



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
61/420,727	12/07/2010		220	RALEP042+		

CONFIRMATION NO. 1137

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

FILING RECEIPT



OC000000044972996

Date Mailed: 12/21/2010

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. 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;

Power of Attorney:

Michael Schallopp--44319

If Required, Foreign Filing License Granted: 12/15/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/420,727**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

Title

SECURE DEVICE DATA RECORDS

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

page 1 of 3

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).

Attorney Docket No. RALEP042+

PROVISIONAL APPLICATION FOR
UNITED STATES PATENT

SECURE DEVICE DATA RECORDS

By Inventor(s):

Gregory G. Raleigh
Woodside, CA
A Citizen of the United States

Assignee: Headwater Partners I LLC, a Delaware limited liability company

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014
Telephone (408) 973-2585

SECURE DEVICE DATA RECORDS

CROSS REFERENCE TO OTHER APPLICATIONS

[0001] This application claims priority to provisional patent applications U.S. Provisional Patent Application No. 61/348,022 (Attorney Docket No. RALEP031+), entitled DEVICE ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY, filed on May 25, 2010, U.S. Provisional Patent Application No. 61/381,159 (Attorney Docket No. RALEP032+), entitled DEVICE ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY, filed on September 9, 2010, and U.S. Provisional Patent Application No. 61/387,247 (Attorney Docket No. RALEP038+), entitled SECURED DEVICE DATA RECORDS, filed on September 28, 2010, which are incorporated herein by reference for all purposes, and this application is a continuation in part of co-pending U.S. Patent Application No. 12/380,780 (Attorney Docket No. RALEP007), entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed on March 2, 2009, co-pending U.S. Patent Application No. 12/695,019 (Attorney Docket No. RALEP022), entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING, filed on January 27, 2010, and co-pending U.S. Patent Application No. 12/694,445 (Attorney Docket No. RALEP025), entitled SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES filed on January 27, 2010, which are incorporated herein by reference for all purposes.

BACKGROUND OF THE INVENTION

[0002] 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.

[0003] 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

[0004] Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

[0005] **Figure 1** illustrates a high level diagram of an advance wireless service platform end-to-end DDR reporting and processing system in accordance with some embodiments.

[0006] **Figure 2** illustrates a process for booting, executing, and updating the DDR firmware in accordance with some embodiments.

[0007] **Figure 3** illustrates an architecture for a secure embedded DDR Processor in an APU implementation in accordance with some embodiments.

[0008] **Figure 4** illustrates another architecture for a secure embedded DDR Processor in an APU implementation along with a modem bus driver in accordance with some embodiments.

[0009] **Figure 5** illustrates another architecture for a secure embedded DDR Processor in an APU implementation along with a modem bus driver in accordance with some embodiments.

[0010] **Figure 6** illustrates an architecture for a secure embedded DDR Processor in an MPU implementation in accordance with some embodiments.

[0011] **Figure 7** illustrates another architecture for a secure embedded DDR Processor in an MPU implementation in accordance with some embodiments.

[0012] **Figure 8** illustrates an architecture for a secure embedded DDR Processor in an APU and a Data Path Security Verifier (DPSV) in an MPU implementation in accordance with some embodiments.

[0013] **Figure 9** illustrates an architecture for a secure embedded DDR Processor in a Subscriber Identity Module (SIM) and a Data Path Security Verifier (DPSV) in an MPU implementation in accordance with some embodiments.

[0014] **Figure 10** illustrates another architecture for a secure embedded DDR Processor in a Subscriber Identity Module (SIM) and a Data Path Security Verifier (DPSV) in an MPU implementation in accordance with some embodiments.

[0015] **Figure 11** illustrates another architecture for a secure embedded DDR Processor in a Subscriber Identity Module (SIM) and a Data Path Security Verifier (DPSV) in an MPU implementation in accordance with some embodiments.

[0016] **Figure 12** illustrates a secure boot sequence flow diagram in accordance with some embodiments.

[0017] **Figure 13** illustrates a functional diagram for passing DDR Service Processor mailbox messages between secure and unsecure memory regions in accordance with some embodiments.

[0018] **Figure 14** illustrates a flow diagram for a DDR Processor Service Controller session authentication and verification in accordance with some embodiments.

[0019] **Figure 15** illustrates a flow diagram for secure device data records for implementing device assisted services (DAS) in accordance with some embodiments.

DETAILED DESCRIPTION

[0020] 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.

[0021] 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.

[0022] In some embodiments, secure device data records (DDRs) are provided. In some embodiments, secure DDRs for device assisted services are provided. In some embodiments, secure DDRs for device assisted services are provided for service usage monitoring of a wireless communication device (e.g., firmware based monitoring of network service usage, such as based on a 5-tuple of a source address, port address, destination address, destination port, and protocol). In some embodiments, a system for secure DDRs includes a processor of a wireless communication device for wireless communication with a wireless network, in which the

processor is configured with a secure execution environment, and in which the secure execution environment is configured to: monitor service usage of the wireless communication device with the wireless network; and generate a plurality of device data records of the monitored service usage of the wireless communication device with the wireless network, in which each device data record is associated with a unique sequence order identifier; and a memory coupled to the processor and configured to provide the processor with instructions. In some embodiments, the secure execution environment including the secure DDR processor is located in an application processor, in a modem processor, and/or in a subscriber identity module (SIM).

[0023] In some embodiments, a system for secure DDRs includes a processor of a wireless communication device for wireless communication with a wireless network, in which the processor is configured with a secure execution environment, and in which the secure execution environment is configured to: monitor service usage of the wireless communication device with the wireless network; and generate a plurality of device data records of the monitored service usage of the wireless communication device with the wireless network, in which each device data record is one of an ordered sequence of device data records with each sequential device data record providing an accounting of service usage over a service usage interval spanned by the device data record, and in which each device data record is associated with a secured unique sequence order identifier; and a memory coupled to the processor and configured to provide the processor with instructions. In some embodiments, the secure execution including the secure DDR processor environment is located in an application processor, in a modem processor, and/or in a subscriber identity module (SIM).

[0024] Various techniques for providing device assisted services (DAS), are disclosed in co-pending U.S. Patent Application No. 12/380,780 (Attorney Docket No. RALEP007), entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed on March 2, 2009, published as U.S. Pub. App. No. 2010/0192212, co-pending U.S. Patent Application No. 12/695,019 (Attorney Docket No. RALEP022), entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING, filed on January 27, 2010, published as U.S. Pub. App. No. 2010/0197266, and co-pending U.S. Patent Application No. 12/694,445 (Attorney Docket No. RALEP025), entitled SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES filed on January 27, 2010, published as U.S. Pub. App. No. 2010/0199325, which are incorporated herein by reference for all purposes.

[0025] In some embodiments, a DDR processor is provided for wireless communication devices (e.g., for assisting in implementation of device assisted services (DAS) for wireless network service usage for wireless communication devices, such as a cellular phone, smart phone, laptop, PDA, gaming device, music device, tablet, computer, and/or any other device with wireless communication access) as described herein with respect to various embodiments. In some embodiments, a secure DDR processor (e.g., implemented/executed in a secure execution environment) is provided. In some embodiments, a DDR processor is secured using various techniques described herein. In some embodiments, the DDR processor includes a DDR generator. In some embodiments, the DDR processor generates DDRs. In some embodiments, the DDR processor reports DDRs to a network element (e.g., a service controller, a DDR network storage system, and/or another network element). In some embodiments, the secure DDR processor reports the DDRs to a device element/function, such as a service processor, which aggregates the DDRs (e.g., and can include other service usage and/or other information) in a report (e.g., or service processor reports) that is communicated to a network element. In some embodiments, DDRs as well as service processor reports are generated and communicated to a network element. In some embodiments, a DDR processor is secured using various techniques described herein.

[0026] In some embodiments, DDRs include device assisted and/or device based monitored service usage (e.g., based on various criteria, such as for a specified time interval, and/or event) as described herein with respect to various embodiments. In some embodiments, DDRs are periodically reported. In some embodiments, DDRs are reported based on an event and/or a request from a network element (e.g., a service controller or another network element/function). In some embodiments, DDRs are communicated to a device service processor (e.g., or another device element/function), which aggregates such DDRs and periodically provides service usage reports including such DDRs or providing such service usage reports based on a request and/or an event. In some embodiments, each DDR includes a unique identifier (e.g., a unique sequence identifier). In some embodiments, a missing DDR can be detected using the unique identifiers (e.g., sequence count and/or time stamp information associated with each DDR allows for detection of a potentially suspicious service usage event, such as a missing, delayed, and/or compromised device data record determined using the sequence count and/or time stamp information, and responsive/corrective actions can be performed upon detection of the suspicious service usage event, as described herein). In some

embodiments, if a DDR is not received within a certain time period, then an access controller is activated to limit network access until DDRs are properly generated and reported (e.g., a network element, such as a service controller, sends a keep alive signal to the device to implement a time out period for verifying receipt of properly generated and validated DDRs from the device, and if the keep alive signal is not received within a specified time period, then the device based secured access controller can implement the restricted network access control function).

[0027] In some embodiments, a DDR network storage system is provided as described herein with respect to various embodiments. In some embodiments, a service controller is provided that includes the DDR network storage system and a DDR reconciliation function (e.g., for reconciling DDR records and/or DDR reports or other device based and/or network based service usage reports, such as CDRs, micro CDRs, and/or IPDRs or other service usage reports). In some embodiments, a network based reconciliation function reconciles DDRs (e.g., aggregated DDRs and/or DDR reports) with one or more network based service usage measures. In some embodiments, the network based reconciliation function reconciles DDRs with two or more network based service usage measures. In some embodiments, the network based reconciliation function reconciles DDRs with two or more network based service usage measures (e.g., CDRs, FDRs, IPDRs, DPI based measures including traffic related events, such as NBS and/or QoS, and/or other network based service usage measures). In some embodiments, the network based reconciliation function reconciles two or more device based service usage measures (e.g., DDRs, service processor reports, and/or other device based service usage measures including traffic related events, such as NBS and/or QoS) with a network based service usage measure. In some embodiments, the network based reconciliation function reconciles two or more device based service usage measures with two or more network based service usage measures. In some embodiments, the network based reconciliation function reconciles two or more device based service usage measures, in which one of the device based service usage measures is secured (e.g., deemed as secured and/or trusted based on various techniques described herein, such as for secure DDRs) and one or more of the other device based service usage measures is not secured (e.g., not completely trusted, such as a service processor reports generated by a service processor that is not implemented in a secure execution environment). In some embodiments, the reconciliation function reconciles based on various different reporting formats, such as time measure intervals, units of measure, and/or other different criteria used by different device and network based various service usage measures.

[0028] In some embodiments, a secure access controller is provided as described herein with respect to various embodiments. In some embodiments, the DDR processor includes the secure access controller. In some embodiments, the secure access control ensures that a wireless communication device with DAS does not have open network access until and/or unless the device is properly generating and reporting secure DDRs.

[0029] In some embodiments, the DDR processor includes a network busy state (NBS) monitoring and reporting function that is secured as described herein with respect to various embodiments. In some embodiments, a network element aggregates NBS information received from one or more wireless communication devices from the same sector and/or from various sectors within the service vicinity and establishes either the same network busy state rules (e.g., access control, charging and notification) and/or changes the exiting NBS rules appropriately.

[0030] In some embodiments, a secured boot sequence is provided. In some embodiments, the secured boot sequence ensures that the DDR processor is secured and properly generating DDRs prior to providing open network access control to the wireless communication device. In some embodiments, the secured boot sequence includes using the secure access controller to restrict network access until the secured boot sequence is completed. In some embodiments, the secure boot sequence includes verifying DDR ACK and receipt frames.

[0031] In some embodiments, a processor of a wireless communication device for wireless communication with a wireless network is provided, in which the processor is configured with a secure software or firmware instruction execution environment, and in which a program in the secure software or firmware instruction execution environment is configured to: monitor service usage of the wireless communication device with the wireless network; generate a plurality of device data records (DDRs) of the monitored service usage of the wireless communication device with the wireless network, in which the device data records are secure device data records for the monitored service usage, in which each device data record forms a portion of an ordered sequence of device data records with each sequential device data record providing an accounting of service usage over a service usage interval spanned by the device data record, and in which each device data record is associated with a unique sequence order identifier that is also secured.

[0032] In some embodiments, the sequence of device data records forms a contiguous and uninterrupted reporting of device service usage while the device is active on the network. In some embodiments, the secure software or firmware instruction execution environment is located and configured such that the network can only be accessed through a data path that is monitored by the program in the secure software or firmware instruction execution environment. In some embodiments, the secure software or firmware instruction execution environment is located in a modem processor (e.g., MPU). In some embodiments, the secure software or firmware instruction execution environment is located in an application processor (e.g., APU). In some embodiments, the secure software or firmware instruction execution environment is located in a subscriber identity module (SIM) (e.g., SIM card). In some embodiments, the secure software or firmware instruction execution environment is located in a combination of an APU, MPU, and/or SIM.

[0033] In some embodiments, the device data records are secured using various cryptographic techniques described herein, such as using one or more of the following: encryption, digital signatures, and integrity checks.

[0034] In some embodiments, a DDR processor located in a secure execution environment is configured to communicate a sequence of device data records to a device data record storage function, such as within a network element (e.g., a service controller), in which the plurality of secure device data records in combination with the unique sequence identifier provides traceability to identify if one or more usage records have been tampered with or omitted from the sequence of data records transmitted to the storage function. In some embodiments, the unique sequence identifier includes one or more of the following: sequence count, time stamp, start time indicator, stop time indicator, contiguous time interval identifier, and aggregate usage count at the beginning or end of the record, reference time, or elapsed time at the beginning or end of the record.

[0035] In some embodiments, the generation of a new device data record is determined by one or more of the following: a predetermined time, elapsed period of time, elapsed period of time since last report, maximum limit on elapsed period of time since last report, amount of one or more aspects of aggregate data usage, amount of one or more aspects of data usage since last report, maximum limit for one or more aspects of data usage since last report, a request to generate a DDR, a limit on maximum amount of memory or storage media required to contain or

process DDR information prior to transmission, device power on or power off, modem or device subsystem power on or power off, modem or device subsystem entering or exiting a power save state, device or device subsystem authentication with a network element or server, or a detected event triggered by one or more service usage activities or detection of a service usage record tampering or fraud event or transition to a new network busy state and/or QoS traffic event.

[0036] In some embodiments, the DDR processor, service processor, or another device based element/function transmits DDRs based on one or more of the following: maximum time increment, maximum service usage increment, polling from service processor, and/or polling from service controller. In some embodiments, a maximum time increment on DDR transmissions is established to ensure minimal or no services can be hijacked once service controller authentication takes place. In some embodiments, at least a portion of the restricted set of network service activities includes access to the service controller or other network elements necessary to manage the ability of the device to access the network once the service controller authenticates with the service processor and conforms proper operation of the secure DDR generator. In some embodiments, at least a portion of the restricted set of network service activities includes access to a minimum set of roaming network service activities required to initiate the process for a roaming network to authenticate access privileges for the device. In some embodiments, at least a portion of the restricted set of network service activities includes access to a minimum set of roaming network service activities required to initiate the process for a corporate network to authenticate access privileges for the device. In some embodiments, at least a portion of the restricted set of network service activities includes access to a minimum set of roaming network service activities required to initiate the process for an MVNO network to authenticate access privileges for the device. In some embodiments, at least a portion of the more permissive set of service activities is the available to access at least a subset of the services available on a roaming network. In some embodiments, at least a portion of the more permissive set of service activities is the available to access at least a subset of the services available on an MVNO network. In some embodiments, at least a portion of the more permissive set of service activities is the available to access at least a subset of the services available on a corporate network.

[0037] In some embodiments, the device data record service usage information includes measurement of one or more of the following: voice service (e.g., VOIP) usage records; text

service usage records; data network service usage records; data network flow data records; data network general purpose, aggregate or bulk service usage records; service usage classified at least in part by far end destination; service usage records classified at least in part by layer 3 network communications information such as IP address or ATM address; service usage classified at least in part by layer 4 network communications information such as IP address and port combinations; data network service usage records comparable to network based flow data records such as network based FDRs, CDRs or IPDRs; service usage classified at least in part by time of day; service usage classified at least in part by geographic location; service usage classified at least in part by the active network servicing the device; service usage classified at least in part by a roaming network connected to the device; service usage classified at least in part by network busy state or network congestion; service usage classified at least in part by QoS, service usage records classified at least in part by layer 7 network communications information such as server name, domain name, URL, referrer host or application service flow information; service usage classified at least in part by network communications protocol such as TCP, UDP, DNS, SMTP, IMAP, POP, FTP, HTTP, HTML, VOIP; service usage classified at least in part by the application name or the application identifier assigned by the operating system or another application identifier unique to the application acquiring or requesting service (e.g., device user ID, such as Android user ID on an Android based device) ; and service usage classified at least in part by service activity.

[0038] In some embodiments, the DDR processor located in the secure execution environment is configured to send the device data records to a network element (e.g., storage function located in the network). In some embodiments, the DDR processor located in the secure execution environment is configured to provide a secure communication channel between the secure software or firmware instruction execution environment and the storage function located in the network (e.g., a network element, such as a service controller), in which the communication channel security protocol is configured to avoid tampering with the secure device data records (DDRs). In some embodiments, the DDR processor located in the secure execution is configured to perform an authentication sequence or process with a network element (e.g., a service controller) in which a secure device data record sequence initiation message is sent to a network destination followed by authentication protocol exchange sequences to authenticate the network element before transmitting the secure data records.

[0039] In some embodiments, the DDR processor located in the secure execution environment is configured to perform the following: send the device data record sequence to a network element (e.g., via a secure channel); implement a secure access controller for restricting network access to a predetermined subset of available network destinations; receive a secure message from a trusted network element (e.g., either directly from the network element or from another function on the device that forwards the secure messages from the network element to the DDR processor in the secure execution environment); if a validated (e.g., properly secured and configured) message is received that acknowledges receipt of one or more secure device data records or acknowledges an access network authentication sequence, then the secure access controller allows unrestricted or less restricted access to the network; if a validated message is not received that acknowledges receipt of one or more secure device data records or acknowledges an access network authentication sequence, then the secure access controller restricts access to a predetermined set of network destinations or functions until a validated message is received that acknowledges receipt of one or more secure device data records or acknowledges an access network authentication sequence.

[0040] In some embodiments, the DDR processor located in the secure execution environment is configured with an access controller that restricts access to a predetermined set of network destinations or functions if a predetermined maximum amount of time passes between: the time that a first message acknowledging receipt of one or more secure device data records or an authentication sequence is received by the DDR processor in the secure execution environment and the time that a second message acknowledging receipt of one or more secure device data records or an authentication sequence is received by the DDR processor in the secure execution environment; or the time that one or more secure device data records are sent by the DDR processor in the secure execution environment and the time that a message acknowledging receipt of one or more secure device data records or an authentication sequence is received by DDR processor in the secure execution environment; and the access controller otherwise allows unrestricted or less restricted access to the network.

[0041] In some embodiments, the DDR processor located in the secure execution environment is configured to send the device data record to the device data record storage function located in the network by first sending it to a second program function located on the device that then forwards the device data record to the device data record storage function

located in the network. In some embodiments, the DDR processor located in the secure execution environment is configured to provide a second service usage report sequence in addition to the secure device data record sequence. In some embodiments, another client function/element (e.g., a service processor function/element or agent) is configured to provide a second service usage report sequence in addition to the secure device data record sequence. In some embodiments, the second service usage report sequence includes service usage classification that is different at least in part from the secure device data records. In some embodiments, the difference between device data usage classification includes at least in part that one record includes one or more of the following: application information, layer 7 network information, service flow association information, user defined input information, network busy state information, active network information or other information while the other record does not.

[0042] In some embodiments, the DDR processor located in the secure execution environment is configured to send the device data record sequence and the second device data record sequence in a manner that allows for simplified reconciliation of the two records. In some embodiments, the DDR processor located in the secure execution environment is configured to provide the second service usage report sequence in a manner that provides approximate alignment of a measurement interval start time and stop time spanned by one or more of the second service usage reports and the measurement interval spanned by one or more of the secure device data records.

[0043] In some embodiments, the DDR processor located in the secure execution environment is configured to: be based on the monitoring of service usage of the wireless communication device with the wireless communication network, create and record characterizations of network performance; analyze the characterizations of network performance and reduce the performance characterizations into one or more network performance statistics that characterize in summary form the performance level or congestion level of the network as experienced by the device; generate a plurality of network performance report messages that include a sequence of the network performance statistics created at different times; in which the network performance report messages are secured network performance reports; and send the secured network performance reports to the storage function located in the network.

[0044] In some embodiments, a processor of a network device configured as a device data record storage and processing function, for wireless communication with a wireless network in wireless communication with a plurality of wireless communication devices, with each wireless device including a secure device data record generator, in which the processor of the network device is further configured to: provide individual secure communication channels between each of the plurality of secure device data record processor and the network device, in which the communication channel security protocol is configured so that tampering with the device data records may be detected; receive over the secure communications channel a plurality of device data records from each of the secure device data record processors, in which the plurality of secure device data records are service usage records of monitored service usage of the wireless communication device with the wireless network, and in which each device data record forms a portion of an ordered sequence of device data records with each sequential device data record providing an uninterrupted accounting of service usage over the service usage interval spanned by the device data record, and in which the sequence of device data records forms a contiguous and uninterrupted reporting of device service usage, and in which each device data record is associated with a unique sequence order identifier; provide a device data record storage function in which the device data record sequence for each device is stored; for each device, analyze the stored sequence of device data records to determine if one or more of the device data records have been compromised by verifying that the information in the service usage record is properly configured according to the secure communication channel protocol; for each device, determine if one or more of the device data records have been removed or blocked from the device data record sequence originally transmitted from the device by determining if the secure contiguous sequence identifiers for the aggregate sequence are all present in the sequence; and if any device data record has been compromised, delayed or removed, set a fraud detection error flag for that device to restrict network access and also signals network apparatus or a network administrator to take further action.

[0045] In some embodiments, the secure device data records included in the device data record sequence include a secure network performance report that characterizes the network performance or congestion at the time the secure device data record was generated. In some embodiments, the device data record sequence is used at least in part as a record of service usage that forms an input factor in the business logic or rules used to compute a service usage bill. In some embodiments, the device data record sequence is used at least in part as a record of service

usage that forms an input factor in the business logic or rules used to determine if one or more device access network service policies are being properly enforced. In some embodiments, the device data record sequence is used at least in part as a record of service usage that forms an input factor in updating an end user service usage notification message, service usage notification display or service purchase message trigger event.

