



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
61/418,509	12/01/2010		220	RALEP041+		

CONFIRMATION NO. 1496

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

FILING RECEIPT



OC000000044891066

Date Mailed: 12/10/2010

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 Schallop--44319

If Required, Foreign Filing License Granted: 12/09/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/418,509**

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

Non-Publication Request: No

Early Publication Request: No

Title

SERVICE USAGE REPORTING RECONCILIATION AND FRAUD DETECTION FOR DEVICE
ASSISTED SERVICES

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

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

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

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

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

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

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

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**SERVICE USAGE REPORTING RECONCILIATION AND FRAUD DETECTION
FOR DEVICE ASSISTED SERVICES

Attorney Docket Number (if applicable)

RALEP041+

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)	2010-12-01
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.



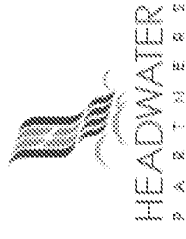
Motivation

In DAS systems, there is a potential for device users to spoof or hack the device Service Processor to fraudulently obtain access services at incorrect lower service usage billing rates.

To prevent this, a variety of fraud detection and Service Processor protection embodiments have been disclosed in previous USPTO filings.

This filing provides additional embodiment details in the area of service usage reconciliation from one or more reporting sources for the purpose of detecting and mitigating potential fraud

Service Usage Reporting Sources



Device

- Service Processor Device Charging Reports (DCRs) – generally not trusted
- Secure DDR processor Device Data Records (DDRs) – can be trusted with secure design of DDR processor and secure DDR report sequencing
- Applications (Apps) – generally not trusted

Carrier (Or MVNO) Network – generally trusted

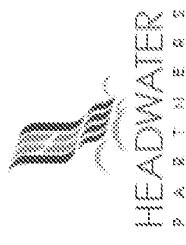
- Gateways (GGSN, SGSN, PDSN, Routers, Switches, etc)
- Home Agent
- Proxy servers
- Charging gateway system
- Mediation
- Reconciliation
- Billing
- AAA
- Etc

- Can be “bulk measures” of general usage, can be FDRs that indicate destinations, can include network state records at time of usage (e.g. Time of Day (TOD), network busy state or congestion state (NBS), type of network (e.g. 2G, 3G, 4G, WiFi, home/roaming, etc), etc)

3rd Parties – can be trusted with correct processes in place to verify reports via sampling etc

- Usage reports, site visits, transaction reports, ad view reports, economic benefit reports, usage credit increase instructions, etc from:
 - Partner service destination servers (e.g. search site, ad site, application service site, shopping site, content site, gaming site, email site, etc)
 - Enterprise customer network
 - Etc

Basic Fraud Prevention Embodiments



Make sure that when device is on network that Service Processor is properly authenticated and reporting usage

Make sure service processor is properly responding to access control commands

Make sure the service processor code integrity is maintained – that the code has not been tampered with

- e.g. Hash or signature checks, execute in secured partitions, etc – see USPTO previous filings for additional embodiments
- e.g. e.g. Hash or signature checks, execute in secured partitions, etc – see USPTO previous filings for additional embodiments

Make sure that an application that has an application specific service has not been tampered with

Make sure usage reports from trusted source(s) indicate usage behavior that is within usage control policies

Make sure usage reports from trusted source(s) match usage reports from Service Processor

Make sure usage does not exceed caps

- Bulk caps
- Service component (e.g. application services, sponsored services) caps

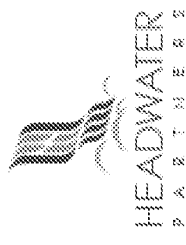
Make sure usage patterns fit within expected usage patterns

- Based on access control policies that should be in place
- Based on statistical assessment of device group population
 - Can be updated dynamically by Service Controller

Make sure network destinations and usage (e.g. reported via FDRs) are consistent with the service plan that should be in place

Make sure that access performance achieved by device (or app) is consistent with service plan policy that should be in place

What to Do When Fraud is Detected



Notify network administrator or network resource for further evaluation

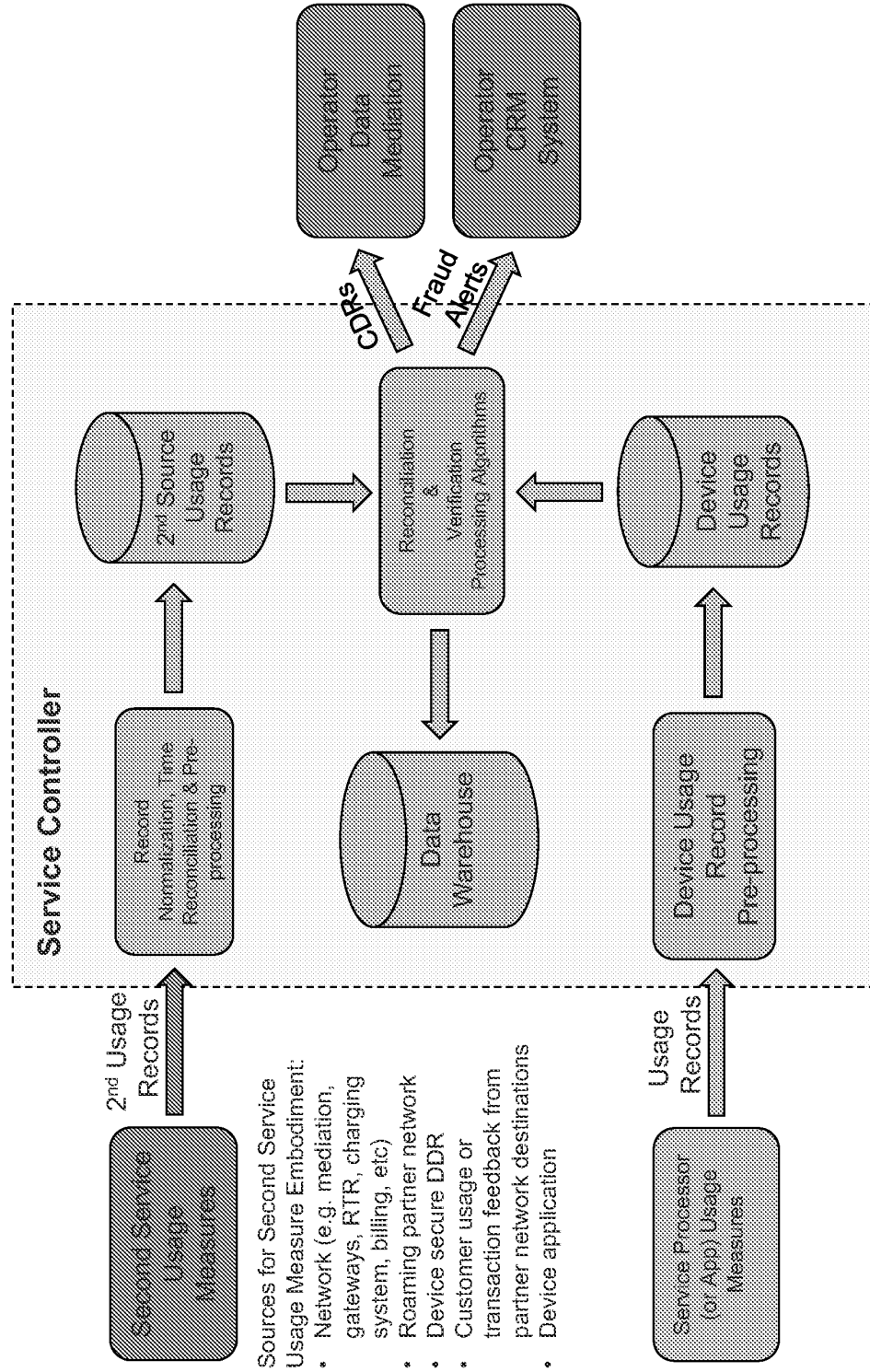
Increase billing rate

Increase billing rate and notify user via one or more communication media (e.g. service processor or device notification client UI, text, email, voice mail, phone call) of service agreement violation and increased billing rate.

