 32 by the Supervisor S1 10 so as to permit further general usage calls.

4b. Supervisory Control System Operation for Outgoing Calls from a Supervisory Control System Subscriber

Operation and signaling of the Supervisory Control System 22 with respect to an outgoing telephone call that is placed by a Supervisory Control System 22 subscriber P2 14 is described below with respect to Fig. 1 and flow charts of Fig. 5 and 6. Fig. 1 is employed to illustrate the circumstance in which the wireless supervised phone P2 14 places a call to phone P5 50 that is initially received by the MSC 18 of the home serving system. It is assumed for purposes of the present discussion that Supervisor S1 10 has established a user profile for phone P2 14 and that the user profile for the phone P2 14 prohibits general phone usage during school hours from 8:00am to 4:00pm weekdays.

In the instant example, the call is placed by a calling party U2 46 from wireless phone P2 14 to a called party and is received at step 110 of Fig. 5 by the associated MSC 18 in SSP 1 20 as shown. The MSC 18 associated with SSP 1 20 accesses the respective Home Location Register (HLR) 56 and performs a lookup based on an extracted MSID. The HLR 56 contains a record that includes an indication whether service is required by the Supervisory Control System service provider. If an entry in the applicable HLR record indicates that the Supervisory Control System 22 should be signaled to advise of the pending call, SSP 1 20 signals the SCP 24 within the Supervisory Control System 22 to indicate that there is a pending call as depicted at step 112. If the applicable HLR record does not indicate that

Supervisory Control System services are required, the call is processed in accordance with conventional call processing protocols.

Once the Supervisory Control System 22 receives a signal
5 indicating that a call is pending from a Supervisory Control System subscriber, the Business Logic 34 within the SDP 30 of the Supervisory Control System 22 executes a program to determine what services and signaling need to be initiated by the Supervisory Control System 22.

10 More specifically, as depicted at step 114 of Fig. 5, the Business Logic 34 performs a lookup within the User Profile Database 32 to ascertain whether the MSID of the calling party corresponds to an MSID within the User Profile Database 32. If, as a consequence of the lookup, it is determined that the
15 MSID corresponds to an MSID within the User Profile Database 32, the Business Logic 34 executes a program to ascertain how the call should be handled. In particular, if the MSID of the calling party corresponds to the MSID of a phone having a record within the User Profile Database 34, the Business Logic
20 34 accesses the relevant data within the applicable record of the User Profile Database 32, accesses current state information, such as time, date and calling number, and determines what action should be taken as illustrated at step 116. An exemplary series of steps that may be executed within
25 the Business Logic 34 is described below with reference to Fig. 6.

As shown at step 120 of Fig. 6, the Business Logic 34 determines whether the called number corresponds to an always-accessible telephone number, i.e. a telephone number that can
30 always be accessed by the respective phone P2 14. For example, in the instant example, it is assumed that calls to one or more numbers associated with the Supervisor S1 10 (such as the Supervisor's home and wireless numbers) may always be

completed. If the called number corresponds to a telephone number that is specified in the User Profile Database 32 as being always accessible, the Business Logic 34 signals the SCP 24 that the call can be put through as depicted at step 122, and the SCP 24 signals the MSC 18 then associated with the phone P2 14 to allow the call to be connected to the called party. In response, the SSP 1 20 routes the call from phone P2 14 through to the called party to establish the desired connection.

10 If the Business Logic 34 determines that the called number does not correspond to a number that is always accessible by the phone P2 14, the Business Logic 34 determines whether the called number corresponds to a number that is never permitted to be accessed by the phone P2 14 as illustrated at
15 step 124. This determination is made by obtaining the called number from the DNIS or any other suitable identifier and by comparing the called number to the never-accessible numbers previously entered into the User Profile Database 32 by the Supervisor S1 10. If the Business Logic 34 determines that the
20 called number is on the never-accessible list, the Business Logic 34 may cause a connection to be established between the Intelligent Peripheral or Voice Response Unit (VRU) 38 and the MSC 18 serving the phone P2 14 via a T1 link 60 as shown or via any other suitable communications link. The Business Logic 34
25 then causes an audible message to be played to the phone P2 14 via the VRU 38 to indicate to the User U2 46 that the called party is not accessible as illustrated at step 126. The Business Logic 34 finally causes the T1 link (or other connection) between the VRU 38 and MSC 18 serving the phone P2
30 14 to be torn down and causes the SCP 24 to signal the SSP 1 20 to prevent the call from the phone P2 14 to the called number from being connected by forwarding a control message to the SSP 1 20.

If the Business Logic 34 determines that the number of the called party does not correspond to an always-accessible number or a never-accessible number, the Business Logic 34 determines whether the present time is within a period during which general phone usage is prohibited as depicted at step 128, e.g. between 8:00am and 4:00pm on a weekday in the instant example. If the present time is within a prohibited period, the Business Logic 34 causes a connection to be established between the VRU 38 and the MSC 18 associated with the calling phone P2 14 and causes the VRU 38 to play a message indicating that the call cannot be connected at the present time. The Business Logic 34 then causes the T1 link 60 between the VRU 38 and the respective SSP 1 20 to be torn down and causes SCP 24 to signal the MSC 18 by forwarding a control message that indicates that the call should be released as shown at step 126.

If the Business Logic 34 determines that the present time is not within a time period specified within the respective user profile as a period during which general phone usage is prohibited, the Business Logic 34 determines whether the total number of allotted minutes for the month have already been exhausted as depicted at step 130. If the total number of minutes have been exhausted, the Business Logic 34 causes a connection to be made between the VRU 38 and the MSC 18 serving the calling phone P2 14, and causes a message to be played by the VRU 38 to the phone P2 14 indicating that the called party is not accessible as illustrated at step 126. The Business Logic 34 then causes the connection between the VRU 38 and the respective MSC 18 to be torn down and initiates signaling by the SCP 24 to have the call from wireless phone P2 14 released by the serving MSC 18.

If the Business Logic 34 determines that the allotment of minutes for the relevant control period have not been

exhausted, the Business Logic 34 determines if the calling phone P2 is subject to a location restriction as depicted at step 132 and as specified in the User Profile Database 32. If the supervised user's phone P2 14 is subject to a location
5 restriction, the Business Logic 34 causes a connection to be made between the VRU 38 and the MSC 18 serving the calling phone P2 14, and causes a message to be played by the VRU 38 to the phone P2 14 indicating that the called party is not accessible as illustrated at step 126. The Business Logic 34
10 then causes the connection between the VRU 38 and the respective MSC 18 to be torn down and initiates signaling by the SCP 24 to have the call from wireless phone P2 14 released by the serving MSC 18.

If the Business Logic 34 determines in step 132 that no
15 location restriction is applicable to the use of the phone P2 14, the Business Logic 34 initiates signaling by the SCP 24 to the respective SSP 1 20 to connect the subscriber's phone P2 14 to the called party as shown at step 134.

It should be recognized that the order of the above steps
20 may be varied and/or selected types of restrictions may be omitted.

4c. Updating of Phone Usage Information

Appropriate signaling between the respective SSP 1 20 and
25 the Supervisory Control System 22 is maintained during a call to update the call usage information so that the total allotment of minutes for general phone usage within the control period is not exceeded unless permitted as specified in the User Profile Database 32. Time monitoring may be performed by
30 the SCP 24, the Business Logic 34, or a combination of both based upon the particular design partitioning for the Supervisory Control System 22. Such time monitoring of call length may be performed by the Supervisory Control System 22

via a signaling path between the SCP 24 and the respective MSC 18 that is maintained while the call is pending. The Supervisory Control System 22 updates the minutes remaining and may cause the SCP 24 to signal the SSP 1 20 associated with the
5 calling party to release the call upon determining that the allotment of minutes for the control period has been exhausted if so specified by the Supervisory Control System 22.

In an alternative embodiment, even if the total number of minutes used by a supervised user within a control period is
10 exceeded during the pendency of a call, the Supervisory Control System 22 permits the call to continue to its completion by the parties. Subsequent general usage calls are blocked until a new control period or modification by the Supervisor S1 10 of the usage controls within the User Profile Database 32 so as to
15 permit further general usage calls.

Other desired supervisory functions may be performed by the Business Logic 34. Signaling between the Supervisory Control System platform 22 and the applicable SSP 1 20 may be accomplished via any suitable signaling technique.

20

4d. Roaming Scenarios

Fig. 2 depicts the circumstance in which a supervised wireless phone is served by an MSC outside the home system. In the instance in which the subscriber U2 46 is roaming, when the
25 subscriber activates the phone P2 14, the MSC 66 accesses a central database 64 using an MSID for the roaming phone to perform a record lookup. The record retrieved from the central database 64 is used to populate the Visitor Location Register (VLR) 65 for the respective MSC 66 as is known in the art.
30 When a call that is placed from the wireless phone P2 is received by the local MSC 66, the MSC 66 uses an MSID associated with the calling wireless phone P2 to perform a lookup within the VLR 65. The record obtained from the VLR

includes information instructing the MSC 66 to signal the Supervisory Control System 22 if Supervisory Control System services may be required. Once the SCP 24 within the Supervisory Control System is signaled that Supervisory Control
5 System services are required, processing within the Supervisory Control System 22 proceeds generally as described above, noting that appropriate SS7 signaling is employed as is known in the art for completion, release, and VRU messaging of wireless calls initiated from serving systems other than the home
10 serving system.

Additionally, the Supervisory Control System 22 is invoked with respect to calls received by the supervised phone P2 14 when the phone P2 14 is roaming, noting that appropriate SS7 signaling is employed as is known in the art for
15 completion, release, VRU messaging and tone injection for wireless calls that are received by the supervised phone P2 14.

4e. Enterprise Embodiment

While the preceding examples have described operation of
20 the disclosed system in the context of a parent supervising the wireless phones of children, the disclosed system may similarly be used by a manager within an enterprise to control the usage of wireless phones by employees under his or her supervision. For example, a business organization with a number of employees
25 may be broken down as the following example indicates:

Senior Management - 4

Sales - 5

Client and Field Support - 10

In the present example, 19 phones are available for
30 senior management, sales, and client and field support, collectively, and each employee is to be separately allocated a number of minutes for phone use during the control period. The business does not plan to control usage among Senior Management

and Sales employees, but desires to control usage among client and field support employees. Accordingly, the Supervisory Control System account for the business is configured by the responsible manager and the 10 phones provided to the Client and Field Support employees may be treated as a single group of users as further discussed.

The manager navigates to a predetermined Web-site and is prompted to create the necessary Supervisory Control System account. The manager provides his name, company name, service account number for the business, and email address, and creates a login name and password. The manager then defines the wireless phones that are to be controlled under the Supervisory Control System account. The wireless phones under supervision are thus associated with a corporate Supervisory Control System account number for the business. For example, in the case where 10 phones are identified in association with the Supervisory Control System account, an account summary screen may be presented on which an identification of the 10 phones is entered. The manager is then permitted to provision a name next to each of the 10 phones. In one embodiment, by default, the 10 phones are initially setup in a single generic "group" in which they are enabled minimally to call each other. However, though they are initially provisioned to call each other, the manager may further add other names and numbers that the phones should be always available, with respect to calls from and/or to the phones in the initial group, including headquarters numbers, other wireless numbers for employees, etc. Additionally, the manager may establish a specific number of allocated "general purpose" minutes that each phone in the group is allocated to use on a periodic basis. This allocation allows the employee to place calls to other numbers until the allocation has been exhausted. Similarly, a never-accessible list of numbers may be defined for the group. The never-

accessible list includes numbers that cannot be the source or destination number for calls involving the respective supervised phone.

At this point, the provisioning process is complete, and the phones are available for use. The manager, for example, is shown an account summary screen, showing the phones as members of a "Default Group". At a subsequent point in time, the manager may wish to perform management functions with respect to the previously defined Supervisory Control System account. When the manager subsequently logs into the system via the Web server, he or she is again taken to the account summary screen. On the account summary screen, the last view of the managed groups is displayed. For example, an "open" default group folder would be displayed, and a "modify properties" button shown with the 10 phones below it, and showing the MSID, Name, Used/Allocated minutes and a "modify properties" button for each phone. If the manager clicks on the "modify properties" button on for the default group, he or she is enabled to perform the following functions:

(a) Modify the numbers listed under the always-accessible and never-accessible lists, by editing numbers on the lists, and adding or deleting number to or from the lists respectively,

(b) Modify the allocation of minutes for the control period for the group,

(c) Modify any incoming or outgoing call time restrictions associated with the group, and

(d) Modify any other restrictions maintained in the User Profile Database 32 that may be specified by the Supervisor.

When modifying group properties, the modifications take effect for all members of the group. Additionally, the usage properties of the phones may be separately modified. Additionally, where particular messages are specified to be

played on the occurrence of certain associated events, such as call blocking, those messages may be defined on a group wide basis. When it is desired to add new phones to the account, for example, when more phones are purchased for new client services employees, the manager can add those phones to the existing group through the Web Server interface after their service is provisioned by the wireless carrier. When the manager logs onto the graphical user interface provided by the Web server 36, the new phones automatically appear as part of the default group, and automatically take on the properties of the default unless the manager "moves" them, for example by a drag-and-drop operation, into another group. The manager is also enabled to define and/or define the name(s) associated with the new phones through the Web Server 36. In this way, multiple user groups can be defined and named with associated use parameters, and users can conveniently be added to and/or moved between the various groups within an Supervisory Control System account.

Additionally, wireless phones of supervised users may include a resident program that permits a client application to be downloaded from the Supervisory Control System 22. For example a Binary Runtime Environment for Wireless (BREW) application that provides a user interface for quick access to the always-accessible numbers they can call, by name, may be downloaded from the Supervisory Control System 22. Such a client application may be configured to connect to the Supervisory Control System 22 at startup to retrieve always-accessible numbers.

30 4f. SIM Embodiment

The disclosed system may employ a Subscriber Identity Module (SIM) module within the wireless phone to provide certain filters for outgoing calls from the respective wireless

phone under supervision. In such an embodiment, parameters relevant to outgoing call restrictions may be downloaded or otherwise communicated to the SIM within the respective wireless phone from the User Profile Database 32 and may then
5 be stored on and processed using the SIM when an outgoing call is dialed from the respective wireless phone. By way of example, and not limitation, location restrictions, never-accessible number restrictions, time of day restrictions and/or date restrictions specific to the user may be stored within the
10 SIM of the respective wireless phone. In response to the dialing of an outgoing number, the restrictions applicable to the respective phone and stored within the SIM may be tested to determine whether the connection of the call would be contrary to any restrictions. The processing logic associated with this
15 determination may be made by a processor within the SIM or within the wireless phone. Additionally, the parameters defining the use restrictions (or permissive uses) may be stored on a memory within the SIM or alternatively within portions of a memory shared with program code executed by a
20 processor within the wireless handset. By filtering outgoing calls in the above-described manner, network traffic and external processing is reduced since signaling to the Supervisory Control System 22 is avoided and processing pertaining to calls filtered by the SIM need not be performed
25 by the Supervisory Control System 22. The relevant parameters for such outgoing call restrictions may be updated when the phone is powered on and registered within the wireless network to assure that the parameters reflect the current parameters pertaining to use restrictions for the respective wireless
30 phone.

5. System Architecture

5 The presently described supervisory system may be employed in conjunction with a billing process for wireless phones. For example, call rating data and other parameters applicable to billing functions may be stored in a first database that is used by a first server to perform the billing functions as known in the art, such as a prepaid billing process for wireless phones.

10 A second database may be used to store parameters applicable to the presently disclosed supervisory restrictions and a second server executing the presently disclosed supervisory process and including the functions of the Business Logic 34 may be employed to determine whether to connect a call in view of the stored supervisory restrictions.

The supervisory process may operate as an overlay to the billing process. For example, in a prepaid wireless environment, a determination may be made whether sufficient funds have been prepaid for the call to be connected upon execution of the billing process in the first server. If sufficient funds exist in the prepaid account for a call to be connected, the supervisory process may then be executed to determine whether the call should be connected. It should be understood that the order of execution of the billing process and the supervisory process may be reversed. The billing process and the supervisory process may be executed within first and second servers that are separate servers. Alternatively, the first and second servers may comprise the same server and the billing process and the supervisory process may be executed within the same server.

It will be further appreciated by those skilled in the art that while the exemplary embodiments are illustrated in terms of wireless phone communications, the inventive concepts described herein are equally applicable to data messaging services, such as short messaging service (SMS) and the presently disclosed concepts may be employed to restrict or permit such communications. With respect to restrictions on data messaging devices, in addition to restrictions applicable to data communication devices, such as time of day, location, and devices associated with specific individuals, restrictions may be imposed on the number of bytes and/or messages to be communicated during a control period. The determination whether to permit a data communication to be completed may be made at the Supervisory Control System 22. Additionally, determinations whether to restrict outgoing messaging from a wireless device may be made using a processor within the wireless device to reduce network traffic.

Those skilled in the art should readily appreciate that programs defining the functions of the present invention can be delivered to a computer in many forms; including, but not limited to: (a) information permanently stored on non-writable storage media (e.g. read only memory devices within a computer such as ROM or CD-ROM disks readable by a computer I/O attachment); or (b) information alterably stored on writable storage media (e.g. floppy disks and hard drives). In addition, while the invention may be embodied in computer software, the functions necessary to implement the invention may alternatively be embodied in part or in whole using hardware components such as Application Specific Integrated Circuits or other hardware, or some combination of hardware components and software.

While the invention is described through the above exemplary embodiments, it will be understood by those of

ordinary skill in the art that modification to and variation of the illustrated embodiments may be made without departing from the inventive concepts herein disclosed. Accordingly, the invention should not be viewed as limited except by the scope
5 and spirit of the appended claims.

CLAIMS

What is claimed is:

1. A method of controlling the usage of a wireless device
5 comprising the steps of:

obtaining a first set of coordinates in a specified
coordinate system representative of a first geographic
location;

- 10 in response to an attempt to establish a communication
involving said wireless device and another communication
device:

obtaining a second set of coordinates in said
specified coordinate system representative of a second
geographic location corresponding to the geographic
15 location of said wireless device;

determining based upon said first and second sets of
coordinates, whether said wireless device is at a
location where use of said wireless device is restricted;
and

20 based on the result of said determining step, if
said wireless device is at a location where use of the
device is restricted, preventing said attempted
communication involving said wireless device and said
other communication device.

- 25 2. The method of claim 1 further including the step of
permitting said attempted communication if said wireless device
is not at a location where use of said wireless device is
restricted.

30 3. The method of claim 2 wherein said preventing step
includes the step of generating a control message of a first
type and said permitting step includes the step of generating a

control message of a second type and forwarding one of said control messages of said first and second types to signal whether said attempted communication should be prevented or permitted.

5

4. The method of claim 3 wherein said determining step comprises the step of determining a first distance between said second geographic location specified by said second set of coordinates and said first geographic location specified by said first set of coordinates and said control message generating steps comprise the steps of generating said control message of said first type in the event said first distance is greater than a specified threshold and generating said control message of said second type in the event said first distance is less than said threshold distance.

10

15

5. The method of claim 1 wherein said wireless device is a wireless phone, said other communication device is another phone and said attempted communication is an attempted call involving said wireless phone and said other phone.

20

6. The method of claim 1 wherein said wireless device is operative to communicate via a data messaging protocol and said other communication device is operative to communicate via said data messaging protocol.

25

7. The method of claim 1 further including the steps of:
receiving as an input at an access point information corresponding to said first geographic location;
communicating said information corresponding to said first geographic location over a first communication network to a first server communicably coupled to a database for storage in said database; and

30

storing said first geographic location in said database.

8. The method of claim 7 further including the steps of:

receiving at said access point a password input by a
5 user;

communicating said password from said access point over
said first communication network to said first server;

comparing said password input to said access point to a
stored password associated with a supervisory account; and

10 performing said storing step in the event said password
input at said access point corresponds to said stored password.

9. The method of claim 8 further including the steps of:

associating at least one user account with said
15 supervisory account, wherein each of said at least one user
account is associated with a corresponding wireless device; and

storing in said database said information corresponding
to said first geographic location in association with said one
of said at least one user account.

20

10. The method of claim 9 wherein said associating step
comprises the step of associating a plurality of user accounts
with said supervisory account; and

said storing step comprises the step of storing in said
25 database said information corresponding to said first
geographic location in association with one of said plurality
of user accounts.

11. The method of claim 1 wherein said step of obtaining said
30 first set of coordinates includes the steps of:

storing in a database a location identifier associated
with said first geographic location; and

converting said location identifier corresponding to said first geographic location into said first set of coordinates in said specified coordinate system and storing said first set of coordinates in said database.

5

12. The method of claim 11 wherein said location identifier comprises an address and said storing step comprises the step of storing said address in said database

10 13. The method of claim 11 wherein said database is communicably coupled to a first server and said converting step comprises the steps of:

retrieving said location identifier from said database;

forwarding said location identifier to a location server;

15 converting said location identifier into said first said of coordinates at said location server; and

forwarding said first set of coordinates to said first server for storage in said database.

20 14. The method of claim 1 further including the steps of:

storing in a database a time specification,

utilizing said time specification and location information corresponding to said first geographic location to determine whether to permit said attempted communication involving said wireless device and said other communication device.

25 15. The method of claim 14 wherein said time specification comprises a time period and said utilizing step comprises the step of determining whether a current time is within said time period.

30

16. The method of claim 14 wherein said time specification comprises at least one day of the week and said utilizing step comprises the step of determining whether a current day of the week matches said at least one day of the week.

5

17. The method of claim 14 wherein said time specification includes at least one date specification and said utilizing step comprises the step of determining whether a current date matches said at least one date specification.

10

18. The method of claim 1 further including the step of:
forwarding said control message to an external device;
and

determining at said external device, based on said
15 control message, whether said attempted communication should be completed or terminated.

19. The method of claim 1 wherein said step of obtaining said second set of coordinates in said specified coordinate system
20 comprises the step of obtaining said second set of coordinates from a global positioning system receiver disposed in said wireless device.

20. The method of claim 19 further including the steps of:
25 communicating said first set of coordinates to said wireless device and retrievably storing said first set of coordinates in a memory in said wireless device, wherein said memory is in communication with a processor within said wireless device; and

30 responsive to the initiation of a communication from said wireless device to said other communication device:

retrieving said first set of coordinates from said memory using said processor within said wireless device;

performing said determining step within said processor utilizing said retrieved first set of coordinates and said second set of coordinates obtained from said global positioning system receiver; and

5 responsive to said performing of said distance determining step by said processor within said wireless phone, determining in said processor whether to prevent said communication from said wireless device to said other communication device.

10 21. The method of claim 1 further including the steps of:
responsive to said attempted communication involving said wireless device and said other communication device by one of said wireless phone and said communication device;

15 retrieving at least one cell sector identifier associated with the geographic location of said wireless phone;

forwarding said at least one cell sector identifier to a location server; and

20 generating said second set of coordinates within said location server based upon said retrieved at least one cell sector identifier.

22. The method of claim 21 wherein said cell sector
25 identifier retrieving step further includes the step of retrieving a signal strength that is associated with each of said at least one cell sector identifier, wherein said forwarding step includes the step of forwarding said signal strength associated with each of said at least one cell sector
30 identifier to said location server with the respective cell sector identifier; and

said second set of coordinates generating step comprises the step of generating said second set of coordinates from said

at least one cell sector identifier and the signal strength associated with each of said at least cell sector identifier.

23. A system of controlling the usage of a wireless device
5 comprising:

a storage device containing a user profile database, said user profile database storing a first set of coordinates representative of a first geographic location;

at least one first processor in communication with said
10 user profile database, said at least first processor operative in response to an attempt to establish a communication involving said wireless device and another communication device:

to obtain a second set of coordinates representative
15 of a second geographic location corresponding to a geographic location of said wireless phone;

to determine based upon said first and second set of coordinates whether said wireless device is at a location at which use of the wireless device is restricted;

20 to generate a control message of a first type in the event said determining step indicates that said wireless device is at a location at which the use of the wireless device is restricted; and

to generate a control message of a second type in
25 the event said determining step indicates that said wireless device is at a location at which the use of the wireless device is not restricted and to utilize said distance in the determination whether the use of said wireless device is restricted.

30

24. The system of claim 23 wherein said at least one first processor is operative to determine a distance between said second geographic location specified by said second set of

coordinates and said first geographic location specified by
said first set of coordinates and to generate said control
message of said first type in the event said distance is less
than a specified distance value and to generate said control
5 message of said second type if said distance is greater than
said specified distance value.

25. The system of claim 23 further including a wireless
device having a global positioning system receiver disposed
10 therein, said global positioning system operative to generate
said second set of coordinates representative of the geographic
location of said wireless phone.

26. The system of claim 25 wherein said wireless device
15 includes logic operative to forward said second set of
coordinates to said at least one first processor for use in the
determination of whether the wireless device is at a location
at which the use of the wireless device is restricted.

20 27. The system of claim 23 wherein said user profile database
further includes a location identifier associated with said
first geographic location, said system further including a
converter operative to generate said first set of coordinates
from said location identifier.

25 28. The system of claim 27 wherein said location identifier
comprises an address.

29. The system of claim 27 wherein said converter comprises a
30 location server.

30. The system of claim 23 wherein said at least one first
processor in communication with said user profile database is

operative to calculate a distance between said first and second geographic locations using said first and second sets of coordinates and to generate a message indicating that said attempted communication should be prevented in the event the distance between the first and second geographic locations is less than a predetermined threshold distance.

31. The system of claim 23 wherein said at least one first processor in communication with said user profile database is operative;

to retrieve at least one cell sector identifier indicative of the location of said wireless device;

to forward said at least one cell sector identifier to a location server; and

to receive from said location server said second set of coordinates.

32. The system of claim 31 wherein said at least one first processor in communication with said user profile database is further operative;

to retrieve at least one signal strength value associated with at least some of said cell sector identifiers;

to forward to said location server, said at least one cell sector identifier and the associated signal strength value; and

to receive from said location server said second set of coordinates derived from said at least one cell sector identifier and the associated signal strength value.

33. A system of controlling the usage of a wireless device comprising:

a supervisory control system comprising:

a storage device containing a user profile database,
said user profile database storing a first set of
coordinates in a specified coordinate system
representative of a first geographic location; and
5 at least one first processor in communication with
said user profile database; and
a wireless device in communication with said supervisory
control system, said wireless device comprising:
a memory; and
10 at least one second processor in communication with
said memory;
said at least one first processor operative to forward
said first set of coordinates to said wireless device for
storage in said memory;
15 said at least one second processor operative in response
to an attempt to establish a communication from said wireless
device to another communication device:
to obtain a second set of coordinates in said
specified coordinate system representative of a second
20 geographic location corresponding to a geographic
location of said wireless device; and
to determine based upon said first and second set of
coordinates whether said wireless device is at a location
at which use of the wireless device is restricted;
25 to generate a control message of a first type upon a
determination that said wireless device is at a location
at which the use of the wireless device is restricted;
and
to generate a control message of a second type upon
30 a determination that said wireless device is at a
location at which the use of the wireless device is not
restricted.

34. The system of claim 33 wherein said wireless device comprises a wireless phone.

35. The system of claim 34 wherein said wireless device
5 comprises a device operative to communicate using a data messaging protocol.

36. A method of controlling communications between a
wireless communication device and another communication device
10 comprising the steps of:

storing within a database at least one parameter
corresponding to at least one restriction on use of said
wireless communication device for outgoing communications, said
at least one restriction comprising at least one of a time of
15 day restriction defining at least one time period during which
an outgoing communication from said wireless communication
device is not permitted, an accessibility restriction
comprising at least one identifier associated with another
communication device that cannot be reached from said wireless
20 communication device, and a location restriction defining at
least one location at which an outgoing communication from said
wireless communication device is not permitted;

forwarding said at least one parameter from said database
to said wireless communication device and storing said at least
25 one parameter in a memory within said wireless communication
device;

in response to an attempt to initiate a communication
from said wireless communication device to said other
communication device, retrieving said at least one parameter
30 from said memory and determining via use of a processor within
said wireless communication device, whether a connection of
said communication from said wireless communication device to

said other communication device is contrary to said at least one restriction;

in the event the connection of said communication from said wireless communication device to said other communication device is not contrary to said at least one restriction, allowing the communication between said wireless communication device and said other communication device; and

in the event the communication from said wireless communication device to said other communication device phone is contrary to said at least one restriction, preventing the communication from said wireless communication device to said other communication device.

37. The method of claim 36, wherein said communication is a telephone call, said wireless communication device comprises a wireless phone, and said other communication device is another telephone and said preventing step includes the step of outputting a predetermined message for delivery to said wireless phone indicating that said call cannot be connected due to a restriction on use.

38. The method of claim 36, wherein said accessibility restriction defining at least one identifier that cannot be reached from said wireless communication device comprises a list of identifiers associated with other communication devices that are inaccessible from said wireless communication device, said method further including the steps of:

determining whether an identifier associated with said other communication device is included in said list of identifiers; and

in the event said identifier is included in said list of identifiers, preventing said communication from being completed.

39. The method of claim 37, wherein said predetermined message indicates that said other communication device associated with said identifier is inaccessible.

5

40. The method of claim 36, further including the step of:

determining whether an identifier corresponding to said other communication device is included in a list of identifiers that can always be reached; and

10 in the event the connection of said communication is contrary to a use restriction comprising one of said time, date and location restriction, and said identifier corresponding to said other communication device is included in said list of identifiers corresponding to other communication devices that
15 can always be reached, allowing said communication between said wireless communication device and said other communication device to proceed.

41. The method of claim 36, wherein said wireless communication
20 device comprises a wireless phone, said other communication device comprise another phone, said communication is a call from said wireless phone to said other phone, the method further including the steps of:

determining whether a predetermined allocation of time
25 for a specified control period associated with said wireless phone has been fully depleted;

determining whether an identifier corresponding to said other phone is included in a list of identifiers associated with other phones that may always be called; and

30 in the event said predetermined allocation of time associated with said wireless phone has been fully depleted and said identifier corresponding to said other phone is in said

list of identifier that may always be called, connecting said wireless phone to said other phone.

42. The method of claim 36 wherein said determining step
5 comprises the step of executing program code on said processor within said wireless device to determine whether the connection of said communication is contrary to said at least one restriction.

10 43. Apparatus for controlling usage of a wireless device comprising:

a first memory within said wireless device for storing at least one parameter specifying at least one restriction on use of said wireless device for outgoing communications, said at
15 least one restriction on use comprising at least one of a time of day restriction defining times during which an outgoing communication from said wireless device is not permitted, an accessibility restriction defining at least one identifier associated with another communication device that is
20 inaccessible for outgoing communications from said wireless device, and a location restriction defining at least one restricted location from which an outgoing communications from said wireless device is not permitted;

at least one processor within said wireless device;
25 a second memory operable to store program code executable on said at least one processor; and

program code stored in said second memory and executable on said at least one processor, said program code operable:

30 to detect the initiation of a communication from said wireless device to said other communication device and, responsive to said initiation, to determine whether a connection of said communication between said wireless

device and said other communication device is contrary to said at least one restriction;

5 to permit said communication from said wireless device to said other communication device in the event said connection is not contrary to said at least one restriction; and

10 to prevent said communication from said wireless device to said other communication device in the event said communication is contrary to at least one of said at least one restriction.

44. The apparatus of claim 43 wherein said first and second memories comprise different portions of the same memory.

15 45. A system for controlling usage of a wireless phone, said system operative in conjunction with a billing system including a first server operable to execute a billing process and a first database containing parameters defining billing parameters applicable to said wireless device, said system
20 comprising:

 a second server operable to execute a supervisory process for controlling usage of said wireless phone as an overlay to said billing process;

25 a second database containing a value defining a time duration that said wireless device may be used within a predetermined period, said second database being communicably coupled to said second server;

 said second server being operative:

30 to maintain a record of time usage for said wireless phone within said predetermined period;

 to prevent a call involving said wireless phone from being connected in the event said record of time usage indicates that said wireless phone has been used within

said predetermined period for a period equal to said time duration; and

to allow a call involving said wireless phone to be connected in the event said record of time usage indicates that said wireless phone has been used in said predetermined period for a period less than said time duration.

46. The system of claim 45 wherein said first and second servers comprise a single server operative to execute said billing process and said supervisory process.

47. The system of claim 45 wherein said first database and said second database comprise portions of a single database.

48. The system of claim 45 wherein said predetermined period comprises a calendar month and said value comprises a specified number of minutes.

49. The system of claim 45 wherein said second database includes an always accessible number associated with another communication device that may always be called by said wireless phone and said second server is operative to exclude time involving calls between said wireless phone and said other communication device from said record of time usage.

50. A computer based method of controlling the use of a wireless device comprising the steps of:
storing in a database a supervisory account identifier associated with a supervisory account, said supervisory account including information pertaining to the use of at least one wireless device including said wireless device, said

information being password protected and at least some of said information being modifiable by said account administrator;

storing in said database in association with said supervisory account identifier at the request of said account administrator, a wireless device identifier associated with
5 said wireless device and at least one modifiable restriction governing the use of said wireless device by a wireless device user, wherein said wireless device user is an individual distinct from said account administrator;

10 storing in said database in association with said supervisory account identifier, a code value corresponding to a cut-through code, wherein said code-value is useable by said account administrator to permit said account administrator to establish communication with said wireless device at a time
15 when the use of said wireless device is restricted;

receiving an indication of an intended communication from a communication device to said wireless device;

determining whether said intended communication violates said at least one restriction governing the use of said
20 wireless device prior to connection of said communication between said communication device and said wireless device;

in the event said determining step indicates that the connection of said intended communication violates said at least one restriction and an input value corresponding to said
25 stored code value is not received from said communication device within a predetermined time interval, generating a control message of a first type to prevent said communication from proceeding; and

in the event said determining step indicates that the
30 connection of said intended communication would violate said at least one restriction pertaining to the use of said wireless device and said input value corresponding to said code value code is received from said communication device within said

predetermined time interval, generating a control message of a second type to allow said communication to be proceed.