[0046] In some embodiments, the network device processor is further configured to receive a device data record sequence from a second device program function that forwards the device data record after receiving it from the secure device data record generator. In some embodiments, the network device processor is further configured to receive a second service usage data record sequence from a second device program function. In some embodiments, the two device data record sequences possess service usage classification that is different at least in part (e.g., use of classification parameters; layer 3/4 and/or layer 7) over the same (or approximately the same or overlapping) time span. In some embodiments, the network device processor is further configured to compare the two data record sequences and determine if the two sequences of service usage reports match one another to within an allowable tolerance limit.

[0047] In some embodiments, the secure device data record(s) can accompany the corresponding layer-7 classification information (e.g., domain names, application id, HTTP information, associative classification, and/or other information as described herein) with the 5-tuple classification information (e.g., source address, port address, destination address, destination port, and protocol) received from the Service Processor included in the DDR report, which, for example, can be sent to the Service Controller (e.g., or another network element) to assist in the service usage reconciliation and/or verification, using various techniques described herein. In some embodiments, one or more of the service usage reconciliation and/or verification operations using the layer-7 classification information and the 5-tuple classification information are performed locally in the client (e.g., in a secure execution area). In some embodiments, one or more of the service usage reconciliation and/or verification operations using the layer-7 classification information and the 5-tuple classification information are performed locally in the client (e.g., in a secure execution area), and one or more of the service usage reconciliation and/or verification operations using the layer-7 classification information and the 5-tuple classification information are performed in the network (e.g., at one or more network elements, such as the Service Controller).

[0048] In some embodiments, a portion of the matching criteria is determining if the two sequences of service usage reports match in the reported network performance levels or network congestion levels. In some embodiments, the tolerance limit is based on total data usage over the usage interval spanned by the two data record sequences.

[0049] In some embodiments, the network device processor is further configured to identify the amount of service usage for one or more classification categories in the second service usage record sequence that can be reconciled with service usage for one or more classification categories in the secure device data record sequence. In some embodiments, a criteria in the classification category reconciliation includes determining if the two sequences of service usage reports match in the reported network performance levels or network congestion levels.

[0050] In some embodiments, the network device processor is further configured to identify the amount of service usage from the second service usage record sequence that cannot be reconciled with known service usage classifications in the secure device data record sequence. In some embodiments, a criteria in the classification category reconciliation includes determining if the two sequences of service usage reports match in the reported network performance levels or network congestion levels.

[0051] In some embodiments, a minimum tolerance limit is placed on the amount, relative amount or percentage of service usage for one or more classification categories in the second service usage record sequence that can be matched to or correlated with one or more classification categories in the secure device data record sequence. In some embodiments, when the minimum tolerance limit is not met a fraud detection error flag for that device is set to restrict network access and also signals network apparatus or a network administrator to take further action.

[0052] In some embodiments, a maximum tolerance limit is placed on the amount, relative amount or percentage of service usage for one or more classification categories in the second service usage record sequence that cannot be matched to or correlated with one or more classification categories in the secure device data record sequence. In some embodiments, when the maximum tolerance limit is exceeded a fraud detection error flag for that device is set to

restrict network access and also signals network apparatus or a network administrator to take further action.

[0053] In some embodiments, the network device processor is further configured to determine if the service usage report spanned by the secure device data record sequence is consistent to within predetermined tolerance limits with one or more device service usage enforcement policies intended to be in place. In some embodiments, if the tolerance limits are exceeded a fraud detection error flag for that device is set to restrict network access and also signals network apparatus or a network administrator to take further action. In some embodiments, the network device processor is further configured to determine if the service usage report spanned by the second device service usage report sequence is consistent to within predetermined tolerance limits with one or more device service usage enforcement policies intended to be in place. In some embodiments, if the tolerance limits are exceeded a fraud detection error flag for that device is set to restrict network access and also signals network apparatus or a network administrator to take further action.

[0054] In some embodiments, the network device processor is further configured to provide one or more secure messages to each of multiple device programs running in a secure software or firmware instruction execution environment, in which the secure messages either acknowledge receipt of one or more secure device data records or acknowledge an access network authentication sequence. In some embodiments, the network device processor is further configured to send, for each device, a series of secure messages that directly or implicitly instruct the programs running in a secure software or firmware instruction execution environment to allow unrestricted or less restricted network access for a period of time that is either predetermined or is specified in a message from the network device processor to the program running in a secure software or firmware instruction execution environment. In some embodiments, the network device processor is further configured to send, for each device, a secure message that instructs the program running in a secure software or firmware instruction execution environment to restrict network access to a predetermined set of network destinations or functions.

[0055] In some embodiments, a secure network busy state (NBS) monitoring and reporting is provided. In some embodiments, the secure NBS monitoring and reporting facilitates NBS charging and control enforcement. In some embodiments, a processor of a

wireless communication device for wireless communication with a wireless network, in which the processor is configured with a secure software or firmware instruction execution environment, and in which a DDR processor in the secure execution environment is configured to: monitor service usage of the wireless communication device with the wireless network; based on the monitoring of service usage of the wireless communication device with the wireless communication network, create and record characterizations of network performance; analyze the characterizations of network performance and reduce the performance characterizations into one or more network performance statistics that provide indications of the performance level or congestion level of the network as experienced by the device; generate a plurality of network performance report messages that include a sequence of the network performance statistics created at different times; in which the network performance report messages are secured network performance reports; and send the secured network performance reports to the storage function located in the network.

[0056] In some embodiments, the measures of network busy state or network congestion are formed by observing one or more of: the number of network access attempts, the number of access successes the number of access failures, the delay between access attempt and access success, network throughput data rate, data error rate, packet error rate, packet repeat rate, one way or round trip delay, one way or round trip delay jitter, TCP traffic back off parameters, TCP window parameters, modem channel quality, modem channel power, modem channel signal to noise ratio, modem over the air data rate, or network throughput data rate versus modem over the air data rate, and the sub network of the network that the device is connected to.

[0057] In some embodiments, the measures of service usage are obtained from observing the network traffic generated by the service usage of the device user. In some embodiments, the measures of service usage are obtained from: communicating one or more network traffic sequences between the device and a network function; and using the subset of service usage monitoring that includes the network traffic sequences to create and record characterizations of network performance.

[0058] In some embodiments, a processor of a network device configured as a device secure network performance record storage and processing function, for wireless communication with a wireless network in wireless communication with a plurality of wireless communication devices, with each wireless device including a secure network performance record generator, in

which the processor of the network device is further configured to: provide individual secure communication channel between each of the plurality of secure network performance record generators and the network device, in which the communication channel security protocol is configured so that tampering with the secure network performance record may be detected; receive over the secure communications channel a plurality of secure network performance records from each of the secure network performance record generators, in which the plurality of secure network performance record are network performance statistics that provide indications of the performance level or congestion level of the network as experienced by the device; provide a device secure network performance record function in which the secure network performance record sequence for each device is stored; determine the sub network of the network that each device is connected to, and analyze the secure network performance records received from multiple devices connected to the same sub network to determine an aggregate characterization of the performance level or congestion level for the sub network, and perform the same operation to determine an aggregate characterization of the performance level or congestion level for other sub networks connected to the network; store the results of the aggregate characterization of the performance level or congestion level for each sub network that is characterized, and make the stored results available to other network devices or functions; and if any device data record has been compromised, delayed or removed, set a fraud detection error flag for that device to restrict network access and also signals network apparatus or a network administrator to take further action.

[0059] In some embodiments, a network performance characterization system is provided. In some embodiments, the network performance characterization system includes a processor of a wireless communication device for wireless communication with a wireless network, in which the processor is configured with a secure software or firmware instruction execution environment, and in which a program in the secure software or firmware instruction execution environment is configured to: communicate a plurality of traffic sequences between the device and a network device, in which the traffic sequences are secured; and initiate each traffic sequence based on one or more of the following: a pre-determined time or time interval, a service usage event or service usage condition that arises on the device, and as a response to a message communicated from the network device; and a processor of the network device in secure communication with the program (e.g., DDR processor) in the secure execution environment is configured to: monitor the plurality of the secure traffic sequences between

service usage of the wireless communication device with the wireless network; use the monitoring results of the secure traffic sequences, create and record characterizations of network performance; analyze the characterizations of network performance and reduce the performance characterizations into one or more network performance statistics that provide indications of the performance level or congestion level of the network as experienced by the device; generate a plurality of network performance reports that include a sequence of the network performance statistics created at different times; in which the network performance reports are stored in a network performance report storage function; and the network performance report storage function is made available to other network devices or functions.

[0060] In some embodiments, the DDRs are applied to one or more of the following activities: service billing, service control, and/or access control; service usage measurement (e.g., fraud resistant and scalable device measurement of service usage); verifying monitored service usage; verifying that service usage control policies are properly implemented on the device; and a source of performance monitoring and/or measurement.

[0061] In some embodiments, the DDRs are communicated to a network element based on a configured time interval; based on a configured usage size (e.g., buffer size limit or predefined size limit for a device or based on other criteria); when modem resources reach a predefined threshold (e.g., usage threshold, such as out of memory or approaching a threshold limit usage of memory); in response to a request from a service processor executed on an application processor of the wireless communication device; in response to a request from a service controller (e.g., either directly or indirectly through a service processor executed on an application/general processor of the wireless communication device).

[0062] In some embodiments, a reconciliation process is provided for reconciling a plurality of device data records and service processor usage reports for monitored wireless communication devices to verify reported service usage for each of the monitored wireless communication devices, which includes one or more of the following: reconcile the received device data records from each of the plurality of monitored wireless communication devices and service processor usage reports for a predefined time period or based on a comparison for each received service processor usage report and associated device data records or based on a predefined service usage amount/bulk usage amount or based on a predefined period of time or based on a service policy verification setting; verify that the monitored wireless communication

device has not been tampered with or compromised (e.g., missing, modified, delayed, and/or unreconciled DDRs – discrepancy between received micro-CDRs and DDRs outside of tolerances); verify that the monitored wireless communication device's service usage is compliant with an associated service policy and/or service plan; verify that the monitored wireless communication device properly implemented a traffic control policy of an associated service policy/service plan for a period of time (e.g., QoS, NBS, throttling); verify an accuracy of the received service usage measures using the received plurality of device data records and service processor usage reports for each of the monitored wireless communication devices; and reconcile using a tolerance threshold. In some embodiments, the tolerance threshold (e.g., fixed amount, percentage based) accounts for variances between the received device data records and service processor usage reports for synchronized monitored time periods, including one or more of the following: a service provider configured tolerances, a configured tolerance in the reconciliation process for unclassified service usage in the received device data records and/or service usage that cannot be correlated with known service activities, redirected service usage activities for content distribution network services, and/or other possible differences and/or variations.

[0063] In some embodiments, a reconciliation engine performs one or more of the following: determine one or more patterns to account for synchronization errors or traffic classification errors over time (e.g., training period, periodic refining using heuristics); determine if the received device data records are properly associated within policy service usage activities (e.g., reverse DNS lookup, white list, or web crawler); perform a classification operation on the received plurality of device data records that is similar to a service processor classification (e.g., layer 7 service usage activity classification, such as reported in micro-CDRs/uCDRs), then group the received plurality of device data records usage into service usage activity classifications used by the service processor; determine the service processor usage reports' service usage measures for each service activity classification, then determine a percentage of each service usage activity that can be verified by classifying the received device data records' service usage measures; implement adaptive ambient techniques for reconciliation (e.g., using threshold based comparison techniques, for example, with DDRs and the use of reverse DNS for packet classification, then using the ratio of allowed usage for host sponsored service vs. ALL white-listed host names, vs. all unknown host names, vs. synchronization error tolerance, perform a comparison (with acceptable percentage of error) and identify potential fraud scenarios; perform

reconciliation for one or more of the following classified services: sponsored services, user (e.g. open access) services, carrier services, network protection services (e.g., services that can be classified as background and thus be delayed in order to protect network bandwidth/resources for foreground/higher priority services) that are a part of the service plan classification definition; and reconcile using a third service usage measure (e.g., network based CDRs, FDRs, and/or IPDRs). In some embodiments, the secure device data record(s) can accompany the corresponding layer-7 classification information (e.g., domain names, application id, HTTP information, associative classification, and/or other information as described herein) with the 5-tuple classification information (e.g., source address, port address, destination address, destination port, and protocol) received from the Service Processor included in the DDR report, which, for example, can be sent to the Service Controller (e.g., or another network element) to assist in the service usage reconciliation and/or verification, using various techniques described herein.

[0064] In some embodiments, DDRs include one or more of the following: 5-tuple classification information, including a source address, a port address, a destination address, a destination port, and a protocol (e.g., inbound and outbound) and byte counts, and the tolerance threshold accounts for one or more of the following: usage measurement differences, time synchronization differences and/or information that is classified by the service processor with the advantage of information not available in the DDR processor classifier (e.g. application information, associative information, simpler classification implementations/algorithms in the DDR processor, etc.). In some embodiments, the service processor usage reports include one or more of the following that is not included in the received device data records: layer 7 monitored service usage information (e.g., domain names, application id, HTTP information, associative classification, and/or other information as described herein), and only a certain percentage of the received device data records are identified as associated traffic with a service usage activity, and for each service usage activity an allowance for unclassified traffic that varies by activity is provided (e.g., Amazon is “closed” while CNN is very diverse), in which a sum of all unclassified allowances does not exceed a total of unclassified received device data records information, and relaxing the tolerance for a first time interval and tightening the tolerance for a second time interval, in which the second time interval is longer than the first time interval. In some embodiments, the secure device data record(s) can accompany the corresponding layer-7 classification information (e.g., domain names, application id, HTTP information, associative

classification, and/or other information as described herein) with the 5-tuple classification information (e.g., source address, port address, destination address, destination port, and protocol) received from the Service Processor included in the DDR report, which, for example, can be sent to the Service Controller (e.g., or another network element) to assist in the service usage reconciliation and/or verification, using various techniques described herein.

[0065] Advanced Wireless Service Platform (AWSP)

[0066] In some embodiments, an Advanced Wireless Service Platform (AWSP) is provided. In some embodiments, AWSP provides an enhanced networking technology platform that supports existing services and also provides for various new Internet and data service capabilities for wireless networks (e.g., 4G, 3G, and/or 2G networks), as described herein with respect to various embodiments. In some embodiments, wireless devices, processor(s), firmware (e.g., DDR firmware, as described herein with respect to various embodiments), and software provide an enhanced role in wireless network service policies for charging, access control and service notification to implement AWSP, as described herein with respect to various embodiments.

[0067] In some embodiments, AWSP supports a wide range of services, devices, and applications for consumer, enterprise, and machine to machine markets, as described herein with respect to various embodiments. In some embodiments, AWSP supports various device types, including the following: 4G and 3G smart phones, 4G and 3G feature phones, 4G and 3G USB dongles and cards, 4G-to-WiFi and 3G-to-WiFi bridge devices, 4G and 3G notebook and netbook computing devices, 4G and 3G slate computing devices, 4G and 3G consumer electronics devices (e.g., cameras, personal navigation devices, music players, and home power meters), and machine to machine devices (e.g., various types of consumer and industrial devices with minimal user interface (UI) capabilities such as geo-location tracking devices, parking meters, and vending machines).

[0068] In some embodiments, AWSP includes a device data record (DDR) processor. In some embodiments, the DDR processor includes firmware that is integrated into a secure hardware execution environment within an AWSP compliant processor (e.g., a processor or set of processors that are compatible with, support, approved for and/or certified for AWSP, such as through a wireless carrier AWSP chipset certification program). In some embodiments, the

AWSP compliant processor is certified to qualify the processor for proper services delivery over AWSP, as described herein with respect to various embodiments.

[0069] In some embodiments, a DDR Firmware Developer's Kit (DDR FDK) is provided. In some embodiments, the DDR FDK includes firmware code (e.g., written in C), detailed DDR Processor specifications, detailed chipset Secure Execution Environment (SEE) specifications, DDR Processor chipset test criteria, and DDR Processor chipset certification procedures. For example, an approved chipset partner can integrate the DDR firmware into a Chipset Certification Device (CCD) for approved or certified processor(s) (e.g., chipsets that have been approved or certified under an AWSP Chipset Certification Program). In some embodiments, the CCD includes an approved chipset partner chipset Board Support Package (BSP) for a smart phone/feature phone device that includes the chipset submitted to the AWSP Chipset Certification Program. In some embodiments, the CCD includes a smart phone/feature phone device that includes the Approved Chipset Partner chipset submitted to the AWSP Chipset Certification Program. In some embodiments, various Operating Systems (OSs) are supported (e.g., Linux, Android, Apple, Microsoft, Palm/HP, Symbian, and/or various other operating systems and/or platforms).

[0070] In some embodiments, enhanced functionality includes integration of a Service Processor (SP) kernel program and application. In some embodiments, in addition to the DDR firmware, a Service Processor Software Developers Kit (SP SDK) is provided. In some embodiments, the SP SDK includes software and descriptive information for integrating the SP SDK kernel program and application software into a device OEM as described herein with respect to various embodiments. In some embodiments, an Approved Chipset Partner CCD connects to either Wireless Carrier's 3G (EVDO/UMTS) network or Wireless Carrier's 4G LTE network using a mutually agreeable WWAN wireless modem chipset that is certified for operation on Wireless Carrier's network.

[0071] DDR Processor Overview

[0072] In some embodiments, the DDR Processor is implemented within secure firmware embedded in either an applications processor unit (APU) or a modem processor unit (MPU). In some embodiments, the DDR Processor is provided as part of the device firmware build installed by an OEM at time of manufacture. In some embodiments, the DDR Processor monitors

incoming and outgoing IP packets and gathers various statistics (e.g., Device Data Records (DDRs)). In some embodiments, a DDR is, in part, a record of the amount of data transmitted or service usage consumed along an IP flow. In some embodiments, an IP flow is specified by a source address, a destination address, a source port, a destination port, and a protocol type. In some embodiments, the secure device data record can also accompany the corresponding layer-7 classification information (e.g., domain names, application id, HTTP information, associative classification, and/or other information as described herein) with an IP flow (e.g., source address, port address, destination address, destination port, and protocol) received from the Service Processor. In some embodiments, DDRs also include other types of classification for network service usage, as described herein with respect to various embodiments. In some embodiments, DDRs also include various statistics related to or based on network service usage, as described herein with respect to various embodiments. In some embodiments, DDRs are used in 2G, 3G, and 4G wireless networks in both home and roaming network conditions for various service usage accounting, access control, and service policy enforcement verification functions, as described herein with respect to various embodiments.

[0073] **Figure 1** illustrates a high level diagram of an advance wireless service platform end-to-end DDR reporting and processing system in accordance with some embodiments. In Figure 1, three DDR implementation options are shown for securely embedding a DDR processor (e.g., DDR processor firmware and/or functionality) into an APU chipset or an MPU chipset. Each of these three options is described at a high level below and in more detail in following sections.

[0074] In some embodiments, a wireless communication device includes a DDR processor 114 in a secure execution environment. In some embodiments, the DDR processor 114 includes a DDR generator function (e.g., a function for generating secure DDRs, which can be reported to another element/function in the device and/or to a network element/function, such as a service controller 122) as described herein with respect to various embodiments. Various architectures are provided for implementing the DDR Processor in a secure execution environment.

[0075] Device architecture 101 includes the DDR processor 114 in a zone of data path security 140 (e.g., located in an application/general processor unit (APU)) as shown. Application programs 130 are monitored (e.g., service usage based monitoring) using a service

processor application program 112. Kernel programs 132 are monitored using a service processor kernel program 113. An operating system (OS) 134 resides above a network stack 136 for network access, which is monitored by the DDR processor 114 for any network access through a modem bus driver and physical bus 142. As shown, 3G or 4G wireless network access is provided through a 3G or 4G modem 150 to a 3G or 4G networks 104, respectively. This device architecture and similar device architectures are described herein in more detail below.

[0076] Device architecture 102 includes the DDR processor 114 in a zone of data path security 143 (e.g., located in a modem processor unit (MPU)) as shown. Device architecture 102 is similar to device architecture 101 except that in device architecture 102 the zone of data path security 143 is located in 3G or 4G modem 151. Network communication via the modem 151 through modem bus driver and physical bus 149 and modem I/O 156 is monitored using the DDR processor 114 for any network access through a modem data path and signal processing 154. This device architecture and similar device architectures are described herein in more detail below.

[0077] Device architecture 103 includes the DDR processor 114 in a zone of data path security 145 (e.g., located in an APU or another processor/memory, such as a SIM card)) as shown. Device architecture 103 is similar to device architecture 101 except that in device architecture 103 the APU's modem bus driver and physical bus does not need to be in a secure zone and instead a data path security verifier 152 is included in the zone of data path security 147 in the MPU to restrict network access to only traffic that has been monitored by the DDR Processor 114 within APU. This device architecture and similar device architectures are described herein in more detail below.

[0078] In some embodiments, a Service Controller 122 is provided as shown. In some embodiments, Service Controller 122 is provided as an AWSP network server cloud system. In some embodiments, Service Controller 122 is provided as an AWSP network server cloud system that is used to perform one or more of the following: collect device service usage reports; manage certain aspects of device based network service policy; ascertain the Network Busy State (NBS) for various base stations on the network (e.g., wireless network(s)); manage the user notification and service plan selection UI processes configured on the device(s) (e.g., wireless communication device(s)); and manage certain aspects of service fraud detection. In some embodiments, the service controller 122 includes a secure DDR processing, usage

reconciliation, and fraud detection function 124 as shown. In some embodiments, the service controller 122 communicates monitored service usage (e.g., reconciled service usage based on processed and reconciled secure DDRs) to network service usage reporting systems 180. In some embodiments, the reported service usage is aggregated and communicated to network billing systems 190 (e.g., for billing for the reported service usage).

[0079] In some embodiments, the Service Controller 122 communicates with various device-based elements of the AWSP system. In some embodiments, the Service Controller 122 communicates with various device-based elements of the AWSP system, including the following: the DDR Processor 114 and a Service Processor. In some embodiments, the Service Processor 112 includes an application Service Processor 112 (e.g., an application space or framework space program) and a kernel service processor 113 (e.g., a kernel space or driver space program). In some embodiments, the application service processor 112 and the kernel service processor 113 execute or perform in an OS partition on an application processor unit (APU) of a device (e.g., a wireless communication device). In some embodiments, the Service Processor is not generally in a secure execution area.