Throttle device access (or app access)

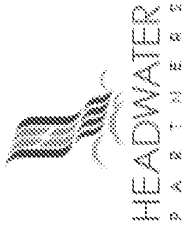
Suspend device access (or app access)

Service Controller CDR and DCR Reconciliation Processing for Fraud Detect



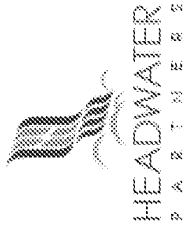
- Verify the service usage measurements the device is reporting:
 - Bulk usage
 - Application specific usage including transaction based
 - Single-App Service
 - Multi-App Service
 - Destination (e.g. IP address, Domain address) specific usage
 - Usage that is sent to an app allowed to go to certain locations but those locations have other content not on known white list
 - Usage for “leases” such as surf-out (aka click-out)
 - Usage that is tagged by background, foreground, TOD, NBS, state modifiers
 - Usage that is tagged by QoS
 - Usage that is tagged by network type
 - Usage that occurs while roaming
 - Usage based on specific content, e.g. streaming audio, video, etc.
 - Usage based on specific layer 3/4 protocol, e.g. TCP, UDP and/or Layer 7 protocol, e.g. IGMP, RTMP, RSTP, etc.
 - Validate that services (including App based services) are properly classified for network access:
 - Confirm that a service control that was supposed to be in place was actually in place. Examples:
 - Caps, grace
 - Speed (e.g. maximum rate)
 - Background, foreground, TOD, NBS, type of network, home/roaming, etc state modifiers
 - QoS limits
 - Determine a second measure of network state to confirm that the device is reporting the correct network state in charging reports:
 - Measure network state with a group of devices, report to Service Controller (or other suitable network function), characterize sub-network portions (e.g. base stations, base station sectors, geographic areas, RAN, etc) based on device population connected to that sub-network portion
 - Gather network busy state measures from network equipment (e.g. base stations, RAN sampling, etc)
 - Determine a second measure of device access behavior vs. network state to make sure the device is implementing the correct controls:
 - Network (BTS, RAN, Core, device assisted)
 - DDR (NBS and network type on device or signal from network)
 - Bulk
 - FDR
 - Network state tagged information
 - DDR network state tagged information

Basic Fraud Detection Procedure Embodiments 2



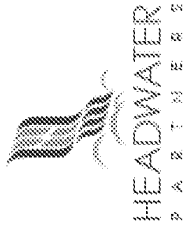
- * Basic methods for reconciling device usage reports and algorithms for reconciling device usage reports to detect fraud
 - * Only bulk usage is available
 - * Cap and verify cap is not exceeded
 - * If multiple services, then verify sum of caps is not exceeded
 - * Throttle (e.g. max rate) and verify throttle policy is not exceeded
 - * Compare bulk usage or sum of component usage that device reports with 2nd measure (Device, Network or app service provider Server based)
 - * Observe rate of bulk usage (e.g. usage velocity) and compare to policy given the set of services that are enabled
 - * Observe usage breakdown of individual usage categories reported by device to determine if each is within plan and/or expected behavioral limits
 - * Limits set by plan parameters
 - * Limits set by expected user behavior
 - * Limits set by observing, collecting and compiling population statistics of user device group
 - * Compare component usage vs. real time network state reported by other devices on same BTS or sub-nets
 - * Observe usage breakdown of network state (e.g. TOD, NBS, type of network, roam/home, etc) dependent controls (caps, speeds, background/foreground, QoS, etc) reported by device to determine if each is within plan and/or expected behavioral limits
 - * Limits set by plan parameters
 - * Limits set by expected user behavior
 - * Limits set by observing, collecting and compiling population statistics of user device group
 - * Compare component usage vs. real time network state reported by other devices on same BTS or sub-nets
 - * Send limiting command (e.g. cap, stop, throttle commands) to device and see if usage is stopped or controls are obeyed}
 - * Bulk plus network state is available
 - * Observe bulk usage behavior vs. network state reported by 2nd source (e.g. network or DDR) and compare to policy
 - * Observe bulk usage behavior vs. population statistics for bulk usage behavior and flag if outside of norm

Basic Fraud Detection Procedure Embodiments 3



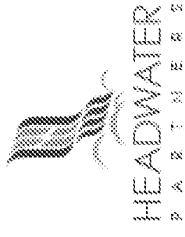
- Basic methods for reconciling device usage reports and algorithms for reconciling device usage reports to detect fraud:
 - FDR level information is available
 - Classify FDRs to known service components, rack up credit of classified usage for each service component, ensure that service component usage does not exceed limits and/or matches with device reports for component, ensure that sum of components matches bulk
 - If not all service component usage can be classified with known sources (e.g. ad servers, content servers, allowed click-out, etc), then create a unclassified usage policy allowance (e.g. proportional to or a percentage of the classified service usage for the component) and "credit" that amount of unclassified service usage to the service component. Then as long as the bulk service usage that remains after each service component policy allowance "credit" is deducted is under the policy limit (if any) for bulk and/or the remaining bulk usage matches what the device is reporting then no fraud alert is generated.
 - The pre-determined usage policy allowance can be based on a set of unclassified usage policy allowance rules determined by various methods including pre-testing such as using the service component and classifying the resulting usage as "classifiable" and "not classifiable", or observing device/user population statistics.
 - Policy allowance can include an amount for "click-out" and/or good customer feedback (see what follows).
 - Algorithm:
 - Accumulate all FDR usage reports that can be classified into known service component usage-
 - For each service component, based on the amount of service usage that could be classified for that component, apply the unclassified usage policy allowance based on the amount of classified usage for that component and application of the unclassified allowance usage policy rules. This amount can be added to the classified service usage for each component to form an estimate of the total service usage (classified plus unclassified allowance) for each service usage component.
 - In the case of multi-service App, the classified traffic includes unshared white-listed services as well as shared services. Shared services will have its own allowance as part of classified traffic
 - Subtract the classified plus unclassified allowance usage for each service component from the total service usage recorded by the second measurement source (e.g. network, DDR, good customer feedback, etc). The amount of service usage remaining after these subtractions from the total service usage is the unclassified or "bulk" service usage-
 - Ensure that the classified plus unclassified allowance service usage for each component is below the policy limits and/or matches device usage reports for that component-
 - Ensure that the remaining "bulk" service usage is below the policy limits and/or matches device usage reports for the device/user "bulk" usage category-
 - For each service component, can also have the device record the network state that existed at the time of usage (and possibly the policy controls that are in place for the usage), then compare this to service policy and/or a second measure (e.g. network measure or DDR) of network state. Ensure that the usage and/or policy controls for each service component are within policy limits
 - FDR level information is available and network state information is available
 - Perform the above algorithm with the appropriate service limits and/or traffic control policy checks for each network state that is recorded with the second usage measure. Classification now includes not only service components, but service components for each network state – run second measurement source classified and unclassified allowance usage checks as described above across all service components for all network states and compare results to usage policy and/or device reports-