51. The method of claim 50 wherein said step of storing said
5 code value corresponding to said cut-through code comprises the step of storing in said database a user name and utilizing a value corresponding to said user name as said code value.

52. A computer based system for controlling the use of a
10 wireless device by a wireless device user, said system comprising:

a database stored in a storage device, said database containing a supervisory account identifier associated with a supervisory account, said database including information
15 pertaining to the use of at least one wireless device, including said wireless device, said information contained in said database being password protected and modifiable by a supervisory account administrator;

said database containing in association with said
20 supervisory account identifier, a wireless device identifier associated with said wireless device and at least one parameter defining at least one restriction governing the use of said wireless device by said wireless device user, wherein said wireless device user is an individual distinct from said
25 account administrator;

said database a code value corresponding to a cut-through code, wherein said code value is stored in association with said supervisory account identifier and wherein said code-value is useable by said account administrator to establish
30 communication with said wireless device at a time when the use of said wireless device is restricted;

at least one computer operative to:

receive an indication of an intended communication from a communication device to said wireless device;

5 determine using said at least one parameter whether said intended communication violates said at least one restriction governing the use of said wireless device prior to connection of said communication between said communication device and said wireless device;

10 generate a control message of a first type to prevent said communication from proceeding in the event said at least one computer determines that the connection of said intended communication would violate said at least one restriction and an input value corresponding to said stored code value is not received from said communication device within a predetermined time interval; and

15 generate a control message of a second type to allow said communication to proceed in the event said at least one computer determines that the connection of said intended communication would violate said at least one restriction pertaining to the use of said wireless device and said input value corresponding to said code value code is received from said communication device within said predetermined time interval.

53. The system of claim 52 further including:
25 an access point and a web server communicably coupled via a data network;

a data path between said web server and said database;
said access point operative to receive as an input from said supervisory account administrator a user name and to
30 communicate said user name to said database;

said database operative to store said user name in association with said supervisory account identifier; and

said at least one computer being operative to utilize said user name stored in said database as said code value.

54. The system of claim 53 wherein said data path includes
5 said at least one computer.

55. A method of communicating information regarding the usage of a wireless device comprising the steps of:

10 storing in a database an identifier of said wireless device in association with an identifier associated with a supervisory account, wherein information in said database pertaining to said supervisory account is modifiable by a supervisor having administrative responsibility for said supervisory account;

15 storing in said database in association with said wireless device identifier at least one parameter defining at least one alert condition relating to the usage of said wireless device;

20 maintaining for said at least one wireless device a time measure indicative of the cumulative usage of said wireless device within a control period;

determining whether said alert condition has occurred by utilizing said time measure and said at least one parameter; and

25 in the event said determining step indicates that said alert condition has occurred, communicating an alert message to said supervisor.

30 56. The method of claim 55 wherein said at least one parameter includes a time value defining the amount of time said wireless device may be used prior to the transmission of said alert message to said supervisor.

57. The method of claim 56 wherein said communicating step further includes the step of communicating said alert message to said supervisor when said determining step indicates that said time measure equals said time value.

5

58. The method of claim 56 wherein said communicating step further includes the step of communicating said alert message to said supervisor each time said determining step indicates that said time measure equals an integral multiple of said time value within said control period.

10

59. The method of claim 58 further including the step of resetting said time measure at the beginning of each control period.

15

60. The method of claim 55 wherein said communicating step comprises the step of communicating said alert message to said supervisor via an audible message directed to a telephone number specified by said supervisor and stored in said database.

20

61. The method of claim 55 wherein said communicating step comprises the step of communicating said alert message to said supervisor via a text message directed to a telephone number specified by said supervisor and stored in said database.

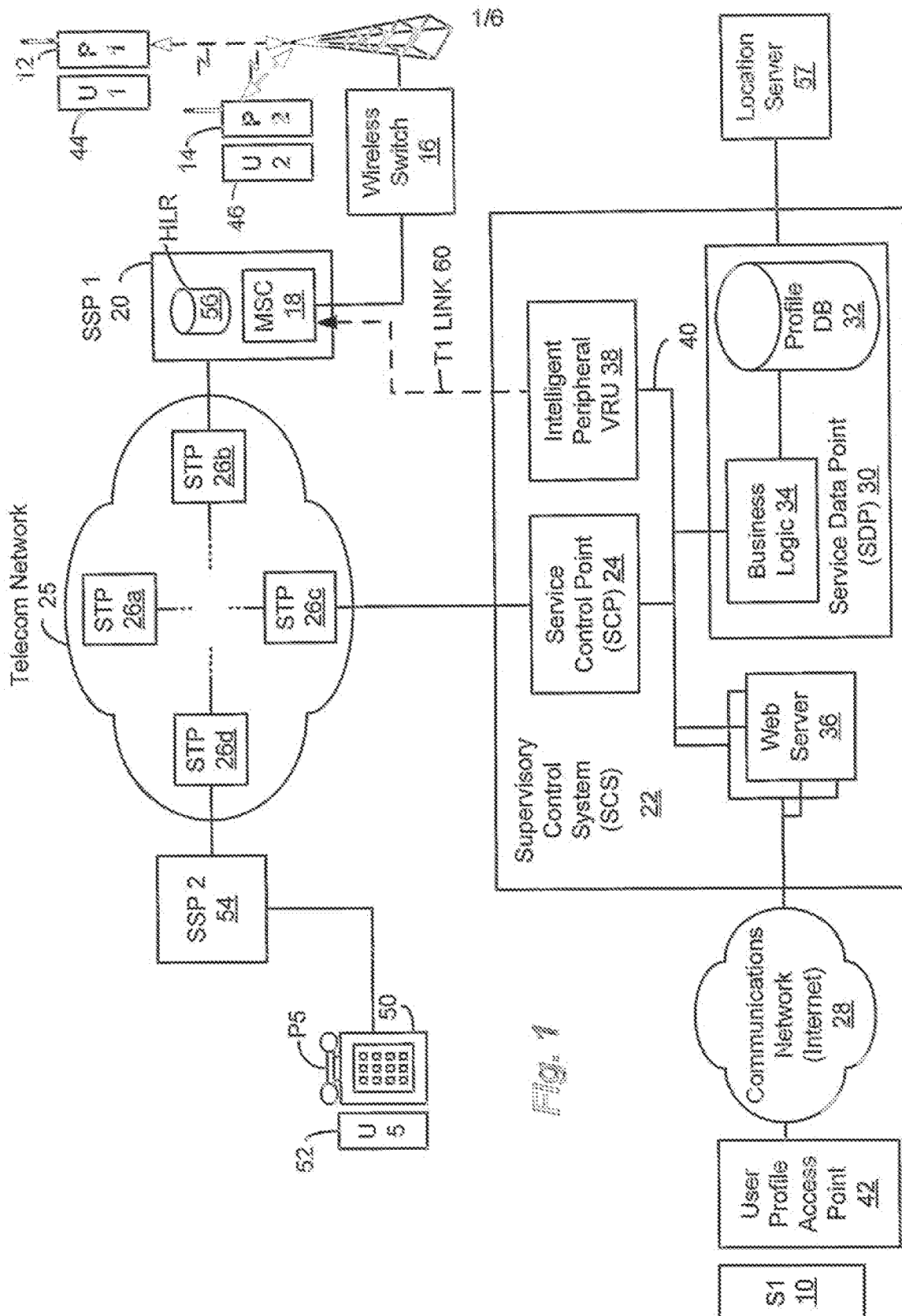
25

62. The method of claim 55 wherein said communicating step comprises the step of communicating said alert message to said supervisor via an email message directed to an email address specified by said supervisor and stored in said database.

30

63. The method of claim 55 wherein said alert message includes an indication of said measure indicative of said

cumulative usage of said wireless device within said control period.



2/8

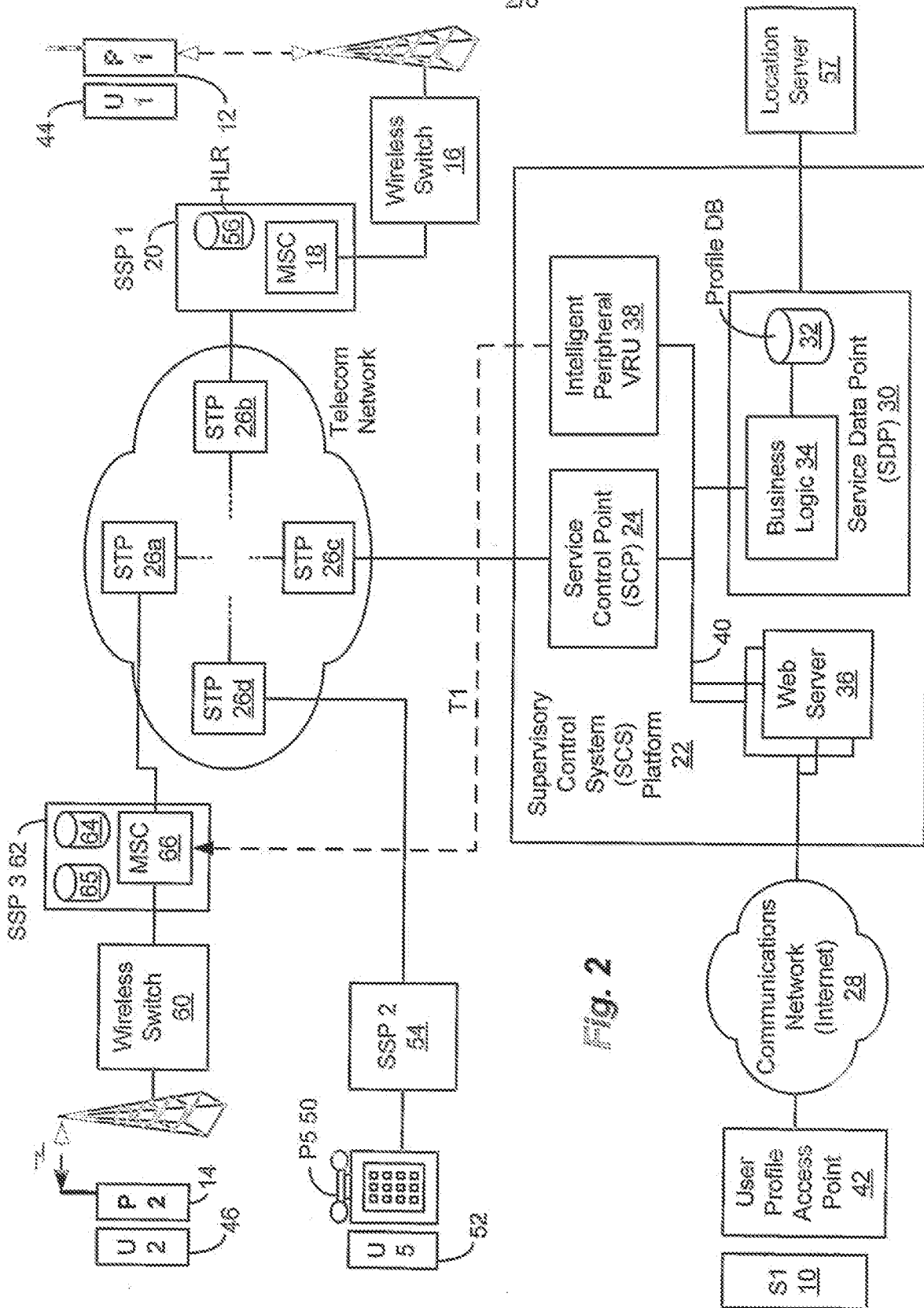
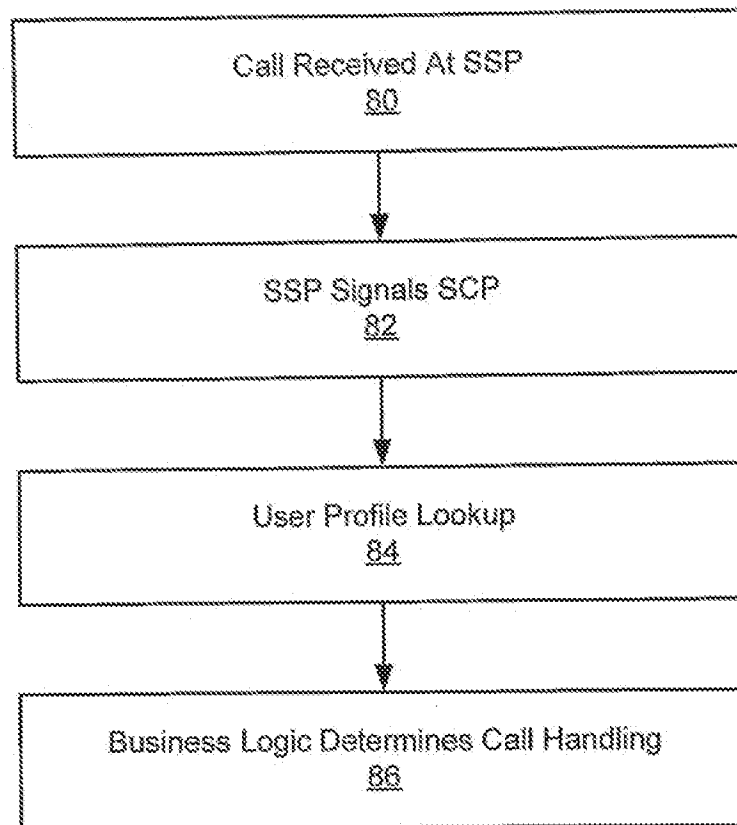
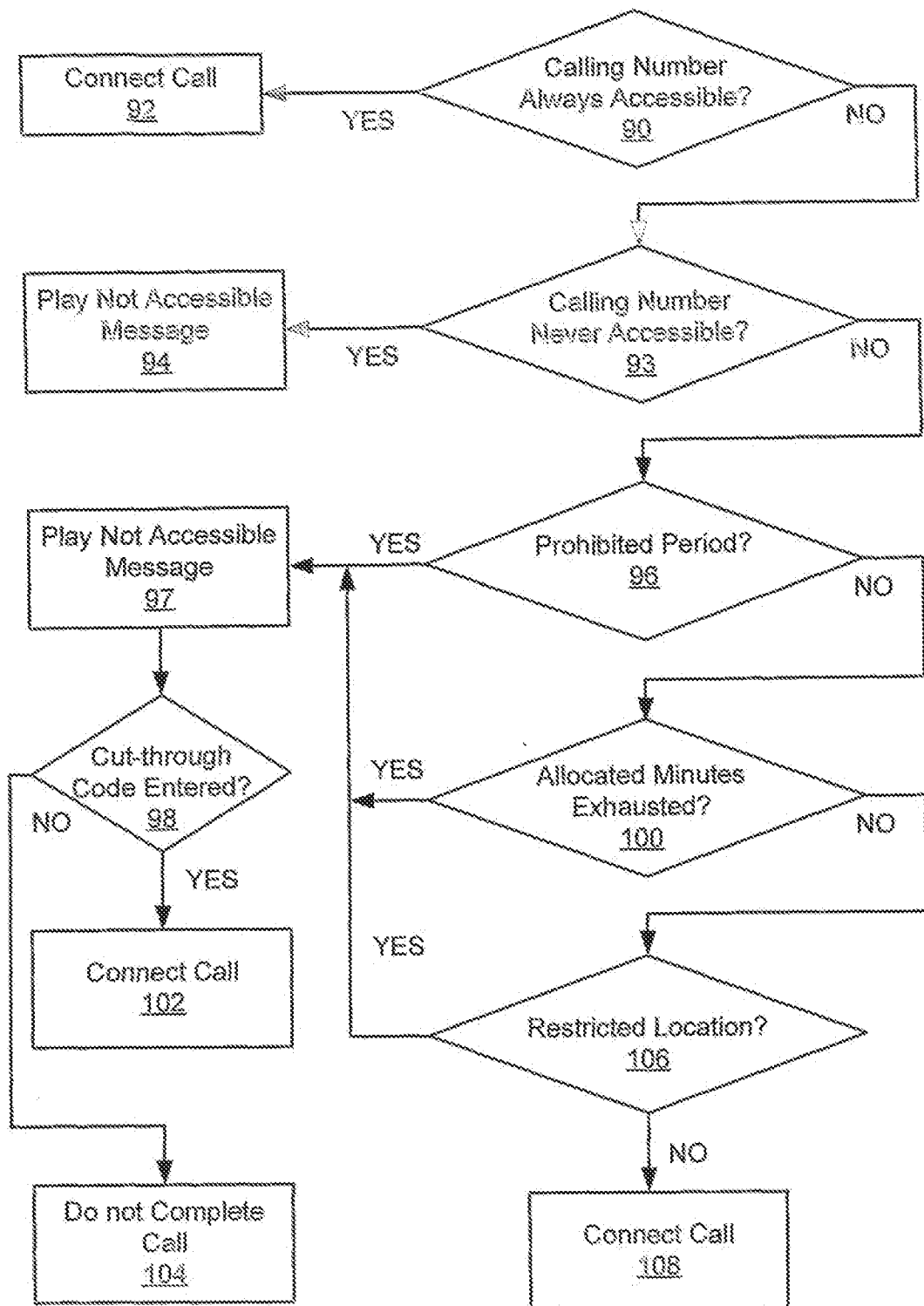


Fig. 2

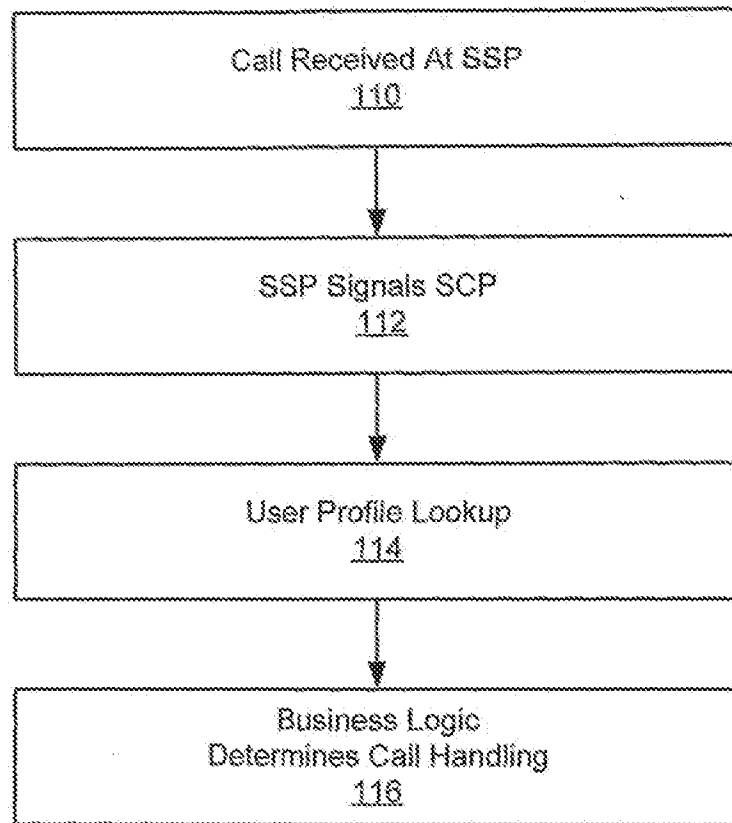
3/6

**Fig. 3**

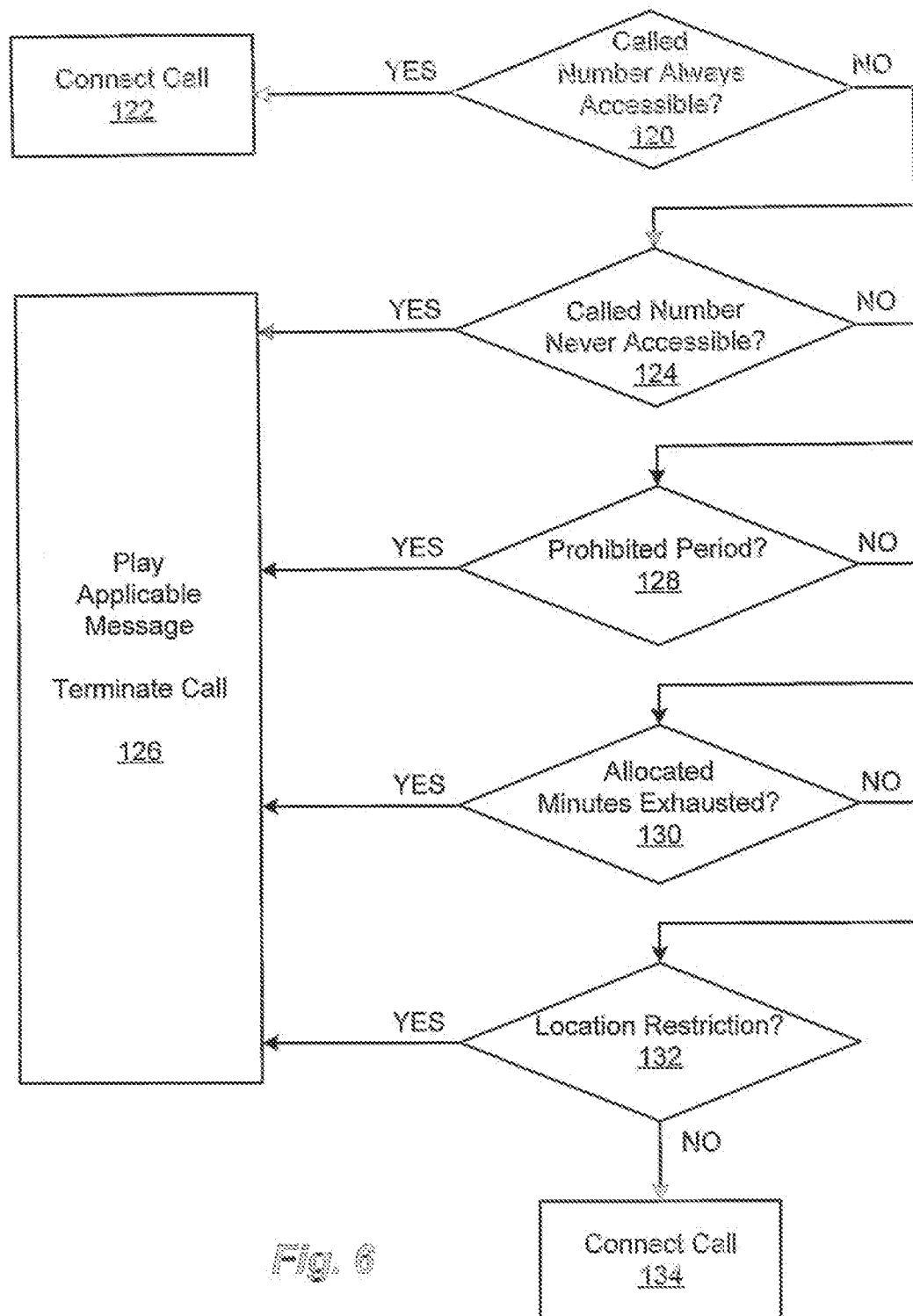
4/6

**Fig. 4**

5/6

**Fig. 5**

6/6

*Fig. 6*

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
4 November 2004 (04.11.2004)

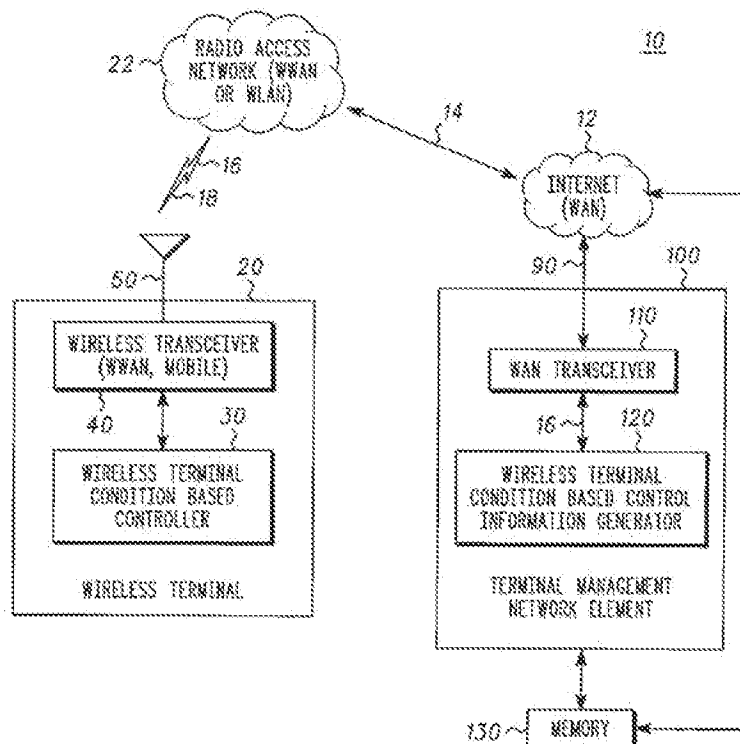
PCT

(10) International Publication Number
WO 2004/095753 A2

- (51) International Patent Classification⁷: H04L 60173 (US); VASUDEVAN, Venugopal [US/US]; 4741 Fairfax Avenue, Palatine, IL 60067 (US).
- (21) International Application Number: PCT/US2004/010070
- (22) International Filing Date: 30 March 2004 (30.03.2004)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 109418,457 17 April 2003 (17.04.2003) US
- (71) Applicant (for all designated States except US): MOTOROLA INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): ADWANKAR, Sandeep, M. [IN/US]; 1224 East Algonquin Road, #3S, Schaumburg, IL 60173 (US); NARASIMHAN, Nitya [IN/US]; 1919 Prairie Square, #304, Schaumburg, IL.
- (74) Agents: WATANABE, Hisashi, David et al.; 600 North US Highway 45, Libertyville, IL 60048 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SI, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK,

[Continued on next page]

(54) Title: A METHOD AND APPARATUS FOR MANAGING WIRELESS MOBILE TERMINALS



(57) Abstract: A method and system for managing a terminal management system including a terminal management network element (100) and at least one wireless terminal (20). The terminal management network element (100) includes a wireless terminal condition based control information generator (120) that generates wireless terminal condition based control information (20) represented by extensible markup language code. The wireless terminal condition based control information (20) includes selected action data (46) based on selectable action data (820) associated with a terminal management action to execute on at least one wireless mobile terminal (22), selected condition data (42) based on selectable condition data (840) wherein the selected condition data (42) is associated with the selected action data (46), and selected attribute data (44) based on selectable attribute data wherein the selected attribute data (44) is associated with the selected action data (46). A wireless terminal condition based controller (30) executes the terminal management action if the

selected condition (42) data associated with the terminal management action is satisfied.



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— without international search report and to be republished upon receipt of that report

A METHOD AND APPARATUS FOR MANAGING WIRELESS MOBILE TERMINALS

FIELD OF THE INVENTION

[0001] The invention relates generally to wireless communication systems, wireless terminals, and network elements, and more particularly, to the control and management of wireless terminals, and related methods.

BACKGROUND OF THE INVENTION

[0002] With the growth of wireless terminals, there is a concurrent growth with managing wireless terminal operations. Wireless terminals, such as hand-held wireless devices, including but not limited to a PDAs, cellular phone, a pager, a smart phone, and other suitable devices, are known to employ limited protocols for managing terminal operations. Wireless terminal operations include operations such as diagnostic testing and the reporting of wireless terminal functions, such as, for example, the reporting of the battery level on the wireless terminal to a network element.

[0003] For example, the Synchronization Markup Language (Synch ML) protocol allows a wireless system operator to perform single terminal management actions for immediate execution on a given wireless terminal. However, the Synch ML protocol does not allow for the performance of multiple terminal management actions at any given time, or for the conditional execution of terminal management actions, or for the delayed execution of terminal management actions. For example, the Synch ML protocol does not allow for an operator to schedule execution of wireless terminal management actions at a predetermined time or upon a condition of a terminal or network to suit different conditions relating to different attributes of a mobile terminal or a condition of the network. As a result, the Synch ML protocol does not support scheduling or conditional management control of the wireless terminal.

[0004] As another example of wireless terminal management technology, J2ME is a Java based technology providing limited management of wireless terminal operations for wireless devices and other resource-constrained devices. However, J2ME technology does not support dynamic class loading which prevents Java from being a viable solution for managing wireless mobile terminals.

[0005] Another system proposes a policy-based management network that enforces a management policy through routers in a wired network. However this system permits only "one-time" enforcement of the policy. Further, the policy in the management network addresses only one criterion. As a result, the policy is not dynamically enforceable or adaptable. Additionally, this policy-based management network executes within a router in a wired network and not in a wireless end-user device.

[0006] Other proposed systems, such as the "Simple Network Management Protocol" (SNMP), allow execution of an application based on a time of day. For example, the "cron" command in a Unix system permits the execution of a command at a particular time of day. These systems, however, are typically limited to wired networks and, additionally, require high levels of bandwidth to operate.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The present invention is illustrated by way of example and not limitation in the accompanying figures, in which like reference numerals indicate similar elements, and in which:

FIG. 1 is a block diagram of a terminal management system in accordance with one exemplary embodiment;

FIG. 2 is a block diagram of the terminal management system shown in Fig. 1 according to another exemplary embodiment;

FIG. 3 is a flow chart of a method for managing at least one wireless mobile terminal;

FIG. 4 is a block diagram of the wireless terminal of FIG. 1 shown in more detail;

FIG. 5 is a flow chart for a method of receiving data according to one exemplary embodiment;

FIG. 6 is a flow chart of a wireless terminal processing termination information and attribute data according to one exemplary embodiment;

FIG. 7 is a flow chart of a method of processing a plurality of terminal management actions according to one exemplary embodiment;

FIG. 8 illustrates a user interface for a terminal management network element according to one exemplary embodiment;

FIG. 9 is a flow chart for updating software on a wireless terminal according to one exemplary embodiment; and

FIG. 10 is a flow chart of a method for managing a terminal management network element.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0008] A communication system and method employs wireless terminals, such as wireless mobile terminals, determine that a condition associated with at least one terminal management action is satisfied based on extensible markup language code that includes at least wireless terminal condition based control information. The wireless terminal condition based control information includes at least terminal condition information and action data wherein the action data identifies at least one terminal management action associated with the wireless mobile terminal. The wireless terminal, in response to determining that a condition associated with the terminal management action is satisfied based on the received terminal condition

information, conditionally executes the terminal management action identified by the received action data.

[0009] FIG. 1 illustrates one exemplary embodiment of a communication system 10 that includes, in this example, at least one wireless terminal 20, and a terminal management network element 100. The wireless terminal 20 is coupled to the terminal management network element 100 through a radio access network such as a "wireless wide area network" or "wireless local access network" (WWAN or WLAN) 22, and a wide area network (WAN) 12, such as the internet or other suitable network. Radio access network 22 and WAN 12 are operably coupled through a suitable communication link 14, such as an Ethernet link. Radio access network 22 may be any conventional communication network for transmitting wireless terminal condition-based control information 16, such as a CDMA wireless network, 802.11(b) wireless network, 3G telecommunications system, or any suitable wireless network. Wireless terminal condition based control information 16 includes condition data for conditionally executing terminal management actions.

[0010] The wireless terminal 20 may be a mobile telephone, a personal data assistant ("PDA"), WIFI device, blue tooth compliant device, personal computer, end device, or any other suitable communication device. Wireless mobile transceiver 20 includes wireless terminal condition-based controller 30 suitably coupled to wireless transceiver 40 for communication with radio access network 22. Wireless terminal condition-based controller 30 communicates with radio access network 22 via wireless transceiver 40, antenna 50, and radio communication link 18. Wireless terminal condition-based controller 30 identifies and executes the terminal management action and the condition associated with the terminal management action. The wireless terminal condition-based controller 30 may be one or more suitably programmed

processors, such as a microprocessor, a microcontroller, a digital signal processor, and therefore includes associated memory that contains executable instructions that when executed causes the wireless terminal condition-based controller 30 to carry out the operations described herein. In addition, controller as used herein includes discreet logic, state machines or any other suitable combination of hardware, software and firmware.

[00011] Terminal management network element 100 includes wireless terminal condition-based control information generator 120 and WAN transceiver 110. WAN transceiver 110 couples wireless terminal condition-based control information generator 120 to wide area network 12 via WAN interface 90. Terminal management network element 100 may be any suitable network element, such as but not limited to a computer, such as a personal computer, server, or plurality of computers or servers.

[00012] FIG. 2 illustrates the communication system 100 as shown in the embodiment of FIG. 1 in more detail. Wireless terminal 20 receives wireless terminal condition-based control information 16 that includes at least terminal condition information 26 and action data 46 associated with a terminal management action. Terminal condition information 26 includes condition data 42 and attribute data 44. Wireless terminal condition-based controller 30 is coupled to input/output "I/O" interface 32 and memory 34. Input/output interface 32 is coupled to exemplary wireless terminal interface battery 36, exemplary action data for terminal management action 28, and an other 38 wireless terminal attribute interface data.

[00013] FIG. 3 illustrates one example of a method 300 for managing the operation of wireless terminal 20 in FIG. 1. At block 310, the wireless terminal 22 determining that a condition associated with at least one terminal management action is satisfied based on extensible markup language code that includes at least wireless terminal condition-based control

information 24 that includes at least terminal condition information 26 and action data 46, wherein the action data 46 identifies at least one terminal management action. The terminal management action performs terminal management operations on the wireless terminal 22, such as asset management, configuration management, fault management, and performance management. As shown in block 320, the wireless terminal conditionally executes the terminal management action identified by the received action data 46. The condition associated with the terminal management action may be an attribute and a condition associated with the wireless mobile terminal, such as a 25% battery level or an 847 area code.