[0080] In some embodiments, the Service Processor performs various functions for the carrier network including collecting Network Busy State (NBS) information, service usage classification and reporting, certain network service policy enforcement functions, and/or certain user notification functions and roaming access policy enforcement functions, as described herein with respect to various embodiments. In some embodiments, the Service Processor also logs and reports device service usage information that assists a carrier (e.g., a service provider for a wireless network service or other services) in determining how to provide users with optimized services, information, and/or content.

[0081] In some embodiments, the DDR Processor 114 communicates DDRs to the Service Controller 122. In some embodiments, the DDR Processor 114 communicates DDRs to the Service Controller 122 via the Internet, a carrier network, and/or other network. In some embodiments, the DDR Processor 114 does not send DDRs directly to the Service Controller 122, but instead the DDR Processor 114 forwards the DDRs to the Service Processor. The Service Processor then forwards or relays the DDRs to the Service Controller 122 and, in some embodiments, along with additional service usage reports and/or other service policy

management and user notification communications generated by or received by the Service Processor.

[0082] For example, the APU OS execution environment is generally not considered secure or trusted even though the Service Processor can be protected by the OS and/or other security elements within the system. In addition, the network data path between the DDR Processor 114 to the Service Processor is generally not considered to be secure or trusted and neither is the data path between the Service Processor and the Service Controller 122. Accordingly, in some embodiments, the DDR Processor 114 and the Service Controller 122 use cryptographic techniques to provide a secure link from the DDR Processor 114 to the Service Controller 122. In some embodiments, the DDR Processor 144 is considered secure and trusted based on various implementations and techniques as described herein with respect to various embodiments. In some embodiments, various techniques for securing the service usage monitoring and control performed by the DDR Processor 114 on a network data path, and securing the DDR reporting channel from the DDR Processor 114 to the Service Controller 122 are described herein with respect to various embodiments.

[0083] In some embodiments, a secure access controller function within the DDR Processor 114 is employed as described below to ensure that if the DDR flow is tampered with or blocked, then the device network access data path connection managed by the DDR Processor 114 is restricted to only those network destinations required to manage the DDR Processor 114 communication with the Service Controller 12. In some embodiments, the access controller function within the DDR Processor 114 receives feedback from the Service Controller 122 to restrict access or allow full access. For example, the restricted access list (e.g., a list of host names, IP addresses, and/or other identifiers for an access list) can either be pre-provisioned within the DDR Processor SEE or configured through the secure path as described in more detail herein.

[0084] In some embodiments, a secure, reliable, and trusted transmission of DDRs from the DDR processor 114 is provided by DDR reporting techniques, including the following: (1) the DDR Processor firmware is securely loaded and executed in a Secure Execution Environment (SEE); (2) the data path between the DDR Processor to the wireless modem antenna connection (e.g., a 3G or 4G network modem antenna connection) is secured to prevent fraudulent software or firmware from forming data paths that circumvent the DDR Processor

data path processing; (3) the DDRs transmitted from the DDR Processor 114 to the Service Controller 122 are integrity checked in a manner that protects them from being tampered with or replayed; and (4) an authentication process between the DDR Processor 114 and the Service Controller 122 combined with a set of unique DDR report sequence identifiers and authentication session keep alive timers are used to maintain and verify the secure connection between the DDR Processor 114 and the Service Controller 122. For example, if the secure session or the flow of DDR records between the DDR Processor 114 and the Service Controller 122 are interrupted, then the secure access control function in the DDR Processor 114 can restrict access to the modem data path to the network destinations necessary to re-establish a securely authenticated session between the DDR Processor 114 and the Service Controller 122.

[0085] In some embodiments, the DDR Processor 114 also includes a secure Network Busy State Monitor function (e.g., NBS Monitor) as similarly described herein with respect to various embodiments. In some embodiments, the NBS Monitor logs and reports various network and modem performance parameters and also computes and reports a measure of network congestion referred to herein as the Network Busy State (NBS). In some embodiments, the NBS is a measure that indicates the level of network congestion at a given base station sector over a given measurement time interval. In some embodiments, all of this information is included in a Network Busy State Report (NBSR) that is part of the DDR message reports sent to the Service Controller 122 via the Service Processor 112.

[0086] Overview of Secure Image Programming, Secure Boot, Secure Execution, and Secure Firmware Update

[0087] In some embodiments, the DDR Processor system includes a dedicated Secure Execution Environment (SEE) within the Application Processor Unit (APU) or modem chipset. In some embodiments, the SEE provides for a secure, trusted generation of DDRs as described herein. The basic functionality of the SEE in accordance with some embodiments is described below.

[0088] In some embodiments, the SEE is a secure memory execution partition that cannot be accessed by any external program, bus, or device port. In some embodiments, the secure memory execution partition includes code space and data space. In some embodiments, a secure boot loader executes within the SEE. In some embodiments, the only other code images

allowed to execute in the SEE are secure images, meaning digitally-signed images whose signature is verified by the secure boot loader. In some embodiments, at time of device manufacture, the secure boot loader is programmed into nonvolatile memory in the on-chip SEE. For example, the secure boot loader can fetch a secure image from nonvolatile memory and install it in the SEE in a trusted and secure manner. In some embodiments, the secure boot loader is the only element capable of loading an image into the SEE.

[0089] In some embodiments, the DDR Processor 114 is implemented as a secure image. Installation of the DDR Processor image into the SEE using the secure boot loader is described below. Other secure images can be similarly installed as will be apparent to one of ordinary skill in the art in view of the embodiments described herein.

[0090] In some embodiments, the DDR Processor image is digitally signed by the device OEM. For example, the secure boot loader can verify the signature using a boot loader verification key and reject the image if the signature is invalid. In some embodiments, the boot loader verification key is a 2048-bit RSA public key embedded within the secure boot loader image.

[0091] In some embodiments, the signed DDR Processor image is stored in on-chip nonvolatile memory. In some embodiments, the signed DDR Processor image is stored in off-chip nonvolatile memory (e.g., if the on-chip storage capacity of the chipsets is too constrained to store this image).

[0092] **Figure 2** illustrates a process for booting, executing, and updating the DDR firmware in accordance with some embodiments. As shown in Figure 2, at 210, when the device boots, the Secure Boot Loader fetches the DDR Processor image from nonvolatile memory, installs it in the SEE, and executes it. In some embodiments, during installation, and prior to execution, the secure boot loader verifies the digital signature of the DDR Processor image using the boot loader verification key. If the signature is invalid, execution does not occur and an error message is sent to the Service Controller via the Service Processor, and the secure boot loader attempts to fall back to a previously stored image, as described herein with respect to various embodiments.

[0093] In some embodiments, the data path from the non-secure OS stack elements to the modem(s) being monitored and controlled by the DDR Processor must pass into the SEE and be made available to the DDR Processor, such as shown at 220 in Figure 2. Once the OS stack data destined for the modem is transferred into SEE memory, the secure DDR Processor program analyzes and acts on the data destined for the modem as described herein with respect to various embodiments. In some embodiments, the DDR Processor includes a secure data interface from the SEE to the modem data path such that there are not any data paths that can circumvent the SEE (e.g., to avoid detecting and/or monitoring by the DDR Processor). Examples of secure execution partition and data interface solutions include a trusted API, an ARM Trust Zone, an Intel Smart & Secure, or a custom solution or proprietary solution specific, such as from a chipset supplier for specific chipsets.

[0094] In some embodiments, a communication channel (e.g., a DDR mail box) provides communication between the DDR Processor program executing in the SEE to a Service Processor application program executing in the non-secure OS environment (e.g., application space or user space), such as shown at 230 in Figure 2. Example techniques for providing the DDR mailbox include shared memory using DMA channels, logical channels (e.g., endpoints) within the modem bus driver (e.g., USB interface) between the APU and MPU, and piggyback channels on top of an already existing logical channel between the APU and MPU.

[0095] In some embodiments, the DDR Processor firmware image is updated, such as shown at 240 in Figure 2. In some embodiments, the DDR Processor firmware image is updated using OEM processes supported by the chipset supplier for over the air (OTA) and over the network (OTN) update(s) of the chipset nonvolatile memory firmware image provided to device OEMs. In some embodiments, the DDR Processor is stored along with other chipset secure firmware drivers loaded by the secure boot loader either during the initial power up cycle, upon exiting from power save state and/or any other times that the download can be performed in secure manner. In some embodiments, the DDR Processor requires enough nonvolatile memory space to accommodate at least two images, one image that is currently running and a new downloaded image (e.g., each image can be of a specified maximum size, such as 0.5 MB or another size limit). In some embodiments, the secure boot loader includes a firmware image switch to use the new image once the download is complete. For example, the image switch function can include a fallback system to switch back to the current image if the new image has

an invalid signature, or if the new image is older than the current image as indicated by revision numbers included within each image. The current image can be retained at least until the new image has been accepted by the secure boot loader.

[0096] Overview of DDR Processor Implementation Embodiments

[0097] The DDR Processor can be provided using different configurations for secure embedded DDR firmware (e.g., in AWSP chipsets) including in an APU implementation, an MPU implementation, and a combined APU/MPU implementation as described herein in accordance with various embodiments. Those of ordinary skill in the art will also appreciate that similar and various other secure partition configurations for providing secure embedded DDR firmware can be provided in view of the various embodiments described herein.

[0098] In some embodiments, the DDR processor is provided using an integration into the APU chipset SEE and nonvolatile memory, such as an APU implementation shown in device architecture 101 in which the DDR processor 114 and a modem bus driver and physical bus 142 are implemented in the zone of data path security 140 as shown in Figure 1. The DDR Processor is securely implemented on the 2G, 3G, or 4G modem data path directly below the modem driver data path processing function and above the modem bus driver data path processing function (e.g., typically USB driver, SDIO driver, or similar bus driver function). For example, using this approach, the entire data path below the DDR Processor through the modem bus driver and through the 2G, 3G or 4G network modem can be secured to prevent data paths that circumvent the DDR Processor data path processing.

[0099] In some embodiments, the DDR processor is provided using an integration into the 2G, 3G, or 4G MPU chipset SEE and nonvolatile memory, such as an MPU implementation shown in device architecture 102 in which the DDR processor 114 and a modem data path and signal processing 154 are implemented in a zone of data path security 143 as shown in Figure 1. The DDR Processor is securely implemented on the 2G, 3G, or 4G modem data path just below the modem bus driver and logical channel interface. For example, using this approach, the entire data path below the DDR Processor to the 2G, 3G or 4G network is secured to prevent data paths that circumvent the DDR Processor data path processing.

[00100] In some embodiments, the DDR processor is provided using an integration into the APU chipset SEE and nonvolatile memory, such as an APU and MPU implementation shown in device architecture 103 in which the DDR processor 114 is implemented in the zone of data path security 145, and a data path security verifier 152 and the modem data path and signal processing 154 are implemented in a zone of data path security 147 as shown in Figure 1. The DDR Processor is securely implemented on the 2G, 3G, or 4G modem data path somewhere below the OS stack and above the modem bus driver. For example, using this approach, rather than securing the entire data path below the DDR Processor through the modem bus driver and through the 2G, 3G, or 4G network modem, the data path between the DDR Processor and the modem wireless network access connection is secured by integrity-checking the data that streams between the DDR Processor and a Data Path Security Verifier (DPSV) 152 function. Any data path information that is not properly accounted for and integrity-checked is not conducted to or from the wireless network connection. For example, this approach eliminates the need to secure APU firmware, hardware, and data path elements other than the DDR Processor itself.

[00101] Embedded DDR Processor Implementation on an Application Processor

[00102] In some embodiments, embedding the DDR processor in an Application Processor Unit (APU) (e.g., smart phone APU or other wireless communication device APU) provides a single secure DDR Processor location in the wireless network data path (e.g., 2G/3G/4G wireless network data path) that provides for service usage monitoring and access control for multiple wireless modems. Also, the APU implementation approach can allow APU chipset suppliers who may not necessarily have WAN modem components or technology to implement solutions compliant with the various AWSP techniques described herein. Further, the APU implementation approach generally more easily allows for OTA and OTN firmware updates for APU implementations as described herein (e.g., which can be more complicated to provide in certain MPU implementations).

[00103] Referring to device architecture 101 as shown in Figure 1, the DDR Processor is embedded into the APU chipset SEE and nonvolatile memory as similarly described above. Along with the DDR Processor SEE, the secure data path environment, shown as the Zone of Data Path Security 140, includes the DDR Processor 114 and the modem bus driver and physical bus 142. For example, provided that the modem bus driver and the physical bus to the modem are secured against (e.g., or otherwise inaccessible to) fraudulent software or firmware

attempting to circumvent the DDR Processor 114, the modem itself (e.g., 3G modem or 4G modem 150) need not be secured. In particular, the DDR Processor 114 is securely implemented on the 2G, 3G or 4G modem data path directly below the modem driver data path processing function and above the modem bus driver data path processing function (e.g., typically USB driver, SDIO driver or similar bus driver function). In some embodiments, the entire data path below the DDR Processor 114 through the modem bus driver and through the 2G, 3G or 4G modem is secured to prevent data paths that circumvent the DDR Processor data path processing. Accordingly, in some embodiments, the modem bus driver is either secured in the DDR SEE or in its own SEE, or the modem bus driver code and data path must be inaccessible to software or firmware on the APU that could circumvent the DDR Processor 114.

[00104] **Figure 3** illustrates an architecture for a secure embedded DDR Processor in an APU implementation in accordance with some embodiments. In particular, Figure 3 shows the major functional elements within an APU based solution in accordance with some embodiments, in which the DDR processor 114 resides in the APU's SEE together with other APU secure programs, and the DDR Processor's communication channel to the Service Processor application program 112 is via a shared mailbox (e.g., a shared memory). Figure 3 also shows an interface to the non-volatile memory (e.g., for software downloads) with the presence of secure boot code to ensure that all secure codes are first digital signature verified before a download is considered complete. In some embodiments, the data path is a separate interface in which data frames are sent to the secure environment for the DDR processor to gain access and perform DDR usage measure in addition to controlling limited or unlimited network access.

[00105] Referring to Figure 3, an APU can be logically partitioned into APU chipset application programs 302, APU chipset kernel programs 304, and a secure execution environment (SEE) shown as APU secure execution environment 306. The APU secure execution environment 306 communicates (e.g., using secure communication techniques, such as those described herein) with a network element/function (e.g., service controller 122 and/or other element(s)/function(s)). In some embodiments, secure program nonvolatile (NV) memory 340 includes OS/OEM secure device system program files 342, secure DDR processor program files 346, and APU secure device system program files 348 that can be fetched by the secure boot loader residing in the APU secure execution environment (SEE) 306 to be downloaded in to the SEE memory before code execution can take place as described herein.

[00106] The APU chipset application programs 302 include user application programs 130, service processor application program 112 (e.g., for performing various service processor functions that need not be implemented in the kernel, as described herein), and OEM application programs 310. The APU chipset kernel programs 304 include OEM kernel program 312, service processor kernel program 113 e.g., for performing various service processor functions that are preferably implemented in the kernel, as described herein), APU system kernel program 314, and APU device drivers and other BSP kernel programs 316. As also shown, OS 134 includes user/application space and kernel space implemented portions as would be apparent to one of ordinary skill in the art. Network access (e.g., 3G or 4G wireless network access) is communicated through APU network stack device driver 318, which resides in kernel space 304 as shown.

[00107] The APU SEE 306 includes a secure execution memory 322 for executing/storing secure DDR processor programs 326, APU secure device system programs (e.g., modem bus driver, modem driver) 328, and OS/OEM secure device system programs 330. The APU SEE 306 also includes a program signature verifier 332 for verifying the secure DDR processor programs 326 and/or other secure programs in the secure execution memory 322 as described herein. The APU SEE 306 also includes NV memory I/O 334 as shown. The APU SEE 306 also includes a secure execution boot loader and updater (e.g., secure on-board NVRAM) 336 for implementing a secure execution boot processes and secure update processes as described herein.

[00108] In some embodiments, the network data path 324 for any user or kernel mode applications or services are communicated from the APU networking stack device driver 318 and monitored using secure DDR processor programs 326.

[00109] As further described herein, secure DDR processor programs 326 communicate to the service processor application program 112 using a DDR mailbox function and communication channel as shown via DDR mailbox data 320. In some embodiments, the DDR mailbox function provides a secure communication channel using various techniques as described herein. In some embodiments, the DDR mailbox function is used to communicate secure DDRs generated using secure DDR processor programs 326 for monitored network service usage to the service processor application program 112. In some embodiments, the service processor application program 112 communicates the secure DDRs to a network element/function, such as the service controller 122. In some embodiments, the service

processor application program 112 communicates the secure DDRs with a service processor report (e.g., which includes device based micro-CDRs /uCDRs based on monitored service usage based on service processor application programs 112 and/or service processor kernel programs 113, such as application based monitoring/layer-7 or application layer based monitoring, as described herein) to a network element/function, such as the service controller 122. In some embodiments, the service processor application program 112 communicates the secure DDRs with a service processor report for overlapping and/or common time periods/intervals (e.g., which facilitates reconciliation of device assisted service usage monitoring based on the two DAS assisted service usage measures by the service controller or other network elements/functions).

[00110] **Figure 4** illustrates another architecture for a secure embedded DDR Processor in an APU implementation along with a modem bus driver in accordance with some embodiments. In particular, Figure 4 shows more detail on how the DDR Processor can be implemented in an APU secure operating environment along with a modem bus driver 428 (e.g., 2G, 3G, or 4G modem bus driver). The DDR Processor monitors IP packets going to and from the modem bus driver 428 (e.g. USB driver/controller), which provide for wireless network access via a secure data path 430 to a modem bus 432 for wireless access using a 2G/3G/4G modem 440 as shown.

[00111] As similarly described above, the secure execution boot loader and updater 336 loads the DDR Processor and modem bus driver images from nonvolatile (NV) memory 334 into the execution memory within SEE, shown as DDR secure execution memory 420, to execute (e.g., after code signature verification using secure program signature verifier 332). The DDR Processor and modem bus driver image and other secure images are all part of secure boot load to be signature verified before such are executed.

[00112] As shown, the DDR Processor sits in line with the 2G, 3G or 4G modem data path and all traffic between the OS stack and the 2G, 3G or 4G network is monitored by the DDR Processor 114. A DDR Processor OS stack data path interface 424 is provided that bridges between the DDR secure execution environment (SEE) 420 and the unsecure OS stack in the kernel. Also, a DDR Processor modem data path interface 426 is provided that similarly connects the DDR Processor 114 to the modem data path fed by the modem bus driver 428. In some embodiments, DDR Processor 114, which is provided in line on the data path and not simply a clone/monitor/drop function, also implements an access controller function to maintain

the integrity of network access, for example, in the event that the DDR reports are tampered with or blocked from reaching the service controller 122 or the DDR Processor 114 is tampered with, or the Service Processor 112 is tampered with, as described herein.

[00113] As also shown, a DDR processor mailbox interface 422 is provided that implements a mailbox function for passing DDR mailbox data 320 between the secure DDR SEE 420 and the unsecure Service Processor application 112. As would be apparent to one of ordinary skill in the art in view of the various embodiments described herein, the DDR mailbox function can be implemented in a variety of ways.

[00114] In some embodiments, the DDR Processor and USB driver execute in a secure environment on the application processor chipset, such as DDR secure execution memory 420. In some embodiments, the secure environment ensures no unauthorized ability to replace or modify the DDR Processor code or modem bus driver/controller code (e.g. USB driver/controller). In some embodiments, the secure environment also ensures that the data path from the DDR Processor to the physical modem bus driver (e.g. USB port) is isolated from firmware outside the secure environment. That is, no firmware outside the secure environment has the ability to affect the accurate gathering of statistics by the DDR Processor. In some embodiments, the secure environment further ensures that there is no ability for code other than the DDR Processor to access sensitive crypto storage, such as keys. For example, this can include shielding sensitive storage from debug monitors and/or other monitoring/access activities or techniques. As would also be apparent to one of ordinary skill in the art, APU firmware, not just the DDR Processor, must be secured and not include bugs or vulnerabilities that can be exploited to allow for unauthorized access. For example, a common attack is buffer overflow, in which an attacker chooses inputs that cause an unchecked buffer to exceed its bounds, resulting in unintended behavior that the attacker can exploit.

[00115] There are various examples of APU chipset SEE Implementation techniques that can be used to meet these requirements as described above. For example, a conventional CPU with upgradeable firmware (e.g., including the DDR Processor) can be provided. The firmware can be stored in nonvolatile (NV) memory, or can be stored in flash memory in which the flash memory can be reprogrammed/updated with new or upgraded firmware. The firmware can be installed at time of manufacture and by design provides a compliant secure environment. Rigorous quality-assurance testing is required to ensure that bugs are unlikely to provide a means

for compromising the secure environment. A new firmware image can be accepted for installation only if it has a valid digital signature. Version control checking can be included to prevent rollback to older versions. The firmware that validates the signature and version resides in firmware that can also be upgradeable. As another example, a security partitioned CPU can be provided, such as an ARM Trustzone or Intel Smart & Secure (e.g., or another suitable substitute including potentially supplier custom security environment CPU partitioning techniques). The DDR Processor, modem bus driver (e.g., USB driver/controller), and any intervening code can execute in the secure partition, such as Trustzone's (e.g., or Smart & Secure's) secure mode. A secure boot procedure enforces the requirement that the DDR Processor, modem bus driver (e.g., USB driver/controller), and intervening code can be included in a digitally signed, version-controlled code image. In such approaches, hardware firewalls can shield sensitive crypto storage from normal mode firmware. Also, the hardware firewalls ensure that normal mode firmware cannot tamper with the data path between the DDR Processor and the physical modem bus driver (e.g., USB port), thus, preventing interference with the gathering of service usage measure data and/or statistics as described herein.

[00116] **Figure 5** illustrates another architecture for a secure embedded DDR Processor in an APU implementation along with a modem bus driver in accordance with some embodiments. In particular, Figure 5 is similar to Figure 4, except that as shown in Figure 5, APU Stack Driver for 2G/3G or 4G Modem 410 is located in the DDR secure execution memory 420 instead of the APU kernel space 404.