Basic Fraud Detection Procedure Embodiments 4



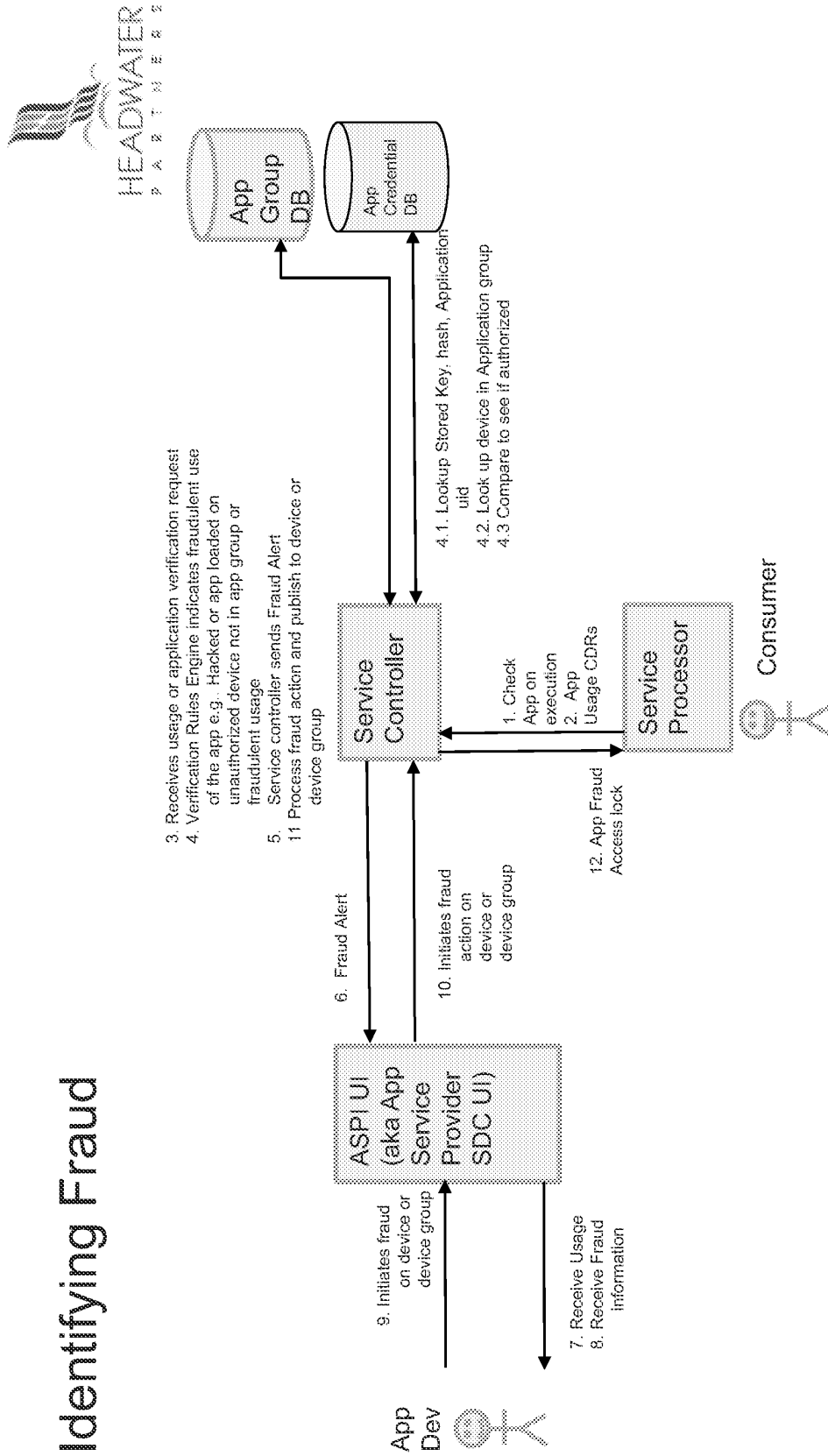
- * How to make sure that App credential is valid:
 - * Service processor validation of App credential (e.g. hash, signature, certificate based verification)
 - * Device OS based validation of App credential (e.g. hash, signature, certificate based verification)
 - * Service Controller assisted App credential validation (e.g. hash, signature, certificate based verification)
 - * Authentication Credential Server based App credential validation (e.g. hash, signature, certificate based verification)
- * **How to use feedback from component service servers, ad sites or stores be used to increase allowances:**
 - * Device credential (e.g. http header info, special side channel, app passes credential, etc) is passed to component service server so that server can log visits, usage and/or transactions
 - * Apply rating rule to convert visits, usage and/or transactions to good customer points
 - * Pass good customer points to Service Controller (or possibly directly back to Service Processor or service component App)
 - * Service Controller (or Service Processor/App) uses rating rule to convert good customer feedback to usage allowance increase-
 - * Usage allowance can be for specific component service, more than one component service, or for general purpose usage
 - * Example: each time a user clicks on an ad (or buys something or visits a web site to view something), they get so much free search, browsing, text, voice, or other services...
- * **How to make sure a user does not exploit free services such as book or music clip browsing:**
 - * Cap usage per unit time
 - * Reduce cap if customer abuses service
 - * Reduce cap if customer abuses service and does not get good customer feedback
 - * Get good customer feedback
 - * Real time feedback
 - * Every so often feedback
 - * Increase limits if good customer feedback is received
- * **How to verify "click-out" usage:**
 - * Good customer feedback
 - * Make sure the "home" site is being accessed between surf outs and not more than a certain amount of surf out is occurring between home site visits.

Basic Fraud Detection Procedure - 5



- Basic methods to determine if the Service Processor is in place and working correctly:
 - Flag possible error when SP does not log in but off-hook, network CDR/FDR or secure DDR report is received
 - Flag possible error when Service Processor authentication procedure is not correctly completed
 - Flag possible error when network counts and/or DDR counts do not match device service processor counts (see additional material herein for more details)
 - To minimize possible fraudulent usage between time device is first used and time that first network usage reports are received, use accelerated secure DDR reports
 - Use DDR processor access controller to prevent general purpose device usage before Service Processor and DDR are securely logged into Service Controller
 - Use securely sequenced DDR reports with maximum timeout between reports to make sure period of time where usage can be fraudulently acquired is minimized
 - When SC has issued "service stopped command" to service processor but then still receives usage report for the device from network, flag error or instruct network to suspend device or charge device user at a higher rate and notify device user

Identifying Fraud

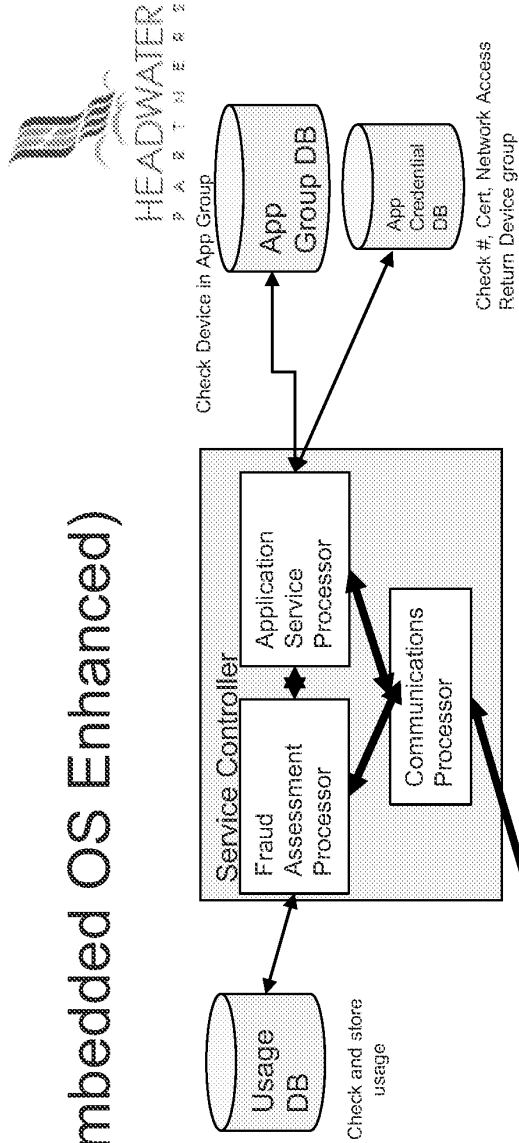


App Dev could choose to have the fraud detection automated in which case steps 9-10 would be skipped