[00014] Referring to memory 130 as shown in FIG. 2, instructions executable by a processor may be stored in memory 130 in order to cause the processor to perform the method 200 described in FIG. 3. These instructions executable by a processor include receiving the extensible markup language code that includes at least wireless terminal condition-based control information. As previously stated, the wireless terminal condition-based control information includes at least terminal condition information and action data where the action data identifies at least one terminal management action associated with the wireless mobile terminal. The instructions executable by the processor may conditionally execute the terminal management action identified by the action data in response to determining that a condition associated with the terminal management action is satisfied, based on the terminal condition information.

[00015] FIG. 4 illustrates the wireless terminal condition-based terminal controller 30, including a synch engine 410, and including a command parser 400, coupled to a policy engine 420, and GUI 416. Command parser 400 is coupled to the wireless transceiver 40 to receive the wireless terminal condition-based control information 16. Command parser 400 parses the terminal condition information 16, and action data 46 associated with the wireless terminal

action and identifies attribute data 44 associated with the action data 46 and condition data 42. In one embodiment, the condition data 42 includes a condition associated with an attribute such as less than, greater than, and equal to. The attribute field may be a threshold level for performing a comparison.

[00016] Command parser 400 is coupled to GUI 416 (Graphical User Interface) via sync engine adapter 412 to send and receive information to a user. Information sent to the user may include, for example, queries, prompts and messages sent to the user via a display on the GUI 416 of wireless terminal 22. The GUI 416 may also provide information to the wireless terminal 20 via the sync engine adapter 412 by providing information input by the user, such as a message, and data input via a keyboard on the wireless terminal 22.

[00017] As shown in FIG. 4, wireless terminal condition-based controller 30 includes a policy reader 430 coupled to the command parser 400 to read the action data 46, attribute data 44 and condition data 42 associated with the terminal management action 410. An attribute monitor 440 is coupled to the policy reader 430 to receive attribute data 44. Attribute monitor 440 is also coupled to input/output interface 32 to monitor current terminal attribute values 460 in response to the attribute monitor 440 receiving attribute data 44. Task manager 450 is coupled to the policy reader 430 and to the attribute monitor 440 to compare the current terminal attribute values 44 from the attribute monitor 440 with the received condition data 42 from the policy reader 430 to determine if the condition data 42 is satisfied. In order to perform this comparison, the attribute monitor 440 may receive current terminal attribute values 460 through: a polling event, an interrupt event, a predetermined time of day trigger event, or a predetermined period of elapsed time trigger event. For example, wireless terminal condition-based controller 30 may include one or more processors to, for example, poll the input/output interface 32 in order to

obtain the received current terminal attribute values 460. Alternatively, an interrupt event may be used to obtain current terminal attribute values 460 from input/output interface 32.

[00018] In one embodiment, the task manager 450 schedules a current terminal management action to execute, according to whether a previous terminal management action is completed. For example, the terminal management action may be a timed terminal management type of action wherein execution of the terminal management action is scheduled for a particular time of day. Alternatively, the current terminal management action schedule may be a periodic type of task. According to one exemplary embodiment, a current terminal management action is started only after a previous terminal management action is completed similar to a cron function on a UNIX operating system.

[00019] FIG. 5 is a block diagram for receiving a payload at block 510 with wireless terminal condition-based control information 16 represented by extensible markup language code for a terminal management action. Command parser 400 reads wireless terminal condition-based control information 24 from a payload at block 520, for identifying the terminal condition information 26 and action data 46 associated with the terminal management action. In this embodiment, the parser 400 of wireless terminal condition-based controller 30 reads attribute data 44 associated with the action data 46 from the terminal condition information 26, as shown in block 530. Additionally, at block 540, parser 400 reads condition data 42, associated with the attribute data 44.

[00020] In one embodiment, a terminal management action may be a battery-level guard operation that specifies a command for fetching an attribute such as the battery level from the wireless terminal 22. For example, the battery-level guard command may prevent execution of the terminal management action specified by the action data if the battery level on the terminal is

below 25%. In this embodiment, the attribute of the terminal management action is the battery level, the condition is greater than 25%, and the action data represents a terminal management action for fetching a current terminal attribute value for the battery level.

[00021] Examples of the terminal condition information associated with the terminal management action include a wireless terminal state (i.e., battery level as previously described) or a network state. For example, a network operator may want to run an automated test where all phones in the 847 area code receive a terminal management action, such as a test of wireless terminal functions. The operator may further want to execute the test on the first 100 mobiles to respond during off-peak hours so as not to drain terminals that are running low on batteries. Therefore, the network state may be the number of cell phones in the 847 area code running the requested terminal management action. The attribute therefore may be the test represented by the terminal management action. Other examples of terminal condition information include a duration since the last terminal management action occurred, a number of action repetitions, a completion of a terminal management action, a software upgrade, a time of day, a terminal management action schedule, a wireless application protocol (WAP) configuration, a user setting, a signal level, a battery level, and terminal location coordinates.

[00022] The wireless terminal condition-based control information 16, as shown in FIGs. 1 and 2, may be transmitted using extensible markup language code. In one embodiment, for example, the extensible markup language code may be based on the Sync ML communications protocol described at www.syncml.org. However, any extensible markup language code may be used such as SMG, HTTP and XML.

[00023] Further, the extensible markup language code may include an assert command, a schedule command, and a perform command. The assert command may associate the terminal

condition information 16 (condition data 42, and attribute data 44) with the received action data 46, and may also associate the terminal condition information 26 with exception action data if the condition data is not satisfied. For example, the assert command may cause the terminal management action to execute in the event the condition data is not satisfied. In another example of the assert command, the terminal management action may be a diagnostic test such as a test to determine if the browser is functioning properly. If the test results indicate that the browser is not functioning, then the browser may be automatically configured by, for example, configuring the WAP settings on the browser.

[00024] The schedule command may associate the terminal condition information with data such as a time of day, a time interval between successive executions of the terminal management action, a number of repetitions to execute the terminal management action, a repetition rate for executing the terminal management action, and a first run of a scheduled execution of a terminal management action. In one example, a terminal management action may be postponed for execution at a particular time. In another example, scheduling may take the form of monitoring, measuring and reporting an elapsed period of time to perform a terminal management action, such as downloading a web page. The wireless terminal may measure the amount of time a web page takes to download over a period of time and for a number of occurrences and report these measurements to the operator for statistical analysis.

[00025] The perform command associates an attribute value such as a network attribute value, or a locally obtained attribute value associated with the wireless mobile terminal, and action data. For example, the perform command performs a non-local service action, such as a "get" terminal attribute value. Accordingly, an operator may use this command to measure service performance on a wireless mobile terminal.

[00026] FIG. 6 is a block diagram for one embodiment of a method 600 to manage at least one wireless mobile terminal. The wireless terminal 20 receives attribute data 44 (i.e., via the command parser 400) associated with the action data at block 610. Condition data 42 associated with the attribute data 44 is received at block 620. The attribute monitor 440 receives locally obtained current terminal attribute values 460 (i.e., via the input/output interface 32) at block 630. As previously stated, the task manager 450 compares the locally obtained current terminal attribute values 460 with the received condition data 42 to determine if the condition data 42 is met at block 640. Optionally, for example, task manager 450 schedules a current terminal management action to conditionally execute, according to whether a previous terminal management action is completed. In this embodiment, the task manager 450 conditionally executes the current terminal management action if the condition data associated with the terminal management action is met. In one exemplary embodiment, the condition data 42 requires that a previous terminal management action is executed at step 670 before the current terminal management action is executed. Since in this embodiment a current terminal management action may be scheduled to perform at a time in the future, the condition of the current terminal attribute values 460 may change by the time the current terminal management action is executed. Accordingly, the current terminal attribute values 460 may be updated at step 660 in order to determine if the condition data is still satisfied at that time.

[00027] FIG. 7 is a block diagram of a method for managing multiple terminal management actions on a wireless terminal 22. The parser 400 at block 710 receives terminal condition information and action data associated with multiple corresponding terminal management actions. Accordingly, each of the multiple action data 46 identifies a corresponding terminal management action. As shown in block 720, the multiple terminal condition

information includes multiple attribute data 44 associated with corresponding action data 46. The terminal condition information includes condition data 42 associated with corresponding attribute data 44.

[00028] Attribute monitor 440 receives current terminal attribute values 460 at block 740 in response to the attribute monitor 440 receiving the multiple attributes for each corresponding terminal management action. At block 750, in one embodiment, the task manager 450 schedules each terminal management action for execution in accordance with the condition data 42. At step 760, task manager 450 compares each current terminal attribute value with the corresponding received-condition data 42 to determine if the condition data 42 is met. If the terminal management action is executed at a later time, then the current terminal attribute values 460 may be updated, if necessary at block 760, to determine whether the current terminal attribute value 460 reflects the state of the attribute. The task manager 450 at block 770 conditionally executes each of the multiple terminal management actions if the condition data 42 associated with the corresponding terminal management action is satisfied. In one embodiment, the condition data 42 requires that a previous terminal management action is executed.

[00029] FIG. 8 illustrates a selectable terminal management action window 800 for the terminal management network element 100, as shown in FIG. 1. As previously stated, the wireless terminal condition-based control information generator 120 generates extensible markup language code that includes wireless terminal condition-based control information 16. This may be generated by an operator through the selectable terminal management action window 800, as shown in FIG. 8. For example, a user may select a type of terminal management action from options displayed on a window menu, as shown in FIG. 8, to perform terminal management operations within the terminal management categories such as (i) performance management,

(ii) asset management, (iii) configuration management, and (iv) fault management. Accordingly, an operator may select one of these terminal management actions from the selectable terminal management action window. As a result, the wireless terminal condition-based control information generator 120 generates selected action data 820 based on the selectable action data associated with a terminal management action for at least one wireless mobile terminal.

[00030] Once a selection is made from the selectable terminal management action window 810, in one embodiment, a selectable condition pull-down window may then be presented to the user for selection of the desired condition associated with the selected action. The wireless terminal condition-based control information generator 120 then generates selected condition data based on the selectable condition data where the selected condition data is associated with the selectable action data. Similarly, a user may select an attribute associated with the desired action through a selectable device attribute pull-down menu window 850. Accordingly, the wireless terminal condition-based control information generator 120 produces selected attribute data based on the selectable attribute data wherein the selected attribute data is associated with the selectable action data. Once the selected action data, selected condition data, and the selected attribute data are identified through, for example, an operator making appropriate selections through the user interface, as shown in FIG. 8, then the wireless terminal condition-based control information generator 120 may generate the extensible markup language code for identifying the wireless terminal base control information.

[00031] In another embodiment, the wireless terminal condition-based control information generator 120 generates multiple terminal management actions defined by corresponding action data. As previously discussed with respect to the execution of multiple terminal management actions in a wireless terminal 22, the execution of a first terminal management action may be

conditioned on the execution of a second terminal management action. In another embodiment, as previously discussed with regards to running tests on wireless terminal devices within the 847 area code, the operator may desire to stop execution of the test when, for example, the first 100 mobile terminals have responded with test results to the terminal management network element 100. In this example, the terminal management network element 100 may transmit a network attribute value to the wireless terminal 22 in order to allow the task manager in each respective wireless terminal 22 to compare the network attribute value with the selected condition data to determine if the selected condition is met. For example, the network attribute value may be a current number of responses under 100, such as 82. The task manager will then compare the network attribute value 82 with the condition data 100 in order to determine if the first 100 wireless mobile telephone devices have completed the test in this example. Since in this example the network attribute value 82 is less than the condition data 100, the condition data is not satisfied, and the terminal management action continues execution.

[00032] In another embodiment, as shown in FIG. 9, during session setup as shown in block 910, the wireless terminal determines if multiple terminal management actions are in operation. At block 920, the wireless terminal determines if a terminal management action is currently pending. If the wireless terminal has a pending terminal management action, then the terminal management network element 100 sends the wireless terminal condition-based control information to the wireless terminal at block 930. If there is no pending task at block 940, then the wireless terminal condition-based control information is not sent to the wireless mobile terminal. In this way, the terminal management network element 100 can determine if the wireless terminal condition-based control information is required to be sent to the wireless mobile terminal.

[00033] FIG. 10 illustrates a method 1000 for managing at least one wireless terminal on a terminal management network element. At block 1010 the terminal management network element 100 presents selectable action data associated with a terminal management action for selection by a user, such as through the selectable terminal management action window 810 of FIG. 8. The wireless terminal condition-based control information generator 120 presents selectable condition data associated with a terminal management action at block 1020 where the selected condition data is associated with the selected action data. At block 1030, the terminal management network element 100 presents selectable attribute data associated with the selectable action data where the selected attribute data is associated with the selected action data. The selected condition data, selected action data, and selected device attribute data is received by the wireless terminal condition-based control information generator 120 at block 1040.

[00034] Optionally, if the operator desires that the terminal management actions are executed according to a schedule, the operator selects the condition data to reflect the desired schedule at step 1050. The wireless terminal condition-based control information generator 120 generates the wireless terminal condition-based control information according to the selected action data, the selected condition data, and the selected attribute data, wherein the wireless terminal condition-based control information is represented by extensible markup language code for at least one wireless terminal at block 1060. According to one embodiment, the wireless terminal for the extensible markup language code for at least one wireless mobile terminal, including the wireless terminal condition-based control information, may be stored into a storage medium such as a CD rom, magnetic tape, any optical type of storage medium at step 1070.

[00035] Although, for purposes of illustration, the wireless terminal condition-based control information was described with reference to the Sync ML protocol, any appropriate

communication protocol or extension of protocol, such as J2ME or SNMP may be used. In addition, terminal management operation of a wireless terminal may be performed in any other way, so that terminal management actions may be associated with conditions such as condition data. Other advantages will be recognized by those with ordinary skill in the art.

[00036] In one embodiment, the system and method described may be incorporated as an extension of the existing SyncML terminal management protocol in a non-invasive manner. For example, the extension information, such as the condition data, attribute data, and action data (i.e. wireless terminal based condition based control information) may be incorporated into the existing SyncML payload. These extensions to the existing SyncML payload are completely transparent to existing SyncML systems. As a result, systems capable of receiving the extension information will extract and interpret the extension information, while older systems will merely discard the extension information without error. Additionally, the extension to the existing SyncML protocol is extensible, and can therefore be easily customized or enhanced to address new requirements and criteria.

[00037] The system and method allows an operator to control the management functions of wireless mobile terminals individually on a per-terminal basis rather than by enforcing a management function on all terminals. Additionally, since the responsibility for terminal management execution and for the execution of multitasking multiple terminal management actions occurs within the wireless terminal 20 rather than in the terminal management network element 100, execution of a terminal management action is more likely to execute successfully. Since execution of the terminal management action on the terminal management network element 100 may be interrupted or aborted if the radio access network 22 becomes unavailable, processing of the terminal management actions by the wireless terminal 20 would be

independent of the radio access network 22. As a result, reliability is improved because the wireless terminal executes the terminal management actions independently from the terminal management network element 100, even if access to the radio access network 16 is unavailable (i.e. in an area without signal).

[00038] Another advantage includes the ability of the wireless terminal 22 to be self-adaptive to reflect changes on the specific terminal. Other advantages include a reduction in bandwidth for performing terminal management actions on the wireless terminal 20 rather than on the terminal management network element 100. As a result, high data rate communication over the radio access network 22 for performing the terminal management operation is not required, and therefore, a reduction in communication bandwidth is realized. Consequently, the cost and effort associated with wireless terminal management is reduced.

[00039] It should be understood that the implementation of other variations and modifications of this invention and its various aspects will be apparent to those of ordinary skill in the art, and that the invention is not limited by specific embodiments described. It is therefore contemplated to cover by the present invention, any and all modifications, variations, or equivalents that fall within the spirit and scope of the basic underlying principles disclosed and claimed herein.

WE CLAIM:

1. A method in a wireless terminal comprising:

determining that a condition associated with at least one terminal management action is satisfied based on extensible markup language code that includes at least wireless terminal condition based control information that includes at least terminal condition information and action data wherein the action data identifies the at least one terminal management action associated with the wireless terminal; and

executing conditionally, by the wireless terminal, the terminal management action identified by the received action data.

2. The method of claim 1 wherein determining that the condition associated with at least one terminal management action is satisfied based on extensible markup language code that includes at least wireless terminal condition based control information includes: attribute data associated with the action data; and condition data associated with the attribute data.

3. The method of claim 2 comprising:

obtaining current terminal attribute values in response to the received attribute data at the wireless terminal; and

comparing the obtained current terminal attribute values to the condition data to determine if the condition data is met.

4. The method of claim 2 comprising:

scheduling a current terminal management action to conditionally execute according to whether a previous terminal management action is completed; and

conditionally executing the current terminal management action if the condition data associated with the current terminal management action is met wherein the condition data requires that the previous terminal management action is executed.

5. The method of claim 1 comprising:

obtaining wirelessly received wireless terminal based control information including a plurality of action data corresponding to a plurality of terminal management actions, a plurality of corresponding attribute data associated with the corresponding plurality of action data, a plurality of corresponding condition data associated with the corresponding plurality of attribute data, and

obtaining a plurality of current terminal attribute values in response to obtaining the plurality of corresponding attribute data associated with the corresponding plurality of action data;

comparing the plurality of current terminal attribute values to the corresponding condition data to determine if the condition data is met; and

conditionally executing the plurality of terminal management actions if the condition data associated with the corresponding terminal management action is satisfied wherein the condition data requires that a previous terminal management action is executed.

6. The method of claim 1 wherein, the terminal condition information associated with the terminal management action includes data representing at least one of: a wireless terminal state, a network state, a duration since a last terminal management action occurred, a number of action repetitions, a completion of a terminal management action, a software upgrade, a time of day, a terminal management action schedule, a wireless application protocol (WAP) configuration, a user setting, a signal level, a battery level, and terminal location coordinates.

7. The method of claim 1 where the wireless terminal condition based control information includes at least one of an, assert command, schedule command, and perform command, wherein:

the assert command associates the terminal condition information with the received action data and with exception action data if the condition data is not satisfied,

the schedule command associates the terminal condition information with data including at least one of a time of day, a time interval between successive executions of the terminal management action, number of repetitions to execute the terminal management action, repetition rate of executing the terminal management action, monitoring, measuring and reporting an elapsed period of time to perform a terminal management action, and a first run of a scheduled execution of a terminal management action, and

the perform command associates action data with an attribute value including at least one of a network attribute value, and a wireless mobile terminal attribute value.

8. A wireless terminal comprising:

a wireless transceiver that receives extensible markup language code that includes at least wireless terminal condition based control information that includes at least terminal condition information and action data wherein the action data identifies at least one terminal management action associated with the wireless mobile terminal; and

a wireless terminal condition based controller, coupled to the wireless transceiver,

the wireless terminal condition based controller for:

determining whether a condition associated with the terminal management action is satisfied, based on the terminal condition information, and

executing the terminal management action identified by the action data if the condition associated with the terminal management action is satisfied.

9. The wireless terminal condition based controller of claim 8 comprising:

a command parser coupled to the wireless transceiver to parse the wireless terminal condition based control information to identify the terminal condition information and the action data associated with the terminal management action.

10. The wireless terminal of claim 9 wherein the wireless terminal condition based controller comprises:

a policy reader coupled to the command parser to read the action data, attribute data, and condition data associated with the terminal management action;

an attribute monitor coupled to the policy reader to receive attribute data from the policy reader and to obtain current terminal attribute values in response to the received attribute data; and

a task manager coupled to the policy reader and to the attribute monitor to compare the current terminal attribute values from the attribute monitor, with the received condition data to determine if the condition data is satisfied.

11. The wireless terminal of claim 10 wherein the task manager:

schedules a current terminal management action to execute according to whether a previous terminal management action is completed; and

conditionally executes the current terminal management action in accordance with the condition data associated with the current terminal management action, wherein the condition data requires that a previous terminal management action is executed.

12. The wireless terminal of claim 8 wherein the wireless terminal condition based controller comprises:

a processing device;

memory containing executable instructions that causes the processing devices to:

identify the at least wireless terminal condition based control information that includes the at least terminal condition information and the

action data wherein the action data identifies at least one terminal management action associated with the wireless mobile terminal; and

in response to determining that the condition associated with the terminal management action is satisfied based on the terminal condition information, conditionally execute, the terminal management action identified by the action data.

13. The wireless terminal of claim 8 wherein the terminal condition information associated with the terminal management action is determined at an event selected from the group consisting of a polling event, an interrupt event, a predetermined time of day, and a predetermined period of elapsed time.

14. The wireless terminal of claim 8 where the extensible markup language code includes at least one of an assert command, a schedule command, and a perform command, wherein:

the assert command associates the terminal condition information with the received action data and associates the terminal condition information with exception action data if the condition data is not satisfied,

the schedule command associates the terminal condition information with data including at least one of a time of day, time interval between successive executions of the terminal management action, number of repetitions to execute the terminal management action, repetition rate of executing the terminal management action, monitoring, measuring and reporting an elapsed period of time to execute the terminal

management action, and a first run of a scheduled execution of a terminal management action, and

the perform command associates the action data with an attribute value including at least one of a network attribute value and an attribute value associated with the wireless mobile terminal.

15. The wireless terminal of claim 8 wherein the wireless terminal based control information identifies a plurality of terminal management actions, wherein the wireless terminal executes the plurality of terminal management actions in accordance with the corresponding terminal condition information wherein the terminal condition information requires that a previous terminal management action is executed.

16. A storage medium having stored therein instructions executable by a processor that causes the processor to:

receive, extensible markup language code that includes at least wireless terminal condition based control information that includes at least terminal condition information and action data wherein the action data identifies at least one terminal management action associated with the wireless mobile terminal; and

in response to determining that a condition associated with the terminal management action is satisfied based on the terminal condition information, conditionally execute, by the processor, the terminal management action identified by the action data.

17. A wireless terminal comprising:

a wireless transceiver that receives extensible mark-up language code that includes a payload, including at least wireless terminal condition based control information; and

a wireless terminal condition based controller comprising:

a command parser coupled to the wireless transceiver that parses the wireless terminal condition based control information wherein the terminal condition information comprises:

action data associated with at least one terminal management action;

attribute data associated with the action data; and

condition data associated with the attribute data,

a policy reader coupled to the command parser operative to read the action data, attribute data and condition data associated with the least one terminal management action;

an attribute monitor coupled to the policy reader to receive the attribute data from the policy reader and to locally obtain current terminal attribute values in response to the received attribute data; and

a task manager coupled to the policy reader to compare the current terminal attribute values to the received condition data to:

determine if the condition data is met, and

conditionally execute the terminal management action identified by the action data.

18. A terminal management network element comprising:

a wireless terminal condition based control information generator that generates extensible markup language code that includes wireless terminal condition based control information that includes:

selected action data based on selectable action data associated with a terminal management action for at least one wireless mobile terminal;

selected condition data based on selectable condition data wherein the selected condition data is associated with the selectable action data; and

selected attribute data based on selectable attribute data wherein the selected attribute data is associated with the selectable action data,

wherein the wireless terminal condition based control information is generated according to the selected action data, the selected condition data and the selected attribute data; and

a transceiver coupled to the wireless terminal control based control information generator to transmit the wireless terminal control based information.

19. The terminal management network element of claim 18 wherein the wireless terminal condition based control information generator generates a plurality of terminal management actions defined by a plurality of action data, and

wherein the terminal management network element defines condition data associated with a first terminal management action to conditionally execute according to whether a second terminal management action completes execution.

20. The terminal management network element of claim 18 wherein the wireless management terminal network element generator:

generates wireless terminal condition based control information to conditionally execute a plurality of terminal management actions each associated with corresponding selected condition data on a plurality of wireless mobile terminals, and

sends network attribute values to the plurality of wireless mobile terminals to compare the network attribute values with the selected condition data to determine if the selected condition data is met.

21. A method for managing a terminal management network element comprising:

presenting selectable action data associated with a terminal management action;

receiving selected action data in response to presenting the selectable action data;

presenting selectable condition data associated with the selectable action data wherein the selected condition data is associated with the selected action data;

receiving selected condition data in response to presenting the selectable condition data;

presenting selectable attribute data associated with the selectable action data wherein the selected attribute data is associated with the selected action data;

receiving selected attribute data in response to presenting the selectable attribute data, and

generating wireless terminal condition based control information according to the selected action data, the selected condition data, and the selected attribute data wherein the wireless terminal condition based control information is represented by extensible markup language code for at least one wireless mobile terminal.

22. The method of claim 21 wherein the selected action data identifies a plurality of terminal management actions, the method comprising;

associating selected condition data with a first terminal management action to conditionally execute the first terminal management actions on a single wireless terminal according to whether a second terminal management action is completed; and

generating the plurality of current terminal management actions associated with the selected condition data.

23. The method of claim 21 comprising;

generating wireless terminal condition based control information for a plurality of wireless mobile terminals; and

sending network attribute values to the plurality of wireless mobile terminals to allow comparing the network attribute values with the selected condition data by each of the plurality of wireless mobile terminals to determine if the selected condition data is met.

24. A terminal management system comprising:

a terminal management network element comprising:

a wireless terminal condition based control information generator that generates wireless terminal condition based control information comprising:

selected action data based on selectable action data associated with a terminal management action to execute on at least one wireless mobile terminal;

selected condition data based on selectable condition data wherein the selected condition data is associated with the selected action data;

selected attribute data based on selectable attribute data wherein the selected attribute data is associated with the selected action data,

wherein the wireless terminal condition based control information is generated according to the selected action data, the selected condition data and the selected attribute data, wherein the wireless terminal condition based control information is represented by extensible markup language code;

at least one wireless terminal comprising:

a wireless transceiver that receives the at least wireless terminal condition based control information, the selected attribute data, the selected condition data, the selected action data and the terminal management action associated with the wireless mobile terminal; and

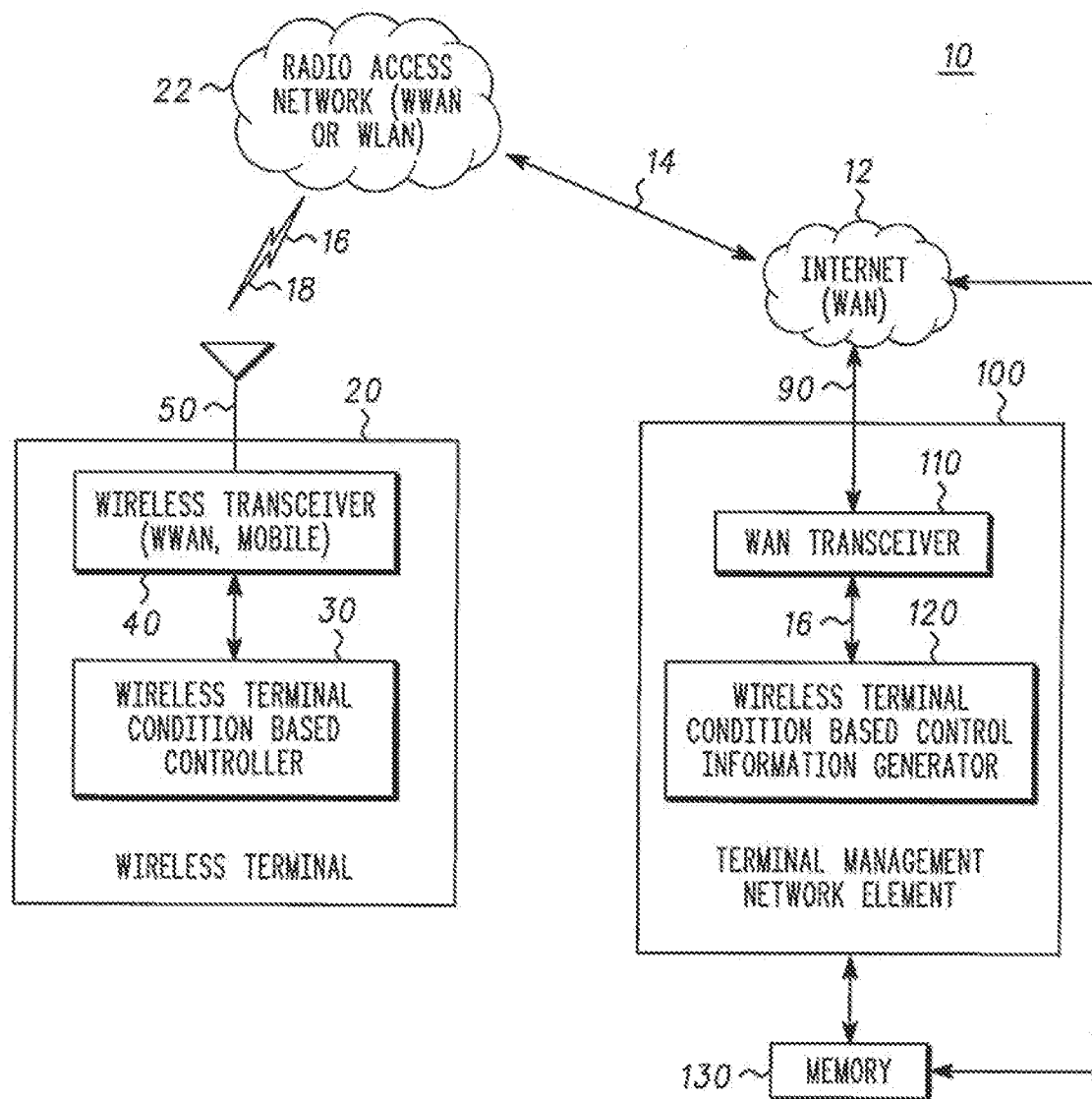
a wireless terminal condition based controller, operatively coupled to the wireless transceiver, and operative to

determine that the selected condition data associated with the terminal management action is satisfied, and

conditionally execute the terminal management action identified by the selected action data if the selected condition data associated with the terminal management action is satisfied.

25. The terminal management system of claim 24 wherein the wireless terminal condition based control information generator generates a plurality of terminal management actions defined by the selected action data and the associated selected condition data, and defines the selected condition data associated with each terminal management action to conditionally execute in accordance with the selected condition data associated with each respective terminal management action.