[00117] **Embedded DDR Processor Implementation on a Modem Processor**

[00118] In some embodiments, in an MPU implementation, the DDR Processor resides in the modem processor with other secure modem data path processing code and hardware functions. For example, in an MPU-based secure DDR Processor implementation, once the data path below the modem bus driver interface is secured, it is relatively difficult to hack the device to create a data path that reaches the network by circumventing the DDR Processor. Also, for some MPU chipset families, it can be more straightforward to implement a secure execution environment, secure boot loader, and secure nonvolatile memory as compared to implementing the same functions in some APU families that do not have standard hardware security partition features, such as ARM Trust Zone and Intel Smart & Secure. Further, an MPU implementation can have less interaction with the OS kernel builds than in the case of an APU implementation.

[00119] However, it should also be observed that in a MPU DDR Processor implementation, the modem processor environment may not have a CPU with the same performance and secure execution memory space as an APU solution. This apparent disadvantage can be mitigated by designing and optimizing the DDR Processor firmware so that the code memory size is small and the CPU performance requirement is appropriate for a typically relatively low powered modem processor chipset CPUs. Also, as mentioned above, the OTA and OTN update process may be more complex than that achieved by certain APU chipset suppliers and their OEMs.

[00120] **Figure 6** illustrates an architecture for a secure embedded DDR Processor in an MPU implementation in accordance with some embodiments. In particular, Figure 6 shows an MPU implementation that includes an embedded DDR Processor and modem data path from the DDR Processor to the network in the zone of data path security. In this approach, the DDR Processor 114 is embedded into secure execution environment (SEE) 604 and secure execution memory 630 of the modem chipset (e.g., 3G or 4G MPU chipset). As shown, to ensure that fraudulent software or firmware cannot circumvent the DDR Processor, the Zone of Data Path Security includes the DDR Processor 114 along with the modem data path processing and the modem signal processing that occurs between the DDR Processor and the antenna. In some embodiments, the DDR Processor 114 is securely implemented on the 3G or 4G modem data path just below the modem bus driver 610 and logical channel interface and the entire data path below the DDR Processor 114 to the 3G or 4G network is secured to prevent data paths that circumvent the DDR Processor data path processing.

[00121] Similar to the APU based approach discussed above, Figure 6 shows the major functional blocks within a modem based solution in which the DDR Processor 114 resides in the modem's SEE monitor service usage via network data path 632, along with other secure modem code 634, below-DDR modem networking protocol code 636, and below-DDR modem data path processing 638, and the DDR processor's communication channel to the Service Processor application program is via a shared mailbox (e.g., serviced by a USB endpoint). This interface can either use a separate logical communication channel or be piggybacked on top of an already existing logical communication channel between APU and MPU. In some embodiments, the recipient of the DDR mailbox data 320 is the Service Processor Application code.

[00122] As also shown in Figure 6, the interface to the non-volatile memory (e.g., for software/firmware downloads/updates) with the presence of secure boot code ensures that all secure codes are first digital signature verified before download is considered complete. The data path is a separate interface in which data frames are sent to the secure environment for the DDR processor to gain access and perform DDR usage measure in addition to controlling limited or unlimited network access.

[00123] Modem chipset unsecure execution environment 602 includes a modem bus communication driver 610. In some embodiments, a logical communication channel for modem data path traffic 622 and above DDR modem data path processing 624 is also provided. In some embodiments, a logical communication channel for modem control settings and status reports 612, modem status data 614, modem control data 616, modem diagnostics data 618, and other unsecured modem functions 620.

[00124] **Figure 7** illustrates another architecture for a secure embedded DDR Processor in an MPU implementation in accordance with some embodiments. In particular, Figure 7 shows how the DDR Processor 114 is implemented in an MPU secure operating environment where the data path through the 3G or 4G modem network processing and signal processing is secured up to the antenna from access from software or firmware other than the DDR Processor. In some embodiments, the secure boot loader process operates as similarly described above.

[00125] As shown, APU chipset application programs 702, which includes DDR mailbox data 710 communicated to the service processor application program 112 as similarly described herein. APU chipset kernel programs 704 includes service processor kernel program 113 along with APU stack interface for 3G/4G modem 712, APU stack interface for other modems 714, and 3G or 4G modem bus driver 716 for communication via modem bus 718 to 3G or 4G modem bus driver 722 of modem chipset unsecure execution environment 706 as shown.

[00126] In some embodiments, the DDR Processor 114 is in line with the data path allowing for secure network/service usage measure and/or access control as similarly described herein with respect to various embodiments. In some embodiments, a DDR Processor OS stack data interface (IF) 728 is provided that bridges between the DDR secure execution environment (SEE) and the (potentially) unsecure modem bus driver interface 722 in modem chipset unsecure execution environment 706. As also shown, a DDR Processor modem data path interface 730 is

provided that similarly connects the DDR Processor 114 to the modem data path processing and the modem signal processing 740 that occurs between the DDR and the antenna. As described herein, the DDR is in line on the data path and is not simply a clone/monitor/drop function, as the DDR Processor also implement an access controller function in accordance with some embodiments to maintain the integrity of network access in the event that the DDR reports are tampered with or blocked from reaching the Service Controller, or the DDR Processor is tampered with, or the Service Processor is tampered with.

[00127] As also shown, a mailbox function is provided that passes data between the secure DDR SEE 725 and the unsecure Service Processor application program 112. In particular, a DDR Processor mailbox interface (IF) 724 is in communication with a DDR mailbox 720, which is located in the modem chipset unsecure execution environment 706. DDR mailbox data 710 is shown as provided to the unsecure Service Processor application program 112, which is provided through the modem communication path via the modem bus driver 722 and the modem bus 718 as shown. The DDR Processor mailbox interface (IF) 724 is in communication with the DDR Processor 114 and is located in the DDR SEE 725. As would be apparent to one of ordinary skill in the art in view of the various embodiments described herein, the mailbox function can be implemented in a variety of ways. As similarly described above with respect to the various APU based embodiments, in accordance with some embodiments, the secure region is inclusive of all data path processing steps below the DDR Processor, and there is not any data path through the modem to the network that circumvents the DDR Processor.

[00128] In some embodiments, the DDR Processor executes in a secure environment in the MPU based embodiments, as similarly described above with respect to the APU based embodiments. In some embodiments, the secure environment ensures no unauthorized ability to replace or modify the DDR Processor code. In some embodiments, the secure environment also ensures that the data path from the DDR Processor to the antenna is isolated from firmware outside the secure environment. That is, no firmware outside the secure environment has the ability to affect the accurate gathering of statistics by the DDR Processor. In some embodiments, the secure environment further ensures that there is no ability for code other than the DDR Processor to access sensitive crypto storage, such as keys. For example, this can include shielding sensitive storage from debug monitors and/or other monitoring/access activities or techniques. As would also be apparent to one of ordinary skill in the art, MPU firmware, not

just the DDR Processor, must be secured and not include bugs or vulnerabilities that can be exploited to allow for unauthorized access. For example, a common attack is buffer overflow, in which an attacker chooses inputs that cause an unchecked buffer to exceed its bounds, resulting in unintended behavior that the attacker can exploit.

[00129] Examples of secure execution environment (SEE) implementations in the MPU embodiments include the examples similarly discussed above for various secure execution environment (SEE) implementations in the APU embodiments.

[00130] **Embedded DDR Processor Implementation on an Application Processor Combined with a Data Path Security Verifier on a Modem Processor**

[00131] In some embodiments, the DDR Processor is embedded in a SEE APU chipset, and a Data Path Security Verifier (DPSV) is embedded in the MPU chipset, such as shown in device architecture 103 of Figure 1. For example, the DPSV can use cryptographic techniques to achieve a secure and trusted data path between the secure DDR Processor and the modem network antenna connection. This prevents a data connection between fraudulent software or firmware and the network without the need to secure the modem bus, the physical modem bus, and the modem data path elements above the DPSV element. By establishing a secure communication channel between the DDR Processor and the DPSV, a secure channel binding is created so that only network data path flows that are securely processed by the DDR Processor can reach the 3G or 4G modem connection to the wireless access network even if fraudulent software or firmware circumvents the DDR Processor by successfully gaining access to the modem bus interface. In the event that fraudulent software or firmware circumvents the DDR Processor and communicates intended unsecured data path information with the modem, the DPSV blocks the network data paths that are not processed and cryptographically secured by the DDR Processor.

[00132] **Figure 8** illustrates an architecture for a secure embedded DDR Processor in an APU and a Data Path Security Verifier (DPSV) in an MPU implementation in accordance with some embodiments. In particular, as shown in Figure 8, the DDR Processor 114 is embedded into the APU chipset SEE, and a second companion firmware image referred to herein as the

Data Path Security Verifier (DPSV) 836 is embedded into the MPU chipset SEE (e.g., a 3G or 4G MPU chipset SEE). As also shown, to ensure that fraudulent software or firmware cannot circumvent the DDR Processor, there are two zones of data path security, one encompassing only the DDR Processor and the second one that includes the DPSV along with the modem data path processing and the modem signal processing that occurs between the DDR and the antenna (e.g., this second zone of data path security is similar to that of a modem-only implementation of the DDR Processor).

[00133] As mentioned above, this approach does not require securing the APU 3G or 4G modem bus driver and physical bus. For example, some vendors and/or chipset suppliers (e.g., AWSP APU chipset suppliers) may consider it easier to create two firmware images and two zones of data path security rather than securing the data path between the DDR Processor SEE and the modem antenna connection. As compared to the APU implementation based approach, the firmware for the APU is somewhat simplified and the security design work involved with securing the modem bus driver and physical bus can be eliminated. As compared to MPU implementation based approach, the modem firmware is also simplified. For example, in some APU chipset architectures, it may be difficult to secure the data path from the DDR Processor through the modem bus driver, the modem physical bus, and the modem itself. Also, in some MPU chipsets, as similarly discussed above, there may be a need to simplify or reduce the size of the secure firmware program image required on the MPU. Simpler and smaller firmware can reduce the frequency of required updates or perhaps eliminate them altogether. The APU DDR Processor and MPU DPSV implementation approach described herein reduces the firmware required on the MPU down to the DPSV. This allows more complex data path processing by the DDR Processor to be implemented on the APU, in which (i) secure firmware execution memory is typically larger and CPU performance is typically higher, and (ii) the firmware update system is typically more capable and more flexible. However, there are also drawbacks with the APU DDR Processor and MPU DPSV implementation approach. The primary drawback is that firmware generally must be embedded in both the wireless network chipset (MPU) and the device Application Processor (APU) chipset.

[00134] As shown in Figure 8, a first SEE 810 is implemented on the APU chipset, which includes the DDR Processor 114 for securely monitoring communications from APU stack driver for 2G/3G/4G modem 806, using OS stack data path interface and/or modem data path interface

818 as similarly described herein. A second SEE 832 is implemented on the MPU chipset, which includes the Data Path Security Verification (DPSV) program 836. The DPSV 836 sits on the data path for the modem as shown. For example, the DPSV function can be quite simple: the DPSV 836 only passes data path information that is processed and acknowledged by the DDR Processor 114. The DPSV 836 is bound to the DDR Processor 114 so that it knows the secret session key of the DDR processor data path and can receive acknowledgements from the DDR Processor 114. Various techniques for how the DDR Processor 114 binds a secure data path channel to the DPSV 836, and how the DPSV 836 ensures that all 3G or 4G modem network service usage is being properly monitored and processed, is provided herein.

[00135] Referring to APU SEE 810, a program signature verifier 820, nonvolatile memory I/O 822, and secure execution boot loader and updater 824 as similarly described herein with respect to various embodiments. The APU SEE 810 also includes a DDR secure execution memory 812. The DDR secure execution memory 812 includes the DDR processor 114 for monitoring the data path through OS stack data path interface 816 and modem data path interface 818 for data path communications via modem bus driver 826 to modem bus 818 as shown. The DDR secure execution memory 812 also includes a DDR processor mailbox interface for providing DDR mailbox data 810 from DDR processor 114 to service processor application program 112 as shown and as similarly described herein. Similarly, the DPSV 836 uses the DPSV mailbox interface 842 as a communication channel to authenticate the DDR processor 114 and establish a secret session key to be used for message integrity check between the two. Various techniques for implementing the security binding between DDR Processor 114 and DPSV 836 are described herein.

[00136] In some embodiments, the DDR Processor executes in a secure environment in the APU based embodiments, as similarly described above with respect to the APU based embodiments. In some embodiments, the secure environment ensures no unauthorized ability to replace or modify the DDR Processor code. In some embodiments, the secure environment further ensures that there is no ability for code other than the DDR Processor to access sensitive crypto storage, such as keys. For example, this can include shielding sensitive storage from debug monitors and/or other monitoring/access activities or techniques. As would also be apparent to one of ordinary skill in the art, APU firmware, not just the DDR Processor, must be secured and not include bugs or vulnerabilities that can be exploited to allow for unauthorized

access. For example, a common attack is buffer overflow, in which an attacker chooses inputs that cause an unchecked buffer to exceed its bounds, resulting in unintended behavior that the attacker can exploit.

[00137] Similarly, in some embodiments, the DPSV executes in a secure environment. In some embodiments, the secure environment ensures no unauthorized ability to replace or modify the DPSV code. In some embodiments, the secure environment further ensures that there is no ability for code other than the DPSV to access sensitive crypto storage, such as keys. In some embodiments, the secure environment further ensures that there is no ability for any code to interfere with the proper crypto functions of the DPSV or communications between the DPSV and the DDR Processor. For example, this can include shielding sensitive storage from debug monitors and/or other monitoring/access activities or techniques. As would also be apparent to one of ordinary skill in the art, MPU firmware, not just the DPSV, must be secured and not include bugs or vulnerabilities that can be exploited to allow for unauthorized access. For example, a common attack is buffer overflow, in which an attacker chooses inputs that cause an unchecked buffer to exceed its bounds, resulting in unintended behavior that the attacker can exploit.

[00138] In some embodiments, the APU includes a Data Path Processor (DPP) that includes the DDR Processor function, which is secured in an APU SEE as described herein. In some embodiments, the APU DPP also includes other service monitoring, control, and notification functions. In some embodiments, the modem includes a Data Path Security Verifier (DPSV) that secures the path between the APU DPP and the modem network data path so that only the DPP can transmit over the modem even if other software, firmware, buses, or ports have access to the modem. In some embodiments, the modem DPSV is bound to the APU DPP by one or more of the techniques described herein and/or similar or other techniques as would be apparent to one of ordinary skill in the art in view of the various embodiments described herein. For example, the APU DPP can be provided in a secured data path to the modem network connection that cannot be circumvented by software, firmware, buses, or ports on the device. This can be a hardwired data path via hardware design or a data path secured with a secure firmware or software execution environment for all the data path elements below the APU DPP. The APU DPP and modem exchange public keys and/or digital certificates and then execute a

key exchange process to authenticate each other which results in a secret shared session key to be used as the basis for message integrity checking.

[00139] Once the secret shared session key is established between APU DPP and DSPV, the APU DPP uses the session key to append an integrity check on each frame to be transmitted, and the modem uses the session key to validate the integrity check. The modem only allows frames that have a valid integrity check to be transmitted, and it blocks frames that do not include a valid integrity check, meaning that only frames that were processed by the APU DPP get transmitted. Similarly, the modem DSPV uses the session key to append an integrity check to each received frame, and the APU DPP uses the session to validate the integrity check before it is sent to the higher layer (e.g., application layer, etc.).

[00140] In some embodiments, modem downstream data path messages between DSPV and DPP are sequenced. In some embodiments, APU DPP upstream messages include downstream sequence information so that modem DSPV can confirm that APU DPP is receiving all downstream packets, and if not, then the modem DSPV can inform the APU DPP, inform the Service Controller, and/or take action such as restricting access and/or other appropriate actions.

[00141] In some embodiments, the APU DPP generates secure DDRs and communicates the secure DDRs to the Service Controller in a sequenced and secure manner as described herein with respect to various embodiments.

[00142] In some embodiments, the Service Processor application and/or Service Processor kernel program informs the APU DPP as to which sockets/flows belong to which applications (e.g., can be or should be associated with which applications for application based service usage monitoring, billing, and/or control) so that the APU DPP knows which application is generating or receiving traffic in order to assist in application classification tag for charging, traffic control, and/or user notification policies.

[00143] In some embodiments, the APU DPP performs a variety of functions. In some embodiments, the APU DPP can perform DDR Processor functions. The APU DPP can perform any or all of the service monitoring functions of the Charging Agent (CA) and/or Policy Decision Agent (PDA). The APU DPP can count all network traffic, and in some examples, classifying traffic by application and/or destination, NBS, time of day, active network, and/or

various other criteria as described herein. The APU DPP can generate charging records. The APU DPP can communicate charging records to the Service Controller (e.g., or another network charging function) and/or device notification UI.

[00144] In some embodiments, the APU DPP performs access controller functions. For example, the APU DPP can instruct the service processor application and/or kernel program to either allow or block/kill or background an application or destination. The service processor application and/or kernel program can either allow/block or background an application by manipulating the application access to the network or by intercepting the application program boot/start sequence, or from suspending/resuming the application. The service processor application and/or kernel program can perform the intercept functions by reprogramming or intercepting application management functions in the OS (e.g., such as the Android activity manager and/or the service manager functions). The APU DPP either instructs service processor application/kernel program to control application and/or traffic, or controls traffic directly in the DPP. The APU DPP can perform policy enforcement functions as described herein with respect to various embodiments.

[00145] In some embodiments, the APU DPP can perform NBS monitor functions and/or reporting functions. For example, the APU DPP can detect NBS, modem performance parameters, network assets involved in link, and/or geo-location information.

[00146] In some embodiments, the APU DPP obtains network time from network with “secure” ping-loop system to verify that network time stamp is not intercepted and delayed. For example, the APU DPP can either have a local reliable clock or can perform a ping-loop each time a report is started and/or stopped.

[00147] Examples of secure execution environment (SEE) implementations in the APU DDR Processor and MPU DPSV embodiments include the examples similarly discussed above for various secure execution environment (SEE) implementations in the APU embodiments. Specific examples are also listed below. Example commercially available APUs include the following: Intel Atom (e.g., Z5xx, Z6xx, D4xx, D5xx series) based solutions with Intel Trusted Execution Technology including TPM support; and ARM based solutions with ARM Trusted Zone Architecture. Example APU specification requirements can also include: common hardware security blocks (e.g., AES, DES, RSA, Diffie-Hellman, SHA, and a random generator).

Example commercially available MPUs include the following: EVDO chipset based solutions (e.g., ARM 11-based CPU architecture, including ARM Trusted Zone Architecture with many common hardware crypto blocks); HSPA chipset based solutions (e.g., Snapdragon/ARM based CPU architecture, including ARM Trusted Zone Architecture with many common hardware crypto blocks); and LTE chipset based solutions (e.g., Snapdragon/ARM based CPU architecture, including ARM Trusted Zone Architecture with many common hardware crypto blocks).

[00148] **Figure 9** illustrates an architecture for a secure embedded DDR Processor in a Subscriber Identity Module (SIM) and a Data Path Security Verifier (DPSV) in an MPU implementation in accordance with some embodiments. In particular, as shown in Figure 9, the DDR Processor 114 is embedded a SIM SEE 918, and the Data Path Security Verifier (DPSV) 936 is embedded into the MPU chipset SEE 932 (e.g., a 3G or 4G MPU chipset SEE). Data communications from the APU, such as those similarly described herein including the mailbox function, communicate using the SIM bus driver 911 using modem and SIM bus 912 as shown.

[00149] As shown in Figure 9, a first SEE 918 is implemented in a SIM 913, which includes the DDR Processor 114 for securely monitoring communications from modem and SIM bus 912 to SIM bus driver 916, using OS stack data path interface 924 and/or modem data path interface 926 as similarly described herein. A mailbox function is similarly provided as described herein using DDR processor mailbox interface 922, DDR mailbox data 914, and DDR mailbox data 910 as shown.

[00150] As also shown in Figure 9, data path communications via modem and SIM bus 913 to 3G/4G modem bus driver 934 to 3G/4G modem data path and signal processing elements 938 are monitored using modem SIM data security verifier 936 as described herein. The modem SIM data security verifier 936 is implemented in a modem chipset SEE 932 of the modem chipset/MPU 930 as shown. Additionally, there is a DPSV mailbox 842 that provides the communication channel to APU which the final destination to be DDR processor within the SIM for authentication and establishment of secret session key to be used as the basis for message integrity checking.

[00151] In some embodiments, the SIM includes a Data Path Processor (DPP) that embeds the DDR function, which is secured in the SIM SEE. For example, the SIM DPP can also

include other service monitoring, control, and notification functions. In some embodiments, the modem includes a Data Path Security Verifier (DPSV) that secures the path between the SIM DPP and the modem network data path so that only the DPP can transmit over the modem even if other software, firmware, buses, or ports have access to the modem.

[00152] In some embodiments, the modem DPSV is bound to the SIM DPP by one of the following techniques and/or similar or other techniques as would be apparent to one of ordinary skill in the art in view of the various embodiments described herein.

[00153] For example, the SIM DPP can be provided in a secured data path to the modem network connection that cannot be circumvented by software, firmware, buses, or ports on the device. The secured data path can be a hardwired data path via hardware design or a data path secured with a secure firmware or software execution environment for all the data path elements below the SIM DPP.

In some embodiments, the communication between the DPSV 936 and DDR Processor 114 is secured using various secure communication techniques, such as those described herein. In some embodiments, the DPSV has a unique private/public key pair and a digital certificate (cert) that attests to the authenticity of its public key. The DDR Processor has a unique private/public key pair and a digital certificate (cert) that attests to the authenticity of its public key. The DPSV and the DDR Processor exchange public keys and certs, then execute a key exchange process that authenticates each other and results in a secret, shared session key. The DDR Processor receives upstream network data flows from the device OS networking stack and, using the session key, it appends an integrity check to each upstream data message that it sends to the DPSV. The DPSV blocks any upstream data path information that does not have a valid integrity check from the DDR Processor and informs the DDR Processor that it is receiving invalid upstream data so that the DDR Processor may inform the Service Controller of a possible fraud event. The DPSV receives downstream network data flows and, using the session key, it appends an integrity check to each downstream data message that it sends to the DDR Processor. Each downstream data message is, for example, sequenced so that data messages cannot be blocked or replayed without being detected by the DDR Processor. If the DDR Processor receives a downstream data message with an invalid integrity check, the DDR Processor rejects the message and informs the Service Controller of a possible fraud event. The DDR Processor acknowledges each non-rejected downstream data message in the next upstream data message it

sends to the DPSV. If the DPSV stops receiving downstream data message acknowledgements, it blocks downstream network data flows and informs the DDR Processor so that the DDR Processor may inform the Service Controller of a possible fraud event. The DDR Processor securely sends DDR reports to the Service Controller by way of the Service Processor as described herein with respect to various embodiments.