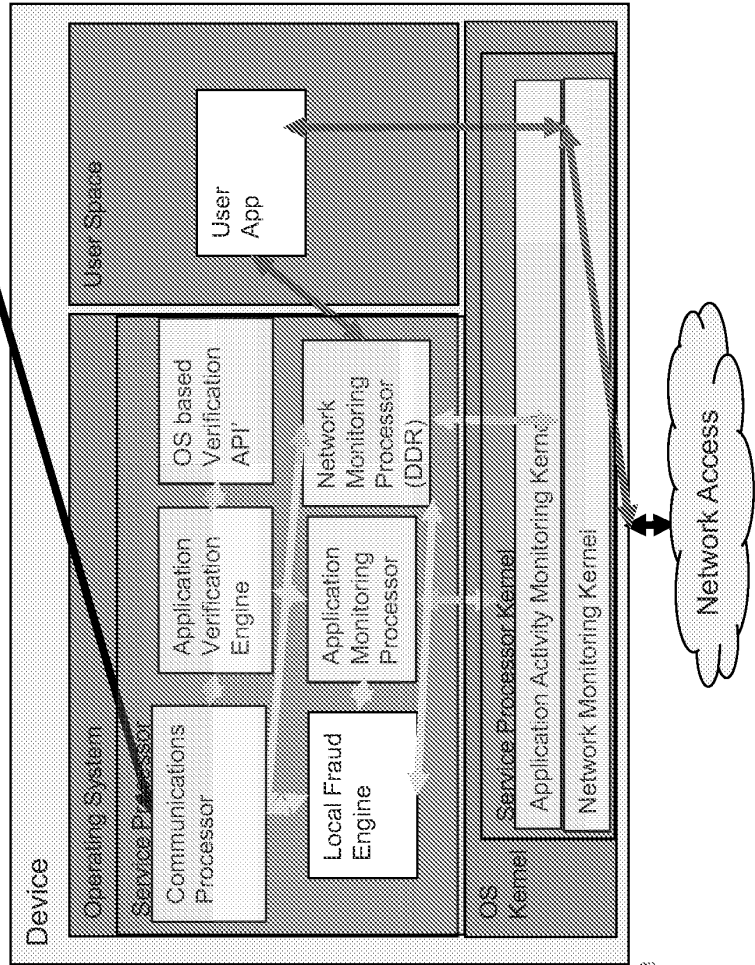
Identifying Fraud (Embedded OS Enhanced)

Server

1. Comm Processor will communicate with the Device package
 1. The use is local priv key to sign the communication package
 2. Update Signed Pub Key as needed
 3. Respond to a verification request
2. The Fraud Assessment Processor will
 1. Store usage records
 2. Run Application Fraud rule set
 3. Perform advance data analytics and data mining to spot Fraud
 4. Alert the App Dev through the portal etc of Fraud alerts
3. The application Service Processor will
 1. Notify the Fraud Assessment Processor of a application usage event that is invalid



Device

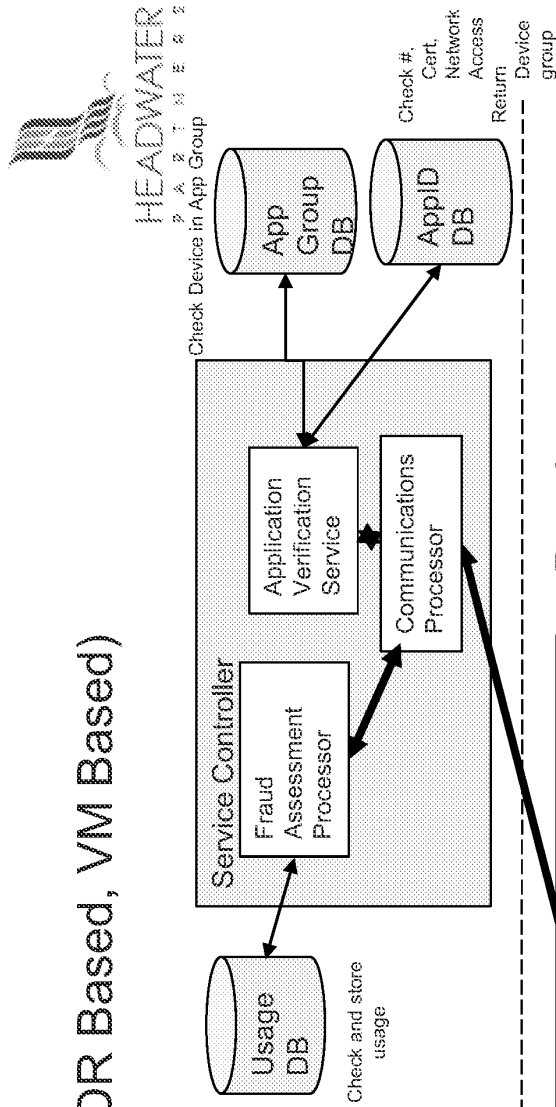


1. Network Monitor Processor monitors application against their network or fraud profile. It will
 1. Look at destination for applications and ensure it meets behavior rules
 2. Signal mis-behavior rules to App Verification Engine
 3. Count Usage
2. Network Monitor Processor will also provide network state information to an app e.g. Network, NBS, Background such as launch etc
3. Application Monitor Processor monitors application activity
4. Communication Processor communicates directly to the SDC could be over DNS, HTTP or some other internet protocol
 1. The use is local key to sign the communication package
 2. Update Signed Key as needed
5. App Verification engine will :
 1. Create hash such as SHA256
 2. Get the applications public key, UID
 3. Gather network events
 4. Communicate to the Comms Processor
6. Local Fraud Engine will:
 1. an used heuristic or similar based event monitoring on events sent to the Comm Processor
 2. Drive throttling or blocking events into the application and Network monitoring Processor to prevent/restrict fraud

Identifying Fraud (Chip DDR Based, VM Based)