1/10

**FIG. 1**

2/10

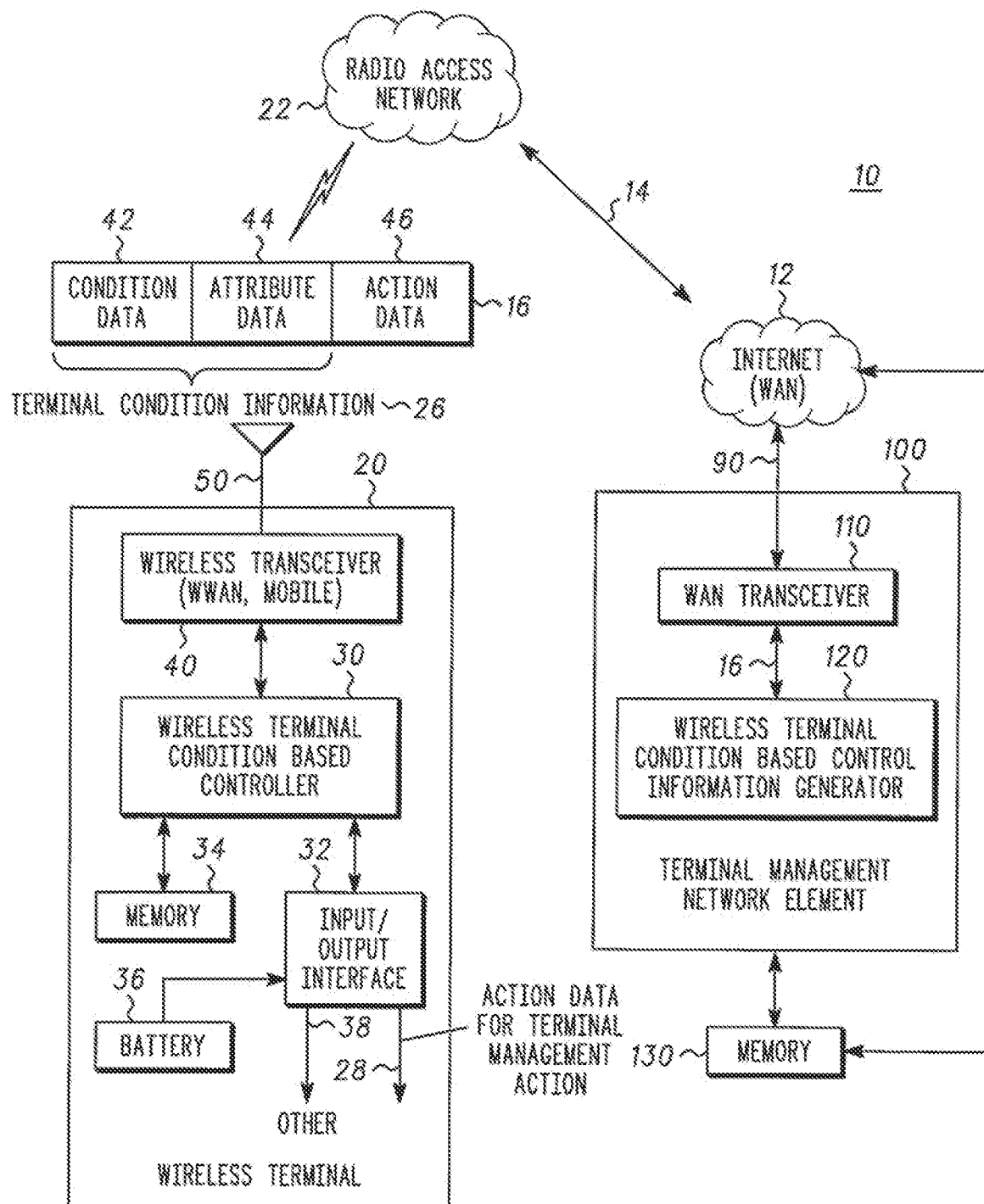
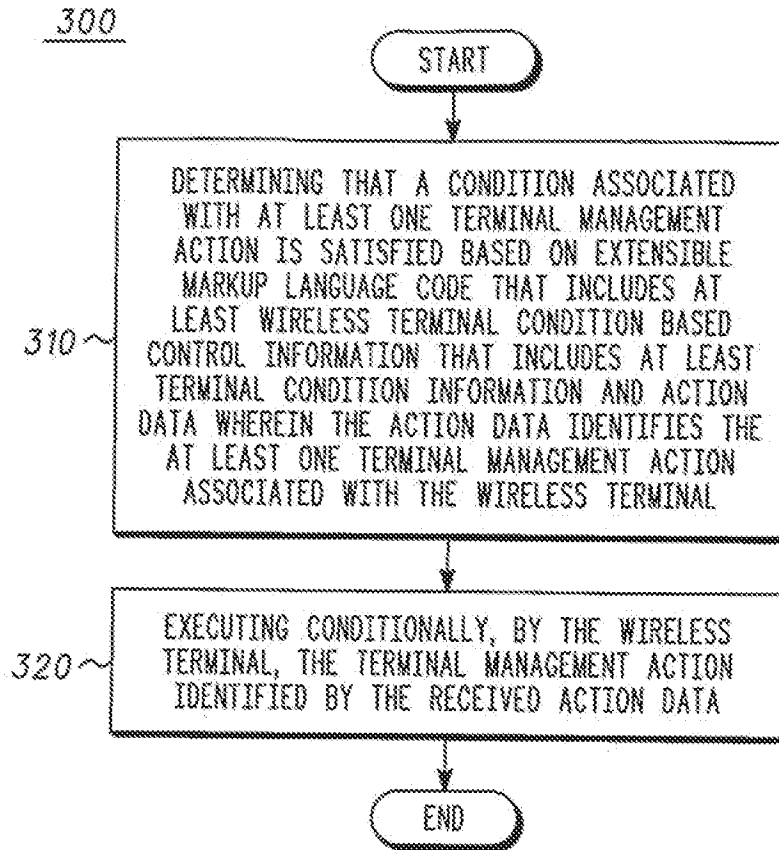
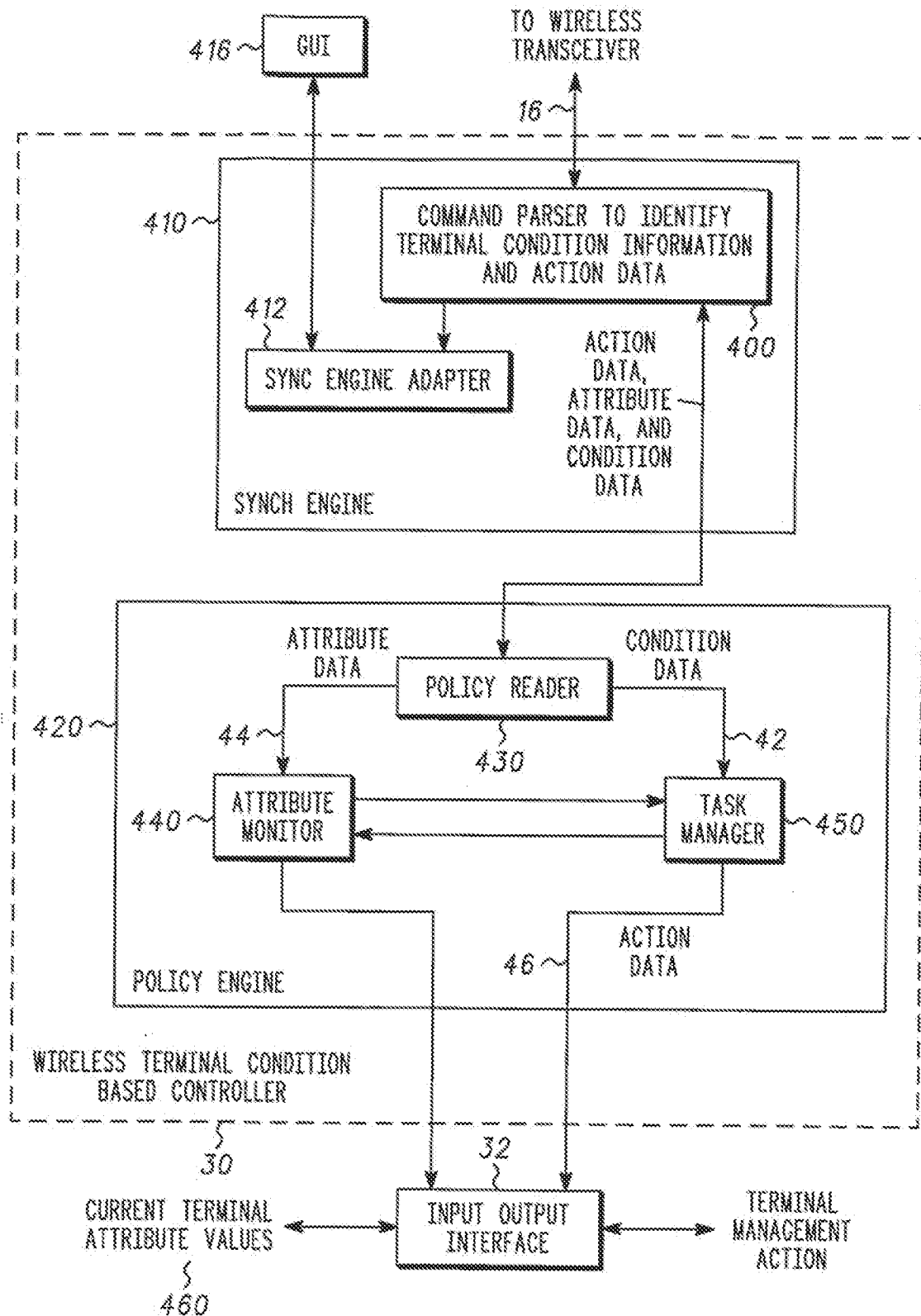


FIG. 2

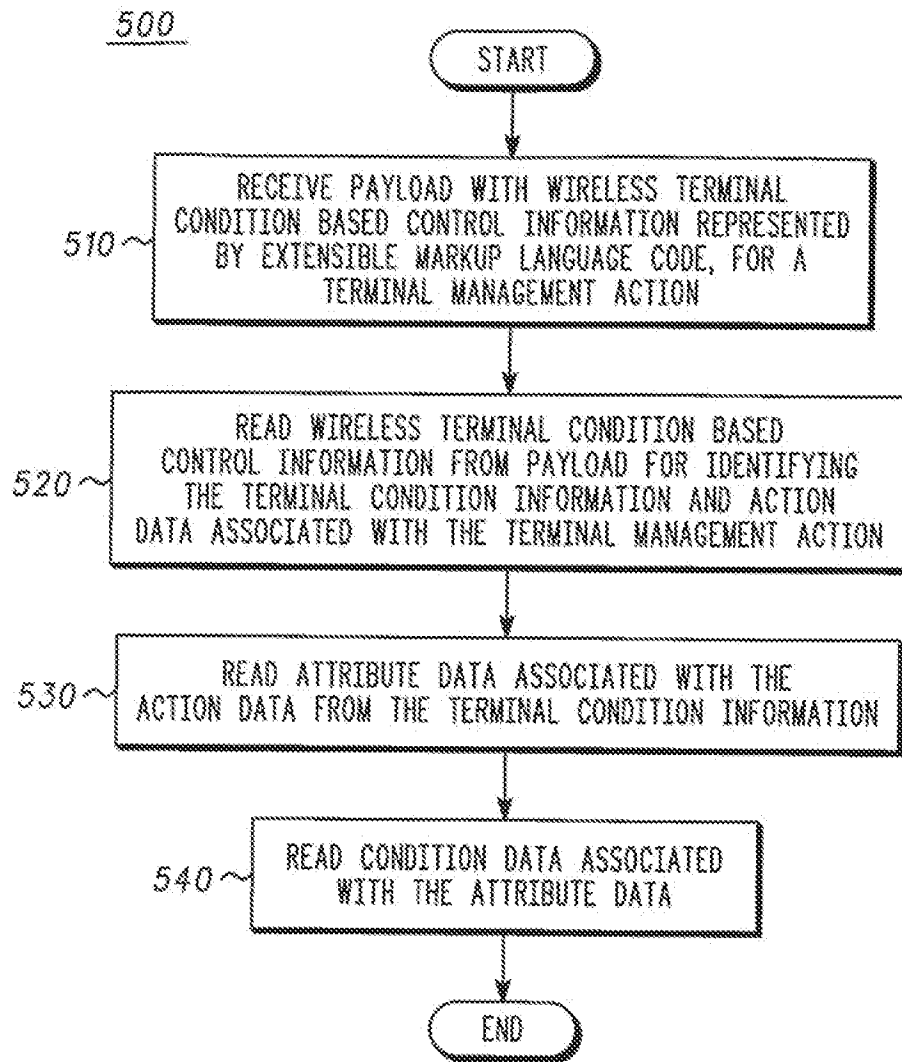
3/10

*FIG. 3*

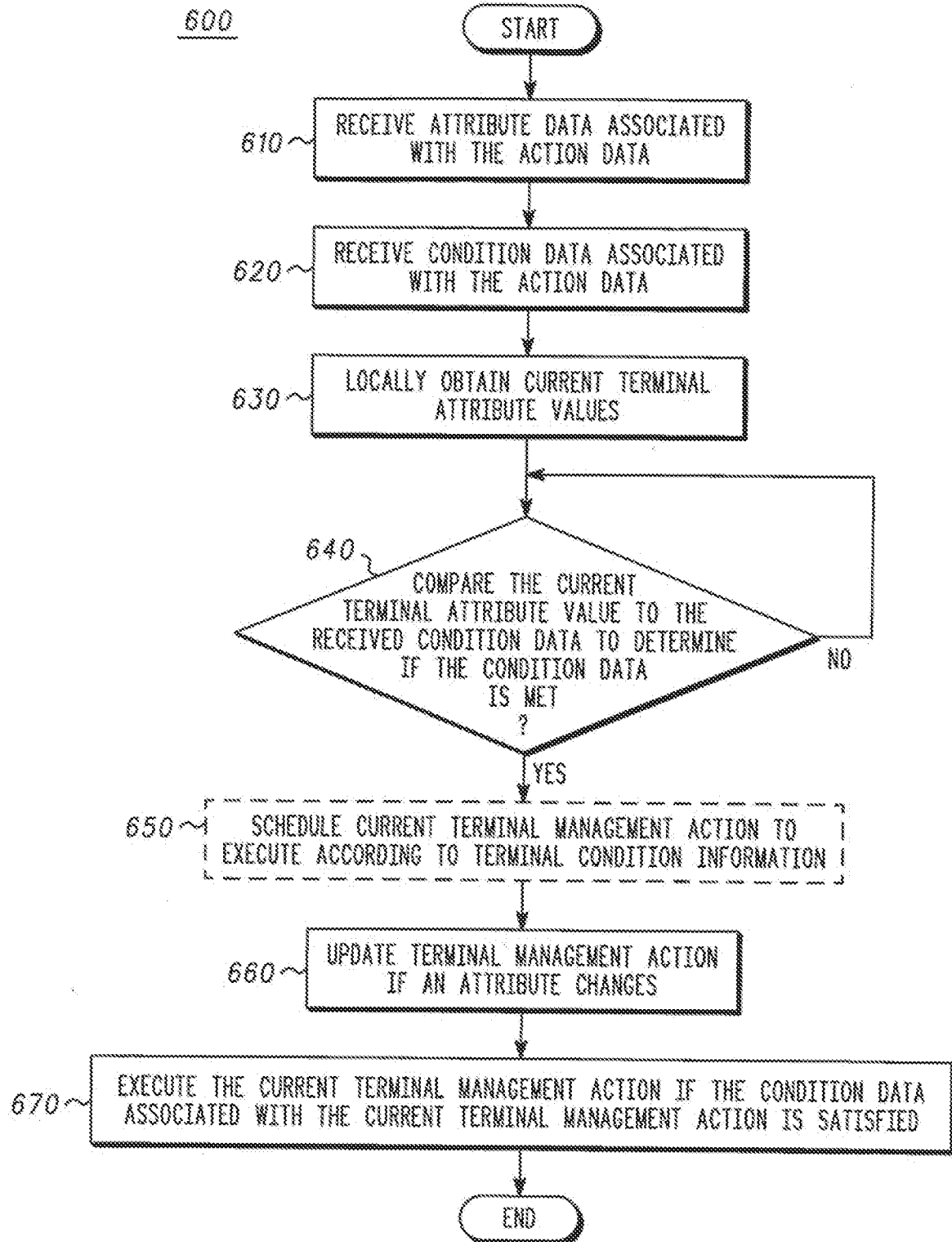
4/10

**FIG. 4**

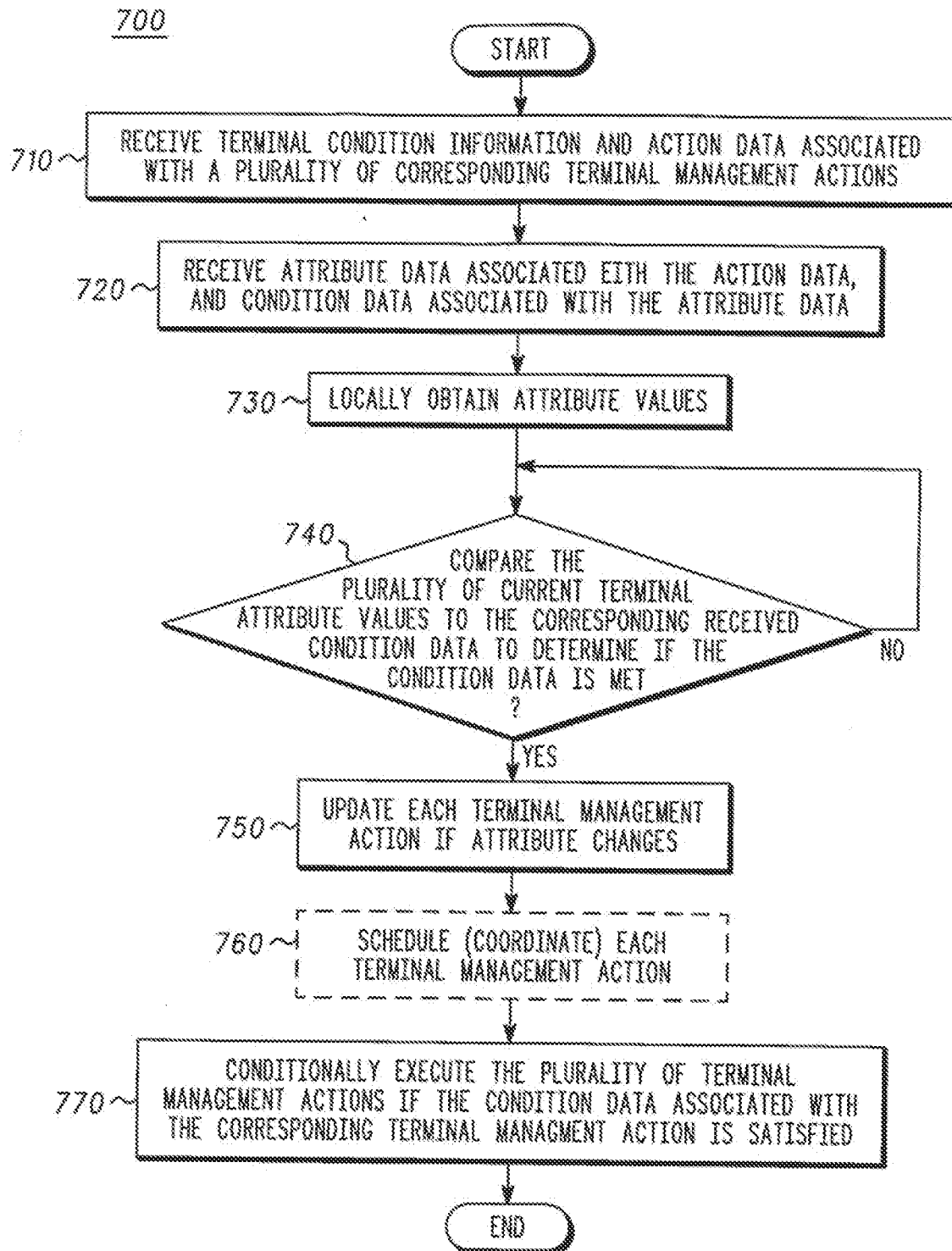
5/10

*FIG. 5*

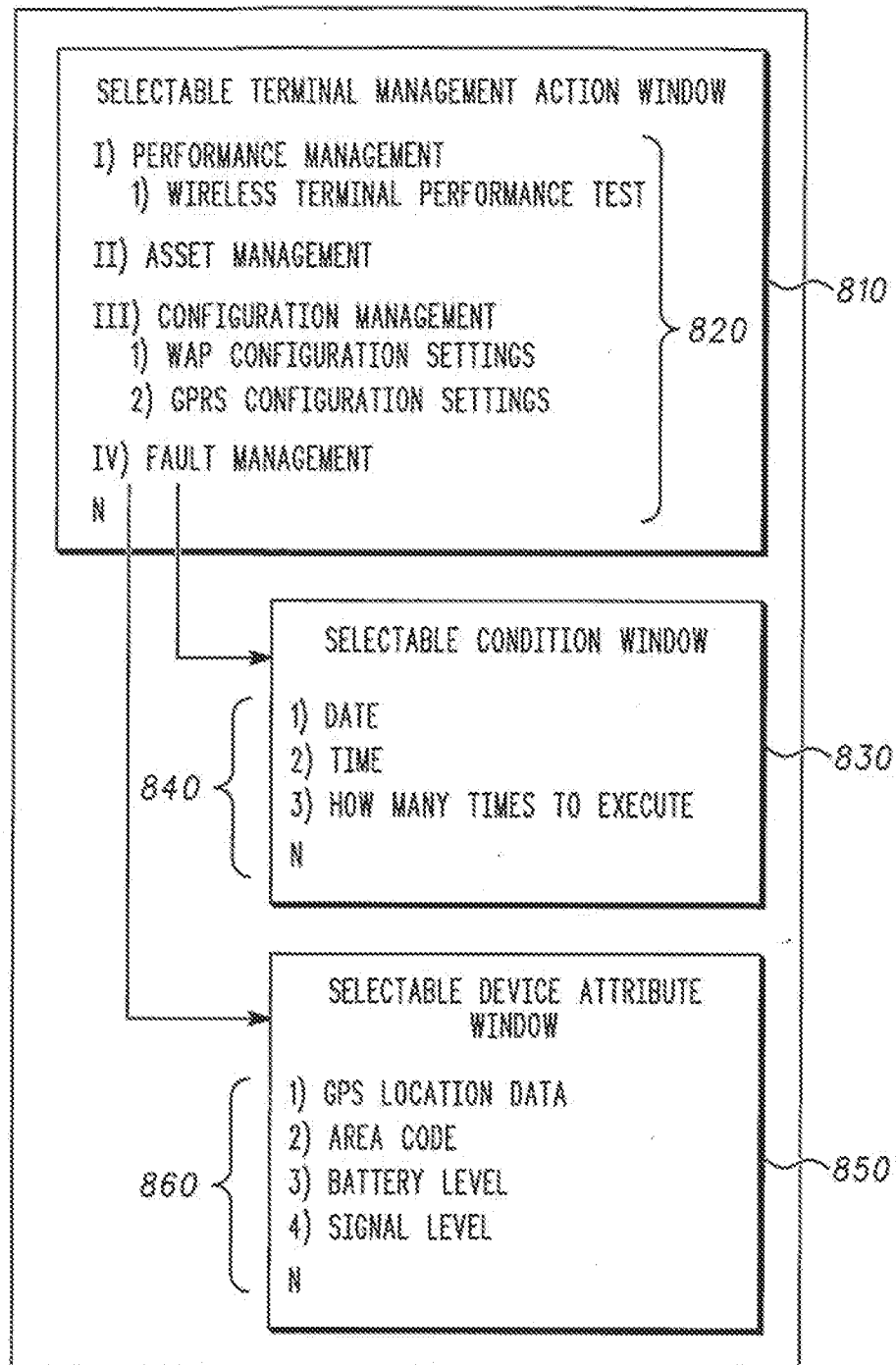
6/10

**FIG. 6**

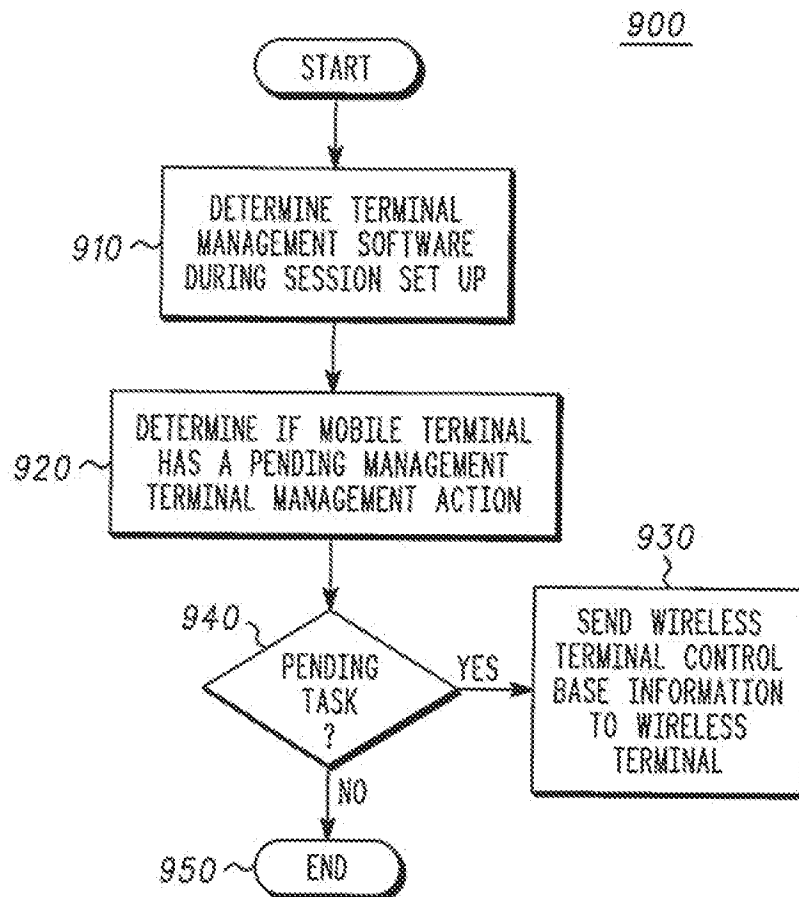
7/10

**FIG. 7**

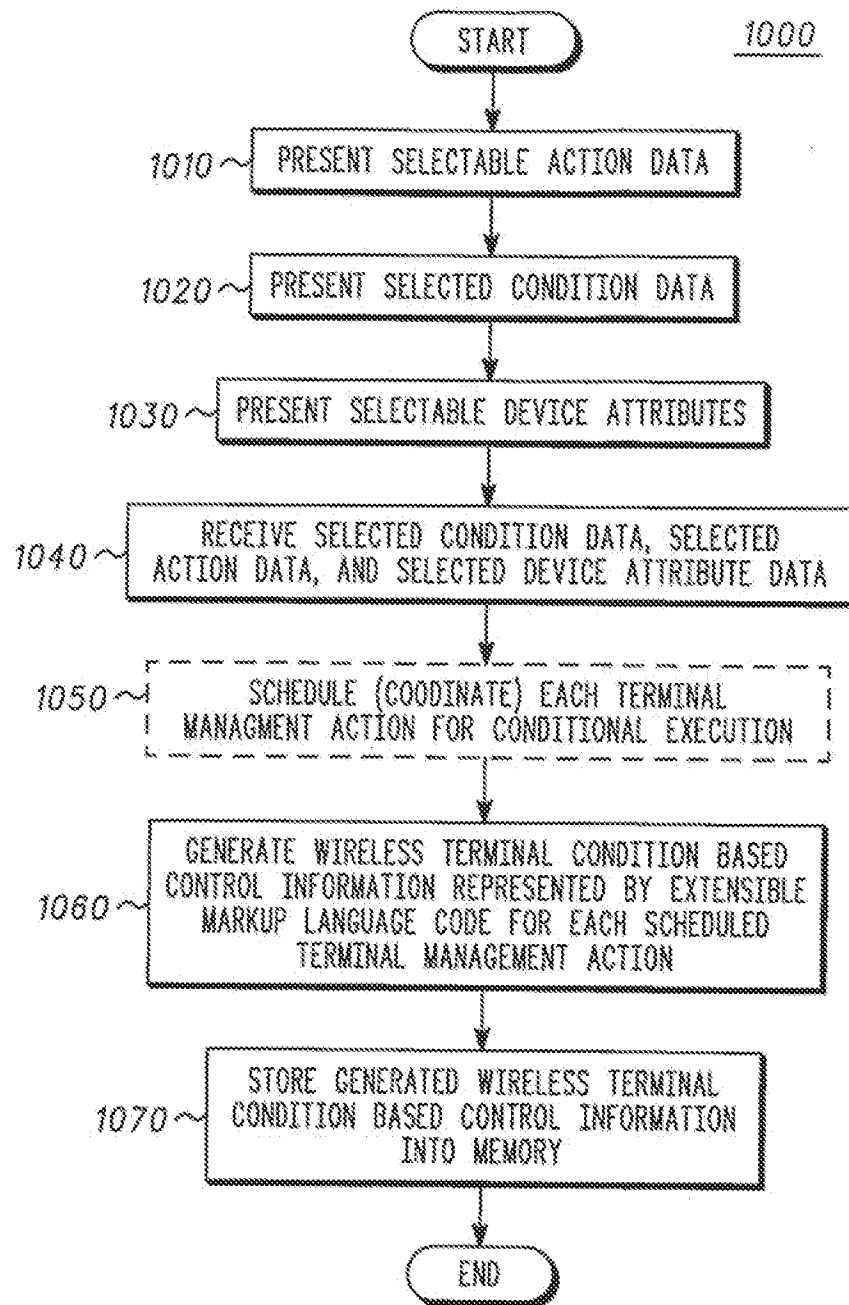
8/10

800**FIG. 8**

9/10

**FIG. 9**

10/10

**FIG. 10**

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
12 January 2006 (12.01.2006)

PCT

(10) International Publication Number
WO 2006/004467 A1(51) International Patent Classification: **H04Q 7/38**,
H04L 12/56(21) International Application Number:
PCT/SE2004/001087

(22) International Filing Date: 5 July 2004 (05.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): TELEFONAKTIEBOLAGET LM ERICSSON (publ)
[SE/SE]: S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants (for US only): SKOG, Robert
[SE/SE]: Gullivestränd 7, S-165 76 Håsselby (SE). PERSSON, Justus [SE/SE]: Sankt Paulsgatan 28B, S-118 48 Stockholm (SE).(74) Agent: DR LUDWIG BRANN PATENTBYRÅ AB; P.O.
Box 171 92, S-104 62 Stockholm (SE).(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HK, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,
MG, ME, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,
PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,
ZW.(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE,
SI, SK, TR), OAPI (BF, BI, CF, CG, CI, CM, GA, GN,
GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

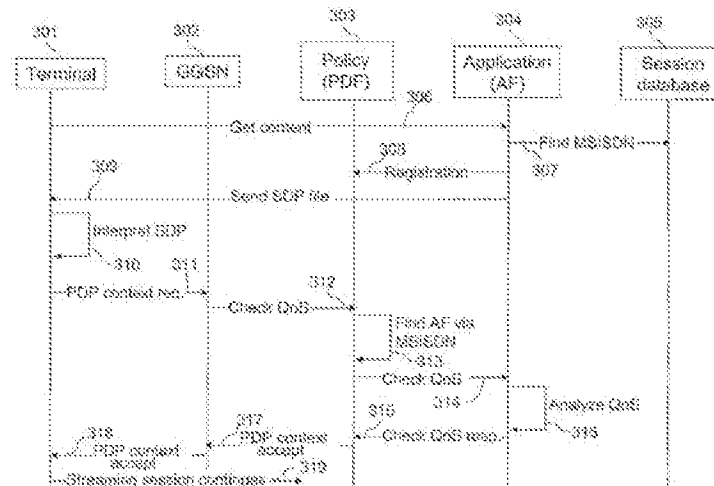
— of inventorship (Rule 4.17(iv)) for US only

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: BINDING MECHANISM FOR QUALITY OF SERVICE MANAGEMENT IN A COMMUNICATION NETWORK



(57) Abstract: The present invention relates to methods and arrangements for setting up a policy controlled bearer service for delivery of a service from an application function (304) to a mobile terminal (301). According to the present invention a terminal identity of the mobile terminal may be used to bind to applicable policy information when setting up the bearer service. Thus the present invention obviates the need to transmit specific binding information to the mobile terminal during application layer signaling for the purpose of policy controlled bearer service set-up. The terminal identity is registered (308) in a register of a policy decision function (303) along with policy identifying information. When a bearer service activation request is received from the mobile terminal (301) the request is mapped (313) to applicable policy information by means of the terminal identity and the matching registration in the register of the policy decision function (303).

WO 2006/004467 A1

BINDING MECHANISM FOR QUALITY OF SERVICE MANAGEMENT IN A COMMUNICATION NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

5 This application is related to commonly-assigned co-pending international patent application No. PCT/SE04/_____, entitled "Devices and Methods for Push Message Initiated Service", filed on July 5, 2004; international patent application No. PCT/SE04/_____, entitled "Methods and Devices for
10 Supplying Quality of Service Parameters in HTTP Message", filed on July 5, 2004; and international patent application No. PCT/SE04/_____, entitled "Methods and Devices for Changing Quality of Service", filed on July 5, 2004, the disclosures of which are incorporated herein by reference.

FIELD OF THE INVENTION

15 The present invention relates to equipment and methods in mobile communication systems, and more particularly, to mechanisms for quality of service management of transmissions relating to a packet data service.

BACKGROUND

20 Communication networks for packet based communication of information in the form of data bits are well known to the person skilled in the art. The growing importance of mobile communication creates the demand to transfer data over wireless connections. The 3rd Generation Partnership
25 Project (3GPP) is a collaboration agreement that brings together a number of telecommunications standards bodies and was established to produce globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the
30 radio access technologies that they support. This includes maintenance and development of the Global System for Mobile communication (GSM) Technical Specifications and Technical Reports including evolved radio access technologies (e.g. General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE)).

One of the issues that the 3GPP is currently working on is a framework for providing end-to-end Quality of Service for services involving GPRS networks as described in the technical specification 3GPP TS 23.207 V6.2.0 (2004-03).
5 This technical specification describes the use of a Policy Control mechanism in order to control and authorize the use of network resources prior to set-up of a service.

In the future it is assumed that packet switched services undergo Policy
10 Control by means of a Policy Decision Function (PDF). The PDF is a logical element that is used as a logical policy decision element and enables coordination between events in the application layer and resource management in the IP bearer layer.

15 Policy Control was developed since it is considered important that network managers and service providers can to monitor, control, and enforce the use of network resources and services based on "policies" derived from certain criteria such as the identity/authority level of users and applications, traffic bandwidth requirements, security considerations, time of day/week etc.
20 Because there are varying circumstances in which various entities are entitled to use the services they request, there is a need for rules, need for enforcement methods of these rules, and a need for a "judge" to decide when they apply. Accordingly, three major components of a policy system include policy rules, which are typically stored in a policy database, policy
25 enforcement, which may be implemented at Policy Enforcement Points (PEP), and Policy Decision Points. The IETF has standardized a protocol for information exchange between PEPs and Policy Decision Points under the term Common Open Policy Service (COPS). In general, a policy may be regarded as a collection of rules that result in one or more actions when
30 specific conditions exist.

Fig. 1 is a schematic block diagram that illustrates the different elements that are involved in the policy control mechanism developed by 3GPP. Fig. 1 illustrates an example where a service is set-up between a mobile User
35 Equipment (UE) 1 and an Application Function (AF) of a service provider. The

UE includes an AF Client 3 which communicates with the AF 2 by means of AF session signaling 4 in order to initiate an application session. The set-up of the session and activation of the service require set-up of a bearer service to carry the data packets of the session. The session may include one or a plurality of different IP flows with specific requirements for bearer resources. The AF session signaling 4 may include information on Quality of Service (QoS) requirements which are translated into bearer QoS parameters by a translation/mapping function 5 in the UE. In order to activate the bearer service the UE sends a request for activation of a PDP context with the bearer QoS parameters that are determined by the translation/mapping function to a GGSN 6. The communication between the UE and the GGSN is in this example handled by means of UMTS BS Managers 7, 8 in the UE and the GGSN respectively. In this example the GGSN functions as a PEP and is provided with an IP BS Manager 9 which is involved in QoS management. The GGSN 6 interacts with a PDF 10, via a Go interface 11, in order to execute policy control. The PDF 10 makes policy decisions based on policy set-up information obtained from the AF 2 via a Gq interface 12. More detailed information regarding the elements illustrated in Fig. 1 and their function can be found in the above mentioned technical specification TS 23.207 V6.2.0.

When 3GPP specified the policy control mechanism an authorization token was also introduced in order to establish a binding mechanism for mapping PDP contexts and IP flows to policy information. The authorization token is generated by the PDF for a particular AF session on request from the AF. The authorization token includes a fully qualified domain name of the PDF and is unique across all PDP contexts associated with an APN (Access Point Name). The AF sends the authorization token to the UE in the AF session signalling. The UE should then include the applicable authorization token in any request to activate or modify a PDP context. The authorization token will then be used in the GGSN and PDF to map to the correct policy information.