[00154] In some embodiments, the modem downstream data path messages between the DPSV and DPP are sequenced. In some embodiments, the SIM DPP upstream messages include downstream sequence information so that modem DPSV can confirm that the SIM DPP is receiving all downstream packets and, if not, then modem DPSV can inform the SIM DPP, inform the Service Controller, and/or take action such as restricting access or another appropriation action(s).

[00155] In some embodiments, the SIM DPP generates secure DDRs and communicates the secure DDRs to the Service Controller in a sequenced and secure manner as described herein with respect to various embodiments.

[00156] In some embodiments, the Service Processor application and/or Service Processor kernel program informs the SIM DPP which sockets/flows belong to which applications so that the SIM DPP knows which application is generating or receiving traffic in order to assist in application classification tag for charging, traffic control, and notification policy.

[00157] In some embodiments, the SIM DPP performs a variety of functions, as described herein. For example, the SIM DPP can perform the DDR Processor functions. The SIM DPP can perform any or all of the service monitoring functions of the Charging Agent (CA) and/or Policy Decision Agent (PDA). The SIM DPP counts all traffic with the network, and in some cases, also classifies the traffic by application and/or destination, NBS, time of day (TOD), active network, and/or various other criteria. The SIM DPP can generate charging records. The SIM DPP can communicate charging records to the Service Controller (e.g., or another network charging function) and/or device notification UI.

[00158] As another example, the SIM DPP can perform various access controller functions. The SIM DPP can instruct the Service Processor application and/or kernel program to either allow, block/kill, or background an application or destination. The Service Processor

application and/or kernel program can allow, block/kill, or background an application by manipulating the application access to the network or by intercepting the application program boot/start sequence, or from suspending/resuming the application. The Service Processor application and/or kernel program can perform the intercept functions by reprogramming or intercepting application management functions in the OS (e.g., such as the Android activity manager and/or the service manager functions). As an example, the SIM DPP can either instruct the Service Processor application and/or kernel program to control the application and/or traffic, or controls traffic directly in the DPP. The SIM DPP can also perform policy enforcement functions as described herein.

[00159] As yet another example, the SIM DPP can perform NBS monitoring and/or reporting functions. The SIM DPP can detect NBS, modem performance parameters, network assets involved in link, and geo-location.

[00160] As yet a further example, SIM DPP can obtain a network time from network with “secure” ping-loop system to verify that network time stamp is not intercepted and delayed. For example, the SIM DPP can either have local reliable clock or can perform ping-loop each time a report is started and/or stopped.

[00161] **Figure 10** illustrates another architecture for a secure embedded DDR Processor in a Subscriber Identity Module (SIM) and a Data Path Security Verifier (DPSV) in an MPU implementation in accordance with some embodiments. In some applications it may be desirable to locate the DDR Processor on a standalone chipset that attaches to the APU or MPU chipset, such as a SIM card. Figure 10 illustrates such an implementation in accordance with some embodiments. For example, an embedded DDR Processor can be implemented on a smart phone APU chipset combined with a Data Path Security Verifier (DPSV) implemented on a 3G or 4G wireless modem chipset.

[00162] In some embodiments, a hardware or firmware secure data path between the DDR Processor and the modem DPSV is not required, such as shown in Figure 10, in which the DDR Processor is implemented on the SIM card (e.g., or another standalone security chipset) by providing a data path logical channel forwarding function on the APU and providing a mailbox data communication function between the Service Controller and the DDR Processor to connect over a SIM data bus. In addition, the DDR Processor reports to the Service Controller can be

secured with none of the system elements on the APU being secured in a hardware assisted secured execution environment (SEE).

[00163] Referring to Figure 10, the secure DDR Processor 114 is located in DDR Secure Execution Memory 1042 of SIM Secure Execution Environment 1040 on the SIM as shown, as similarly described above with respect to Figure 9. The architecture of the APU is similar to that shown in and discussed above with respect to Figure 9, except that an APU SIM to modem bus forwarding function 1012 and an APU bus driver function 1014 are added to the APU in the APU Chipset Kernel Programs 1004 as shown in Figure 10. A secure DPSV 1026 is located in modem chipset SEE 1024 of the modem for monitoring communications from 3G/4G modem bus driver using 3G/4G modem data path and signal processing elements 1028 as similarly described above with respect to Figure 9. However, in Figure 10 in comparison with Figure 9, the MPU and SIM are separate hardware or chipsets that communicate with the APU via independent communication buses. In particular, the MPU communicates with the APU via modem bus 1018 using 3G/4G modem bus driver 1022 to APU modem bus driver 1014 and APU SIM to modem bus forwarding function 1012 as shown. The SIM communicates with the APU via SIM bus 1016 using SIM bus driver 1032 to SIM bus driver 1010 as shown. Also, the DPSV uses DPSV mailbox 842 as the communication channel to authenticate the DDR processor 114 in the SIM where the connection is established within the APU. As shown the APU has two communication channels; a first communication channel with the DDR processor and a second communication channel with the DPSV.

[00164] In some embodiments, a first logical communication channel is created over the SIM bus 1016 between the Service Processor DDR mailbox 910 on the APU and the DDR mailbox 1034 on the SIM, and this supports the communication between the Service Processor (e.g., Service Processor application program 112 and/or Service Processor kernel program 113) and the DDR Processor 114 using DDR processor mailbox interface 1044 to DDR mailbox data 1034 to SIM bus driver 1032 as shown. A second logical data channel is created over the SIM bus 1016 between the OS networking stack and the DDR Processor 114, and this is the logical channel intended for all OS networking stack communications with the 3G or 4G network using OS stack data path interface 1046 to SIM bus driver 1032 as also shown. A third logical communication channel is created between the SIM DDR Processor 114 and the modem DPSV 1026. This third logical communication channel is formed by forwarding data between the SIM

bus interface (e.g., modem data path interface 1048 to SIM bus driver 1032) located on the SIM, the SIM bus driver 1010 located on the APU, the SIM to modem bus forwarding function 1012 located on the APU, the modem bus driver 1014 located on the APU, and the modem bus interface 1022 located on the modem as also shown.

[00165] In some embodiments, the communication between the DPSV 1026 and DDR Processor 114 is secured using various secure communication techniques, such as those described herein. In some embodiments, the DPSV has a unique private/public key pair and a digital certificate (cert) that attests to the authenticity of its public key. The DDR Processor has a unique private/public key pair and a digital certificate (cert) that attests to the authenticity of its public key. The DPSV and the DDR Processor exchange public keys and certs, then execute a key exchange process that authenticates each other and results in a secret, shared session key. The DDR Processor receives upstream network data flows from the device OS networking stack and, using the session key, it appends an integrity check to each upstream data message that it sends to the DPSV. The DPSV blocks any upstream data path information that does not have a valid integrity check from the DDR Processor and informs the DDR Processor that it is receiving invalid upstream data so that the DDR Processor may inform the Service Controller of a possible fraud event. The DPSV receives downstream network data flows and, using the session key, it appends an integrity check to each downstream data message that it sends to the DDR Processor. Each downstream data message is, for example, sequenced so that data messages cannot be blocked or replayed without being detected by the DDR Processor. If the DDR Processor receives a downstream data message with an invalid integrity check, the DDR Processor rejects the message and informs the Service Controller of a possible fraud event. The DDR Processor acknowledges each non-rejected downstream data message in the next upstream data message it sends to the DPSV. If the DPSV stops receiving downstream data message acknowledgements, it blocks downstream network data flows and informs the DDR Processor so that the DDR Processor may inform the Service Controller of a possible fraud event. The DDR Processor securely sends DDR reports to the Service Controller by way of the Service Processor as described herein with respect to various embodiments.

[00166] In some embodiments, the DDRs transmitted from the DDR Processor to the Service Controller are integrity checked and sequenced in a manner that cannot be tampered with or replayed. An authentication process between the DDR Processor and the Service Controller

combined with a set of unique DDR report sequence identifiers and authentication session keep-alive timers are used to maintain and confirm the secure connection between the DDR Processor and the Service Controller. If the secure session or the flow of DDR records between the DDR Processor and the Service Controller are interrupted, then the access control function in the DDR Processor restricts access of the 3G or 4G modem data path to the network destinations necessary to reestablish a securely authenticated session with between the DDR and the Service Controller.

[00167] **Figure 11** illustrates another architecture for a secure embedded DDR Processor in a Subscriber Identity Module (SIM) and a Data Path Security Verifier (DPSV) in an MPU implementation in accordance with some embodiments. Figure 11 is similar to Figure 9 except that as shown a SIM data path interface 1110 is provided for direct communication from the SIM with 3G or 4G modem bus driver 934 on the MPU. SIM communications, such as those similarly described herein to the APU including the mailbox function, communicate using the SIM data path interface 1110 to the 3G or 4G modem bus driver 934 using modem bus 1112 to communicate with the APU via modem bus driver 911 and the APU stack interface for 3G or 4G modem 906 as shown.

[00168] In some embodiments, various other architectures including various other locations of the DDR Processor can be provided using these or similar techniques as will now be apparent to one of ordinary skill in the art in view of the embodiments described herein.

[00169] In some embodiments, various other architectures including various other locations of the DDR Processor and/or DPSV can be provided using these or similar techniques as will now be apparent to one of ordinary skill in the art in view of the embodiments described herein.

[00170] For example, the DDR Processor (e.g., and/or various secured elements of the Service Processor) can be located in various other locations (e.g., in various secure operating environments) that involve network access policy enforcement at higher levels in the network stack. In particular, certain functions performed by the Service Processor without hardware security can be located in hardware secured execution memory. Such functions can include 3G and 4G network data path processing and usage report functions, 3G and 4G network application

access management and usage reporting functions, and 3G and 4G service user notification and customer activity status functions.

[00171] In some embodiments, using advanced secure CPU partitioning technology, large portions or the entire Service Processor functionality is implemented in hardware secured execution environments in the APU or MPU. For example, Service Processor functions that can be executed within a hardware secured execution environment include 3G and 4G network application access management and traffic processing that is more sophisticated, such as (i) a secure application manager that differentially manages 3G and 4G application access according to network access policy set by the Service Controller and network busy state determined on the device, and (ii) 3G and 4G network traffic that is classified and processed according to application ID, layer 7 destination as well as layer 3/4 destination and network busy state. Securing such Service Processor functions may be desirable provided that: (i) the same level of security from hacking and malware that is available in the lower levels of stack processing can be achieved, (ii) the data path between the DDR Processor (e.g., and/or elements of the Service Processor) and the modem antenna connection can be secured from circumvention or tampering by device malware, and (iii) there are sufficient memory and CPU cycles to execute the more sophisticated data path processing functions.

[00172] Additional embodiments are now provided for various aspects of DDR Processor functional operations.

[00173] **DDR Firmware Installation, Security Credential Configuration, and Update**

[00174] **Figure 12** illustrates a secure boot sequence flow diagram in accordance with some embodiments. In some embodiments, upon a reset and/or power up at 1202, the system (e.g., APU, SIM, and/or MPU, whichever the DDR is embedded on in the wireless communication device) starts by executing a secure boot (e.g., executing secure boot code) at 1204. As part of the secure boot, an initialization routine is performed to configure system parameters (e.g., configures registers to ensure secure region, such as HW/firmware firewall memory) to establish the secure/normal region boundary and interfaces. The secure boot code also has access to the root of trust, which is hidden to all other firmware/software. At 1206, a public keys certificate validation step is performed in which the secure boot downloads and verifies its own public key (e.g., using a hashing technique) and then downloads public keys of

all secure codes at 1206. At 1208, the secure boot proceeds to download and verify/validate digital signatures of every secure software package (e.g., including the DDR Processor including a DDR generator) before allowing normal software routines to be downloaded. For example, this can be performed using a chain of trust built on the root of trust. At 1210, the secure boot determines if all signatures are properly validated. If any digital signature fails, then the secure boot stays looped in the idle state as shown at 1212 until it gets reset as shown at 1202 (e.g., watch dog timer expires) and/or the platform is flashed with a new image. If all of the digital signatures are properly validated, then the secure boot proceeds with other downloads (e.g., including applications) at 1214. Normal operation proceeds and the secure boot is completed at 1216. At 1218, whether there is a new image is determined. If not, then normal operation continues at 1216. When new secure software image is downloaded (e.g., the image is stored in new area of the flash memory with a “secure” flag set), and the system can return to reset state to have the secure boot reading the new image (e.g., based on the flag) and validate the digital signature of the image before it becomes the current image.

[00175] Mailbox Communication Channel Between the Service Processor and DDR Processor

[00176] **Figure 13** illustrates a functional diagram for passing DDR Service Processor mailbox messages between secure and unsecure memory regions in accordance with some embodiments. In some embodiments, a logical communication channel between the DDR Processor 1314 and the Service Processor 1312 is provided in order to send secure DDR messages (e.g., DDR message bundles) to the Service Controller (e.g., via the Service Processor’s communication agent). In some embodiments, this logical communication channel is referred to in various embodiments described herein as the DDR Mailbox Data functional element/block. For example, for ease of implementation, it can be assumed that the DDR processor does not have an IP address of its own hence can only send its message to the Service Controller through the Service Processor using this logical channel. The logical channel can be based on shared memory (e.g., normal region) architecture, shown as normal region shared memory 1310. As described herein with respect to various embodiments, the DDR messages are encrypted and can only be decrypted by the Service Controller. This logical channel can also be used for Service Controller to send down new DDR software updates.

[00177] In some embodiments, in which the DDR Processor is located in the APU, then the shared memory can be accessed via both Service Processor and DDR Processor using the APU's direct memory access (DMA) engines.

[00178] In some embodiments, in which the DDR Processor is located in the MPU, then a modem interface is provided to support an additional logical channel (e.g., USB endpoint for 2G/3G/4G) to satisfy this requirement. In some embodiments, the logical channel is piggybacked on top of an existing configuration and status channel that provides the control channel between the APU and the MPU.

[00179] **DDR Processor Record Generator**

[00180] In some embodiments, a DDR report spans a measurement period. Measurement periods are generally contiguous, meaning the next period begins immediately after the current period ends, with no traffic falling between periods. At the start of a period, all prior DDRs are deleted. During the period, the table of DDRs grows, since each observed IP flow creates an entry in the table. The period ends when either DDR storage exceeds a predefined threshold, or when a DDR report is requested by the Service Processor. DDR data not yet sent to the Service Processor application remains in memory across power cycles and battery pulls.

[00181] In some embodiments, at the end of the measurement period, the DDR report is prepared by the DDR Processor and sent to the Service Processor. For example, various secure communication and/or crypto techniques can be used to ensure that the contents of the report are kept private, and to ensure that any tampering with the DDR report will be detected by the Service Controller.

[00182] In some embodiments, the report also includes time stamps that identify the start and end of the measurement period. Timestamps are calibrated and confirmed via a periodic handshake with the Service Controller to ensure that the DDR Processor time base has not been altered. Data compression is used to minimize the size of the report.

[00183] In some embodiments, each DDR report message includes a unique sequence identifier that allows the Service Controller to determine if any DDRs have been blocked from the sequence. The report is stored by the Service Processor for subsequent forwarding to the

Service Controller. Data stored by the Service Processor remains in memory across power cycles and battery pulls.

[00184] In some embodiments, the DDR processor resides in the modem where the secure DDR usage report is then sent to the Service Processor (e.g., communication agent within the Service Processor) to be sent to the Service Controller.

[00185] **DDR Processor Access Controller**

[00186] **Figure 14** illustrates a flow diagram for a DDR Processor Service Controller session authentication and verification in accordance with some embodiments. In some embodiments, the DDR Processor includes an access controller function (e.g., Access Controller). In some embodiments, upon reset and/or powering up a DDR Processor access control function, such as the Access Controller, restricts network access (e.g., to only a few pre-configured IP addresses and/or host names including certain carrier/wireless service provider services).

[00187] In some embodiments, the Access Controller ensures that the Service Processor correctly delivers DDRs to the Service Controller. If the DDR flow is blocked or tampered with, then the Access Controller blocks cellular (e.g., or managed WiFi) wireless network access until the proper flow of DDRs is restored. In some embodiments, the network access restriction is only applied to networks that have network access services maintained and managed by the network operator. For example, this function can be disabled for WiFi access that is not managed by the network operator.

[00188] In some embodiments, once a modem is authenticated (e.g., via a PPP session) via AAA, either after initial power up and/or after restoring from power save, the Access Controller restricts limited network access (e.g., based on set of IP addresses/host names and/or other criteria) until it gets feedback from the Service Controller to allow open access. Also, while traffic is running and the DDR Processor sending DDR records/reports, it continually expects to receive secure DDR ACK frames to allow open access, otherwise it enters a restrict access state again.

[00189] Referring now to Figure 14, at reset and/or initial power up or power up after a power save mode, the process begins, as shown at 1402. At 1404, the Access Controller restricts

network access to limited streams (e.g., preconfigured or configured within the secure region. At 1406, the Access Controller waits for feedback from the Service Controller to open network access. At 1408, whether the feedback is received from the Service Controller is determined. If not, then the process returns to 1406 to continue to wait for feedback from the Service Controller. If the feedback is received (e.g., and the secured Service Controller feedback is properly verified and/or validated, as described herein), then the Access Controller opens network access and DDR reports begin to be sent at 1410. At 1412, whether a DDR ACK frame is received in response to such DDR report(s) is determined. If not, then the process returns to 1404 and network access is restricted. If the DDR ACK frame is received (e.g., and the secured DDR ACK frame is properly verified and/or validated, as described herein), then the Access Controller continues to maintain open network access and to send DDR reports at 1414.

[00190] DDR Processor Network Busy State (NBS) Monitor

[00191] In some embodiments, the Network Busy State (NBS) Monitor is a secure firmware program element in the DDR Processor that monitors, records, and/or securely reports information on network busy state (e.g., or network congestion state) to the Service Controller for storage, network congestion analysis, and/or service charging and control policy security purposes. For example, the NBS Monitor can perform one or more of the following functions within the SEE: log active network information (e.g., active network type, home/roaming, current carrier, base station, and/or base station sector); monitor network access attempts and successes; monitor network speed; monitors round trip delay; monitor packet error rate; monitor modem performance parameters (e.g., RF channel, RF signal strength and variability, SNR, raw modem bit rate, raw modem bit error rate, and/or channel bandwidth); implements algorithm to classify busy state of network; and report network busy state history within DDRs.

[00192] Binding and Securing the Secure Communication Channel Between the DDR Processor and the Service Controller

[00193] In some embodiments, binding and securing the secure communication channel between the DDR Processor and the Service Controller is provided as described below. The DDR Processor has a unique private/public key pair and a digital certificate (cert) that attests to the authenticity of its public key. The Service Controller has a unique private/public key pair. Its public key is well known and included in the DDR Processor code image. The DDR

Processor sends its public key and cert to the Service Controller, and the two execute a key exchange process that authenticates each other and results in a secret, shared session key. The DDR Processor uses the session key to encrypt DDR reports it sends to the Service Controller and to append an integrity check to messages it sends to the Service Controller. The Service Controller uses the session key to append an integrity check to messages it sends to the DDR Processor.

[00194] As will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein, various other secure communication and crypto techniques can be used to provide for binding and securing the secure communication between the DDR Processor and the Service Controller.

[00195] **Binding and Securing the Secure Communication Channel Between the DDR Processor and the DPSV In An APU/MPU Implementation**

[00196] In some embodiments, binding and securing the secure communication channel between the DDR Processor and the DPSV in an APU/MPU implementation is provided as described below. The DPSV has a unique private/public key pair and a digital certificate (cert) that attests to the authenticity of its public key. The DDR processor has a unique private/public key pair and a digital certificate (cert) that attests to the authenticity of its public key. The DPSV and the DDR Processor exchange public keys and certs, then execute a key exchange process that authenticates each other and results in a secret, shared session key. The DDR Processor receives upstream network data flows from the device OS networking stack and, using the session key, it appends an integrity check to each upstream data message that it sends to the DPSV. The DPSV blocks any upstream data path information that does not have a valid integrity check from the DDR Processor and informs the DDR Processor that it is receiving invalid upstream data so that the DDR Processor may inform the Service Controller of a possible fraud event. The DPSV receives downstream network data flows and, using the session key, it appends an integrity check to each downstream data message that it sends to the DDR Processor. Each downstream data message is sequenced so that data messages cannot be blocked or replayed without being detected by the DDR Processor. If the DDR Processor receives a downstream data message with an invalid integrity check, the DDR Processor rejects the message and informs the Service Controller of a possible fraud event. The DDR Processor acknowledges each non-rejected downstream data message in the next upstream data message it

sends to the DPSV. If the DPSV stops receiving downstream data message acknowledgements, it blocks downstream network data flows and informs the DDR Processor so that the DDR Processor may inform the Service Controller of a possible fraud event. The DDR Processor securely sends DDR reports to the Service Controller by way of the Service Processor as described herein. The DDRs transmitted from the DDR Processor to the Service Controller are integrity checked and sequenced in a manner that cannot be tampered with or replayed. An authentication process between the DDR Processor and the Service Controller combined with a set of unique DDR report sequence identifiers and authentication session keep alive timers are used to maintain and confirm the secure connection between the DDR Processor and the Service Controller. If the secure session or the flow of DDR records between the DDR Processor and the Service Controller are interrupted, then the Access Controller function in the DDR Processor restricts access of the 2G, 3G, or 4G modem data path to the network destinations necessary to reestablish a securely authenticated session with between the DDR and the Service Controller.

[00197] As will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein, various other secure communication and crypto techniques can be used to provide for binding and securing the secure communication channel between the DDR Processor and the DPSV in an APU/MPU implementation.

[00198] Security Requirements for OEM Programming of DDR Processor

[00199] In some embodiments, code signing for the DDR Processor is provided. In particular, the DDR Processor code image is digitally signed by the device OEM. The signature is verified by the Secure Boot Loader using a fixed public key embedded within the Secure Boot Loader code image. This imposes the security requirement that the OEM operate a secure code-signing facility that preserves the secrecy of the fixed signing key. The OEM ensures that only authorized personnel are able to access the code-signing facility and that they do so only for legitimate DDR Processor images.