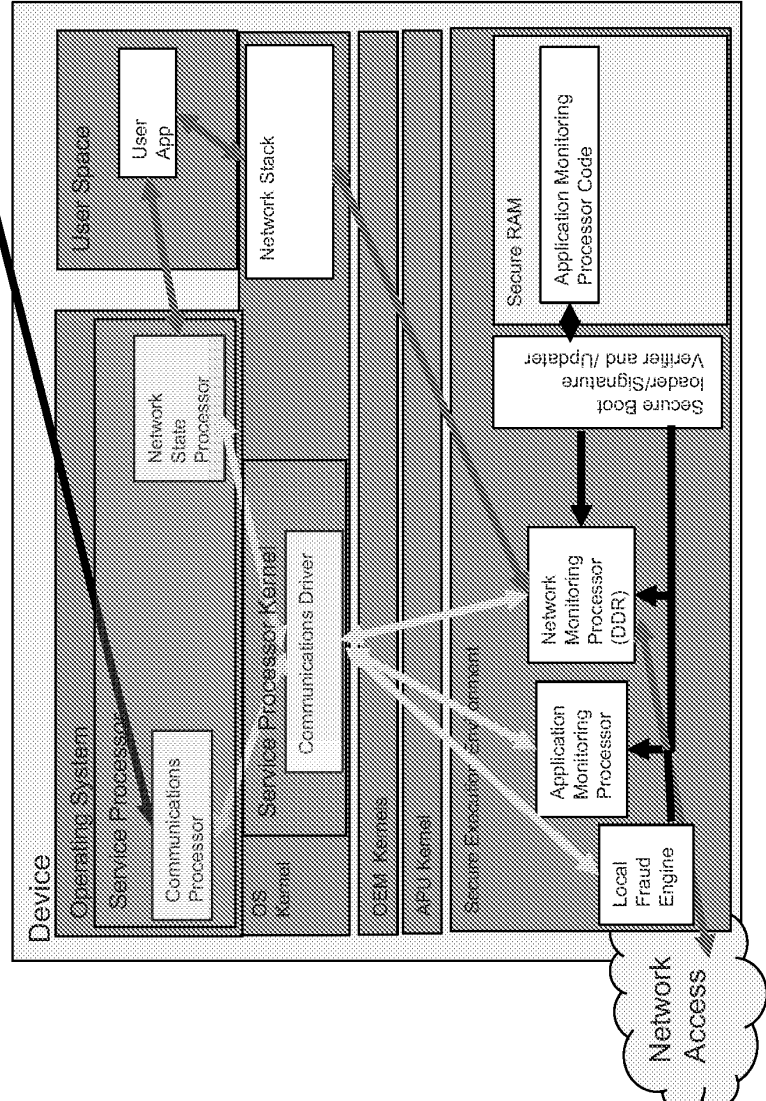
Server

1. Comm Processor will communicate with the Device
 1. The use is local priv key to sign the communication package
 2. Update Signed Pub Key as needed
 3. Respond to a verification request
2. The Fraud Assessment Processor will
 1. Store usage records
 2. Run Application Fraud rule set
 3. Perform advance data analytics and data mining to spot Fraud
 4. Alert the App Dev through the portal etc of Fraud alerts
3. The application Service Processor will
 1. Notify the Fraud Assessment Processor of a application usage event that is invalid

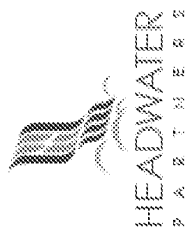


Device

1. Network Monitor Processor monitors application against their network or fraud profile. It will
 1. Look at destination for applications and ensure it meets behavior rules
 2. Signal mis-behavior rules to App Verification Engine
 3. Count Usage
2. Network Monitor Processor will also provide network state information to an app e.g. Network, NBS, Background such as launch etc
3. Application Monitor Processor monitors application activity
4. Communication Processor communicates directly to the SDC could be over DNS, HTTP or some other internet protocol
 1. The use is local key to sign the communication package
 2. Update Signed Key as needed
5. App Verification engine will :
 1. Create hash such as SHA256
 2. Get the applications public key, UID
 3. Gather network events
 4. Communicate to the Comms Processor
6. Local Fraud Engine will:
 1. an used heuristic based or similar event monitoring on events sent to the Comm Processor
 2. Drive throttling or blocking events into the application and Network monitoring Processor to prevent/restrict fraud

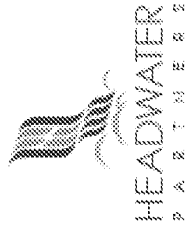


Fraud Scenarios



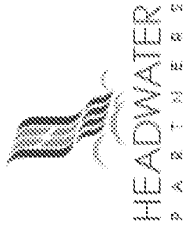
- * Service Processor (SP) doesn't attempt authentication within acceptable window after the Service Controller (SC) receives "data session started" indication from the network
 - * Cause: SP disabled, SIM in a non-Service Processor enabled device (non-fraud)
- * SP fails authentication with SC
 - * Cause: Invalid credentials, device spoofing
- * SC receives Usage Data Records (UDR) from SP after receiving "data session stopped" trigger from the network
 - * Cause: Device spoofing
- * Service Controller receives CDRs but does not receive UDRs
 - * Cause: SP disabled, SIM in a non-Service Processor enabled device (non-fraud, unless SP has authenticated with SC during this data session)
- * SC receives CDRs and UDRs but the usage counts don't align
 - * Cause: SP tampering
- * SC receives CDRs and UDRs but the UDRs indicate usage over Charging Policy (CP) limit(s)
 - * Cause: SP tampering
- * SC receives UDRs but charging codes do not correspond to CP(s) for current active services
 - * Cause: SP tampering, device spoofing

Fraud Scenarios (cont'd)



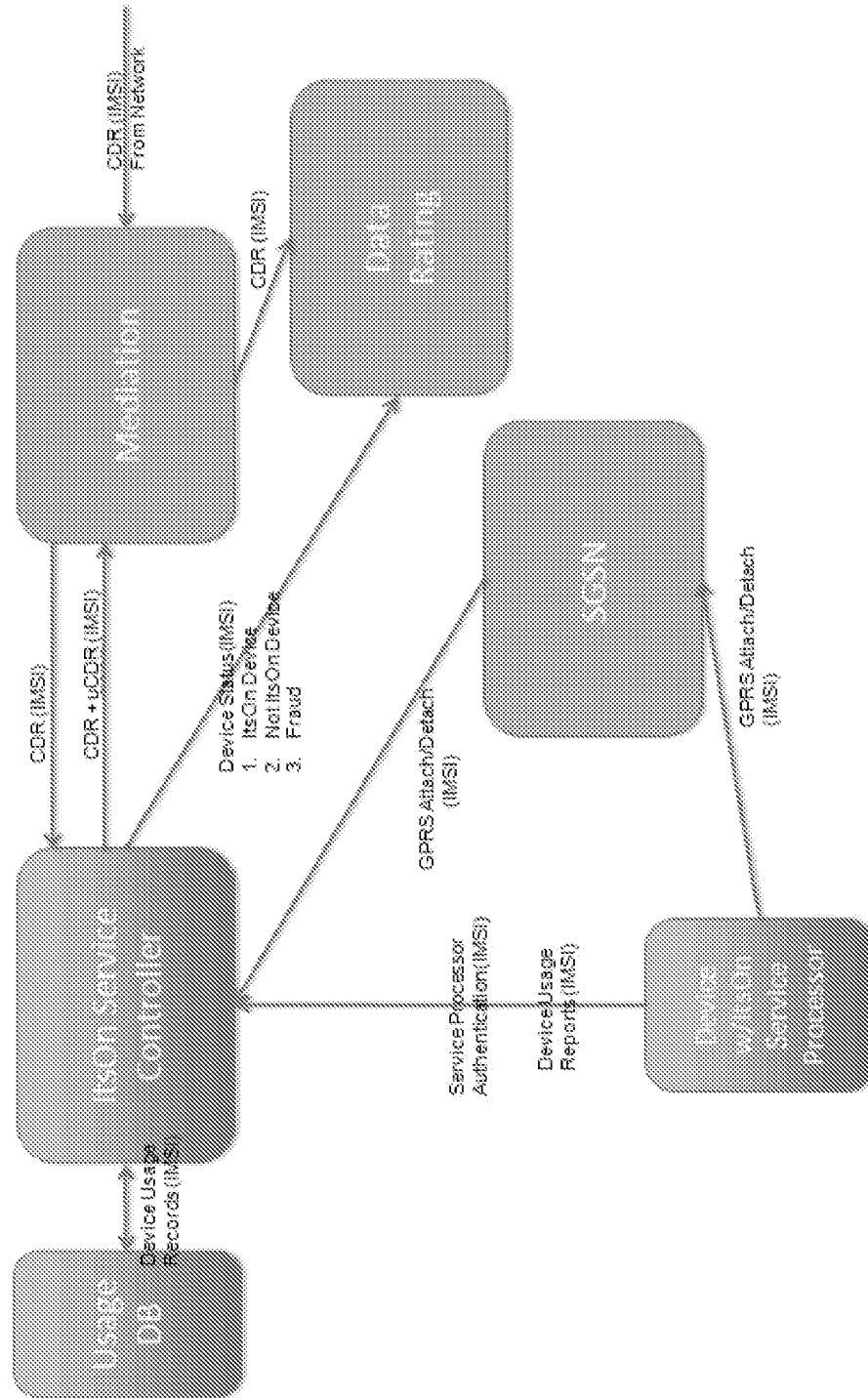
- SC receives CDRs and UDRs, counts align, charging codes are correct, but data is mis-categorized (needs FDRs to corroborate)
 - Cause: SP tampering
- SC receives CDRs and UDRs, counts align, but usage velocity within a Service Component or Service Activity is greater than the rate limit(s) set via the Control Policy
 - Cause: SP tampering
- SC receives CDRs and UDRs, counts align, but usage velocity at the Service Activity or Service Component level deviates “significantly” from average user usage velocity
 - Cause: SP tampering, Service Activity/Component usage patterns changing (e.g., service adds streaming content) (non-fraud)