The plan to introduce the authorization token and the associated handling of it when implementing policy control in 3G systems has a number of

disadvantages. One major disadvantage is that it requires modification of existing UEs in order to make them capable to handle authorization tokens. Another disadvantage is that the introduction of the authorization token requires new standardization for the RTSP (Real-Time Streaming Protocol),
5 SIP (Session Initiation Protocol), and SDP (Session Description Protocol) and other protocols used in set-up and handling of application sessions.

SUMMARY OF THE INVENTION

An object of the present invention is to provide devices and methods for
10 employing a simple binding mechanism when setting up a policy controlled bearer service for delivery of a service to a mobile terminal.

The above stated object is achieved by means of methods according to claim
1 and 10, and by means of a policy decision function according to claim 19.

15 The basic idea of the present invention is to use a terminal identity as binding information in order to bind a bearer service activation request to the applicable policy information and thereby obviate the need to transmit an authorization token to the terminal during bearer service activation.

20 According to a first aspect of the present invention a method for setting up a policy controlled bearer service for delivery of a service from an application function to a mobile terminal is provided. The method includes the steps of registering a terminal identity of the terminal associated with policy
25 identifying information in a register of a policy decision function; receiving a bearer service activation request from the terminal, via a core network node, which bearer service activation request includes the terminal identity, such as MSISDN, IMEI, IMSI etc. and a set of requested QoS parameters for the bearer service; binding the bearer service activation request to the policy
30 identifying information by means of the terminal identity to determine applicable policy information for the bearer service; performing a policy check by means of checking if the requested QoS parameters fulfill said applicable policy information; and sending an accept message to the core network node

to initiate completion of the bearer service set-up if the policy check was successful.

According to a second aspect the present invention a method in a policy
5 decision function for performing policy control on a bearer service for delivery
of a service from an application function to a mobile terminal is provided. The
method according to the second aspect of the invention comprises the steps
of receiving a registration message, including a terminal identity and policy
10 identifying information; registering the terminal identity associated with the
policy identifying information in a register; receiving a bearer service
activation request from the terminal, via a core network node, which bearer
service activation request includes the terminal identity and a set of
requested QoS parameters for the bearer service; binding the bearer service
15 activation request to the policy identifying information in the policy decision
function by means of the terminal identity to determine applicable policy
information for the bearer service; performing a policy check by means of
checking if the requested QoS parameters fulfill said applicable policy
information; and sending an accept message to the core network node to
20 initiate completion of the bearer service set-up if the policy check was
successful.

According to a third aspect of the present invention a policy decision function
for performing policy control on a bearer service for delivery of a service from
an application function to a mobile terminal is provided. The policy decision
25 function includes a first interface for receiving a registration message,
including a terminal identity and policy identifying information; a register
for registering the terminal identity associated with the policy identifying
information; a second interface for receiving a bearer service activation
request from the terminal, via a core network node, which bearer service
30 activation request includes the terminal identity and a set of requested QoS
parameters for the bearer service; and processing means for binding the
bearer service activation request to the policy identifying information in the
policy decision function by means of the terminal identity to determine
applicable policy information for the bearer service, performing a policy check

by means of checking if the requested QoS parameters fulfill said applicable policy information, and for sending an accept message to the core network node to initiate completion of the bearer service set-up if the policy check was successful.

5

An advantage of the present invention is that it obviates the need to transmit an authorization token to the terminal for the purpose of setting up a policy controlled bearer service. This means that there is no impact on the terminals from a standard on the terminal.

10

Another advantage of the present invention is that by means of the present invention, no new standardization is required for RTSP (Real-Time Streaming Protocol), SIP (Session Initiation Protocol), and SDP (Session Description Protocol) and other protocols used in set-up and handling of application sessions.

15

A further advantage of the present invention is that the policy mechanism and QoS control mechanism of the invention are possible to implement in the mobile terminals that are available on the market today. Thus there is no need to modify the mobile terminals in order to implement the present invention.

20

Another advantage according to an embodiment of the present invention is that it allows for a service provider to upgrade the QoS parameters that a terminal requests for a bearer service if the requested QoS parameters do not fulfill the service providers QoS demand. This is possible since an embodiment of the present invention allows for the possibility to check if the requested QoS parameters fulfill a set of predefined minimum QoS requirements provided by the application function. If the predefined minimum QoS requirements are not fulfilled by the requested QoS parameters it is possible to determine modified QoS parameters for use when setting up the bearer service.

25

30

Further advantages and features of embodiments of the present invention will become apparent when reading the following detailed description in conjunction with the drawings.

5 BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic block diagram illustrating the different elements that are involved in the policy control mechanism developed by 3GPP

10 Fig. 2 is a schematic block diagram illustrating the general network architecture of a mobile communication system in which the present invention may be used.

Fig. 3 is a schematic flow diagram illustrating an embodiment of a method according to the present invention.

15 Fig. 4 is a schematic flow diagram illustrating an alternative embodiment according to the present invention.

DETAILED DESCRIPTION

20 The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. In the drawings, like numbers refer to like elements.

30 The present invention is applicable to packet switched services in a mobile communication system. Such services include packet switched communication between a mobile client terminal of an end-user and an application server. The mobile communication system includes a radio

network such as for example a WCDMA, CDMA2000, Wireless LAN or GPRS network in which the mobile client terminal resides.

Fig. 2 is a schematic block diagram illustrating the general network architecture of a mobile communication system in which the present invention may be used. The mobile system 101 in fig. 1 comprises a mobile client terminal 102 which may communicate with a network node 106 of a service provider and thereby receive a service that is offered by the service provider. The communication between the client terminal 102 and the network node 106 is carried out via a radio network 103, a core network 104 and a service network 105. The radio network 103 may for instance be a UTRAN (UMTS Terrestrial Radio Access Network), the core network 104 may for instance be a UMTS Core Network and the service network may for instance be the Internet or a private IP network of a service provider. The network node 106 of the service provider may for instance be an application server.

Fig. 3 is a schematic flow diagram illustrating an embodiment of a method according to the present invention. The figure illustrates the interaction between a mobile terminal 301, a GGSN (Gateway GPRS Support Node) 302, a policy decision function (PDF) 303, an application function (AF) 304 and a session database 305 when setting up a policy controlled bearer service. Further network nodes may be involved in the process of setting up the bearer service but only the nodes that are of particular relevance to the present invention are illustrated in fig. 3 to simplify the description of the invention.

In fig. 3 it is assumed that a primary PDP context exists and that the terminal 301 asks the AF 304 for a streaming content, step 306. The AF is in this example a streaming server. The AF could also be for instance an MMS or Download server.

After receiving the request for a streaming content the AF 304 finds a terminal identity associated with the terminal 301. In this example the

terminal identity is an MSISDN (Mobile Identification Number) which is found by asking the session database 305 for a mapping between a terminal IP-address and MSISDN according to a method that is well known to the person skilled in the art, step 307. The AF then registers in the PDF 303 that
5 it is interested in checking the QoS of the PDP context that is to be set up for delivery of the requested streaming content, step 308. The registration involves registering the MSISDN associated with policy identifying information in a register in the PDF. In this example the policy identifying information is an IP address of the AF so that the AF can be asked for
10 applicable policy information. It is assumed that the address to the PDF is previously known to the AF. After the registration in the PDF, the AF sends an SDP-file to the terminal, step 309. The terminal then interprets the SDP-file and deduces QoS parameters to request for the bearer service to be set-up for delivery of the streaming content, step 310. The terminal then initiates
15 a secondary PDP context by means of sending a activation request for a second PDP context, step 311. The activation request includes the QoS parameters that were deduced from the interpretation of the SDP-file. These QoS parameters will hereafter be denoted as requested QoS parameters. The steps 309, 310 and 311 are well known to the person skilled in the art and
20 will therefore not be described in greater detail herein.

The GGSN 302 receives the PDP context activation request. The GGSN sends a request to the PDF to check the requested QoS parameters, step 312. The check request includes the MSISDN of the mobile terminal and the requested
25 QoS parameters. It is assumed that the address of the PDF is known to the GGSN. When receiving the check request the PDF 303 finds the address of the AF 304 by mapping the MSISDN received in the check request to the register in which the AF's previous registration is stored, step 313. The PDF 303 then sends a check request to the AF 304 with the address that matches
30 the MSISDN of the terminal in the register, step 314. The check request includes the MSISDN of the terminal and the requested QoS parameters. The AF 304 processes the QoS parameters and performs a policy check of the QoS parameters, step 315. The policy check may include checking that the QoS requirements does not exceed the limits of a subscription of the user of

the mobile terminal according to the principles described for the policy mechanism specified by 3GPP.

5 According to an embodiment of the present invention the policy check may also include a supplemental check that includes checking that the requested QoS parameters fulfil a set of predefined minimum QoS parameters which define the QoS that the service provide considers desired or needed for the bearer service. This supplemental check allows for the application function to initiate an upgrade of the QoS requirements if the requested QoS
10 parameters do not achieve the QoS that the service provider considers desired or needed. The supplemental check and the mechanism for upgrading the requested QoS parameters will be described in further detail below.

15 After the AF 304 has checked the requested QoS parameters the AF sends an accept message or a modify message back to the PDF, step 316. If the policy check showed that the requested QoS parameters fulfilled the applicable policy, and selectively also the predefined minimum QoS parameters an accept message is sent. A modify message may be sent if the requested QoS
20 parameters exceed the applicable policy and will in that case include an order to downgrade the requested QoS parameters. The order to downgrade the requested QoS parameters may be in the form of a set of downgraded QoS parameters to be used when setting up the bearer service. If the policy check includes checking that the requested QoS parameters match the
25 predefined minimum QoS parameters a modify message may be sent if the requested QoS parameters are considered to result in a QoS that is poorer than what the service provider has defined as desired or needed. In that case the modify message may include an order to upgrade the requested QoS parameters. The order to upgrade the requested QoS parameters may be in
30 the form of a set of upgraded QoS parameters to be used when setting up the bearer service.

After receiving the accept or modify message from the AF 304 the PDF 303 answers back to the GGSN. In this example the PDF sends a message

accepting the secondary PDP context to the GGSN, step 317. If the policy check resulted in a decision to modify the requested QoS parameters the message from the PDF 303 to the GGSN 302 may include modified QoS parameters to be used when setting up the secondary PDP context.

5

The set-up of the secondary PDP context is then completed by means of the PDP context set-up messages that are well known to a person skilled in the art. This includes that the GGSN answers back to the terminal via radio and core network nodes (not shown), step 318. When the PDP context is set-up the streaming session continues, step 319 and the streaming content may be delivered to the terminal over the secondary PDP context.

10

In fig. 3 it was illustrated that the policy check included that the PDF 303 asked the AF 304 to check the requested QoS parameters. It is however possible that this check is performed by the PDF. The AF may for instance send the applicable policy information and selectively also the set of predefined minimum QoS parameters to the PDF when it received the check request from the PDF. It is also possible that the applicable policy information was transferred to the PDF during the step 308 of registering the terminal identity in the PDF. The applicable policy information could then be stored in the register in the PDF along with the terminal identity.

15

20

In the above description of an embodiment of the invention it was mentioned that it was assumed that the AF and the GGSN was aware of the address of the PDF. This may for instance be the case if the network architecture was configured such that there is a preconfigured relationship between a single PDF and a number of GGSNs and a number of APs. Each GGSN and each AF should in that case however be configured to only communicate with the single PDF for the purpose of achieving policy control.

25

30

A prerequisite of the binding mechanism that is provided by the present invention and which uses a terminal identity as binding information is that the mobile terminal requests activation of a single bearer service, such as a PDP context, at a time. The registration of the terminal identity in the PDF

should preferably be removed after the policy check is completed so that the terminal may request set-up of another bearer service and have a new request mapped correctly to applicable policy information.

5 The supplemental check described above to determine if the requested QoS requirements match the QoS that the service provider considers desired or needed for the bearer service is optional but may be very advantageous since it allows the service provider to control the QoS to a higher degree than provided by prior art solutions. The service provider may be interested in
10 making sure that the terminal does not map a received SDP-file to QoS parameters that the service provider considers unsuitable for the bearer service since they result in poor QoS. Poor QoS may have a bad reflection on the service provider even if the poor QoS is a result of the implementation of the terminal. The supplemental check is here presented in combination with
15 a token unaware terminal (i.e. a terminal that is not aware of an authorization token according to prior art), but the supplemental check may also be implemented in a system that makes use of an authorization token as binding mechanism instead of the terminal identity as described herein.

20 If it is of interest to perform the supplemental check the AF should be implemented with information that defines a set of minimum QoS parameters against which the requested QoS requirements may be checked. If the supplemental check results in a decision to upgrade the requested QoS parameters modified QoS parameters which correspond to an upgrade of the
25 requested QoS parameters may be determined by the AF or the PDF. It is also necessary that the GGSN is implemented such that it is able to handle an upgrade of the requested QoS parameters. The upgrade scenario may require new signalling between the GGSN and other core network nodes and radio network nodes.

30

Fig. 4 is a schematic flow diagram that illustrates a scenario in which the requested QoS parameters are upgraded because the requested bandwidth was considered to low from the viewpoint of the service provider/AF. Fig. 4 illustrates, apart from the mobile terminal 301, the GGSN 302, the PDF 303

and the AF 304, also a radio network node 401, which e.g may be a Radio Network Controller (RNC) or a Base Station Controller (BSC), and a SGSN (Serving GPRS Support Node) 402. The session database 305 is not shown in fig. 4, but the AF 304 may have an interface to the session database for
 5 retrieving specific session information. The dashed box 403 surrounds the new signalling scheme, compared with what is supported by the current 3GPP standard and which is needed in order to handle an upgrade of the requested QoS parameters. The steps 411-424 illustrated in fig. 4 will now be described.

10

- Step 411 The user has an interactive/browsing session established.
- Step 412 The user clicks on an "rtsp-link".
- Step 413 Streaming session establishment is performed.
- Step 414 The AF (Application/Streaming server) registers the terminal
 15 identity in the PDF (this step corresponds to step 308 of fig. 3).
- Step 415 The terminal requests activation of a secondary PDP context (this step corresponds to step 311 of fig. 3).
- Step 416 The GGSN initiates a policy/QoS check with the PDF (this step corresponds to step 312 of fig. 3).
- 20 Step 417 The PDF checks that the needed resource reservation that is defined by the requested QoS parameters, is within the subscribed limits and issues a check request towards the AF (this step corresponds to step 314 of fig. 3).
- Step 418 The AF sees that the bandwidth must be updated to ensure
 25 satisfactory end-user QoS during the service provisioning. Thus, it requests more bandwidth than the terminal initially requested (this step corresponds to step 316 of fig. 3).
- Step 419 The PDF replies back to the GGSN. The GGSN discovers that the bandwidth parameter has been changed to a higher value
 30 than what requested by the terminal. Thus, the GGSN needs to request an update of the secondary PDP context.
- Step 420 The requests a modification (bandwidth upgrade) of the terminal's requested secondary PDP Context by sending a PDP

- Context update request message to the SGSN 402 which forwards the request to the radio network node 401.
- Step 421 The radio network node 401 checks if it has enough resources to upgrade the bandwidth parameter. In this scenario it has enough resources and replies back to the SGSN (and the GGSN via the SGSN) with an acknowledgement. If the radio network node had not had enough resources, it is possible that the set-up of the service would be interrupted and that the requested service would be denied.
- 10 Step 422 The SGSN responds (possible in parallel with step 421) to the terminal's PDP context activation request with a different bandwidth parameter than the terminal initially requested.
- Step 423 The terminal issues a "Play request".
- Step 424 The application session starts.
- 15 The reason why a supplemental check as described above may be desired is that it is the terminal that translates or maps the application level QoS parameters to bearer service QoS parameters such as PDP context parameters. The implementation of the translation/mapping function in the terminal is vendor specific and may thus vary between different terminals. If the service provider is interested in delivering services with good quality irrespective of the terminal that requests the service the supplemental check may be desirable.
- 20 An example of application level QoS parameters are those defined for UMTS (Universal Mobile Telecommunication System). In UMTS QoS is defined with a set of attributes that specifies the UMTS bearer service. The UMTS QoS attributes are the following:
- Traffic class
 - 30 - Maximum bit-rate
 - Guaranteed bit-rate
 - Delivery order
 - Maximum SDU size
 - SDU format information

- SDU error ratio
- Residual bit error ration
- Delivery of erroneous SDUs
- Transfer delay
- 5 - Traffic handling priority
- Allocation/Retention Priority
- Source statistics descriptor
- Signaling Indication

These attributes can be mapped to the pre-defined UMTS QoS classes:
10 Conversational class, Streaming class, Interactive class and Background class. More detailed information about UMTS QoS can be found in the technical specifications 3GPP TS 23.107 V6.1.0 (2004-03) and 3GPP TS 23.207 V6.2.0 (2004-03).

15 The QoS classes can be negotiated and managed by using PDP context management. Application level QoS requirements are mapped to PDP context parameters in the mobile client terminal. In prior art solutions pre-configurations of PDP contexts are made in the client terminal such that when a packet switched application starts and connects to the network a
20 matching pre-configured PDP context is activated. This PDP context has a selected QoS class that should match the desired QoS requirements of the application. If for instance the application is a WAP browser or MMS client the QoS class of the activated PDP context is usually the Interactive class.

25 Thus in the prior art solutions the selection of QoS parameters for the bearer service that is set up for delivery of the service in the example depends on the terminal vendor's configuration of the mobile client terminal. The service provider cannot influence the selection of the QoS parameters. As mentioned above this is in many instances problematic, especially from the viewpoint of
30 the service provider, but also from a user perspective, when it results in set-up of a bearer service with a QoS that is not appropriate for the delivery of the service. The service provider is usually interested in being able to ensure that the offered service is delivered with a certain minimum quality. If the quality of service is bad this may have a negative impact on the service

provider's reputation even if the bad quality is caused by a network operator or terminal vendor. The user of the service will become annoyed if the QoS is bad and will probably blame the service provider for the bad quality. It is also possible that a user with one terminal gets unacceptably bad QoS when
5 receiving a particular service content while another user, with a terminal from another vendor, gets acceptable QoS when receiving the same service content.

However, as shown above, the embodiment of the present invention that
10 includes a supplemental check, in which the service provider can control the requested QoS parameters and also modify them if is considered necessary, makes it possible to overcome many of the disadvantages that may arise when the terminal translates/maps application level QoS requirements into bearer service QoS parameters.

15 In the drawings and specification, there have been disclosed typical preferred embodiments of the invention and, although specific terms are employed, they are used in a generic and descriptive sense only and not for purposes of limitation, the scope of the invention being set forth in the following claims.

20

CLAIMS

1. A method for setting up a policy controlled bearer service for delivery of a service from an application function (304) to a mobile terminal (301), which method comprises
- 5 registering (308) a terminal identity of the terminal (301) associated with policy identifying information in a register of a policy decision function (303);
- receiving (312) a bearer service activation request from the terminal, via a core network node (302), which bearer service activation request includes the terminal identity and a set of requested QoS parameters for the bearer service;
- 10 binding (313) the bearer service activation request to the policy identifying information by means of the terminal identity to determine applicable policy information for the bearer service;
- 15 performing (314, 315, 316) a policy check by means of checking if the requested QoS parameters fulfill said applicable policy information; and
- sending (317, 318) an accept message to the core network node to initiate completion of the bearer service set-up if the policy check was successful.
- 20 2. The method according to claim 1, wherein said terminal identity is a Mobile Identification Number, MSISDN, an International Mobile Subscriber Identity, IMSI, or an International Mobile Equipment Identity, IMEI, associated with the terminal (301).
- 25 3. The method according to claim 1 or 2, wherein said policy identifying information includes an address of the application function (304) and wherein the step (313) of binding the bearer service activation request to the policy identifying information includes requesting (314) the applicable policy information from the application function (304) identified by the application
- 30 address in the policy identifying information.
4. The method according to claim 1 or 2, wherein said policy identifying information includes the applicable policy information for the bearer service to be set up.

- 5 5. The method according to any of claims 1-4, wherein said step of performing a policy check includes checking (315) if the requested QoS parameters fulfill a set of predefined minimum QoS requirements provided by the application function (304).
- 10 6. The method according to claim 5, wherein the method includes a further step of determining a set of modified QoS parameters that match the set of predefined minimum QoS requirements if the requested QoS parameters do not fulfill the set of predefined minimum QoS requirements, and a further step of sending (316, 317) the set of modified QoS parameters to the core network node (302) for use when setting up the bearer service.
- 15 7. The method according to any of claims 1-6, wherein the core network node (302) is a Gateway GPRS Support Node, GGSN.
- 20 8. The method according to any of claims 1-7, wherein the method includes a further step of removing the registration of the terminal identity and the policy identifying information from the register of the policy decision function (303) after the step (314, 315, 316) of performing the policy check.
9. The method according to any of claims 1-8, wherein said bearer service is a Packet Data Protocol, PDP, context.
- 25 10. A method in a policy decision function (303) for performing policy control on a bearer service for delivery of a service from an application function (304) to a mobile terminal (301), which method comprises the steps of
- 30 receiving (308) a registration message, including a terminal identity and policy identifying information;
- registering the terminal identity associated with the policy identifying information in a register;
- receiving (312) a bearer service activation request from the terminal (301), via a core network node (302), which bearer service activation request

includes the terminal identity and a set of requested QoS parameters for the bearer service;

binding (313) the bearer service activation request to the policy identifying information in the register by means of the terminal identity to determine
5 applicable policy information for the bearer service;

performing (314) a policy check by means of checking if the requested QoS parameters fulfill said applicable policy information; and

sending (317) an accept message to the core network node (302) to initiate completion of the bearer service set-up if the policy check was successful.

10

11. The method according to claim 10, wherein said terminal identity is a Mobile Identification Number, MSISDN, an International Mobile Subscriber Identity, IMSI, or an International Mobile Equipment Identity, IMEI, associated with the terminal (301).

15

12. The method according to claim 10 or 11, wherein said policy identifying information includes an address of the application function (304) and wherein the step (313) of binding the bearer service activation request to the policy identifying information includes requesting (314) the applicable policy
20 information from the application function (304) identified by the application address in the policy identifying information.

13. The method according to claim 10 or 11, wherein said policy identifying information includes the applicable policy information for the bearer service
25 to be set up.

14. The method according to any of claims 10-13, wherein said step of performing a policy check includes checking if the requested QoS parameters fulfill a set of predefined minimum QoS requirements provided by the
30 application function (304).

15. The method according to claim 14, wherein the method includes a further step of determining a set of modified QoS parameters that match the set of predefined minimum QoS requirements if the requested QoS

parameters do not fulfill the set of predefined minimum QoS requirements, and a further step of sending (317) the set of modified QoS parameters to the core network node (302) for use when setting up the bearer service.

5 16. The method according to any of claims 10-15, wherein the core network node (302) is a Gateway GPRS Support Node, GGSN.

10 17. The method according to any of claims 10-16, wherein the method includes a further step of removing the registration of the terminal identity and the policy identifying information from the register after the step of performing the policy check.

15 18. The method according to any of claims 10-17, wherein said bearer service is a Packet Data Protocol, PDP, context.

19. A policy decision function (303) for performing policy control on a bearer service for delivery of a service from an application function (304) to a mobile terminal (301), which policy decision function includes

20 a first interface for receiving (308) a registration message, including a terminal identity and policy identifying information;

a register for registering the terminal identity associated with the policy identifying information;

25 a second interface for receiving (312) a bearer service activation request from the terminal, via a core network node (302), which bearer service activation request includes the terminal identity and a set of requested QoS parameters for the bearer service; and

processing means for

30 binding (313) the bearer service activation request to the policy identifying information in the policy decision function by means of the terminal identity to determine applicable policy information for the bearer service;

performing (314) a policy check by means of checking if the requested QoS parameters fulfill said applicable policy information; and

sending (317) an accept message to the core network node (302) to initiate completion of the bearer service set-up if the policy check was successful.

- 5 20. The policy decision function (303) according to claim 19, wherein said terminal identity is a Mobile Identification Number, MSISDN, an International Mobile Subscriber Identity, IMSI, or an International Mobile Equipment Identity, IMEI, associated with the terminal (301).
- 10 21. The policy decision function (303) according to claim 19 or 20, wherein said policy identifying information includes an address of the application function (304) and wherein the processing means are arranged to request the applicable policy information from the application function (304) identified by the application address in the policy identifying information.
- 15 22. The policy decision function (303) according to claim 19 or 20, wherein said policy identifying information includes the applicable policy information for the bearer service to be set up.
- 20 23. The policy decision function (303) according to any of claims 19-22, the processing means are further arranged to check if the requested QoS parameters fulfill a set of predefined minimum QoS requirements provided by the application function (304).
- 25 24. The policy decision function (303) according to claim 23, wherein the processing means are further arranged to determine a set of modified QoS parameters that match the set of predefined minimum QoS requirements if the requested QoS parameters do not fulfill the set of predefined minimum QoS requirements, and to send (317) the set of modified QoS parameters to
- 30 the core network node for use when setting up the bearer service.
25. The policy decision function (303) according to any of claims 19-24, wherein said processing means are arranged to remove the registration of the

terminal identity and the policy identifying information from the register after the processing means has completed the policy check.

1/4

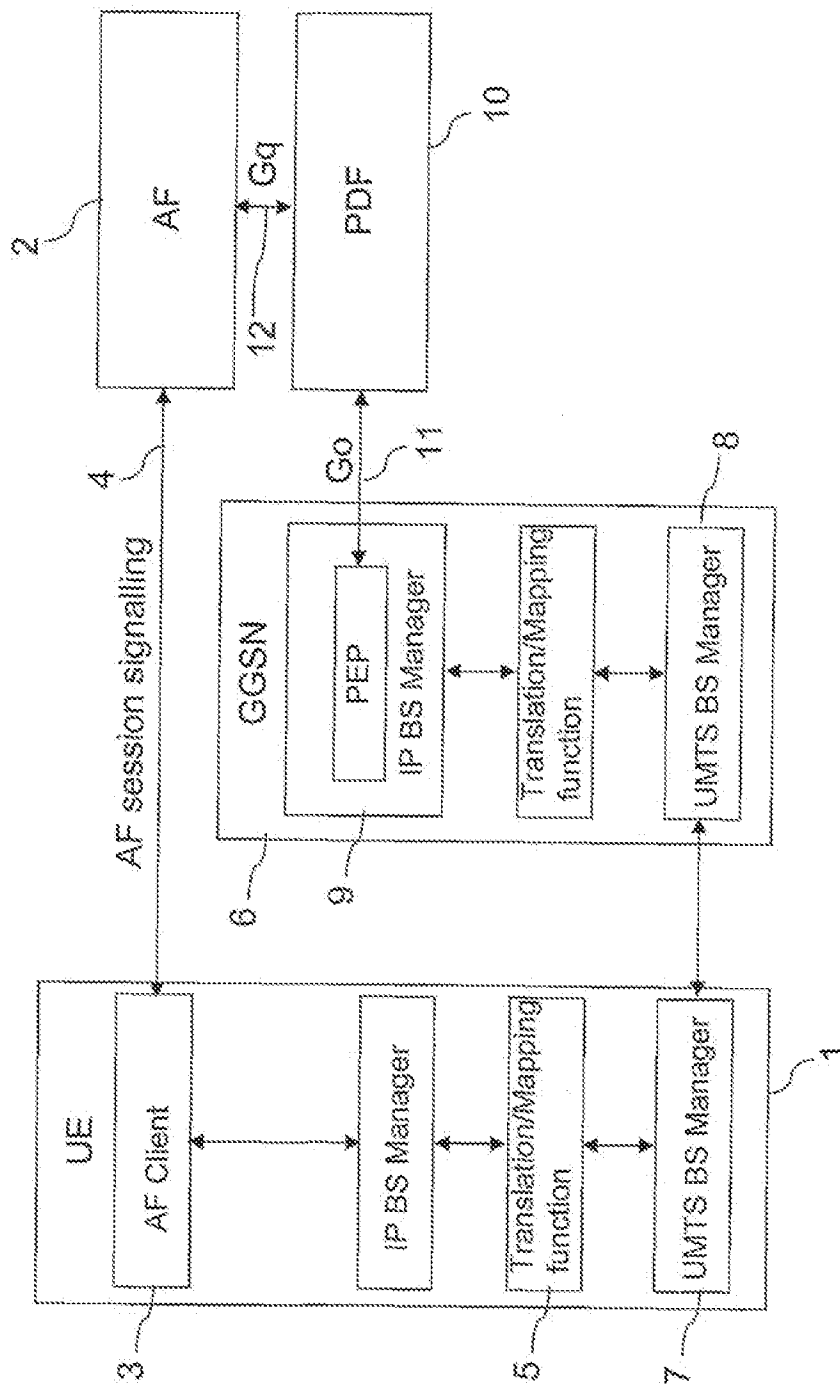


Fig. 1

2/4

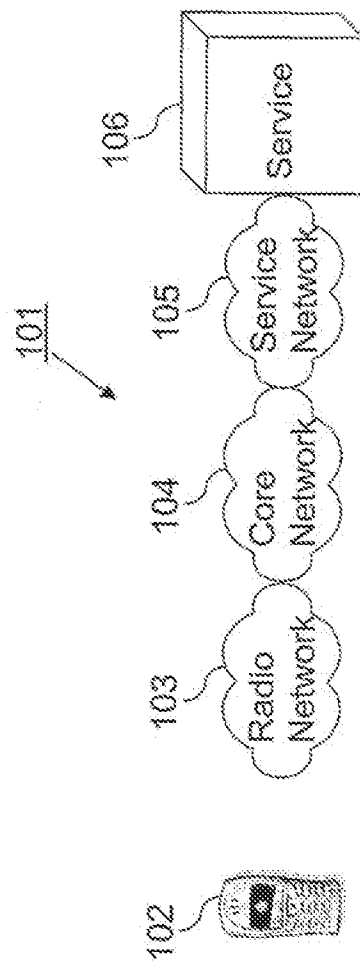


Fig. 2

3/4

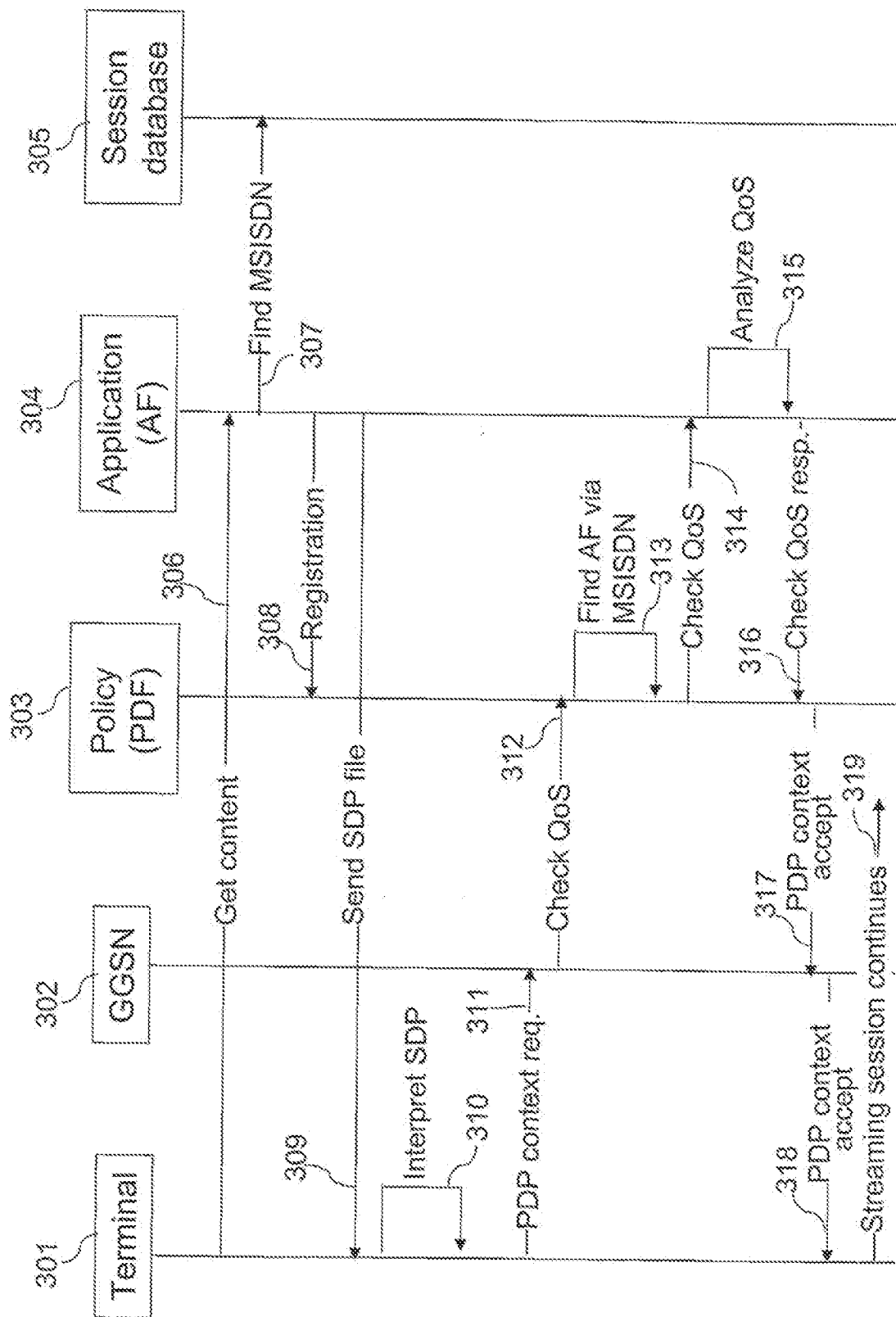
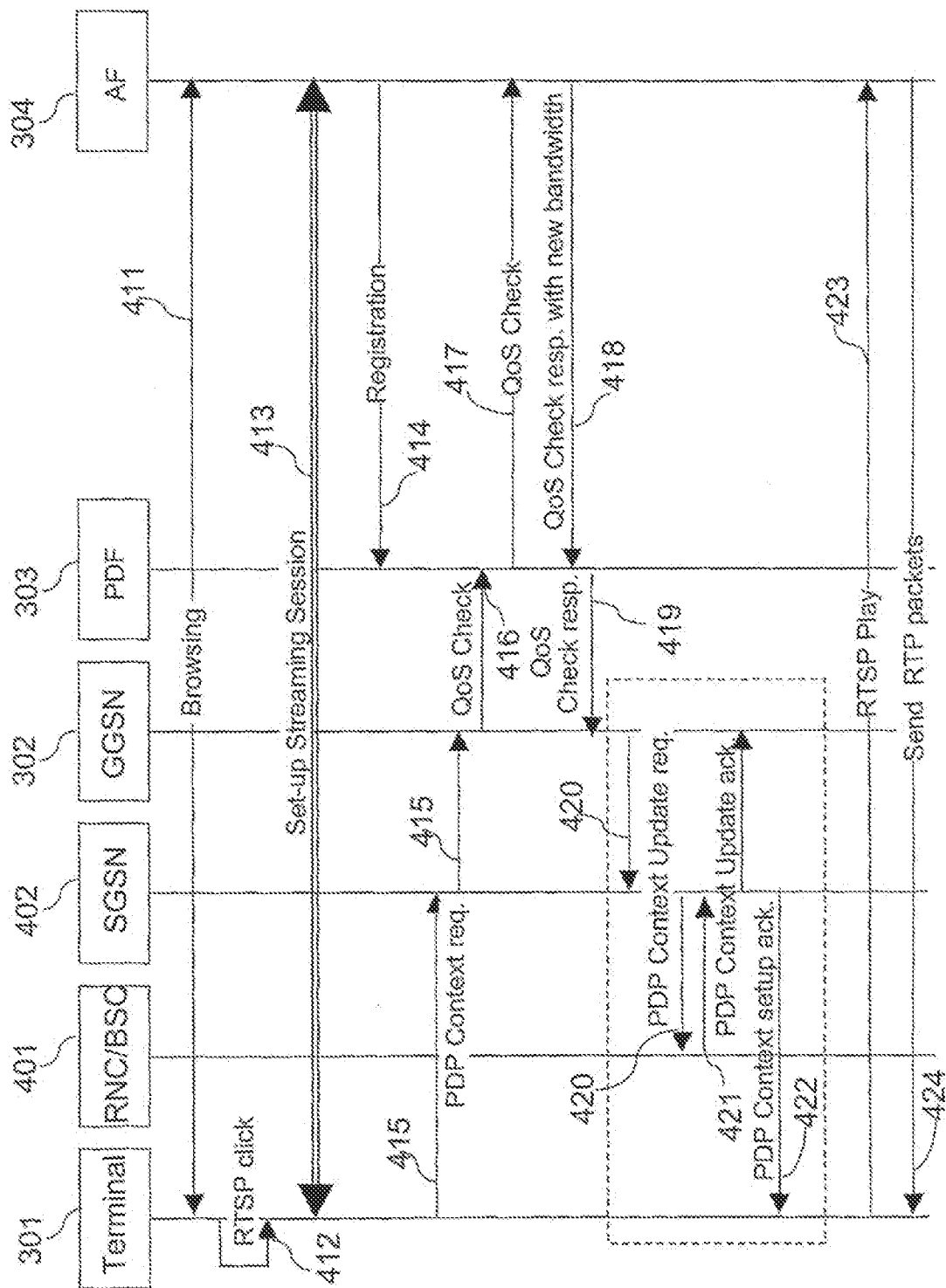


Fig. 3

4/4








INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 2004/001087

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38, H04L 12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ETSI TS 123 207 V5.9.0 (2004-03) Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); End-to-end Quality of Service (QoS) concept and architecture (3GPP TS 23.207 version 5.9.0 Release 5). See chapter 6 --	1-25
A	WO 03049348 A2 (NOKIA INC), 12 June 2003 (12.06.2003), claims 1,8,9, abstract -- -----	1-25

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

18 February 2005

Date of mailing of the international search report

24-02-2005

Name and mailing address of the ISA/

Swedish Patent Office

Box 5055, S-102 42 STOCKHOLM

Facsimile No. +46 8 666 02 86

Authorized officer

Lisbeth Andersson /LR

Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

30/01/2005

International application No.