[00200] In some embodiments, a random seed for the DDR device private key is provided. In particular, at the time of device manufacture, a private/public key pair called the DDR Device Key is assigned. The DDR Device Key is unique to each device and is used to establish a secure communications link to the Service Controller. For example, the DDR Device Key can be a Diffie-Hellman key pair with a 1024-bit modulus, 1024-bit base, and a 128-bit private exponent.

The private exponent of the DDR Device Key (DDR Device Private Key) is unique to each device and stored in, for example, 128 bits of on-chip nonvolatile memory (e.g., OTP memory) in the SEE. The modulus and base are common to all devices and are embedded within the DDR Processor image. The public portion of the DDR Device Key (e.g., DDR Device Public Key) is not permanently stored; instead, it is calculated by the DDR Processor using the modulus, base, and private exponent. The DDR Processor includes a factory initialization routine that is executed while the device is being initialized and tested at the factory. The factory initialization routine generates the DDR Device Private Key and programs it into the nonvolatile memory of the SEE. The DDR Device Private Key never leaves the device and is accessible only to the DDR Processor. The factory initialization routine computes the DDR Device Public Key and exports it to the factory tester. For example, the factory tester can provide a 128-bit random string to be used by the factory initialization routine as a seed to generate the DDR Device Private Key. This requires that the factory tester include or have access to a high-quality random bit source. Various suitable methods can be used, such as FIPS 140-2 (“deterministic random number generators”) seeded with the output of a hardware random source.

[00201] In some embodiments, at the time of device manufacture, a digital certificate called the DDR Device Cert is assigned to the device. The DDR Device Cert is unique to each device and is used to establish a secure communications link to the Service Controller. The contents of the DDR Device Cert include the DDR Device Public Key. The DDR Device Cert is signed by the issuing certificate authority, and the signature is verified by the Service Controller when establishing a secure link. The DDR Device Cert is not sensitive information and, for example, can be stored in either on-chip or off-chip nonvolatile memory. The OEM issues a DDR Device Cert for the DDR Device Public Key exported by the factory initialization routine, which imposes the security requirement that the OEM operates, or has access to, a certificate authority (CA). If the OEM chooses to access an outsourced CA, then the OEM’s primary obligation is to ensure that only authorized personnel are able to request certificates, and that they do so only for devices that have DDR Device Public Keys legitimately exported by the FI routine. If the OEM chooses to operate a CA, the OEM has the additional obligation of maintaining the security of the CA, specifically, preserving the secrecy of the CA’s fixed key that signs certificates.

[00202] As will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein, various other security techniques can be used or required for OEM programming for the DDR Processor.

[00203] **Figure 15** illustrates a flow diagram for secure device data records for implementing device assisted services (DAS) in accordance with some embodiments. At 1502, the process begins. At 1504, service usage of a wireless communication device with a wireless network is monitored (e.g., using DAS client based monitoring techniques, such as including the various techniques described herein for implementing secure DDRs). At 1506, secure device data records of the monitored service usage of the wireless communication device with the wireless network are generated. In some embodiments, each device data record is one of an ordered sequence of device data records with each sequential device data record providing an accounting of service usage over a service usage interval spanned by the device data record, and each device data record is associated with a secured unique sequence order identifier. At 1508, the device data records (DDR) are reconciled and verified using the various reconciliation and verification techniques described herein. For example, the DDRs can be verified using the unique sequence order identifier (e.g., and various other integrity checking based techniques, as described herein with respect to various embodiments). As another example, the DDRs can be reconciled with other service usage reports by comparison with service processor reports (e.g., layer -7 classification reports) and/or by comparison with network based service usage reports (e.g., network flow records, such as CDRs or IPDRs), as described herein with respect to various embodiments. At 1510, the process ends (e.g., and can repeat for continued service usage monitoring).

[00204] 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.

[00205] WHAT IS CLAIMED IS:

CLAIMS

1. A system, comprising:
a processor of a wireless communication device for wireless communication with a wireless network, wherein the processor is configured with a secure execution environment, and
5 wherein the secure execution environment is configured to:
monitor service usage of the wireless communication device with the wireless network; and
generate a plurality of device data records of the monitored service usage of the wireless communication device with the wireless network, wherein each device data
10 record is one of an ordered sequence of device data records with each sequential device data record providing an accounting of service usage over a service usage interval spanned by the device data record, and wherein each device data record is associated with a secured unique sequence order identifier; and
a memory coupled to the processor and configured to provide the processor with
15 instructions.
2. The system recited in claim 1, wherein the device data records include secure device data records for the monitored service usage system.
3. The system recited in claim 1, wherein the secure execution environment includes a secure software or firmware instruction execution environment.
20
4. The system recited in claim 1, wherein the sequence of device data records forms a contiguous and uninterrupted reporting of device service usage while the device is active on the network, including voice related service usage and data related service usage.
5. The system recited in claim 1, wherein the secure execution environment is located in an
25 application processor.
6. The system recited in claim 1, wherein the secure execution environment is located in a modem processor.
7. The system recited in claim 1, wherein the secure execution environment is located in a subscriber identity module (SIM).

8. The system recited in claim 1, wherein the unique sequence identifier includes one or more of: a sequence count, a time stamp, a start time indicator, a stop time indicator, a contiguous time interval identifier, an aggregate usage count at the beginning or end of a record, a reference time, and an elapsed time at the beginning or end of a record.

5 9. The system recited in claim 1, wherein a new device data record is generated based on one or more of the following: a predetermined time, an elapsed period of time, a device data record related request, a device data record related storage limit, device power on or power off event, a modem or device subsystem power on or power off event, a modem or device subsystem entering or exiting a power save state, a device or device subsystem authentication with a
10 network element or server, and a detected event triggered by one or more service usage activities or detection of a service usage record tampering or fraud event.

10. The system recited in claim 1, wherein the secure execution environment is further configured to provide the processor with instructions which when executed cause the processor to:

15 communicate the ordered sequence of device data records to a device data record storage function using a secure communication channel, wherein the ordered sequence device data records in combination with each associated unique sequence identifier provides traceability to identify if one or more of the ordered sequence of device data records has been tampered with or omitted from the ordered sequence of data records transmitted to the storage function.

20 11. The system recited in claim 1, wherein the secure execution environment is further configured to provide the processor with instructions which when executed cause the processor to:

25 send a service usage report to a trusted network element using a secure communication channel, wherein the trusted network element verifies the service usage report using validation of message integrity check bytes and the ordered sequence of device data records.

12. The system recited in claim 1, wherein the secure execution environment is further configured to provide the processor with instructions which when executed cause the processor to:

30 send a service usage report to a trusted network element using a secure communication channel, wherein the service usage report includes a second device assisted service usage measure that includes application layer service usage monitoring information, and wherein the

trusted network element verifies the service usage report using the ordered sequence of device data records.

13. A method, comprising:

monitoring service usage of a wireless communication device with a wireless network;
5 and

generating a plurality of device data records of the monitored service usage of the wireless communication device with the wireless network, wherein each device data record is one of an ordered sequence of device data records with each sequential device data record providing an accounting of service usage over a service usage interval spanned by the device
10 data record, and wherein each device data record is associated with a secured unique sequence order identifier.

14. A computer program product, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

monitoring service usage of a wireless communication device with a wireless network;
15 and

generating a plurality of device data records of the monitored service usage of the wireless communication device with the wireless network, wherein each device data record is one of an ordered sequence of device data records with each sequential device data record providing an accounting of service usage over a service usage interval spanned by the device
20 data record, and wherein each device data record is associated with a secured unique sequence order identifier.

15. A system, comprising:

a processor of a wireless communication device for wireless communication with a wireless network, wherein the processor is configured with a secure execution environment, and
25 wherein the secure execution environment is configured to:

monitor service usage of the wireless communication device with the wireless network; and

generate a plurality of device data records of the monitored service usage of the wireless communication device with the wireless network, wherein each device data record is one of an ordered sequence of device data records with each sequential device
30 data record providing an accounting of service usage over a service usage interval

spanned by the device data record, and wherein each device data record is associated with a secured unique sequence order identifier;

send the device data record sequence to a trusted network element using a secure communication channel;

5 implement a secure access controller for restricting wireless network access to a predetermined subset of available network destinations;

receive a secure message from the trusted network element;

if a validated message is received that acknowledges receipt of one or more secure device data records or acknowledges an access network authentication sequence,

10 then the secure access controller allows unrestricted or less restricted access to the wireless network;

if a validated is not received that acknowledges receipt of one or more secure device data records or acknowledges an access network authentication sequence, then the secure access controller restricts access to the predetermined set of network destinations

15 or functions until a validated is received that acknowledges receipt of one or more secure device data records or acknowledges an access network authentication sequence; and

a memory coupled to the processor and configured to provide the processor with instructions.

16. The system recited in claim 15, wherein the program in the secure software or firmware

20 instruction execution environment is further configured with an access controller that restricts access to a predetermined set of network destinations or functions if a predetermined maximum amount of time passes between either the time that a first message acknowledging receipt of one or more secure device data records or an authentication sequence is received by the program in the secure software or firmware instruction execution environment and the time that a second

25 message acknowledging receipt of one or more secure device data records or an authentication sequence is received by the program in the secure software or firmware instruction execution environment, or the time that one or more secure device data records are sent by the program in the secure software or firmware instruction execution environment and the time that a message acknowledging receipt of one or more secure device data records or an authentication sequence

30 is received by the program in the secure software or firmware instruction execution environment; and the access controller otherwise allows unrestricted or less restricted access to the wireless network.

17. A system, comprising:

a processor of a wireless communication device for wireless communication with a wireless network, wherein the processor is configured with a secure execution environment, and wherein the secure execution environment is configured to:

5 monitor service usage of the wireless communication device with the wireless network;

 based on the monitoring of service usage of the wireless communication device with the wireless communication network, create and record characterizations of network performance;

10 analyze the characterizations of network performance and reduce the performance characterizations into one or more network performance statistics that characterize in summary form the performance level or congestion level of the network as experienced by the device;

 generate a plurality of network performance report messages that include a sequence of the network performance statistics created at different times; wherein the network performance report messages are secured network performance reports; and

 send the secured network performance reports to the storage function located in the network; and

20 a memory coupled to the processor and configured to provide the processor with instructions.

18. A system, comprising:

a processor of a network device configured as a device data record storage and processing function, for wireless communication with a wireless network in wireless communication with a plurality of wireless communication devices, with each wireless device including a secure device data record generator, wherein the processor of the network device is further configured to:

25 provide individual secure communication channels between each of the plurality of secure device data record generators and the network device, wherein the communication channel security protocol is configured so that tampering with the device data records may be detected;

30 receive over the secure communications channel a plurality of device data records from each of the secure device data record generators, wherein the plurality of secure device data records are service usage records of monitored service usage of the wireless

communication device with the wireless network, and wherein each device data record forms a portion of an ordered sequence of device data records with each sequential device data record providing an uninterrupted accounting of service usage over the service usage interval spanned by the device data record, and wherein the sequence of device data records forms a contiguous and uninterrupted reporting of device service usage, and
5 wherein each device data record is associated with a unique sequence order identifier;

provide a device data record storage function wherein the device data record sequence for each device is stored;

for each device, analyze the stored sequence of device data records to determine if
10 one or more of the device data records have been compromised by verifying that the information in the service usage record is properly configured according to the secure communication channel protocol;

for each device, determine if one or more of the device data records have been removed or blocked from the device data record sequence originally transmitted from the device by determining if the secure contiguous sequence identifiers for the aggregate
15 sequence are all present in the sequence;

if any device data record has been compromised, delayed or removed, set a fraud detection error flag for that device that signals network apparatus or a network administrator to take further action; and

20 a memory coupled to the processor and configured to provide the processor with instructions.

19. The system recited in claim 18, wherein the processor of the network device is further configured to:

receive a second service usage measure reports from each of the plurality of monitored
25 devices;

reconcile the second service usage measure reports and respective device data records for each monitored device; and

verify the second service usage measure reports using respective device data records for each monitored device to determine whether or not service usage is being accurately reported for
30 each monitored device.

20. The system recited in claim 18, wherein the processor of the network device is further configured to:

receive a second service usage measure reports from each of the plurality of monitored devices;

reconcile the second service usage measure reports and respective device data records for each monitored device; and

5 verify the second service usage measure reports using respective device data records for each monitored device to determine whether or not service usage is being accurately reported for each monitored device, wherein when a minimum tolerance limit for a first device is not met a service usage monitoring or policy enforcement action is initiated to determine or prevent potential out of policy or fraudulent service usage.

10 21. The system recited in claim 18, wherein the processor of the network device is further configured to:

 send a secure message to an access controller executing in a secure execution environment in a monitored device, wherein the secure message either acknowledges receipt of one or more secure device data records or acknowledges an access network authentication
15 sequence.

22. The system recited in claim 18, wherein the processor of the network device is further configured to:

 send a restrict network access message to an access controller executing in a secure execution environment in a monitored device, wherein the access controller restricts wireless
20 network access to a predetermined set of network destinations in response to a validated restrict network access message.

23. A system, comprising:

 a processor of a wireless communication device for wireless communication with a wireless network, wherein the processor is configured with a secure execution environment, and
25 wherein the secure execution environment is configured to:

 monitor service usage of the wireless communication device with the wireless network;

 based on the monitoring of service usage of the wireless communication device with the wireless communication network, create and record characterizations of network
30 performance;

 analyze the characterizations of network performance and reduce the performance

characterizations into one or more network performance statistics that provide indications of the performance level or congestion level of the network as experienced by the device;
generate a plurality of network performance report messages that include a sequence of the network performance statistics created at different times; wherein the network performance report messages are secured network performance reports;
send the secured network performance reports to the storage function located in the network; and
a memory coupled to the processor and configured to provide the processor with instructions.

24. A system, comprising:

a processor of a network device configured as a device secure network performance record storage and processing function, for wireless communication with a wireless network in wireless communication with a plurality of wireless communication devices, with each wireless device including a secure network performance record generator, wherein the processor of the network device is further configured to:

provide individual secure communication channel between each of the plurality of secure network performance record generators and the network device, wherein the communication channel security protocol is configured so that tampering with the secure network performance record may be detected;

receive over the secure communications channel a plurality of secure network performance records from each of the secure network performance record generators, wherein the plurality of secure network performance record are network performance statistics that provide indications of the performance level or congestion level of the network as experienced by the device;

provide a device secure network performance record function wherein the secure network performance record sequence for each device is stored;

determine the sub network of the network that each device is connected to, and analyze the secure network performance records received from multiple devices connected to the same sub network to determine an aggregate characterization of the performance level or congestion level for the sub network, and perform the same operation to determine an aggregate characterization of the performance level or congestion level for other sub networks connected to the network;

store the results of the aggregate characterization of the performance level or congestion level for each sub network that is characterized, and make the stored results available to other network devices or functions;

5 if any device data record has been compromised, delayed or removed, set a fraud detection error flag for that device that signals network apparatus or a network administrator to take further action; and

a memory coupled to the processor and configured to provide the processor with instructions.

25. A system, comprising:

10 a processor of a of a wireless communication device for wireless communication with a wireless network, wherein the processor is configured with a secure software or firmware instruction execution environment, and wherein a program in the secure software or firmware instruction execution environment is configured to:

15 communicate a plurality of traffic sequences between the device and a network device, wherein the traffic sequences are secured;

initiate each traffic sequence based on one or more of: a pre-determined time or time interval, a service usage event or service usage condition that arises on the device, as a response to a message communicated from the network device; and

20 a memory coupled to the wireless device processor and configured to provide the processor with instructions; and

and a processor of the network device in secure communication with the program in the secure software or firmware instruction execution environment is configured to:

monitor the plurality of the secure traffic sequences between service usage of the wireless communication device with the wireless network;

25 using the monitoring results of the secure traffic sequences, create and record characterizations of network performance;

analyze the characterizations of network performance and reduce the performance characterizations into one or more network performance statistics that provide indications of the performance level or congestion level of the network as experienced by the device;

30 generate a plurality of network performance reports that include a sequence of the network performance statistics created at different times; wherein the network performance reports are stored in a network performance report storage function;

the network performance report storage function is made available to other network devices or functions; and
a memory coupled to the processor and configured to provide the processor with instructions.

SECURE DEVICE DATA RECORDS

ABSTRACT OF THE DISCLOSURE

[00206] Secure device data records (DDR) are provided. In some embodiments, a system for secure DDRs includes a processor of a wireless communication device for wireless communication with a wireless network, in which the processor is configured with a secure execution environment, and in which the secure execution environment is configured to: monitor service usage of the wireless communication device with the wireless network; and generate a plurality of device data records of the monitored service usage of the wireless communication device with the wireless network, in which each device data record is associated with a unique sequence order identifier; and a memory coupled to the processor and configured to provide the processor with instructions. In some embodiments, the secure execution environment is located in an application processor, in a modem processor, and/or in a subscriber identity module (SIM).