Active Service Processor Verification

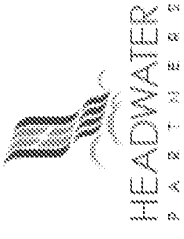


- Service Controller receives a start session message from the network
 - Could be a "Start Accounting" RADIUS message from a GGSN, AAA or PDSN, or successful "GPRS Attach" notification from an SGSN
- Service Controller sets an "Expecting Service Processor Login" timer
- If Service Controller successfully authenticates the Service Processor within the timer interval, Service Processor is deemed to be running and valid.
- If the Service Controller does not successfully authenticate the Service Processor within the timer interval, it is assumed that: 1) the device does not contain a Service Processor; or 2) the Service Processor on the device has been disabled.
 - When this event occurs, the Service Controller can either 1) trigger to the network to charge for usage at "standard" bulk rates; or 2) specify a "standard" bulk rate charging code in the CDRs sent to data mediation
- Following slides depict sample high-level implementation options of this functionality in a GSM/GRPS core data network

SGSN Notification of Start/Stop Data Session

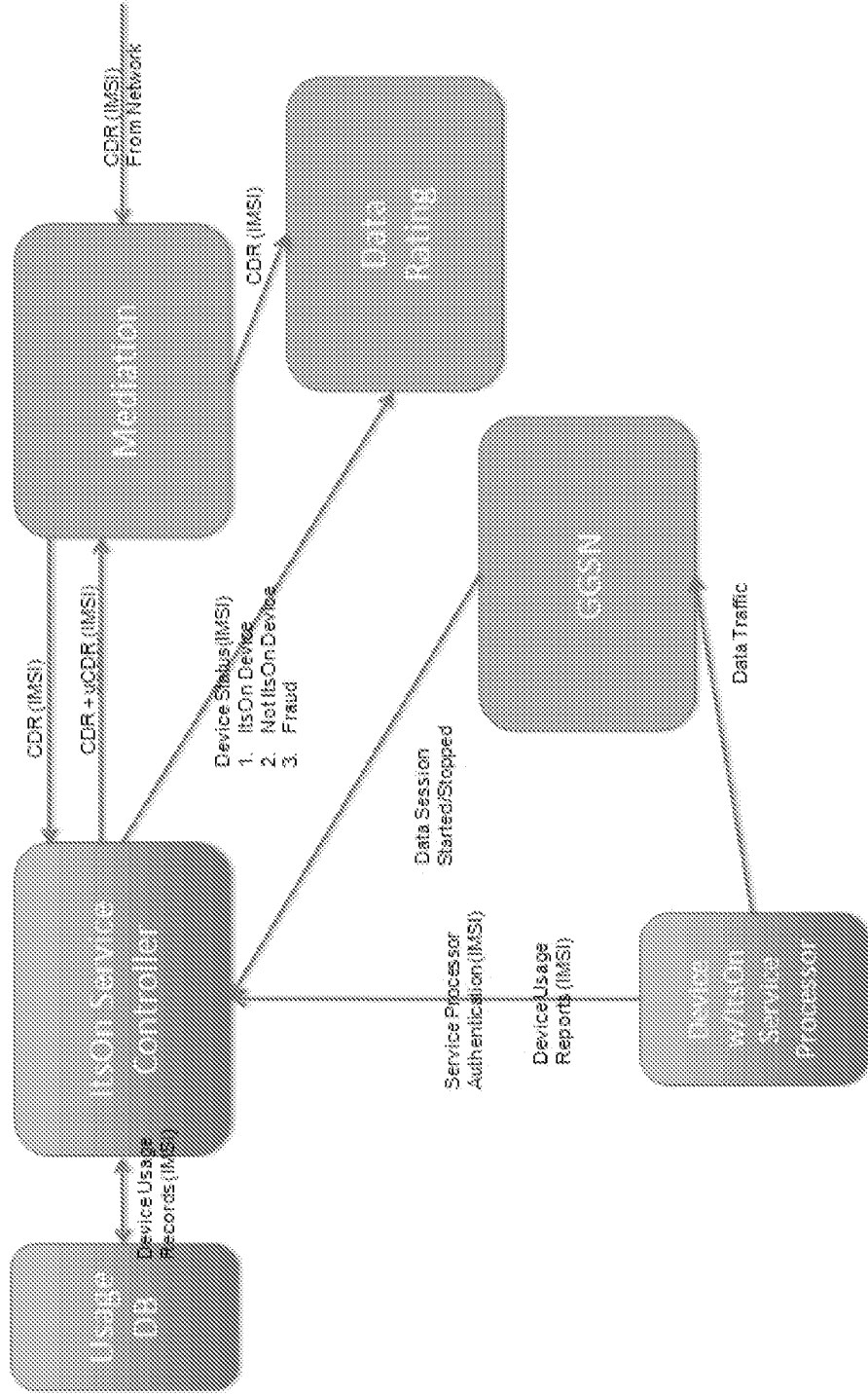


SGSN Notification of Start/Stop Data Session – Process

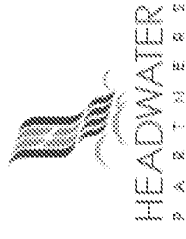


- Device attempts data session and sends GPRS Attach to SGSN
- SGSN notifies Service Controller that the device has started a data session
- Service Controller waits for a pre-determined time (e.g., one minute) to receive a login/authentication request from the Service Processor on the device
 - If the Service Controller sees the request, it sends a notification to Data Rating to indicate that the device has an Service Processor and expect Device Charging Record (DCR) reports via Data Mediation.
 - If the Service Controller does not see the request, it sends a notification to Data Rating to indicate that the device does not have an Service Processor and to process usage based on carrier CDR reports.
- Service Controller receives usage reports from the Service Processor
 - If Service Controller does not receive usage reports from the device based on time/usage intervals , it sends a notification to Data Rating to indicate that the device is in a Fraud state and usage should be billed based on carrier CDR reports.
- Data Mediation sends CDRs to Service Controller.
- Service Controller queries it's device usage database for DCRs for the device.
- Service Controller compares carrier CDR data usage byte counts vs.. DCRs.
 - If Service Controller determines that the carrier usage counts don't match the DCR usage counts (e.g. Fraud), it sends a notification to Data Rating to indicate that the device is in a Fraud state and usage should be billed based on carrier CDR reports.
- Service Controller sends carrier CDR and Service Processor DCRs to Data Mediation.
- When GPRS Detach is received by the SGSN, SGSN sends a notification to the Service Controller that the device data session is closed.