PCT/SE 2004/001087

WO	03049348	A2	12/06/2003	AU	2002353271	A	00/00/0000
				US	6661780	B	09/12/2003
				US	20030108015	A	12/06/2003

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
18 May 2006 (18.05.2006)(10) International Publication Number
WO 2006/050758 A1(51) International Patent Classification: **H04L 29/06**(21) International Application Number:
PCT/JP2005/002837

(22) International Filing Date: 17 March 2005 (17.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
00626,691 10 November 2004 (10.11.2004) US(71) Applicant (for all designated States except US): TELEFONAKTIEBOLAGET LM ERICSSON (publ)
[SE/SE]; S-164 83 Stockholm (SE).

(72) Inventor; and

(75) Inventor/Applicant (for US only): BOMAN, Krister
[SE/SE]; Nimbussgatan 3, S-431 44 Mölndal (SE).(74) Agents: BERGENTALL, Annika et al.; Cogumark AB,
P.O. Box 53047, S-400 14 Göteborg (SE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

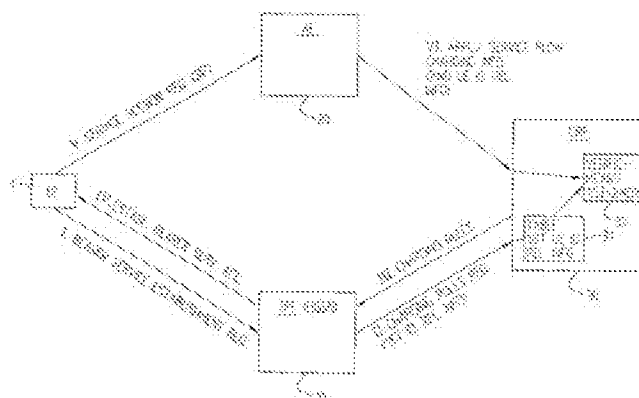
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: AN ARRANGEMENT, NODES AND A METHOD RELATING TO SERVICES ACCESS OVER A COMMUNICATION SYSTEM



(57) Abstract: The present invention relates to an arrangement in a communications system participating in user station (UE), service request and/or access procedures and comprising a number of packet data support nodes (10), a number of charging and/or policy handling nodes (30) and a number of application functions (20) handling mobility management and call control of mobile user stations requesting and/or accessing services. The packet data support node(s) (10) comprise(s) means adapted to send first mobile user station identity related information over a first interface (Gx/Gy/Gx/Gy) to a charging and/or policy handling node (30), at reception of a request for bearer services from a mobile user station (1). The application function(s) (20) comprise(s) means for, at reception of a request for a service session (SIP) from a mobile user station (1), sending second mobile user station identity related information to the charging and/or policy handling node (30), over a second interface (Rx/Rx/Cg). The policy and/or charging handling node (30) comprises verification means (32) adapted to establish whether the request for a bearer service to the packet data support node (10) and the request for a service session to the application function (20) (AF/P/SA-CSCF) originate from one and the same mobile user station (1).

WO 2006/050758 A1

Title:

5 AN ARRANGEMENT, NODES AND A METHOD RELATING TO SERVICES ACCESS
OVER A COMMUNICATION SYSTEM

10 FIELD OF THE INVENTION

The present invention relates to an arrangement in a communications system participating in user station service request or access procedures and it comprises a number of packet data support nodes, a number of charging and/or policy handling
15 nodes and a number of application functions handling mobility management and call control of mobile user stations requesting or accessing services. The invention also relates to a node in a communications system supporting communication of packet data which is arranged to communicate with an application function and
20 a packet data support node.

Still further the invention relates to a method involved in service request/access, in a communications system supporting communication of packet data and comprising a number of packet
25 data nodes, a number of charging and/or policy handling nodes and a number of application functions handling mobility management and call control of mobile user stations requesting/accessing services.

30 STATE OF THE ART

So called IM (Internet IP Multimedia) services are getting more and more attractive and are already widely used. 3GPP IMS (IP Multimedia Subsystems) provides an IP-based session control

capability which is based on the SIP protocol (Session based Initiation Protocol). IMS may for example be used for the provisioning of services such as push-to-talk, instant messaging, presence and conferencing. IMS in UMTS (Universal Mobile Telecommunication System) will support IP multimedia applications such as video, audio and multimedia conferences. As referred to above, 3GPP will use the SIP, Session Initiation Protocol, as the signalling protocol for creating and terminating multimedia sessions, c.f. for example IETF RFC (Request For Comments) 3261, which deals with how the SIP signalling is protected between the subscriber and the IMS, how the subscriber is authenticated and how the subscriber authenticates the IMS.

The current security architecture for IMS is specified in 3GPP TS 33.203. However, it is a problem that implementations of the services referred to above will exist which are not fully compliant with 3GPP IMS. 3GPP IMS for example exclusively uses IPv6 (Internet Protocol version 6) although there may still be IMS implementations based on IPv4. However, the use of IPv4 instead of IPv6 is only one of the differences between "early" IMS implementations and implementations complying with 3GPP IMS to a full extent. It has been recognized that non-compliance with 3GPP TS 33.203 security features, will mainly produce problems at the user equipment (UE) due to the potential lack of support of the USIM/ISIM interface, particularly for user stations only complying with 2G. It has therefore been realized that, for such "early" IMS implementations, mechanisms are needed to protect against the most significant security threats.

30

Such a temporary solution for "early" IMS implementations is suggested in 3GPP TR 33.878. The approach in this document is that the GGSN (Gateway GPRS Support Node) shall send MSISDN and

the IP address of a user station (User Equipment UE) towards a Radius server over the Gi interface. The Radius server then forwards the MSISDN and IP address to the HSS (Home Subscriber Server). When the user station, or the UE, sends a SIP register
5 request towards a Serving-Call/Session Control Function (S-CSCF), including the IM (IP Multimedia) private identity, the S-CSCF will query the HSS, which, based on the IMS identity can identify the matching MSISDN and IP address of the UE and return the IP address to the S-CSCF. The S-CSCF will check with the
10 stored IP address in the S-CSCF to see if it matches the received IP address from the UE. If the two IP addresses are the same, the S-CSCF can proceed with the registration procedure but if they are not the same, presumably due to an attack being in progress, the session is terminated. This gives a possibility to
15 avoid certain attacks such as for example an attacker using the IMS identities of a victim, which may have as a consequence that the attacked user has to pay for the service accessed by the attacker.

20 An operator also runs the risk that the attacker does not pay for the bearer, e.g. a conversational bearer, due to the fact that for example FBC (Flow Based Charging) is implemented and zero rates the bearer. This means that for some use cases, an attacker could use certain services for free.

25 3GPP TR 33.878 assumes that "During a PDP-context request towards the IMS, the GGSN shall send a "Radius Accounting-Request-Start" message to a Radius server attached to the HSS. This may lead to the assumption that an operator uses a specific
30 IMS APN (Access Point Name) or that the UE uses a signalling PDP-context. It is however believed that the assumption relating to the use of a specific IMS APN is too restrictive from an architectural point of view. 3GPP TS 23.228 stipulates that

"When the UE uses GPRS-access for IMS services, it shall be able to establish a dedicated signalling PDP-context for IM subsystem related signalling or utilize a general-purpose PDP-context for IM subsystem signalling traffic". There is hence no guarantee that the UE uses a signalling PDP-context for IMS, may lead to the conclusion that the GGSN should then send the IP address of a UE towards a Radius server for all services. Further, an UE may have several IP addresses towards one and the same GGSN and it appears necessary that the GGSN, in such a case, has to send all these IP addresses towards the Radius server. Furthermore, in the general case a UE may be attached to more than one GGSNs or it may have activated more than one IP network connections. Such scenarios are not discussed in 3GPP TR 33.878.

Furthermore, the solution discussed in this document suggests the introduction of a so called "idle timer" in GGSN. This has an impact on how IP addresses towards an UE are allocated or released and an IP address can be reused for a user when re-establishing a PDP-context at a later stage. Apparently the reason for the introduction of the idle timer is to reduce the load on the HSS and, when there is no PDP-context available between GGSN and an UE, the GGSN stores or reserves the allocated IP address for a specific UE for a time which is equal to the time period set in the idle timer. This means that the GGSN does not upon termination of all bearers send an accounting-request stop until the idle timer has expired. Thus the idle timer has not been introduced for security reasons but in order to reduce the communication towards the HSS which is responsible for the creation of authentication vectors and hence the intention is to reduce communication with the HSS, or not to allow more communication with HSS than necessary in order to avoid that it becomes overloaded, which might have the effect that other services, for example voice, would suffer. The use of

the idle timer is disadvantageous for example in that there will be an increasing risk for conflicts between dynamically allocated IP addresses. Furthermore resources are held more than necessary.

5

The suggested solution is also disadvantageous in that more and more information is sent from GGSN over the Gi interface which will become more and more loaded. It is also disadvantageous that a Radius server is needed in order to verify the IP
10 addresses and, as referred to above, it does not take general architectures into account such as when a UE for example is attached to more than one GGSN and/or has activated more than one IP network connection etc.

15 SUMMARY OF THE INVENTION

Therefore an arrangement as initially referred to is needed through which IMS security can be provided for in a straight-forward and easy manner. Particularly an arrangement is needed through which so called "early" IMS security can be provided,
20 i.e. in networks still not (fully) complying with the 3GPP TS 33.203 Release 5. Particularly an arrangement is needed through which attacks can be detected and prevented and particularly through which security can be increased for end users as well as for operators, for example such that an attacker is prevented
25 from using certain services for free or making someone else pay for it, and that an attack can be detected as early as possible which is extremely important for the end user as well as for the operator.

30 Particularly an arrangement is needed which is flexible and which can be adapted to different network environments, such as for example so called aware network environments. Still further an arrangement is needed which takes into account and takes

advantage of the development for example within 3GPP or similar systems. Still further an arrangement is needed through which the amount of information sent over the so called Gi interface from Gateway GPRS Support Nodes or similar can be reduced instead of increased. Most particularly an arrangement is needed through which there is no need for the introduction of additional nodes and more generally through which the number of nodes involved and affected can be kept as low as possible. An arrangement is also needed which reduces or even eliminates the drawbacks and impacts on IP address allocation or release towards an UE arising through the introduction of a so called idle timer in a GGSN.

Still further an arrangement is needed which can be used in a general architecture and which takes into account situations, as for example when a user equipment is attached to more than one GGSN (or CGSNs or other gateways) and/or when a user equipment has activated more than one IP network connection. Still further a node is needed which assists in provisioning of one or more of the objects referred to above. Still further a method is needed through which one or more of the abovementioned objects can be achieved.

Therefore an arrangement as initially referred to is provided wherein the packet data support node(s)/comprise(s) means adapted to send first mobile user station identity related information over a first interface (Gx,Gy;Gx/Gy) to a charging and/or policy handling node, at reception of a request for bearer services from a mobile user station, the application function(s) comprise(s) means for, at reception of a request for a service session (SIP) from a mobile user station (UE), sending second mobile user station identity related information to the charging and/or policy handling node, over a second interface (Rx,Rx/Gq), and wherein the

policy and/or charging handling node comprises verification means adapted to establish whether the request for a bearer service to the packet data support node and the request for a service session to the application function (AF;P/S/I-CSCF) originate from one and
5 the same mobile user station (UE). Particularly the first mobile user station identity related information comprises one or more of MSISDN, IMSI and IP address of the mobile user station, and the second mobile user station identity related information comprises IMS private identity (IMPI) and/or IMS public identity (IMPU), or
10 IMSI and/or MSISDN, e.g. derived from IMS private or public identity (IMPI,IMPU), or the application function being adapted to fetch said information externally, e.g. from a HSS.

Particularly the IP addresses are received in, or derived from,
15 the first mobile user station related information and the second mobile user station identity related information, and the verification means are adapted to compare the IP address obtained from the application function (AF) with the IP address obtained from the packet data support node. In one embodiment the
20 verification means are adapted to, if required, establish and, use IMSI and/or MSISDN of said first and second mobile user station identity related information respectively, to compare the associated IP addresses. The charging and/or policy handling node may also be adapted to deduce IMSI and/or MSISDN from a received
25 IMS private and/or public user identity (IMPI/IMPU).

In an advantageous embodiment the charging and/or policy handling node is adapted to construe a private user identity using IMSI of a mobile user station, e.g. when no ISIM application is
30 implemented and further it is particularly adapted to identify and install charging rules to be applied at reception of a request therefor from a packet data support node.

According to the invention, if the first and second user identity related information do originate from one and the same mobile user station, the charging and/or policy handling node is particularly adapted to implement the provisioned charging rules. If, on the other hand, the first and second user identity related information do not originate from one and the same mobile user station, the charging and/or policy handling node may be adapted to reject the charging rules and/or deactivate implemented charging rules and discard concerned IP flow traffic, and further be adapted to inform the application function (AF) that no PDP-context is available.

Alternatively, if the first and second user identity related information do not originate from one and the same mobile user station, the charging and/or policy handling node may be adapted to select whether to or deactivate the charging rules in the packet data support node, or to keep them active (or activate them). In a particular embodiment the packet data support node comprises a node handling Traffic Plane Functions (TPF), e.g. a GGSN implementing TPF or a CGSN implementing TPF. It may alternatively comprise a stand-alone node or a gateway node handling TPF or TPF and policy enforcement (PEP).

According to different embodiments the charging and/or policy handling node comprises a CRF, a PDF or a PCCN. Particularly the first interface is Gx or Go/Gx merged with Gy if the charging and/or policy handling node is merged with an OCS, and the second interface comprises Rx or Rx merged with Gq.

A node (functional, logical or physical) in a communication system as initially referred to is also provided which is adapted to receive first mobile user station identity related information from a packet data support node relating to a bearer service

request for a mobile user station, or at reception of a request for a bearer service from a mobile user station (UE) in the packet data support node, to receive second mobile user station identity related information from an application function relating to a service session or at reception of a request for a service session therein, and comprises verification means for establishing whether the request for a bearer service (to the packet data support node) and the request for a service session (to the application function) originate from the same mobile user station. Particularly the first mobile user station identity related information comprises one or more of MSISDN, IMSI and IP address of the mobile user station. Even more particularly the second mobile user station identity related information comprises IMS private identity (IMPI) and/or IMS public identity (IMPU) of the mobile user station or IMSI and/or the handling node is adapted to derive IMSI and/or MSISDN from IMPI and/or IMPU and/or adapted to request said IMSI and/or MSISDN from the application function.

The verification means are preferably adapted to compare the IP address corresponding to or included in the first mobile user station identity related information and the IP address corresponding to or included in the second mobile user station identity related information, and particularly to, if required establish and, use IMSI and/or MSISDN of said first and second mobile user station identity related information, to compare the associated IP addresses. Alternatively it is adapted to derive IMSI and/or MSISDN from a received IMS private and/or public user identity (IMPI/IMPU). Particularly the charging and/or policy handling node is adapted to construe a private user identity using IMSI of a mobile user station, e.g. when no IMSI application is implemented.

10

It may also be adapted to identify and install charging rules to be applied at reception of a request therefor from a packet data support node. Particularly it is adapted to identify and install charging rules to be applied at reception of request therefor from
5 a packet data support node, and if the first and second user identity related information do originate from one and the same mobile user station, to implement the provisioned charging rules, and, if the first and second user identity related information do not originate from one and the same mobile user station, to reject
10 the charging rules and/or deactivate implemented charging rules and discard concerned IP flow traffic, to inform the application function (AF) that no PDP-context is available or, to select whether to deactivate the charging rules in the packet data support node, or keep them active, if activated. Particularly it
15 comprises a CRF, a PDF or a PCCN or a node with a similar functionality.

Still further a method as initially referred to is provided which comprises the steps of; receiving a request for bearer
20 services from a mobile user station in a packet data support node; sending, from the packet data support node, first mobile user station identity related information of the mobile user station to a charging and/or policy handling node; receiving, subsequently, before or substantially simultaneously, a request for a service
25 session from the mobile user station in an application function; sending, from the application function, second mobile user station identity related information to the charging and/or policy handling node; establishing, in the charging and/or policy handling node, whether the request for a bearer service to the
30 packet data support node and the request for a service session to the application function originate from the same mobile user station.

11

As referred to earlier, particularly the first mobile user station identity related information comprises one or more of the MSISDN, IMSI and IP address of the mobile user station, and the second mobile user station identity related information comprises IMS private identity (IMPI) and/or IMS public identity (IMPU), or the second user identity related information comprises IMSI and/or MSISDN, e.g. derived from IMS private or public identity (IMPI, IMPU), or the application function is adapted to fetch said information from a HSS. Particularly the method further comprises the steps of; establishing or finding IMSI and/or MSISDN of said first and second mobile user station identity related information, comparing at least part of said first and said second mobile user station identity related information with each other, and even more particularly of comparing the IP addresses of said first and second mobile user station identity related information and/or deriving IMSI and/or MSISDN from received IMS private and/or public user identities (IMPI/IMPU), and/or construing, in the charging and/or policy handling node, a private user identity using IMSI of the mobile user station, e.g. when no ISIM application is implemented.

Advantageously it also comprises the step of; identifying and installing applicable charging and/or policy rules at reception of a request from a packet data support node. Most particularly the method further comprises the steps of; if the first and second mobile user station identity related information do originate from one and the same mobile user station; implementing the provisioned applicable charging rules and/or policy rules in the charging and/or policy handling node, otherwise, discarding concerned IP flow traffic; or selecting whether to keep active or deactivate the charging rules. In preferred implementations the packet data support node comprises a node handling Traffic Plane Functions, and is a stand-alone node, or a GGSN or a CGSN or a gateway node

handling TPF and policy enforcement (PEP), and the charging and/or policy handling node comprises a CRF, a PDF or a PCCN or a node with a similar functionality.

5 BRIEF DESCRIPTION OF THE DRAWINGS

The invention will in the following be further described, in a non-limiting manner, and with reference to the accompanying drawings in which:

- 10 Fig. 1 shows a "state of the art" solution,
- Fig. 2 is a schematical block diagram illustrating an arrangement according to the present invention,
- 15 Fig. 3 is a simplified sequence diagram illustrating the provisioning of the first mobile user station identity related information to a charging and/or policy handling node,
- 20 Fig. 4 is a simplified sequence diagram including the procedure when the second mobile user station identity related information is provided to the charging and/or policy handling node,
- 25 Fig. 5 is a sequence diagram illustrating an exemplary procedure of the provisioning of the second mobile user station identity related information and verification thereof,
- 30 Fig. 6A is a sequence diagram describing an exemplary implementation and wherein the verification result is positive,

Fig. 6B is a sequence diagram describing the exemplary implementation of Fig. 6A but wherein the verification result is negative,

5 Fig. 7 is a schematical block diagram illustrating the inventive concept implemented in one general architecture,

10 Fig. 8A illustrates another general architecture in which the inventive concept can be implemented,

Fig. 8B shows still another architecture in which the inventive concept can be implemented, and

15 Fig. 9 is a flow diagram describing the procedure according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Fig. 1 shows the state of the art solution discussed earlier in the application for providing security for IMS accesses, particularly for early implementations of IMS not yet complying with the requirements of 3GPP TS 33.203. Such a solution is among others discussed in 3GPP TR 33.878. It is supposed that an UE 1₀ requests a bearer from GGSN 10₀. PDP-contexts are set-up in a conventional manner, primary or secondary depending on which is the relevant procedure. The user equipment UE 1₀ may have several IP addresses, one IP address per IP network connection. GGSN comprises an idle timer 11₀ through use of which an IP address can be reused for a user when re-establishing a PDP-context at a later stage. There is no specific IMS APN (Access Point Name) and GGSN cannot assume use of a signalling PDP-context. Knowing, in a conventional manner MSISDN and the IP address of UE 1₀, GGSN 10₀ sends MSISDN and the IP addresses over

20
25
30

the Gi interface towards Radius Server 30₀, i.e. all UE IP addresses and MSISDN are sent. The idle timer used in GGSN 10₀ apparently is intended mainly to reduce the load on the HSS. This is suggested to be in the order of hours working in such a way that when there is no PDP-context available between GGSN and UE, the GGSN stores or reserves the allocated IP address for a specific UE for a time period which corresponds to the time set in the idle timer. This would mean that the GGSN does not upon termination of all bearers send any accounting-request-stop until the idle timer has actually expired. This idle timer does influence how IP addresses towards the UE are allocated or released.

The Radius Server 30₀ forwards the information, i.e. MSISDN and the IP address to HSS 40₀. All UE IP addresses and the MSISDN are sent according to the idle timer 11₀ in the GGSN 10₀, i.e. the sending will generally be slowed down, or delayed, until the idle timer expires.

Then a request for a SIP registration (SIP REGISTER) is sent from UE 1₀ to S-CSCF, the S-CSCF sends the IMS identity onto the HSS 40₀. HSS 40₀ returns a reply to S-CSCF with the registered IP address back to the S-CSCF 20₀. S-CSCF 20₀ comprises a verification means 21₀ or a functionality for performing a verification through verifying that the IP address from HSS 40₀ is the same as the stored IP address in S-CSCF. If they are not the same, the session is terminated because it is assumed that an attack is ongoing.

The disadvantages of such a solution has been discussed earlier in the application.

Fig. 2 shows an arrangement according to one implementation of the inventive concept according which a FBC (Flow Based Charging) architecture is reused. The problem that is solved through the arrangement consists in the provisioning of a mechanism ensuring that the network is enabled to verify that the IP address of a user equipment UE 1 and the IMS identity of the UE 1 at SIP layer correspond to the same user at the bearer level. According to invention, the involved nodes or functions are the GGSN 10 handling traffic plane function TPF, (according to the inventive concept it is the traffic plane function that is used and it may be realized as a stand-alone node, provided in a GGSN or in a CGSN or in any node at least including the TPF functionality), a charging and/or a policy handling node 30 which in this embodiment is implemented as a CRF (Charging Rules Functionality) and an application function AF 20 which may be implemented as a S-CSCF, a P-CSCF or similar, and the concerned user equipment UE 1. CRF 30 comprises storing means, e.g. a table for storing first user equipment identity related information as will be explained below, and verification means 32 for verifying if at least a given part of a first UE identity related information corresponds to second UE identity related information, e.g. through comparing at least parts of said first and second identity related information respectively. By at least part of is meant that it might not be necessary to compare all the information depending on implementations, as also will be explained below. It is, however, in Fig. 2 supposed that UE 1 sends a request for bearer service establishment (I) to TPF 10 which may be implemented in a GGSN. TPF 10 then, in for example a CRF based implementation, as in Fig. 2, requests for charging rules (II) from CRF 30. First UE identity related information accompanies the request. The first UE identity related information may be provided from the UE or provided from TPF 10 (if it for example relates to a secondary PDP-context request).

16

How this is done or acquired is not of importance for the functioning of the present invention, the main thing being that the first UE identity related information is available in TPF 10. The first UE identity related information accompanying the charging rules request is then stored into table 31 in CRF 30, CRF 30 among others using the first UE identity related information and possibly other information, for example QoS information about application function etc., identifies which are the relevant charging rules to be installed, and then provides the charging rules to TPF 10 (III). TPF 10 performs the relevant charging rule actions or provides for implementation of the provisioned charging rules, and sends an acceptance message relating to the establishment of the bearer service request, (IV) to UE 1.

15

Once a bearer has been established, UE 1 sends a request for a service session using SIP, (V) to AF 20. In GPRS systems, and from an FBC point of view, a proxy-CFCS and/or a serving-CFCS and/or an Interrogating CSCF may, depending on operator configuration, act as an AF operating the Rx interface and/or the Gq interface. In the request using the SIP protocol, second user identity related information of the requesting is included. AF 20 then sends application/service flow charging information, including the second UE identity related information to CRF 30 (VI). If for example an S-CSCF acts as an AF, it may, before a registration session is proceeded, unsolicited forward the private user identity along with the IP address of the UE over Rx towards CRF 30. At PDP-context activation, FBC assumes that the IP address of the UE and IMSI (or MSISDN) are sent towards the CRF 30 over the Gx interface. Based on the above assumptions, CRF 30 is then aware of the IMSI both from the AF 20, particularly S-CSCF, and the TPF 10, particularly GGSN, and the corresponding IP addresses and hence capable to, in the

30

verification means 32, check if the IP addresses match or originate from one and the same user (in Fig. 1 they actually both originate from the same UE, namely UE 1). If they do not correspond, or do not originate from one and the same end user, i.e. if there is no match between the IP addresses, CRF 30 (in this case; it should be clear that for policy handling the node could be a PDF, but it may also be a PCN for handling policy and/or charging) notifies the AF 20, particularly S-CSCF, in order to provide for a termination of the SIP session, and the CRF 30 should deactivate any corresponding rule(s) at the TPF 10.

It could of course also be optional whether the session should be terminated or not and optionally it may be operator controlled, such that under certain circumstances for example an operator might want to localize or track an attacker and therefore would let the session proceed. Also for other reasons an operator might allow the session under certain conditions etc. The invention is not limited to any particular measures to be taken, but it is fundamental that an awareness is provided concerning the correspondence of addresses and possible attacks or similar.

The second user identity related information sent from AF 20 to CRF 30 may for example contain IMPI (IMS Private Identity), IMPU (IMS Public Identity), and the IP address. Alternatively the AF 20 may send IMSI or MSISDN directly. This can either be derived from the private identity or alternatively the AF, e.g. S-CSCF may contact HSS to identify IMSI or MSISDN.

30

If for example the UE does not contain an ISIM, (but for example an USIM) IMPI may be derived and the private user identity

18

should take the form of a NAI and shall have the form username@realm as specified in IETF RFC 2486, clause 3.

5 A representation of the IMSI may be contained within the NAI for the private identity.

If there is no ISIM application, the private user identity is not known and it may then be derived from IMSI. The private user identity may be construed out of the IMSI by using the whole string of digits as username part of the private user identity, and by converting the leading digits of the IMSI, i.e. MNC and MCC into a domain name.

The result will be a private user identity of the form:
15 "<IMSI>@ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org". For example: If the IMSI is 234150999999999 (MCC=234, MNC=15), the private user identity will takes the form
234150999999999@ims.mnc015.mcc234.3gppnetwork.org

20 Hence, CRF/PDF (PCCN) is capable to, based upon the reception of IMPI, i.e. the IMS Private Identity, or even IMPU, the Public User Identity, and IP address from an AF, for example a CSCF such as P-CSCF, S-CSCF, or I-CSCF, over Rx or Gq or Rx merged with Gq, derive IMSI (or MSISDN) of the UE. It should be noted
25 that the AF alternatively may send MSISDN and/or IMSI directly over Rx/Gq as referred to above.

Furthermore, since the TPF, here TPF implemented in a GGSN, shall have the capability to send the IMSI or MSISDN to the
30 CRF/PDF/PCCN (over Gz or Gx/Gy if merged), the CRF/PDF can then match the IMSI (or MSISDN) from CRF and TPF (here GGSN) with the respective IP addresses, i.e., CRF 30 is capable to find IMSI (MSISDN) from, here, GGSN and AF and check that it is the same

IP address associated. If there is a match, the CRF preferably implements, in this case, charging rules as specified in 3GPP TS 23.125. If, on the other hand, the IP addresses do not originate from one and the same UE, the CRF may decide not to implement the charging rules or deactivate already implemented charging rules as referred to above, and hence the traffic may be discarded for the concerned IP flow. The CRF then informs the AF, e.g. a P-CSCF/S-CSCF that no PDP context is available.

Alternatively, may, in certain situations, as also referred to above, an operator want to allow the traffic, for example in order to track an attacker. Hence it may be an option for the charging and/or policy handling node 30 to keep rules in the TPF 10 active or to deactivate them.

In some implementations the TPF is implemented in a GGSN (or CGSN) but, as referred to above, TPF may be implemented in a stand-alone node or function or be allocated elsewhere than in a GGSN/CGSN, the main thing being that it is the traffic plane function TPF that is involved according to the inventive concept, since it is TPF that operates Gx towards CRF/PDF (or PCCN) (or Gx/Gy when merged).

The invention functions in a similar way for public user identities as for private user identities. 3GPP TS 23.003 specifies that when no ISIM is used, the temporary public user identity should be of the form "user@domain", and should therefore be equal to the private user identity. It is further possible to use a public user identity rather than the private identity at SIP layer. Then the AF, e.g. S-CSCF, may e.g. request an IMSI from HSS based on the public user identity, derive IMSI from the public user identity or send the public user identity towards CRF/PDF/PCCN that derives IMSI or sends a

query to a Subscription Profile Repository, if implemented, cf. Fig. 5, for getting IMSI or MSISDN.

Fig. 3 is a schematical sequence diagram illustrating the messaging between an UE, a TPF and, in this case a CRF. It should be clear, as referred to above, that the TPF can be provided for as a stand-alone node, in a GGSN, in a CGSN or in any other node or functioning means at least providing the TPF functionality. It should also be clear that instead of a CRF handling charging rules, it could as well be a PDF handling policy rules or a combined node or functionality handling e.g. both policy and charging. Hence, it is supposed that the UE, in a conventional manner, sends a request for establishment of a bearer service, 1, to e.g. a GGSN providing the TPF functionality. At PDP-context activation, first or primary, the GGSN, in this case, will send terminal identities such as one or more of IP address, MSISDN and IMSI towards CRF over the Gx interface in a request for charging rules, 2, i.e. the first user equipment identity related information is accompanying the request for charging rules. CRF stores the received first UE identity related information, 3, and identifies which are the charging rules that are applicable and should be installed, 4. Subsequently the charging rules are provisioned to TPF, 5. TPF at reception of the charging rules performs the charging rule action or actions, 6, and sends an establish bearer service acceptance message to UE, 7.