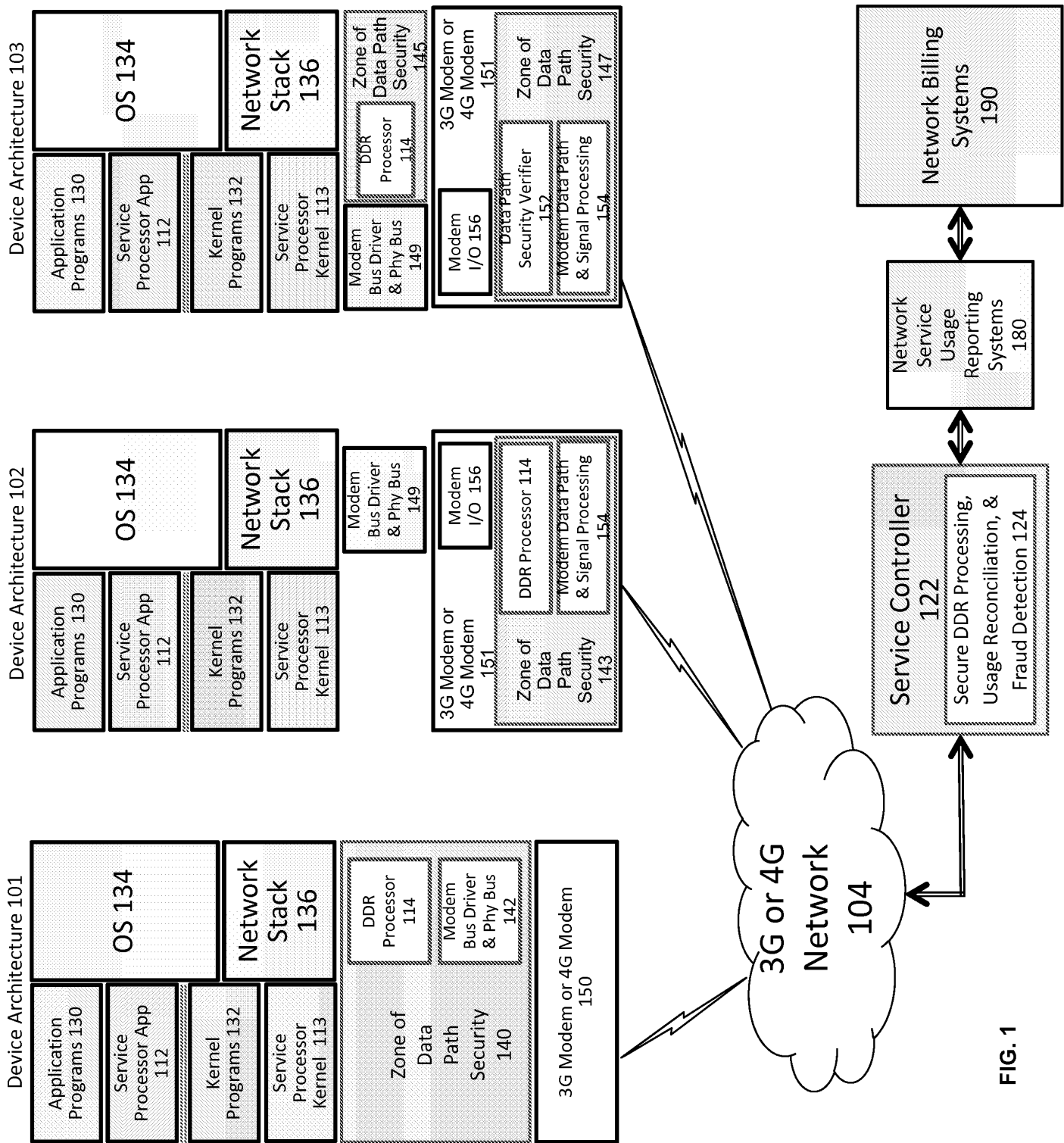


FIG. 1

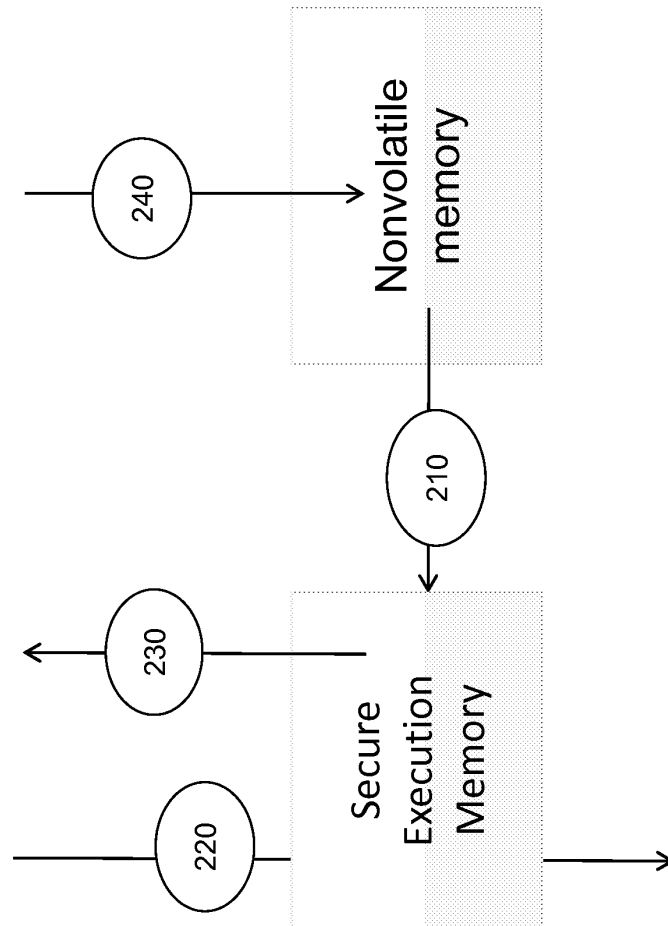


FIG. 2

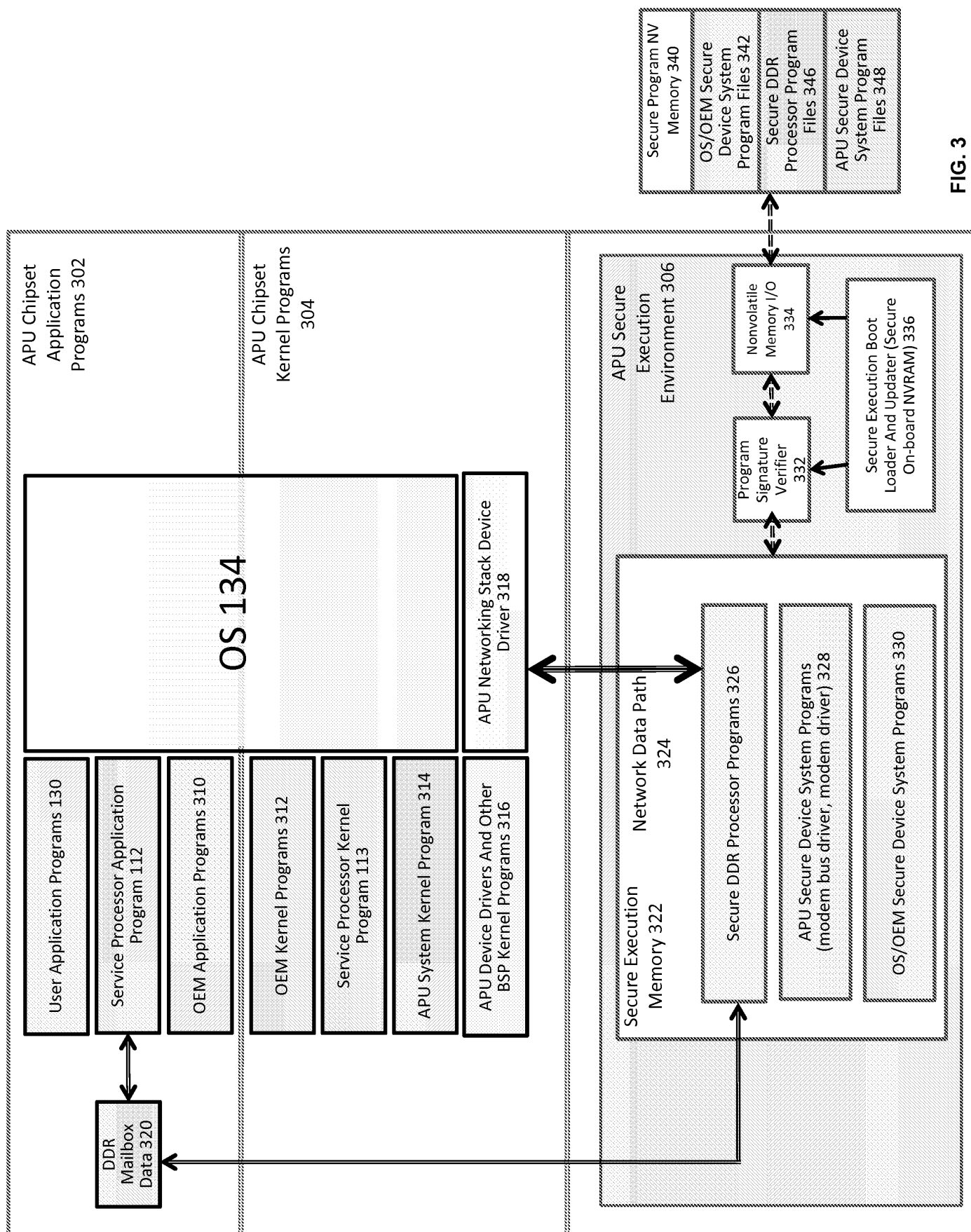


FIG. 3

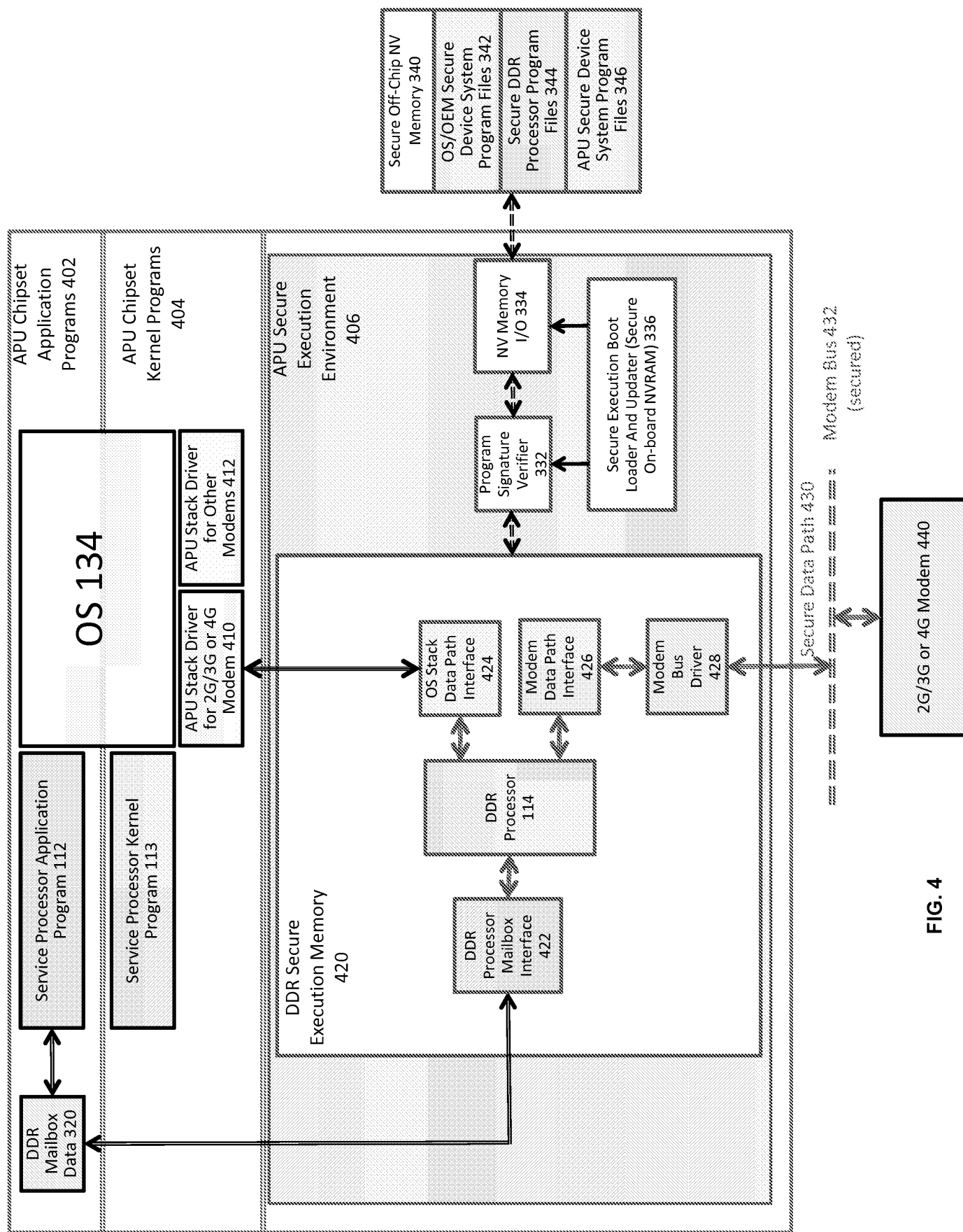


FIG. 4

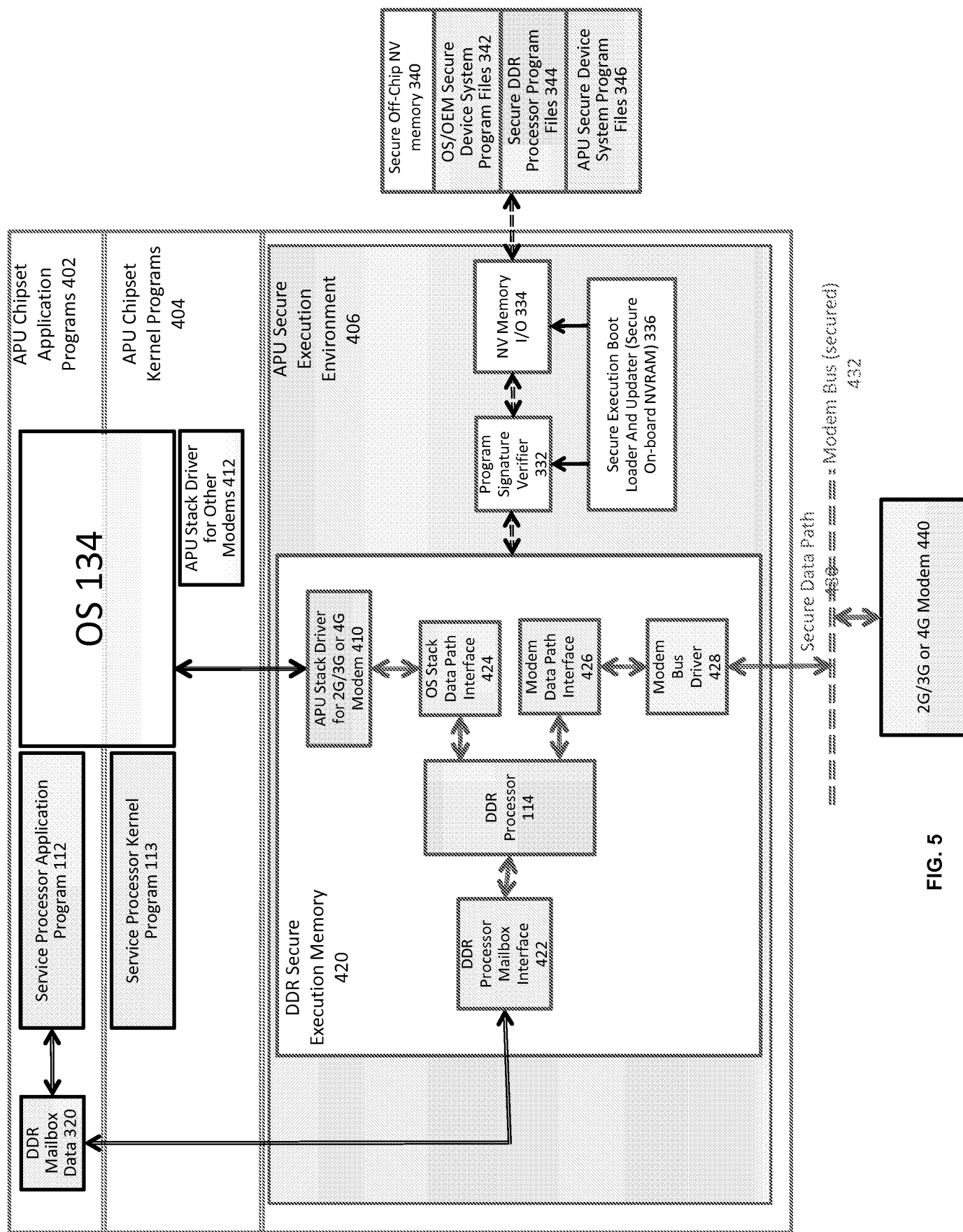


FIG. 5

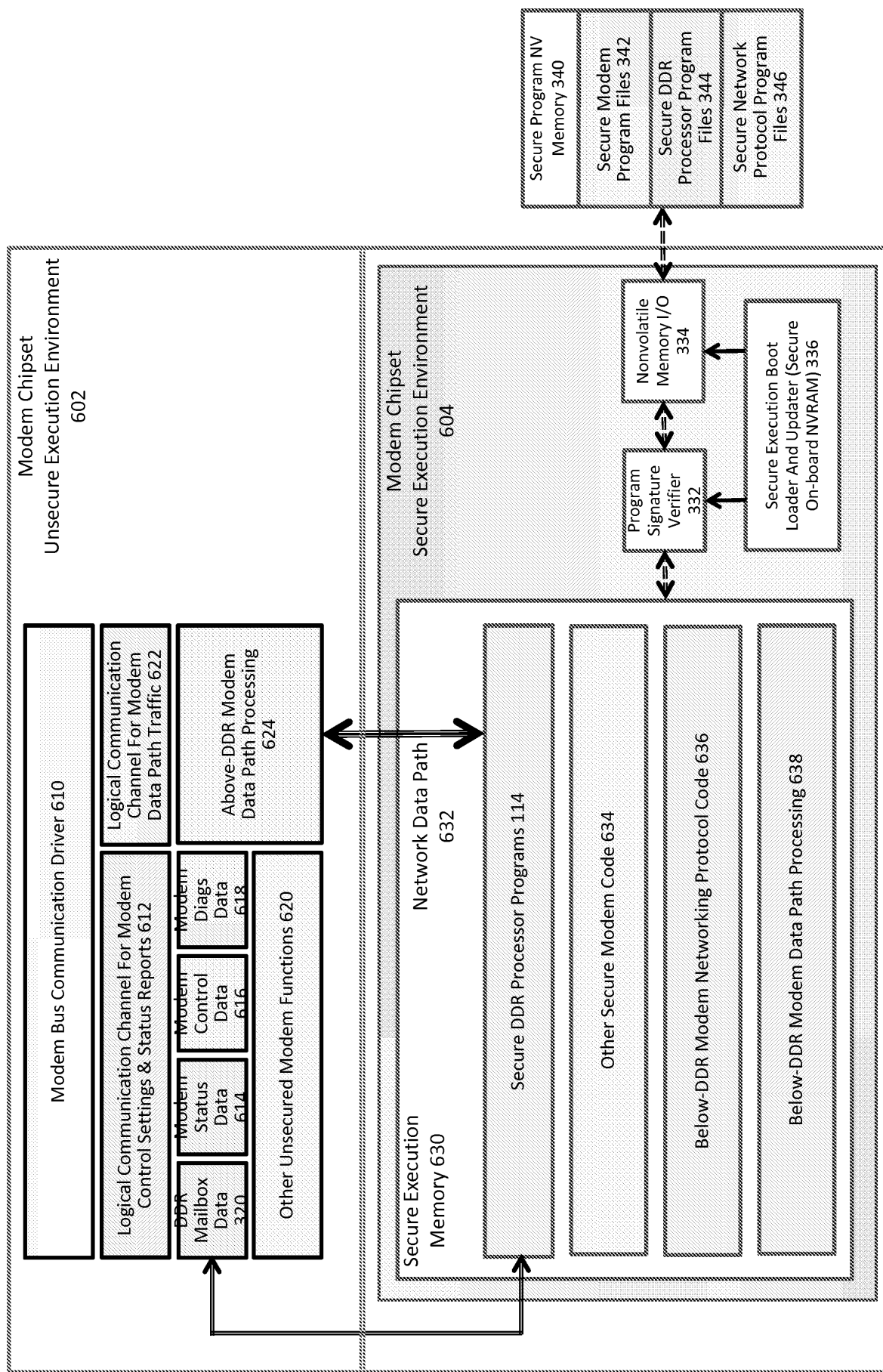


FIG. 6

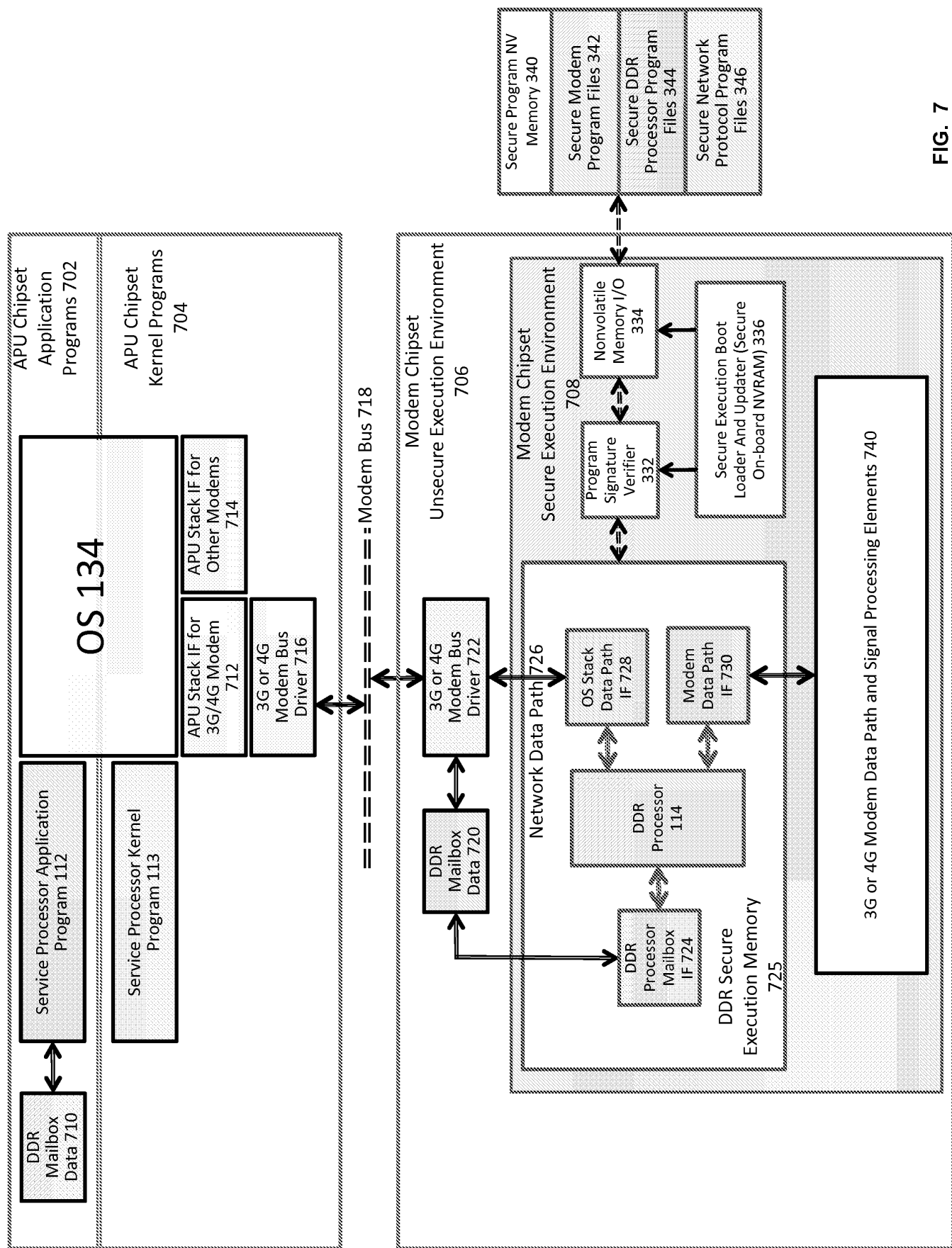


FIG. 7

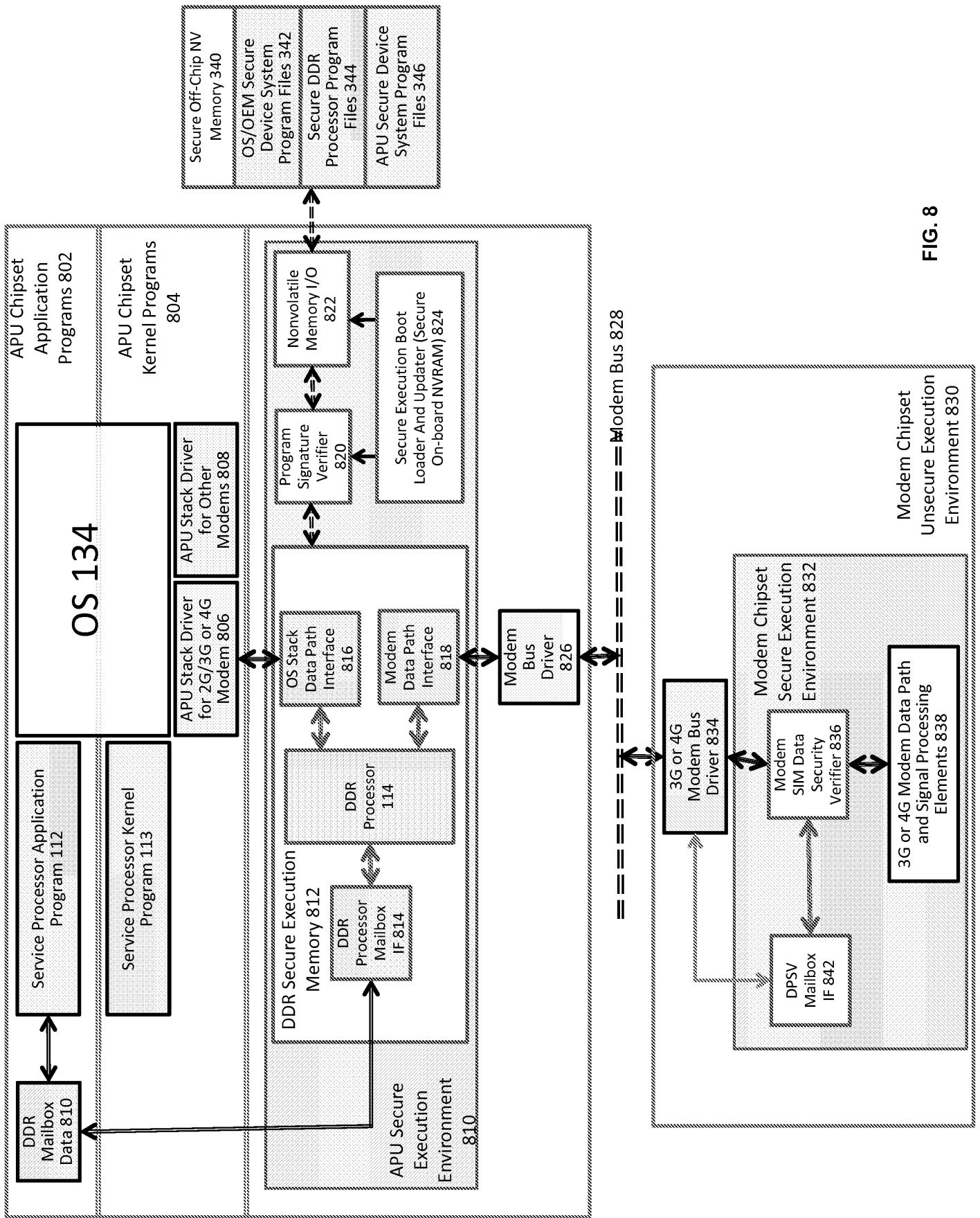


FIG. 8

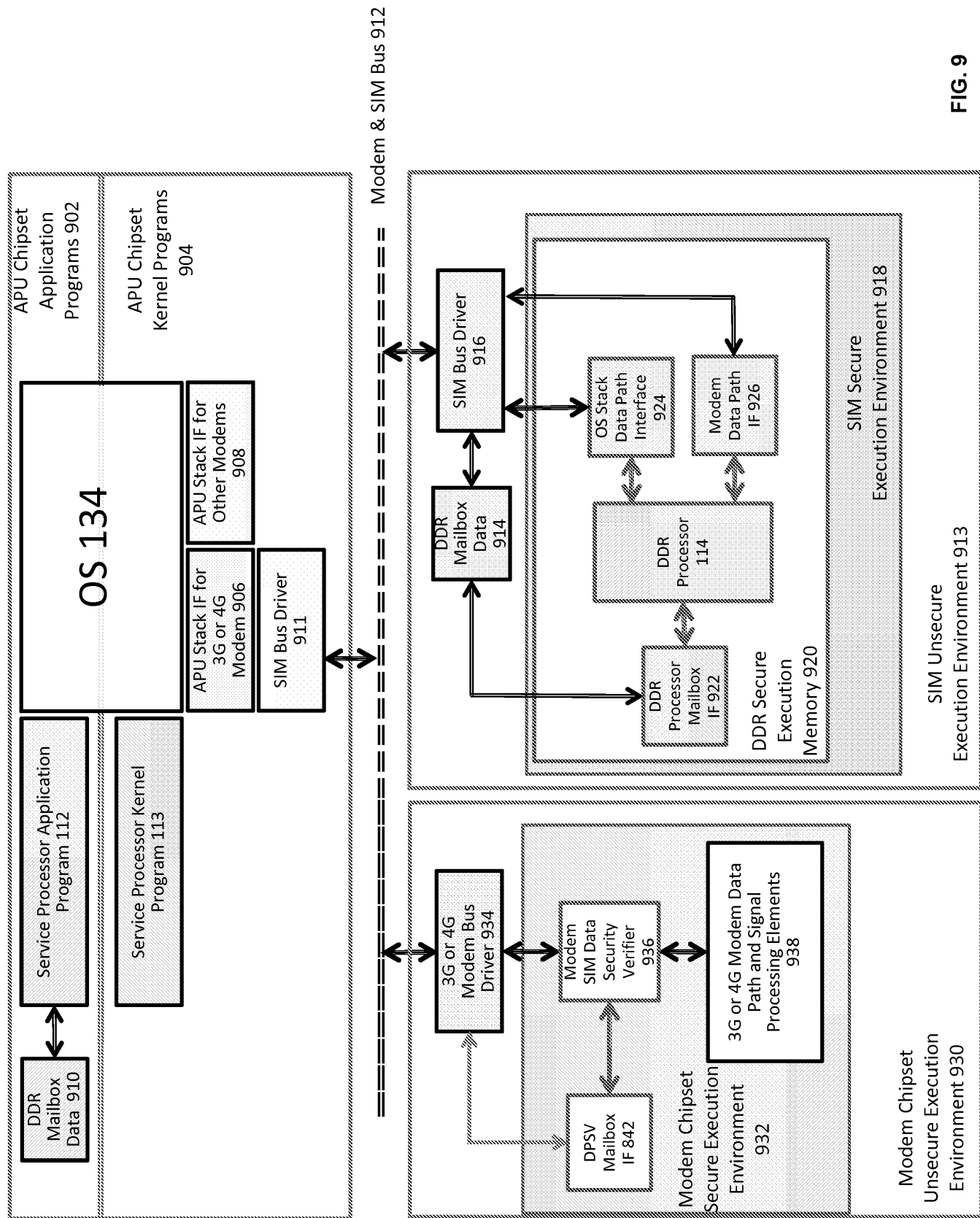


FIG. 9

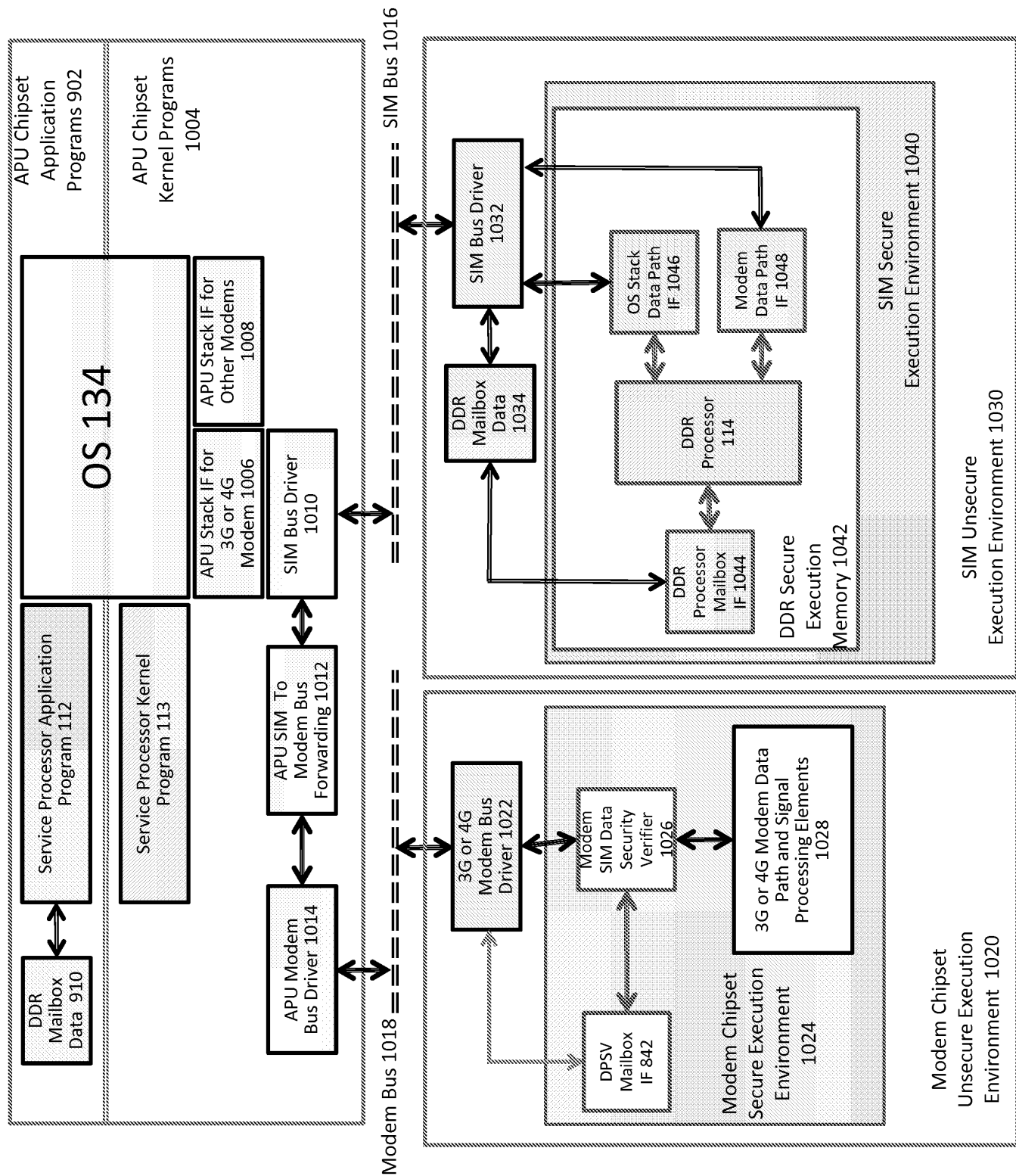


FIG. 10

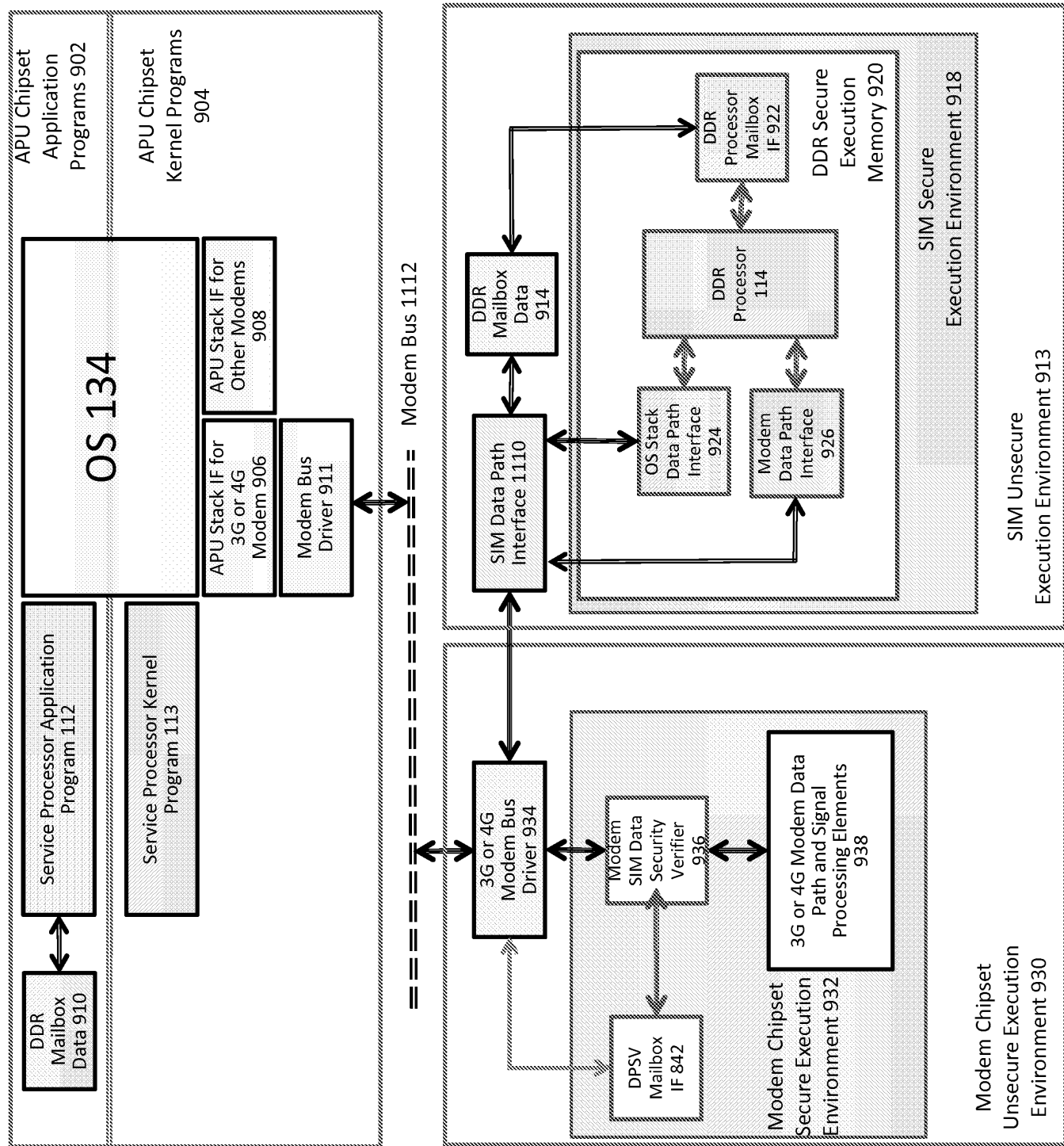


FIG. 11

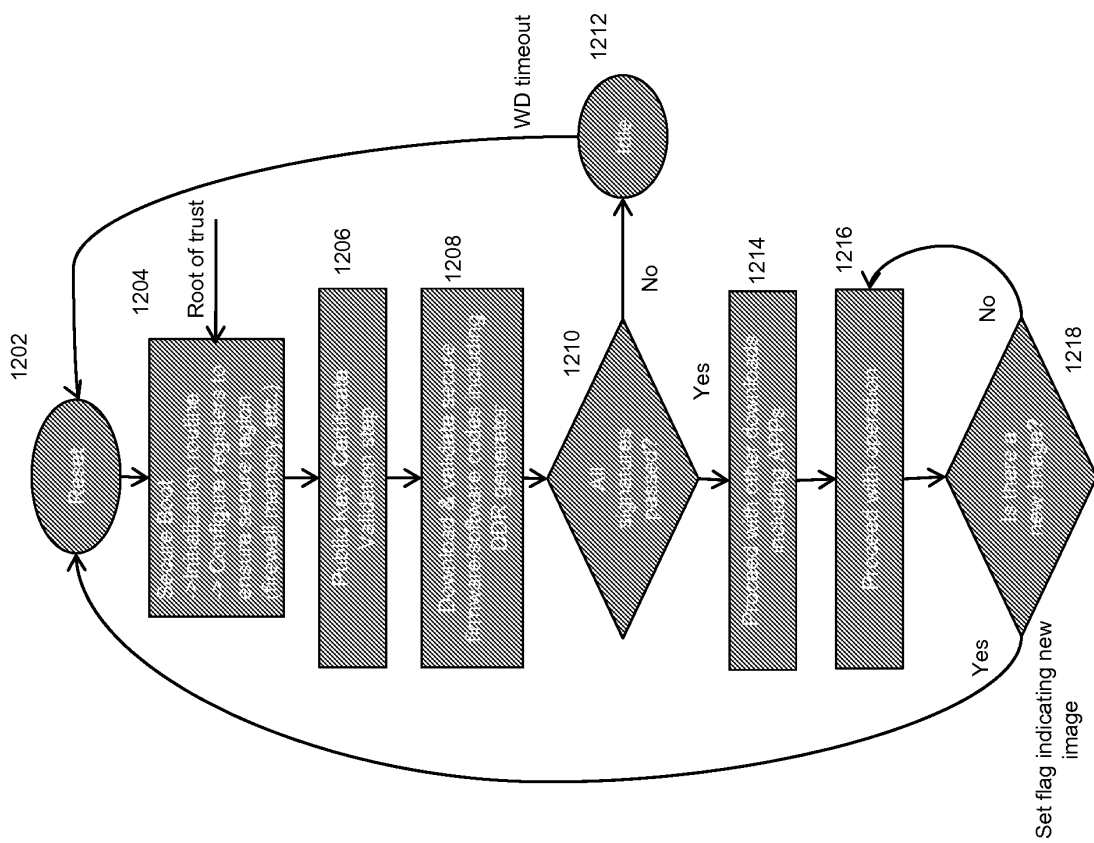


FIG. 12

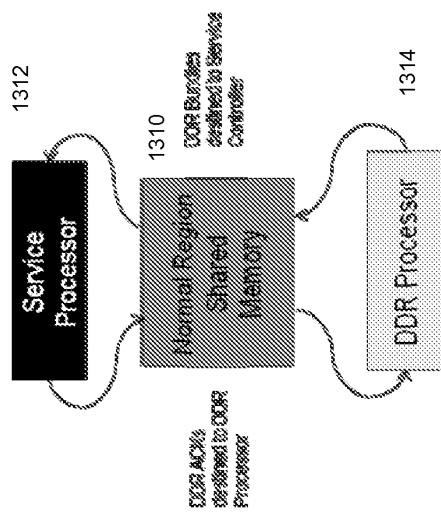


FIG. 13

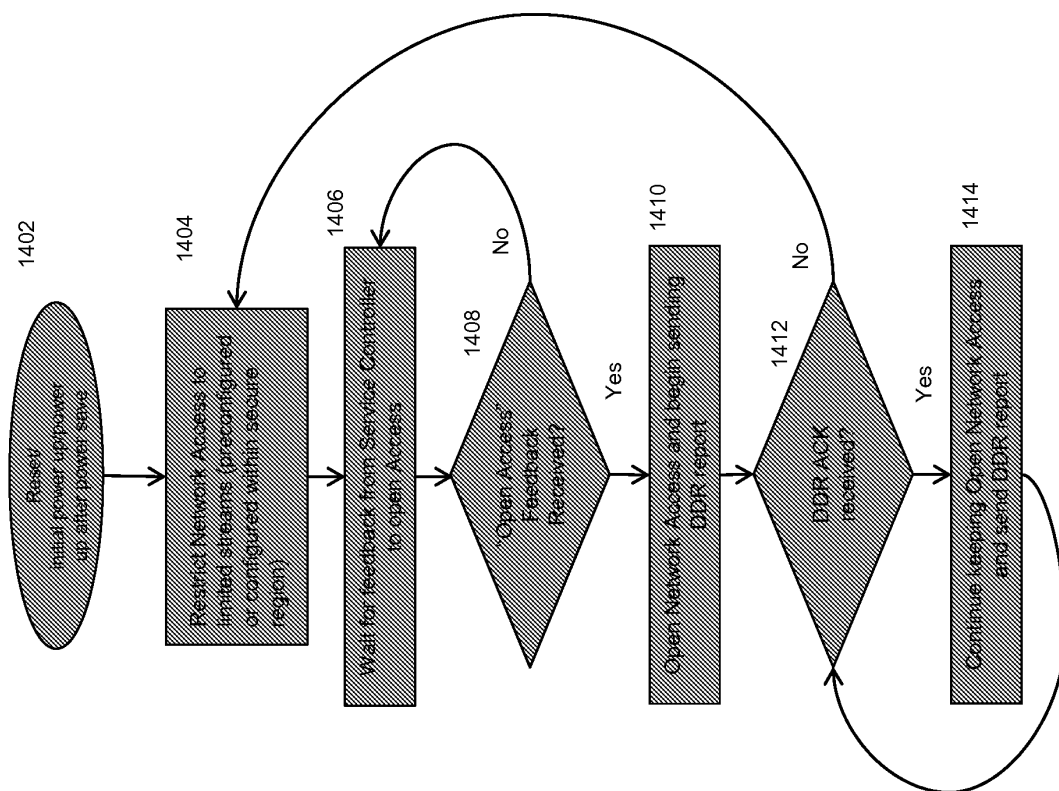


FIG. 14

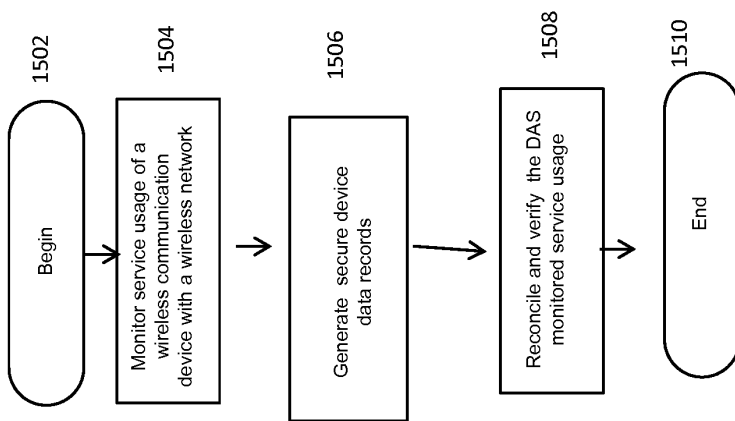


FIG. 15

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		SECURE DEVICE DATA RECORDS		
First Named Inventor/Applicant Name:		Gregory G. Raleigh		
Filer:		Michael J. Schallop		
Attorney Docket Number:		RALEP042+		
Filed as Large Entity				
Provisional Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Provisional application filing	1005	1	220	220
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				220

Electronic Acknowledgement Receipt	
EFS ID:	8985503
Application Number:	61420727
International Application Number:	
Confirmation Number:	1137
Title of Invention:	SECURE DEVICE DATA RECORDS
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	21912
Filer:	Michael J. Schallop/Veronica Pula
Filer Authorized By:	Michael J. Schallop
Attorney Docket Number:	RALEP042+
Receipt Date:	07-DEC-2010
Filing Date:	
Time Stamp:	20:23:33
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$220
RAM confirmation Number	6459
Deposit Account	500685
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 1.21 (Miscellaneous fees and charges)	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Provisional Cover Sheet (SB16)	RALEP042plus_Provisional_Application_Coversheet.pdf	999973	no	3
			c35409f53aa0d3aaa286e2862a9baaac8484b7d4		
Warnings:					
Information:					
2		RALEP042plus_App.pdf	278266	yes	76