GGSN Notification of Start/Stop Data Session

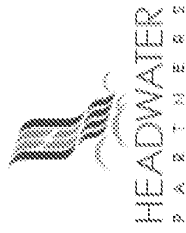


GGSN Notification of Start/Stop Data Session – Process



- * Device starts data session.
- * GGSN recognizes start of a new data session.
- * GGSN notifies Service Controller that the device has started a data session
- * Service Controller waits for a pre-determined time (e.g., one minute) to receive a login/authentication request from the Service Processor on the device
 - * If the Service Controller sees the request, it sends a notification to Data Rating to indicate that the device has an Service Processor and expect CDR reports via Data Mediation.
 - * If the Service Controller does not see the request, it sends a notification to Data Rating to indicate that the device does not have an Service Processor and to process usage based on carrier CDR reports.
- * Service Controller receives usage reports from the Service Processor
 - * If Service Controller does not receive usage reports from the device based on time/usage intervals , it sends a notification to Data Rating to indicate that the device is in a Fraud state and usage should be billed based on carrier CDR reports.
- * Data Mediation sends CDRs to Service Controller.
- * Service Controller queries it's device usage database for CDRs for the device.
- * Service Controller compares carrier CDR data usage byte counts vs.. CDRs.
 - * If Service Controller determines that the carrier usage counts don't match the DCR usage counts (e.g. Fraud), it sends a notification to Data Rating to indicate that the device is in a Fraud state and usage should be billed based on carrier CDR reports.
- * Service Controller sends carrier CDR and Service Processor CDRs to Data Mediation.
- * When GGSN determines that the data session has closed, it sends a notification to the Service Controller that the device data session is closed.

Service Processor/Service Controller Authentication

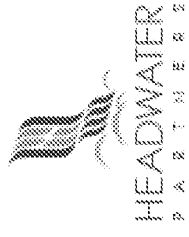


- * Device starts data session
- * Service Controller receives "Start Data Session" notification from Operator network and starts "Expected Login" timer for device
- * Service Processor on the device establishes data session with Service Controller
- * Service Controller cancels "Expected Login" timer
- * Service Controller attempts to authenticate Service Processor (algorithm TBD)
- * If authentication fails, Service Controller either 1) sends trigger to network to charge device data usage at "standard" bulk rate (implementation TBD based on operator network implementation); or 2) specifies a charging code for "standard" bulk rate on DCRs sent to operator data mediation in response to CDRs received from data mediation
- * If authentication succeeds, Service Controller marks the device as "Successfully Authenticated".
- * If "Expected Login" timer interval expires, Service Controller either 1) sends trigger to network to charge device data usage at "standard" bulk rate (implementation TBD based on operator network implementation); or 2) specifies a charging code for "standard" bulk rate on DCRs sent to operator data mediation in response to CDRs received from data mediation

SC Receives UDRs From SP After Receiving “Data Session Stopped” Trigger From Network

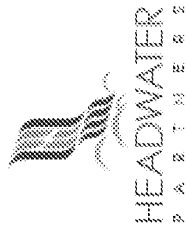
- * Authenticated SP active on operator network
- * SC receives “Data Session Stopped” trigger from operator network
- * SC marks the SP as “inactive”
- * SP attempts session with SC via operator network
- * SC detects device status as “inactive”
- * SC closes data session
- * SC marks the device a “fraudulent”
- * SC generates “potential fraud alert” to operator CRM
- * How to handle UDR from WiFi and not 3G/4G?

Service Controller Receives CDRs But Does not Receive UDRs



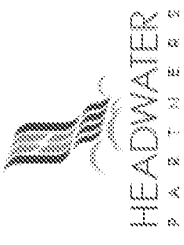
- SC receives CDR from operator data mediation
- SC attempts to verify usage by requesting all UDRs for the time period indicated in the CDR
- No UDRs with charging codes associated with 3G/4G access are returned for the time period specified by the CDR
- SC marks the device a “fraudulent”
- SC generates “potential fraud alert” to operator CRM

SC Receives CDRs and UDRs But the Usage Counts Don't Align



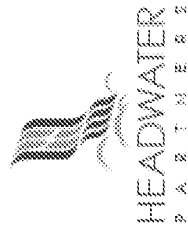
- SC receives CDR from operator data mediation
- SC attempts to verify usage by requesting all UDRs for the time period indicated in the CDR
- SC aggregates all of the usage counts associated with charging codes assigned to 3G/4G access
- SC verifies that UDR totals vs.. CDR total for the same time period are within the "fraud discrepancy" threshold.
- If the discrepancy is outside the "fraud discrepancy" threshold, SC marks the device a "fraudulent" and generates a "potential fraud alert" to operator CRM

SC Receives CDRs and UDRs but SC Detects Usage Over Charging Policy (CP) Limit(s)



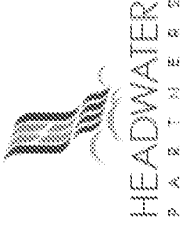
- * SC receives CDR from operator data mediation
- * SC attempts to verify usage by requesting all UDRs for the time period indicated in the CDR
- * SC aggregates all of the usage counts associated with charging codes assigned to 3G/4G access
- * SC verifies that UDR totals vs.. CDR total for the same time period are within the "fraud discrepancy" threshold.
- * Usage counts verify
- * SC computes "total usage" per active Charging Policy
- * SC verifies that aggregate usage within each active Charging Policy is under the usage cap defined by the charging policy
- * If SC detects usage within an active Charging Policy that is over the usage cap, SC marks the device a "fraudulent" and generates a "potential fraud alert" to operator CRM

SC Receives UDRs but Charging Codes do not Correspond to CP(s) for Current Active Services



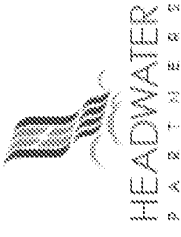
- * SC receives CDR from operator data mediation
- * SC attempts to verify usage by requesting all UDRs for the time period indicated in the CDR
- * SC aggregates all of the usage counts associated with charging codes assigned to 3G/4G access
- * SC verifies that UDR totals vs.. CDR total for the same time period are within the "fraud discrepancy" threshold.
- * Usage counts verify
- * SC detects charging codes not associated with CP(s) for current active services on the device
- * SC marks the device a "fraudulent" and generates a "potential fraud alert" to operator CRM

SC receives CDRs and UDRs, counts align, but usage velocity within a Service Component or Service Activity is greater than rate limit(s) set via CP



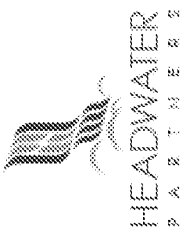
- * SC receives CDR from operator data mediation
- * SC attempts to verify usage by requesting all UDRs for the time period indicated in the CDR
- * SC aggregates all of the usage counts associated with charging codes assigned to 3G/4G access
- * SC verifies that UDR totals vs.. CDR total for the same time period are within the "fraud discrepancy" threshold.
- * Usage counts verify
- * SC detects usage associated with charging codes that have rate limits set is greater than the maximum rate limit for a continuous stream over the time period specified by the UDR (check performed on a UDR-by-UDR basis)
- * SC marks the device a "fraudulent" and generates a "potential fraud alert" to operator CRM

SC receives CDRs and UDRs, counts align, but usage velocity at the Service Activity or Service Component level deviates “significantly” from average user usage velocity



- * SC receives CDR from operator data mediation
- * SC attempts to verify usage by requesting all UDRs for the time period indicated in the CDR
- * SC aggregates all of the usage counts associated with charging codes assigned to 3G/4G access
- * SC verifies that UDR totals vs.. CDR total for the same time period are within the “fraud discrepancy” threshold.
- * Usage counts verify
- * SC detects usage velocity (bps) associated a Service Activity or Component over the time period specified by the UDR (check performed on a UDR-by-UDR basis) is “significantly” greater than average user usage velocity (bps)
- * SC marks the device a “fraudulent” and generates a “potential fraud alert” to operator CRM