It should be clear that, as referred to above, the CRF may be merged with a PDF. Even more particularly CRF (and/or PDF or PCCN) may be merged with an Online Charging System OCS in which case Gx may be merged with Gy. These interfaces are defined in TS 23.125, and may e.g. in one embodiment both be based on Diameter Credit Control.

Fig. 4 is schematical sequence diagram illustrating the procedure through which the second UE identity related information is provided to CRF (for example) such that a verification can be carried out according to the inventive concept.

Hence, it is supposed that when UE sends a request for a service session using the SIP protocol, 8, to AF which e.g. may comprise a P-CSCF or an S-CSCF or an I-CSCF acting as an AF, this includes sending user identities to the CRF over Rx, which is described in 3GPP TS 23.228, which herewith is incorporated herein by reference. In other words, the UE sets up a SIP Register towards the IMS network. Hence, when a request for service session, SIP Register, 8, is sent to AF, AF provides application/service data flow charging information including second UE identity related information, e.g. IMPI, IMPU, IP address, to CRF, 9. CRF, having stored the first UE identity related information in storing means, fetches said first UE identity related information and compares it with the second UE identity related information received from the AF, 10. It is here supposed that the first and the second UE identity related information respectively originates from one and the same UE, and hence an acknowledgment, 11, is sent to AF and the service is setup implementing the relevant charging rules or similar.

It should be clear that the Rx interface may be merged with Gq and the AF may hence operate Rx/Gq. Rx and Gq may in particular embodiments both be based on Diameter Nasreq.

It should be clear that, as an alternative of sending IMPI and IMPU i.e. IMS private and public identity respectively as described in TS 23.228 and TS 23.003, the AF, or any CSCF, may

send IMSI or MSISDN directly to CRF. IMSI or MSISDN may be derived from the private identity or communication with HSS may be needed for identification of IMSI or MSISDN. This has been discussed earlier with reference to Fig. 2.

5

The CRF particularly comprises a table for translation between IMPI and IMSI.

Fig. 5 is a sequence diagram illustrating the procedure when the
10 second UE identity related information is provided to e.g. a CRF or a PCCN etc., where (here) a successful verification is performed. It is here supposed that a PDP-context is established, and that the first UE identity related information is available in a CRF, PCCN etc. It is supposed that the UE is
15 in a visited network and sends a SIP register, 80, with public user ID, private user ID, UE IP address to P-CSCF. The SIP register is sent from P-CSCF to I-CSCF of the UE home network, 81. I-CSCF sends a Diameter (in this particular embodiment) Cx-Query/Cx-Select-Pull message, 82, to HSS, which returns the
20 corresponding response, 83, concerning IMS identities. SIP register with Public User ID, Private User ID, UE IP Address is then sent from I-CSCF to S-CSCF, 84. In this particular embodiment it is supposed that S-CSCF act as an AF. In alternative embodiments P-CSCF or I-CSCF may acts as AF. It
25 shall be clear that here TFF and the subscription information repository are not visible.

Steps 85,86 relate to provisioning of security parameters, application IP address etc. which however is not of relevance
30 for the inventive concept.

Subsequently it is supposed that the second UE identity related information, Public User ID, Private User ID, UE IP Address are

provided to CRF (PCCN etc.), 87, and after verification (here supposed to be affirmative) with the first UE identity related information (not shown here), an acknowledgement is sent to S-CSCF, 88. S-CSCF sends a positive verification message, 2XX OK to I-CSCF, 89, which forwards it to P-CSCF, 90, which in turn forwards it to UE, 91.

Fig. 6A shows one example of an implementation in which it is supposed that the 1st and 2nd UE identity related information can be positively verified (i.e. there is correspondence) and in which the Diameter protocol is used.

Thus, first the UE sends (here) an Activate PDP Context Request to (here) an SGSN, 1₁. In a conventional manner SGSN sends a Create PDP Context Request to GGSN, 2₁, which here uses a Radius Client to obtain IP addresses of UEs.

In this embodiment it is supposed that the Diameter protocol is used (cf. 3GPP TS 29.210), and GGSN sends a request for rules, here a Diameter CCR (Credit Control Request) with IMSI, MSISDN IP Address, over Gx to CRF (or PCCN etc.), 3₁. CRF responds with a Diameter CCA (Credit Control Answer) with charging rules over Gx, 4₁, to GGSN, which sends a Create PDP Context response to SGSN, 5₁. SGSN sends an Activate PDP Context Accept to UE, 6₁, with the allocated PDP Address (IP Address). As described earlier, it is supposed that the UE sends a SIP register to GGSN, 7₁, which checks for IP address spoofing (i.e. checks that the UE has not changed, i.e. uses another, IP address than the one it has been given). When it is verified that the UE uses the "correct" IP address, a SIP register is sent to P-CSCF, 8₁, which sends it to I-CSCF, 9₁. I-CSCF then sends the SIP register to C-CSCF (here acting as AF), 10₁.

In this embodiment it is supposed that S-CSCF sends a Diameter Message (Nasreg application) AAR to CRF, 11₁, over Rx and containing the public user ID of the UE, and the private user ID and the IP address of the UE. CRF maps private and/or public
5 user identity to MSISDN and/or IMSI to retrieve the associated IP address. CRF then performs the verification, i.e. checks whether the information received from GGSN (cf. step 3₁) is the same, and acknowledges that the verification was successful (in this case) over Rx to S-CSCF in an AAA answer, 12₁.

10

Finally a SIP 2XX OK message is sent from S-CSCF to UE, 13₁.

Fig. 6B is similar to Fig. 6A with the difference that the mapping in CRF is unsuccessful. Hence steps 1₁-11₁ are similar to
15 steps 1₁-11₁ in Fig. 6A and therefore bear the same reference numerals.

Upon establishing in CRF that the mapping is unsuccessful, i.e. that the first and second UE identity related information is not
20 the same, an error message is sent over Rx (Diameter) to S-CSCF, 12₂. Optionally CRF may then send a Diameter CCA message over Gx to GGSN, 13₂, that the relevant charging rules should be removed. GGSN then confirms the removal to CRF, 14₂, and (in any case, irrespectively of whether steps 13₂, 14₂ are implemented or not)
25 an error message is sent from S-CSCF to UE, e.g. a SIP 4XX Forbidden, 15₂.

It should be clear that the inventive concept is not restricted to the use of Diameter. Radius may also be used or any other
30 appropriate protocol. As referred to above, the flow will also be different if a CGSN is used, instead of a GGSN and a SGSN which however is not explicitly illustrated since the alterations should be obvious.

As also referred to above, it does not have to be S-CSCF that acts as an AP, and instead of a CRF it may e.g. be a PDF, PCCN etc.

5

Fig. 7 shows a particular embodiment in which the charging and/or policy handling node comprises a PCCN 30A (Policy and Charging Control Node). PCCN 30A communicates with service data flow based credit control 36A or more generally OCS. If for example PCCN 30A receives an IMS identity, e.g. IMPI from an AP (not shown) it may request IMSI from the subscription profile repository 35 over the Sp reference point (or particularly Sp-interface). More generally, if PCCN 30A receives an IMS identity, it may query subscription profile repository 35 in order to get a connection between the IMS identity (IMPI or IMPU) and the MSISDN or IMSI received from the TPF, e.g. in GGSN. This is advantageous in that it also covers cases when users utilize an ISIM which may have another structure for the IMPI, which for example is not based on IMSI or MSISDN. In still another embodiment (not shown) PCCN (or PDF 33A or CRF 34A in PCCN as an alternative to a PCCN), may query the service data flow based credit control 36A in order to get a connection between the IMS identity and the MSISDN/IMSI received from the TPF.

25

Fig. 8A schematically illustrates another architecture in which the inventive concept is applicable. Such an architecture is for example described in TR 23.803. The charging and/or policy handling node here comprises a PCCN 30B with a PDF 33B and a CRF 34B communicating with an AP 20B over a merged Rx/Gq interface. The packet data support node including TPF functionality 11 here comprises a gateway 10B which in addition to the TPF functionality 11 also includes a PEP (Policy Enforcement Point)

30

functionality, 12. Communication between PCCN 30B and gateway GW 10B takes place over the merged interface Go/Gx. PCCN 30B communicates with OCS (Online Charging System) 36B with a Camel SCP 37B and Service Data Flow Based Credit Control means 38B over the Ry interface. GW 10B communicates with OSC 36B over the Gy interface. GW 10B also communicates with a charging gateway function 15B₁ and a charging collection function 15B₂ over the Gz interface.

Fig. 8B shows still another embodiment similar to that of Fig. 8A but with the difference that OSC and PCCN are merged into one node 30C, communicating with GW 10C over a merged interface comprising interfaces Gy/Go/Gx merged with one another. In other aspects Fig. 8B is similar to Fig. 8A and OCS/PCCN 30C communicate over a merged interface Gq/Rx with AF 20C and GW 10C communicates over Gz with charging gateway function 15C₁ and charging collection function 15C₂.

It should be clear that these figures are merely illustrated in order to show some additional examples on architectures in which the inventive concept can be applied.

Hence, according to the invention, through only a slight addition to existing FBC architectures or similar early IMS security can be provided for. Operators using FBC for non-IMS based services migrating towards IMS are given the opportunity to simply upgrade FBC instead of HSS and Radius server, which is very advantageous. The inventive concept involves no implications on for example a GGSN architecture e.g. IP address allocation or release as it is the case with the proposal given in TR 33.878 and there is also no need to introduce an idle timer in GGSN. According to the invention identities from IMS

can be connected to e.g. GPRS based identities by using Rx and Gx interfaces.

Fig. 9 is a flow diagram describing one implementation of the inventive concept. It is here supposed that an UE requests TPF for bearer service establishment, 100. In the request, the UE includes first UE identity related information, or if it is a secondary PDP-context request, the first UE identity related information is already stored in the node handling TPF. This is however known in the art.

TPF then sends a request for charging and/or policy rules to CRF or PDF, or a PCCN, depending on the applicable implementation, including said first UE identity related information, 101. CRF/PDF (or PCCN) stores the first UE identity related information in storing means, e.g. a table, 102. Subsequently CRF/PDF (or PCCN) identifies and installs, using said first UE identity related information and possibly other information as referred to above, the relevant charging and/or policy rules, 103. Then CRF/PDF (or PCCN) provides the charging and/or policy rules to TPF, 104. A Bearer Service Establishment Acceptance message is then sent from TPF to UE, 105. Once a bearer service has been established, it is supposed that UE sends a SIP message or a SIP request, e.g. a SIP invite, to an Application Function AF, 106. It may then be checked whether the private user identity is known from the SIP message, 107. If not, it may be derived somehow either in AF or in communication with some other node or function as discussed above, 107A. Then, as well as if the private user identity actually was known from the SIP message or SIP request, the second UE identity related information is sent to CRF/PDF or PCCN, 108. In CRF/PDF or PCCN it is thus then examined whether the first UE identity related information and the second UE identity related information

- originate from one and the same UE, 109. If not, it is checked whether the charging and/or policy handling rules are to be deactivated, 109A, if yes, they are deactivated and/or the concerned traffic is discarded, 109B. If however the option is
5 selected that the rules are not to be deactivated in step 109A, as well as if the first and the second UE identity related information respectively do originate from one and the same UE, the charging and/or policy rules are implemented, 110.
- 10 It should be clear that the invention is not limited to the specifically illustrated embodiments but that it can be varied in a number of ways within the scope of the appended claims.

CLAIMS

1. An arrangement in a communications system participating in user station service request and/or access procedures and comprising a number of packet data support nodes (GGSN; CGSN; TPF; 10; 10B; 10C), a number of charging and/or policy handling nodes (CRF; TPF; PCCN; 30; 30A; 30B; 30C) and a number of application functions (AF; (P), (S), (I)CSCF; 20; 20B; 20C) handling mobility management and call control of mobile user stations (UE; 1) requesting and/or accessing services, characterized in that the packet data support node(s) (10; 10B; 10C) comprise(s) means adapted to send first mobile user station (UE; 1) identity related information over a first interface (Gx, Gy; Gx/Gy) to a charging and/or policy handling node (CRF; PDF; PCCN; 30; 30A; 30B; 30C), at reception of a request for bearer services from a mobile user station (UE; 1), that the application function(s) (AF; (P), (S), (I)CSCF; 20; 20B; 20C) comprise(s) means for, at reception of a request for a service session (SIP) from a mobile user station (UE; 1), sending second mobile user station identity related information to the charging and/or policy handling node (CRF; PDF; PCCN; 30; 30A; 30B; 30C), over a second interface (Rx, Rx/Gq), and in that the policy and/or charging handling node (CRF; PDF; PCCN; 30; 30A; 30B; 30C), comprises verification means (32; 32A) adapted to establish whether the request for a bearer service to the packet data support node (10; 10B; 10C) and the request for a service session to the application function (AF; P/S/I-CSCF; 20; 20B; 20C) originate from one and the same mobile user station (UE; 1).
2. An arrangement according to claim 1,

characterized in
that the first mobile user station identity related information
comprises one or more of MSISDN, IMSI and IP address of the mobile
user station (UE;1).

5

3. An arrangement according to claim 1 or 2,
characterized in
that the second mobile user station identity related information
comprises IMS private identity (IMPI) and/or IMS public identity
10 (IMPU).

4. An arrangement according to claim 1 or 2,
characterized in
that the second mobile user station identity related information
15 comprises IMSI and/or MSISDN, e.g. derived from IMS private or
public identity (IMPI,IMPU), or that the application function
(20;20B;20C) is adapted to fetch said information externally, e.g.
from a HSS.

20 5. An arrangement according to any one of the preceding claims,
characterized in
that the IP addresses are received in, or derived from, the first
mobile user station related information and the second mobile user
station identity related information, and in that the verification
25 means (32;32A) are adapted to compare the IP address obtained from
the application function (20;20B;20C) with the IP address obtained
from the packet data support node.

6. An arrangement according to claim 5,
30 characterized in
that the verification means (32;32A) are adapted to, if required,
establish and, use IMSI and/or MSISDN of said first and second

mobile user station identity related information respectively, to compare the associated IP addresses.

7. An arrangement according to claim 4,

5 c h a r a c t e r i z e d i n

that the charging and/or policy handling node (30;30A;30B;30C) is adapted to deduce IMSI and/or MSISDN from a received IMS private and/or public user identity (IMPI/IMPU).

10 8. An arrangement according to any one of the preceding claims,

c h a r a c t e r i z e d i n

that the charging and/or policy handling node (30;30A;30B;30C) is adapted to construe a private user identity using IMSI of a mobile user station, e.g. when no ISIM application is implemented.

15

9. An arrangement according to any one of the preceding claims,

c h a r a c t e r i z e d i n

that the charging and/or policy handling node (30;30A;30B;30C) is adapted to identify and install charging rules to be applied at
20 reception of request therefor from a packet data support node (10;10B;15B₁,15B₂;10C).

10. An arrangement according to claim 9,

c h a r a c t e r i z e d i n

25 that if the first and second user identity related information do originate from one and the same mobile user station (UE;1), the charging and/or policy handling node (20;30A,36A;30B,36B;30C) is adapted to implement the provisioned charging rules.

30 11. An arrangement according to claim 9,

c h a r a c t e r i z e d i n

that if the first and second user identity related information do not originate from one and the same mobile user station, the

charging and/or policy handling node (20;30A,36A;30B,36B;30C) is adapted to reject the charging rules and/or deactivate implemented charging rules and discard concerned IP flow traffic, and in that it is adapted to inform the application function (20;20B;20C) that
5 no PDP-context is available.

12. An arrangement according to claim 9,
c h a r a c t e r i z e d i n
that if the first and second user identity related information do
10 not originate from one and the same mobile user station, the charging and/or policy handling node (30;30A;30B;30C) is adapted to select whether to activate or deactivate the charging rules in the packet data support node.

15 13. An arrangement according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the packet data support node (10;10B;10C) comprises a node handling Traffic Plane Functions (TPF).

20 14. A user according to claim 13,
c h a r a c t e r i z e d i n
that the packet data support node comprises a GGSN (10) implementing TPF.

25 15. An arrangement according to claim 13,
c h a r a c t e r i z e d i n
that the packet data support node comprises a CGSN implementing TPF.

30 16. An arrangement according to claim 13,
c h a r a c t e r i z e d i n
that it comprises a stand-alone node or a gateway node (10B;10C) handling TPF or TPF and policy enforcement (PEP).

17. An arrangement according to any one of the preceding claims,
characterized in
that the charging and/or policy handling node (30;30A;30B;30C)
5 comprises a CRF, a PDF or a PCCN.

18. An arrangement according to any one of the preceding claims,
characterized in
that the first interface is Gx or Go/Gx merged with Gy if the
10 charging and/or policy handling node (30A;30B) is merged with an
OCS (36A;36B).

19. An arrangement according to any one of the preceding claims,
characterized in
15 that the second interface comprises Rx or Rx merged with Gq.

20. A charging and/or policy handling node (30;30A;30B;30C) in a
communications system supporting communication of packet data and
arranged to communicate with an application function (20;20B;20C)
20 and a packet data support node (10;10B;10C),
characterized in
that it is adapted to receive first mobile user station identity
related information from the packet data support node (10;10B;10C)
at reception of a request for a bearer service from a mobile user
25 station (UE;1) in the packet data support node (10;10B;10C), to
receive second mobile user station identity related information
from the application function at reception of a request for a
service session therein, and in that it comprises verification
means (32;32A) for establishing whether the request for a bearer
30 service to the packet data support node (10;10B;10C) and the
request for a service session to the application function
(20;20B;20C) originate from the same mobile user station (UE;1).

21. A charging and/or policy handling node according to claim 20,
c h a r a c t e r i z e d i n
that the first mobile user station identity related information
comprises one or more of MSISDN, IMSI and IP address of the mobile
5 user station.
22. A charging and/or policy handling node according to claim 20
or 21,
c h a r a c t e r i z e d i n
10 that the second mobile user station identity related information
comprises IMS private identity (IMPI) and/or IMS public identity
(IMPU) of the mobile user station or IMSI and/or that the handling
node is adapted to derive IMSI and/or MSISDN from IMPI and/or IMPU
and/or adapted to request said IMSI and/or MSISDN from the
15 application function.
23. A charging and/or policy handling node according to any one of
claims 20-22,
c h a r a c t e r i z e d i n
20 that the verification means (32;32A) are adapted to compare the IP
address corresponding to or included in the first mobile user
station identity related information and the IP address
corresponding to or included in the second mobile user station
identity related information.
- 25 24. A charging and/or policy handling node according to claim 23,
c h a r a c t e r i z e d i n
that the verification means (32;32A) are adapted to, if required
establish and, use IMSI and/or MSISDN of said first and second
30 mobile user station identity related information, to compare the
associated IP addresses.
25. A charging and/or policy handling node according to claim 22,

characterized in
that it is adapted to derive IMSI and/or MSISDN from a received
IMS private and/or public user identity (IMPI/IMPU).

5 26. A charging and/or policy handling node according to any one of
claims 20-25,

characterized in
that it is adapted to construe a private user identity using IMSI
of a mobile user station, e.g. when no IMSI application is
10 implemented.

27. A charging and/or policy handling node according to any one of
claims 20-26,

characterized in
15 that it is adapted to identify and install charging rules to be
applied at reception of a request therefor from a packet data
support node (10;10B;10C).

28. A charging and/or policy handling node according to any one of
20 claims 20-27,

characterized in
that it is adapted to identify and install charging rules to be
applied at reception of request therefor from a packet data
support node (10;10B;10C), and if the first and second user
25 identity related information do originate from one and the same
mobile user station (1), it is adapted to implement the
provisioned charging rules, and, if the first and second user
identity related information do not originate from one and the
same mobile user station,

30 it is adapted to reject the charging rules and/or deactivate
implemented charging rules and discard concerned IP flow traffic,
to inform the application function (20;20B;20C) that no PDP-
context is available or, to select whether to deactivate the

charging rules in the packet data support node (10;10B;10C) or to keep them active.

29. A charging and/or policy handling node according to any one of
5 claims 20-28,

characterized in

that it comprises a CRF, a PDF or a PCCN or a node with a similar functionality.

10 30. A method in controlling service access, in a communication system supporting communication of packet data and comprising a number of packet data nodes, a number of charging and/or policy handling nodes and a number of application functions handling mobility management and call control of mobile user stations
15 requesting/accessing services, comprising the steps of:

- receiving a request for bearer services from a mobile user station in a packet data support node,
- sending, from the packet data support node, first mobile user station identity related information of the mobile user
20 station to a charging and/or policy handling node,
- receiving, subsequently, before or substantially simultaneously, a request for a service session from the mobile user station in an application function,
- sending, from the application function, second mobile user
25 station identity related information to the charging and/or policy handling node,
- establishing, in the charging and/or policy handling node, whether the request for a bearer service to the packet data support node and the request for a service session to the
30 application function originate from the same mobile user station.

31. A method according to claim 30,

37

wherein the first mobile user station identity related information comprises one or more of the MSISDN, IMSI and IP address of the mobile user station, and wherein the second mobile user station identity related information comprises IMS private identity (IMPI) and/or IMS public identity (IMPU), or the second user identity related information comprises IMSI and/or MSISDN, e.g. derived from IMS private or public identity (IMPI, IMPU), or the application function is adapted to fetch said information from a RSS.

10

32. A method according to claim 30 or 31, further comprising the steps of:

- establishing or finding IMSI and/or MSISDN of said first and second mobile user station identity related information,
- 15 - comparing at least part of said first and said second mobile user station identity related information with each other.

33. A method according to claim 30, 31 or 32, comprising the step of:

- 20 - comparing the IP addresses of said first and second mobile user station identity related information.

34. A method according to any one of claims 30-33, comprising the step of:

- 25 - deriving IMSI and/or MSISDN from received IMS private and/or public user identities (IMPI/IMPU).

35. A method according to any one of claims 30-34, comprising the step of:

- 30 - construing, in the charging and/or policy handling node, a private user identity using IMSI of the mobile user station, e.g. when no ISIM application is implemented.

38

36. A method according to any one of claims 30-35,
comprising the step of:

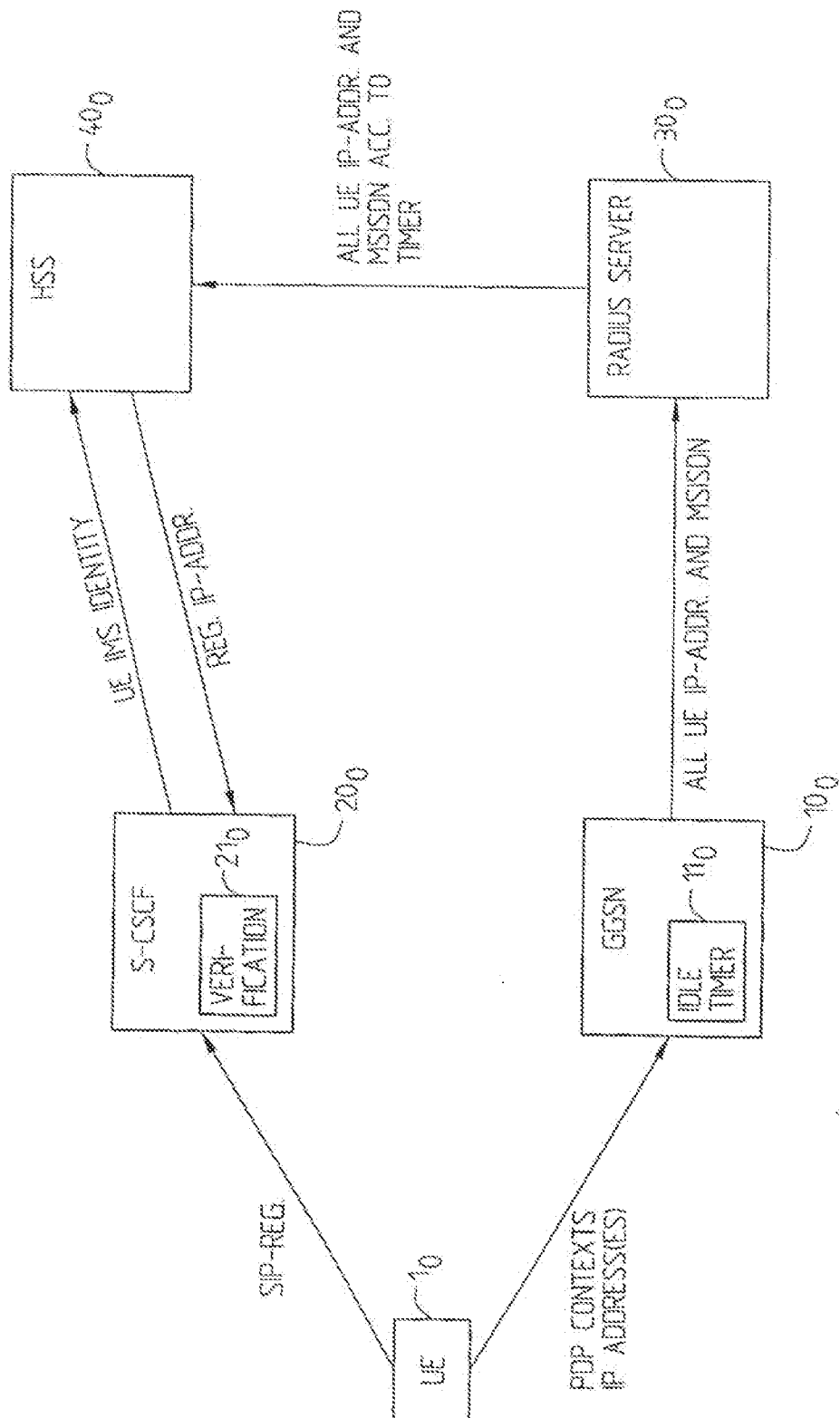
- identifying and installing applicable charging and/or policy
rules at reception of a request from a packet data support
node.

37. A method according to claim 36,
further comprises the steps of:

- if the first and second mobile user station identity related
information do originate from one and the same mobile user
station,
- implementing the provisioned applicable charging rules
and/or policy rules in the charging and/or policy handling
node, otherwise,
- discarding concerned IP flow traffic, or
- selecting whether to activate or deactivate the charging
rules.

38. A method according to any one of claims 30-37,
wherein the packet data support node comprises a node handling
Traffic Plane Functions, and is a stand-alone node, or a GGSN or a
CGSN or a gateway node handling TPF and policy enforcement (PEP),
and wherein the charging and/or policy handling node comprises a
CRF, a PDF or a PCCN or a node with a similar functionality.