			4930fbddf3daad76f474433af6bf77ab7bc008		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal of New Application		1	1	
	Specification		2	65	
	Claims		66	75	
	Abstract		76	76	
Warnings:					
Information:					
3	Drawings-only black and white line drawings	RALEP042plus_Figures.pdf	370787	no	15
			bc1d0bf6c660d907e3b619389828e087e7b16457		
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	29070	no	2
			e101e94addf3241a6c0e680e83ba0334be630be8		
Warnings:					
Information:					
Total Files Size (in bytes):			1678096		

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.

Doc Code: **TR.PROV**

Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (04-07)

Approved for use through 06/30/2010 OMB 0851-0032

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

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

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1

Remove

Given Name	Middle Name	Family Name	City	State	Country i
Gregory	G.	Raleigh	Woodside	CA	US

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.

Add

Title of Invention	SECURE DEVICE DATA RECORDS
Attorney Docket Number (if applicable)	RALEP042+

Correspondence Address

Direct all correspondence to (select one):

☒ The address corresponding to Customer Number ☐ Firm or Individual Name

Customer Number 21912

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Entity Status

Applicant claims small entity status under 37 CFR 1.27

- ☐ Yes, applicant qualifies for small entity status under 37 CFR 1.27
- ☒ No

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 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.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Michael J. Schallop/			Date (YYYY-MM-DD)	2010-12-07
First Name	Michael	Last Name	Schallop	Registration Number (If appropriate)	44319

This collection of information is required by 37 CFR 1.51. 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 8 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. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that : (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to a n other federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.