1/11



STATE OF THE ART

Fig. 1

2/11

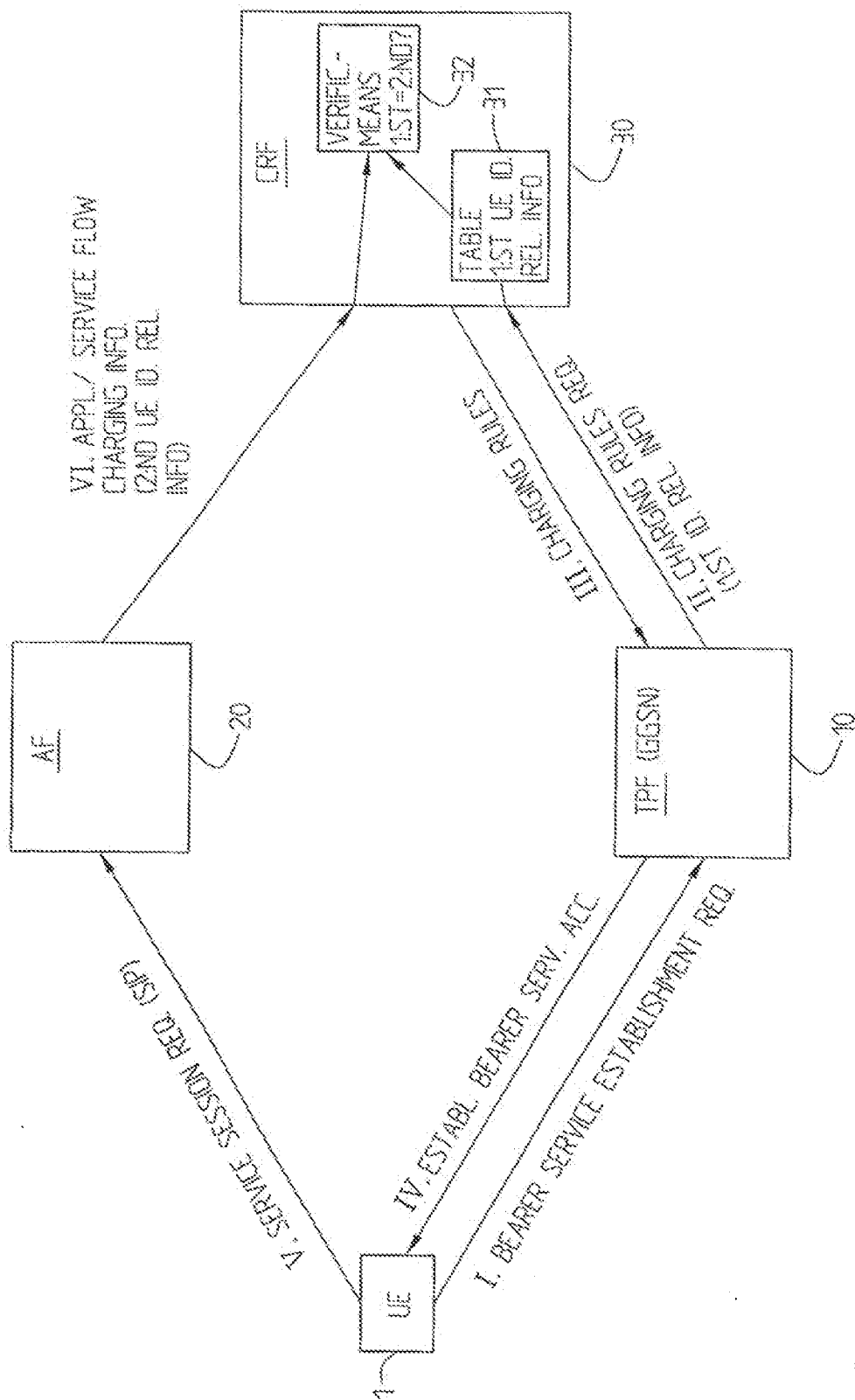


Fig.2

3/11

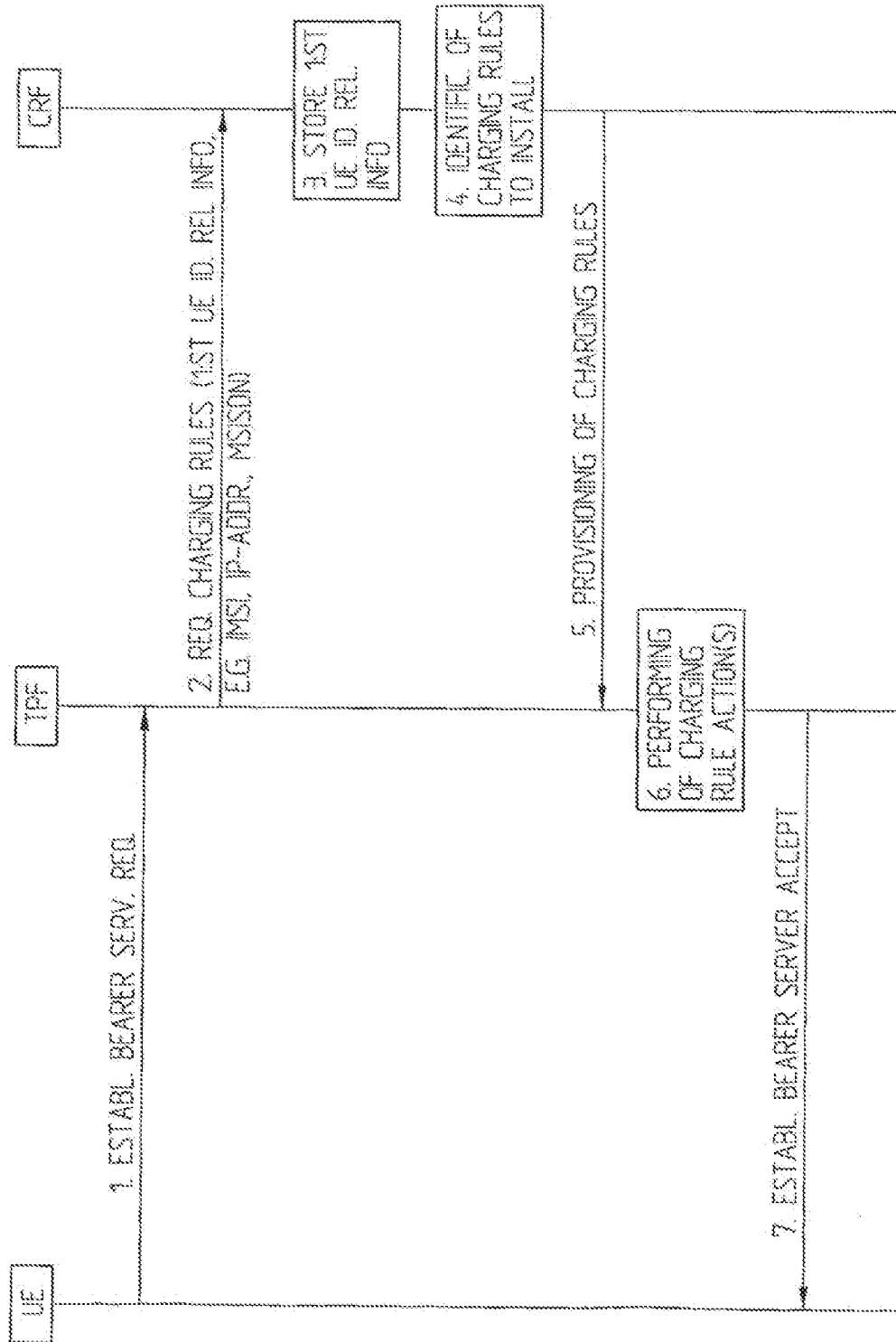


Fig. 3

4/11

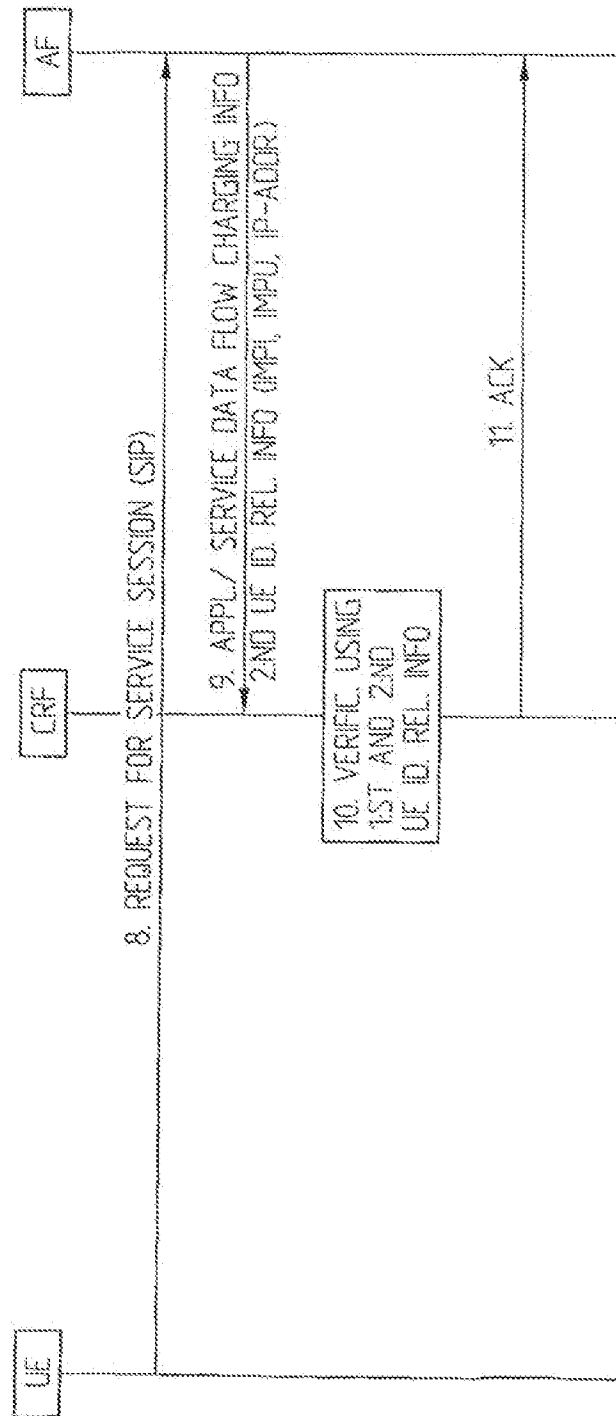


Fig. 4

5/11

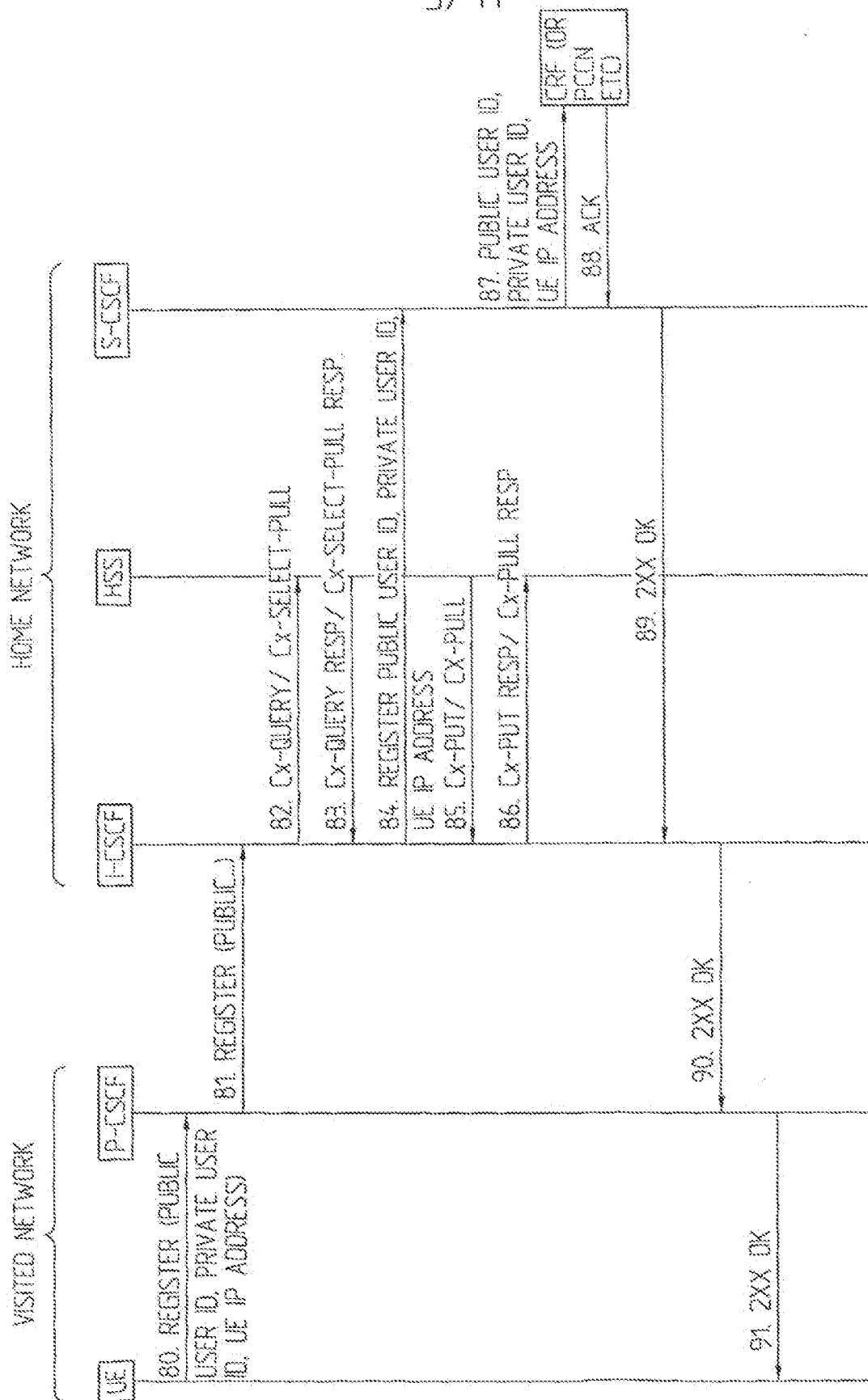


Fig. 5

6/11

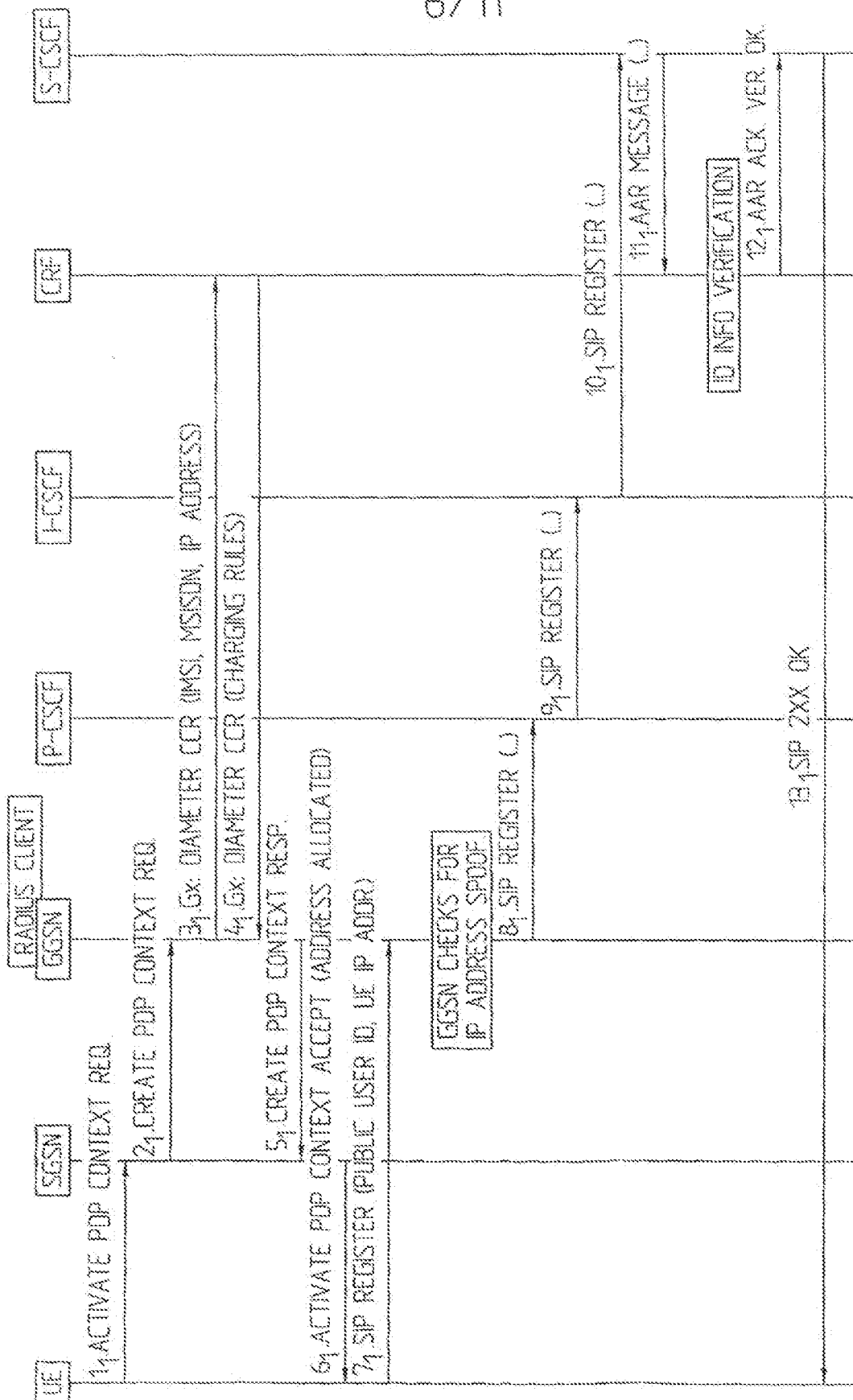


Fig. 6A

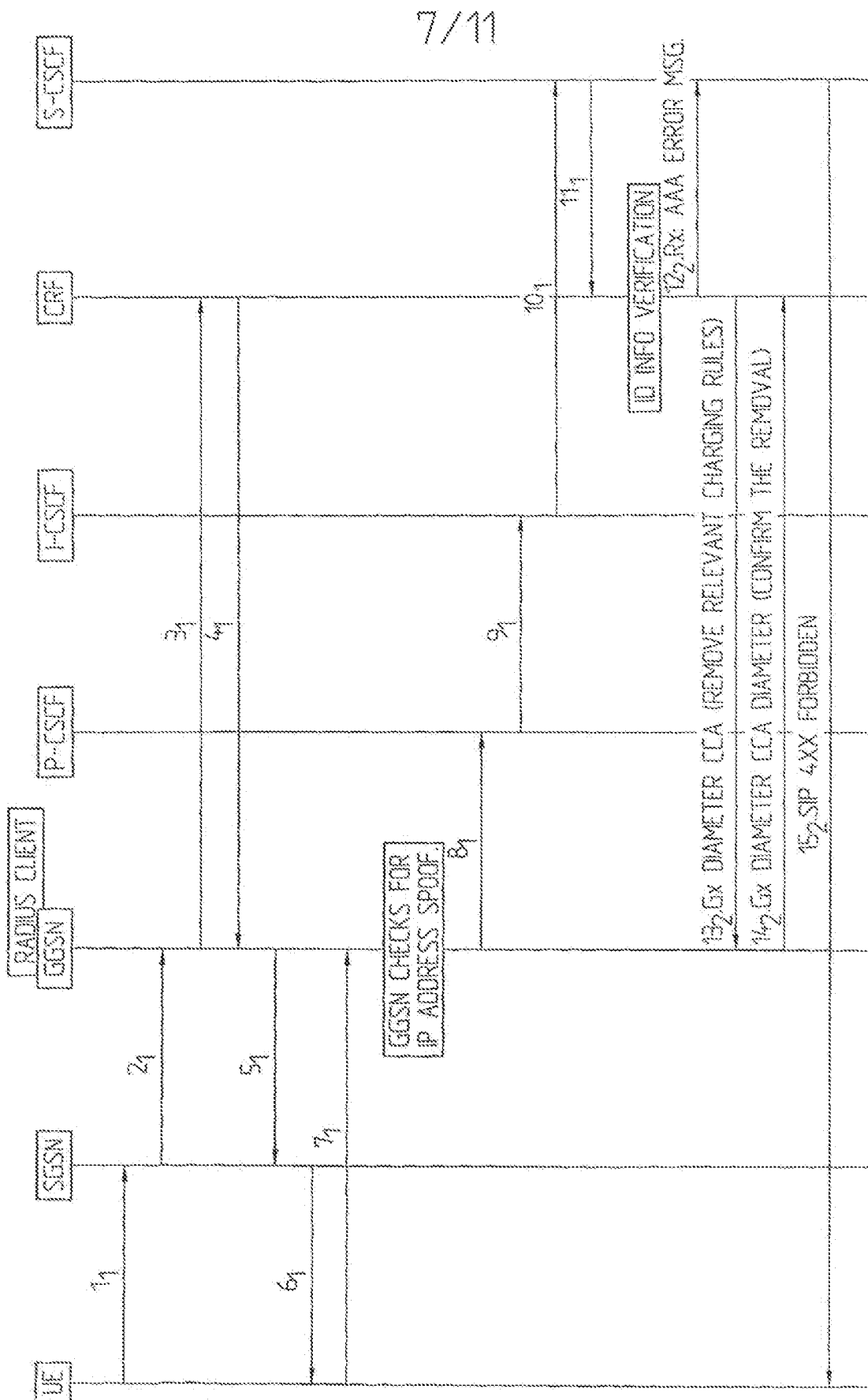


Fig. 6B

8/11

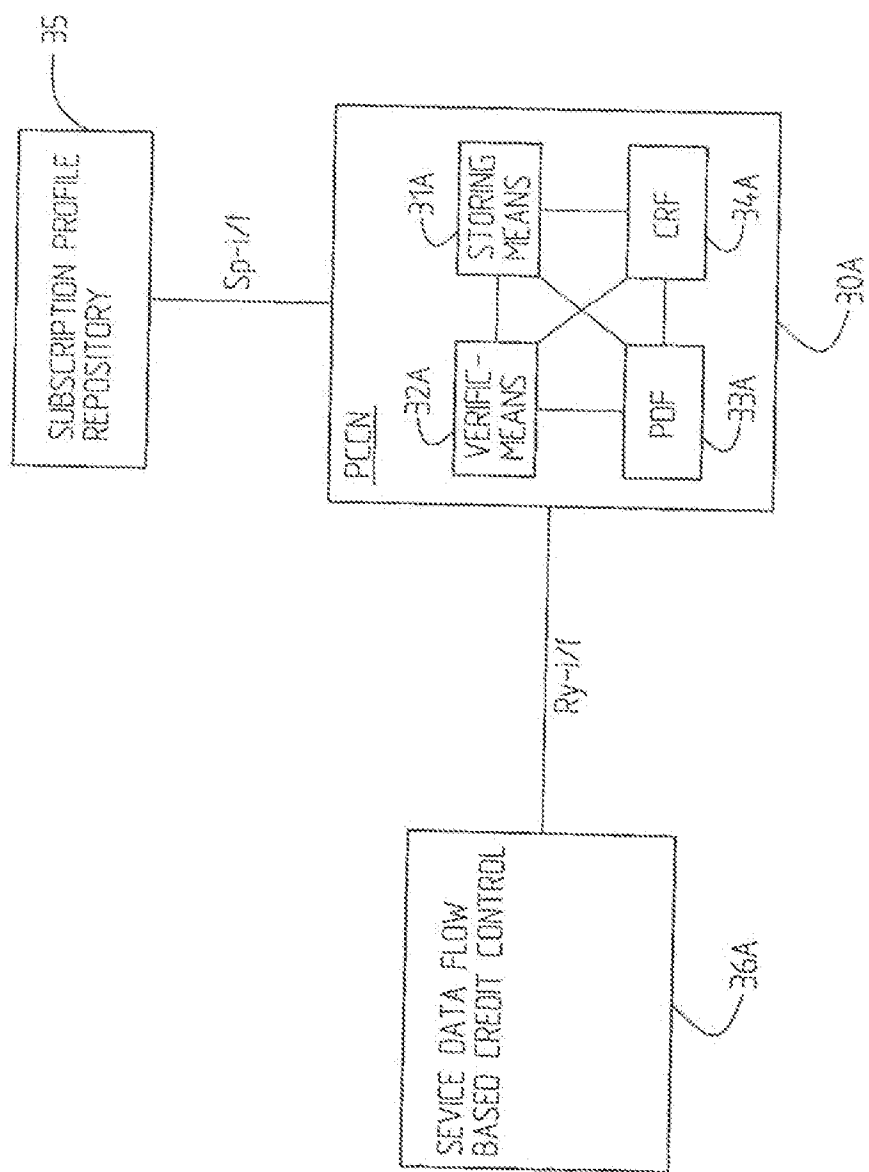


Fig. 7

9/11

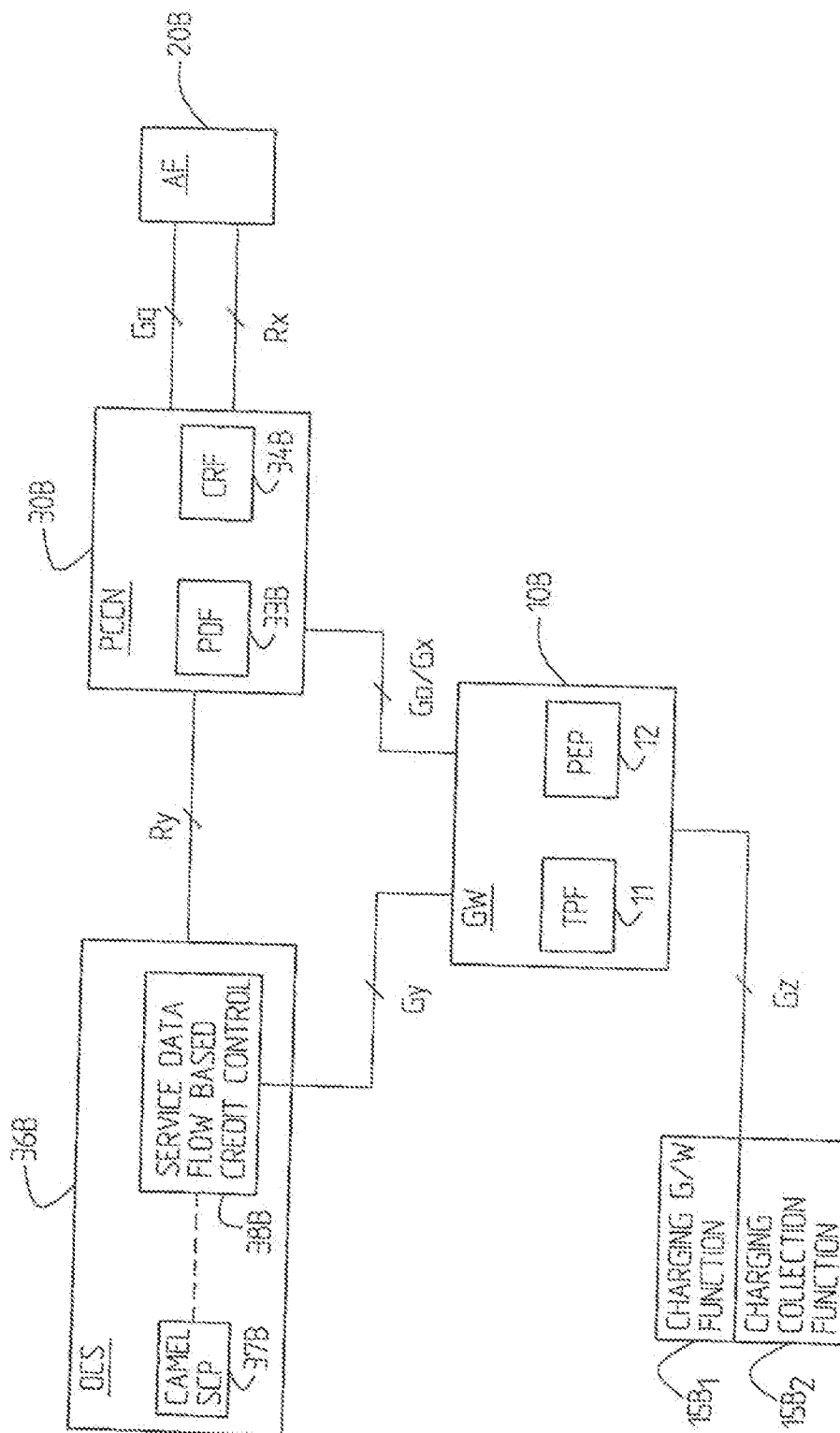


Fig. 8A

10/11

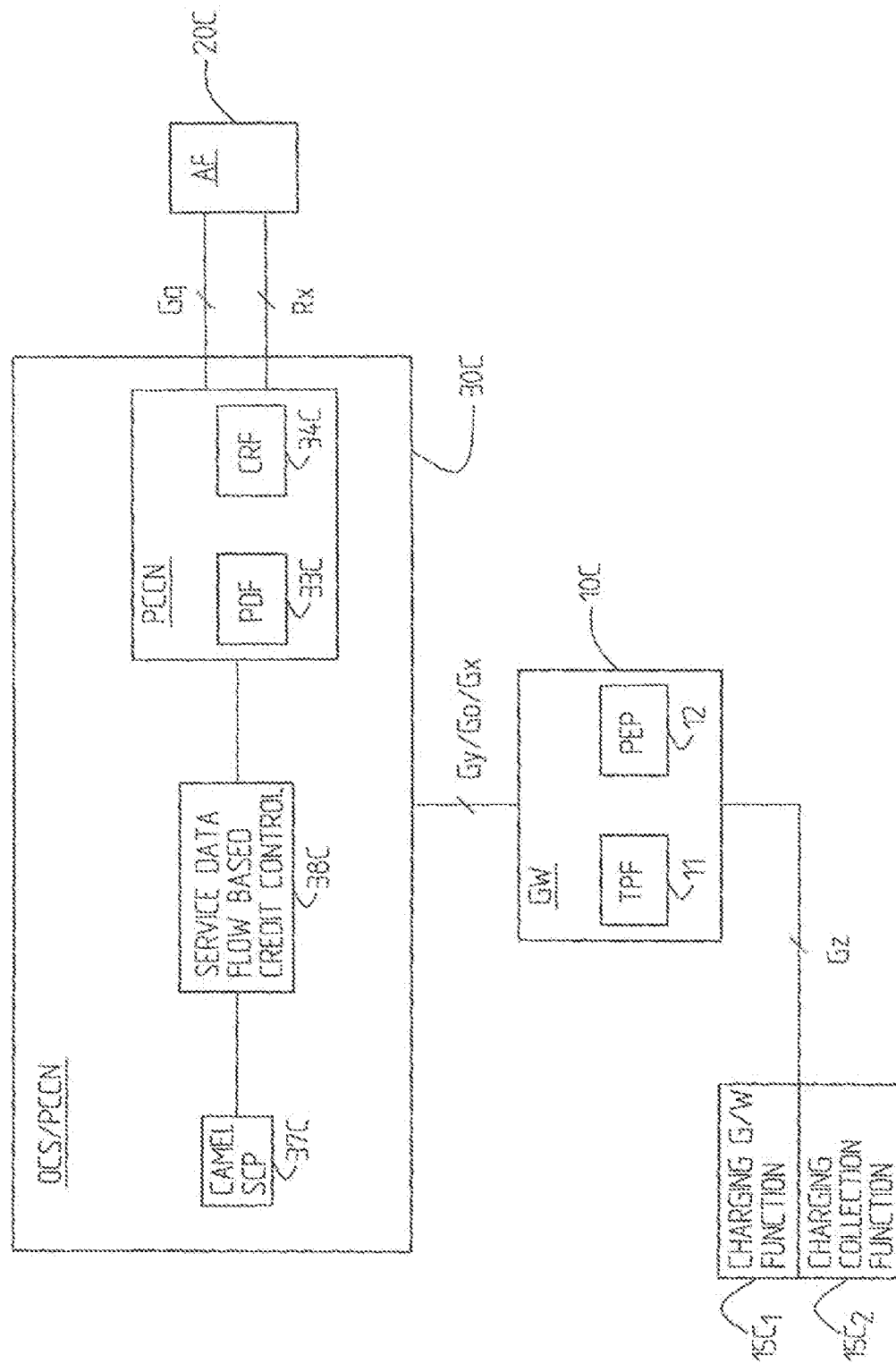


Fig. 8B

11/11

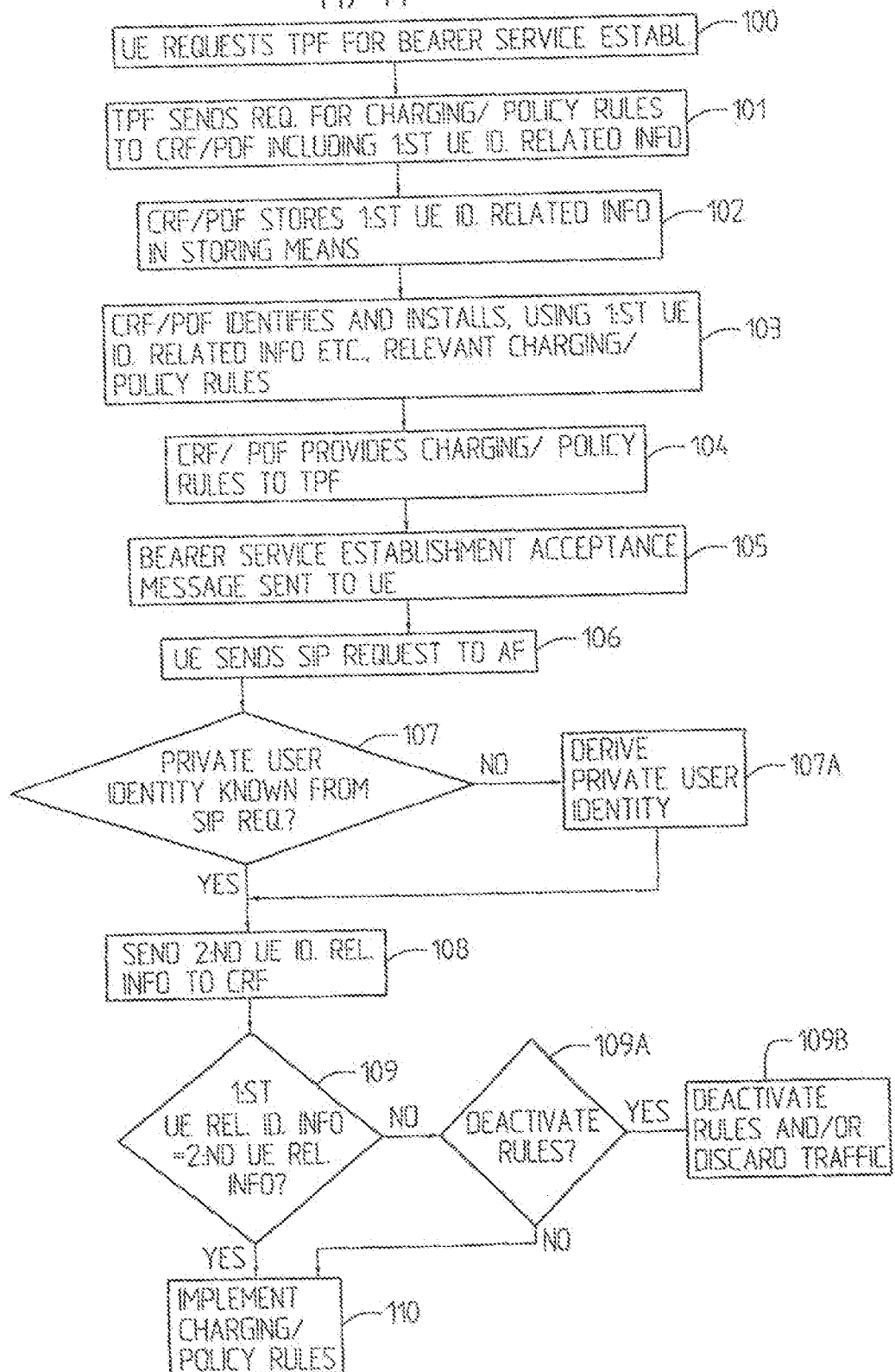


Fig. 9

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/EP2005/002837

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L H04M H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01/91446 A (NOKIA CORPORATION; NOKIA INC) 29 November 2001 (2001-11-29) page 4, line 7 - page 5, line 2	1-38



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"S" document member of the same patent family

Date of the actual completion of the international search

28 June 2005

Date of mailing of the international search report

06/07/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentele 2
NL - 2200 HV Rijswijk
Tel (+31-70) 345-2040, Tx. 81 651 epo nl
Fax: (+31-70) 340-3015

Authorized officer

Veen, G

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.

PCT/EP2005/002837

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0191446	A	29-11-2001	
		US 2002127995 A1	12-09-2002
		CN 1444824 A	24-09-2003
		EP 1310085 A2	14-05-2003
		WO 0191446 A2	29-11-2001
		JP 2004507127 T	04-03-2004

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
13 July 2006 (13.07.2006)(10) International Publication Number
WO 2006/073837 A2(51) International Patent Classification:
H04L 9/00 (2006.01)(74) Agents: AMIN, Himanshu et al.; Amin & Turvey, LLP
1900 E. 9th Street, 24th Floor, National City Center, Cleveland, OH 44114 (US).(21) International Application Number:
PCT/US2005/046422(22) International Filing Date:
21 December 2005 (21.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/928,814 4 January 2005 (04.01.2005) US

(71) Applicant (for all designated States except US): SYMBOL TECHNOLOGIES, INC. [US/US]; One Symbol Plaza, Holtsville, NY 11742-1300 (US).

(72) Inventor; and

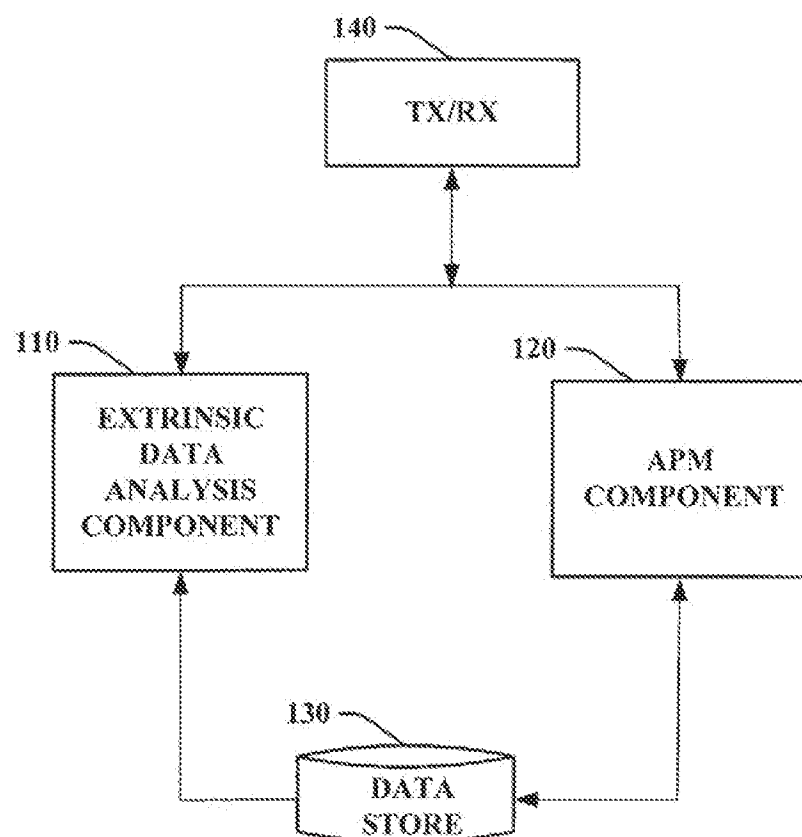
(75) Inventor/Applicant (for US only): D'AGOSTINO, Anthony [US/US]; 57 Ridge Road, Smithtown, NY 11787 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT,

[Continued on next page]

(54) Title: METHOD AND APPARATUS OF ADAPTIVE NETWORK POLICY MANAGEMENT FOR WIRELESS MOBILE COMPUTERS



(57) Abstract: System(s) and method(s) are provided that utilize external resources and protect the integrity of data within a mobile communication device and data communicated with the mobile communication device. The device includes an extrinsic data analysis component that receives information about both an external environment and an internal state. The device also includes an adaptive policy manager (APM) component. The APM component is adapted to analyze and prioritize policies based upon received input from external resources, stimuli, threats and/or parameters. The method of protecting data integrity is performed automatically and autonomously with minimal user intervention and awareness. The APM component includes a profile component, a policy modification component, a rules component, an authentication component, and an access control component.

WO 2006/073837 A2



RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA,
GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

----- *without international search report and to be republished upon receipt of that report.*