CDR-based Verification Algorithm



- * Assumes CDR input contains: start time, end time, MO bytes, MT bytes
- * Collect Service Processor Charging Reports from the device, order them by network time, store on the server
- * Collect CDRs from carrier for each device, order them by network time, store on the server
- * Verify device usage is consistent with the sum of all active service usage allowances (caps)
- * Verify that usage within services is within service-level caps
- * If a service has an “associative traffic” filter
 - * Verify that the ratio of associative traffic vs.. non-associative traffic is within service policy limits
 - * Verify that the ratio of traffic between the filters in the service are within policy limits
- * For the time window specified in a CDR:
 - * Sum device usage based on all of the charging reports received from the device for the same period
 - * For windows where the CDR and the charging reports don't match exactly, compute “average usage/minute” for the charging interval and add that to the device usage total
 - * Compare totals
 - ... If comparison is within <x>% everything is OK
 - ... If Charging Report < CDR by <y>% then either Service Processor reporting bug or potential fraud
 - ... If Charging Report > CDR by <z>% then Service Processor reporting bug, carrier reporting error or failed fraud attempt
 - * Generate micro-CDRs to the carrier based on time window specified in the original CDR

FDR-based Verification Algorithm

- Assumes FDR input contains: start time, end time, remote IP/port, MO bytes, MT bytes
- Perform CDR algorithm on FDRs to get totals
- If total usage is within policy, everything is OK so far
- For each “non-bulk-allow” service reporting during that period
 - Get service policy definition
 - Translate hostnames to IP addresses
 - Count all FDR matching Policy’s IP addresses
 - Count all device usage records for the service
 - If the service has an “associative traffic” filter
 - Verify that the ratio of associative traffic vs.. non-associative traffic is within service policy limits
 - Verify totals of non-associative filters vs.. FDR counts
 - Verify that the ratio of traffic between the filters in the service are within policy limits
 - Compare totals
 - If comparison is within <x>% everything is OK
 - If Charging Report < FDR by <y>% then either Service Processor reporting bug or potential fraud
 - If Charging Report > FDR by <z>% then Service Processor reporting bug, carrier reporting error or failed fraud attempt
- If there is a “bulk-allow” service
 - Sum the charging report totals for all non-bulk services (including associative traffic)
 - Subtract charging report total from carrier FDR total
 - Compare previous result with charging records for bulk service
 - If comparison is within <x>% everything is OK
 - If Charging Report < FDR by <y>% then either Service Processor reporting bug or potential fraud
 - If Charging Report > FDR by <z>% then Service Processor reporting bug, carrier reporting error or failed fraud attempt

Behavior-based Verification Algorithm

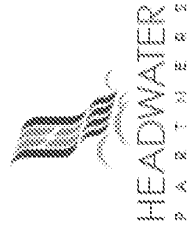


- * Service Controller keeps a database, based on service and filter that contains the following information:
 - * Service Name
 - * Filter Name
 - * Average use per time period (e.g. per day, actual value TBD)
 - * Average ratio of non-associative vs.. associative traffic for the service
 - * Expected ratio of filter matches vs.. total service usage
 - * Allowed percentage of variance (before indicating potential fraud event)
- * Service controller keeps a data warehouse to track both aggregated usage within a service and usage at the filter level to compute the above information
- * Periodically (e.g., daily), Service Controller compares user usage within a service and/or filter to the “average” usage data in the database
- * If user usage within the service/filter is outside the parameters specified for the service/filter, a “potential fraud” alert is generated
- * Example:
 - * Amazon service:
 - * 2 filters: amazon.com and images-amazon.com + associative
 - * Service cap of 10 MB/day
 - * Ratio of usage within the service is: amazon.com: 20%, images-amazon.com: 70%, associative: 10%
 - * Ratio of non-associative vs.. associative is 9:1 (or 90% non-associative)

Production Deployment Considerations

- * CDR-based Verification can be accomplished on all devices all of the time
 - * CDR feed delivered to Service Controller via operator Data Mediation
- * Behavior-based Verification can be accomplished on all of the devices on a daily basis
 - * Requires Service Processor usage reporting records only (no operator dependency)
 - * Can be augmented by FDR to validate the non-associative traffic counts within a service
- * FDR-based Verification should be used when there is a discrepancy in one or more of the following checks:
 - * Service Processor reported service-level usage is statistically higher than defined caps (e.g., Amazon Sponsored Service has a 10 MB daily cap, but the Service Processor is reporting 15 MB of usage within the daily period)
 - * CDR reported usage is statistically higher than Service Processor reported usage
 - * Average ratio of non-associative vs.. associative traffic within a service is statistically higher than expected
 - * Behavior-based Verification indicates usage within a service does not follow statistical norms
- * FDR-based Verification can also be used to randomly verify Service Processor usage reports at the service level (e.g., Amazon Sponsored Service usage reported by Service Processor matches FDR-based usage reports)
- * Ideally, retrieval of FDR's by Service Controller would be via a request mechanism (e.g., UserID, start time, end time)

Fraud Analysis Considerations

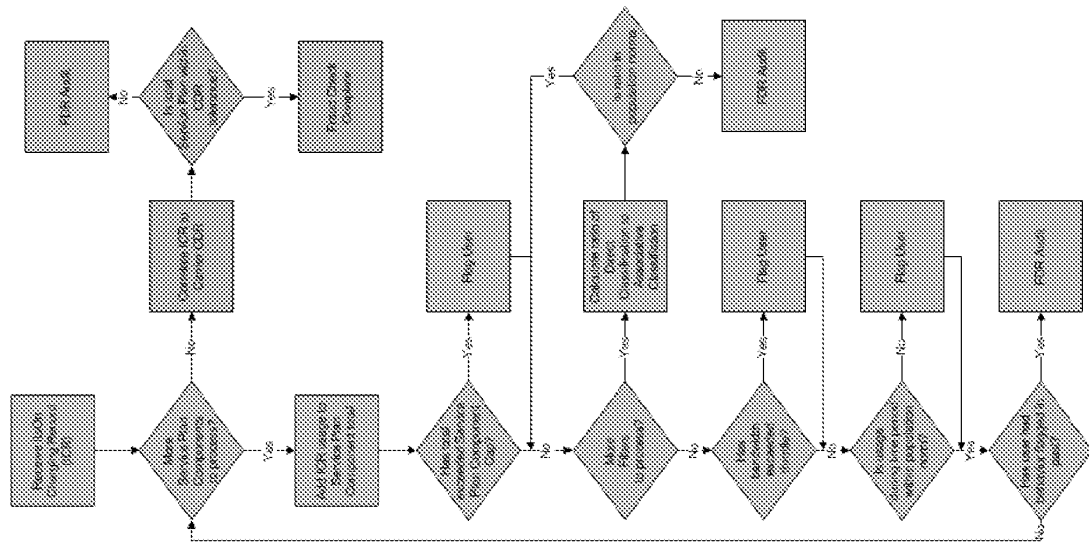


- * Device Charging Record (DCR) verification is sufficient to detect the following fraud
 - * Singly Defeating the Service Processor Controls
 - * Service cap violation detected by comparing total usage to service maximum
 - * Service throttle violation detected by comparing usage over time to expected bandwidth
 - * Singly performing Charging Record Spoofing
 - * Per filter bucketing of traffic classification method allows comparison to expected classification ratios
 - * Service level ratio of non-associative vs.. associative traffic
 - * Filter level ratio of filter matches as a percent of overall service usage vs.. expected percentage
 - * Behavioral analysis allows usage over time period comparisons to user population statistics (at the service level)
- * Carrier CDR-based verification is sufficient to detect the following fraud
 - * Disabling the Service Processor
 - * Carrier CDR's without Device Charging Records (DCR) signal DAS service interruption
 - * Defeating Service Processor Controls & Performing Charging Record Spoofing
 - * Carrier usage will show discrepancy from DCR reported usage
- * Carrier FDR-based verification is sufficient to detect the following fraud
 - * Substituting Sponsored Service charging for bulk service usage
 - * Per filter totals of non-associative classification must match FDR totals otherwise fraud has occurred

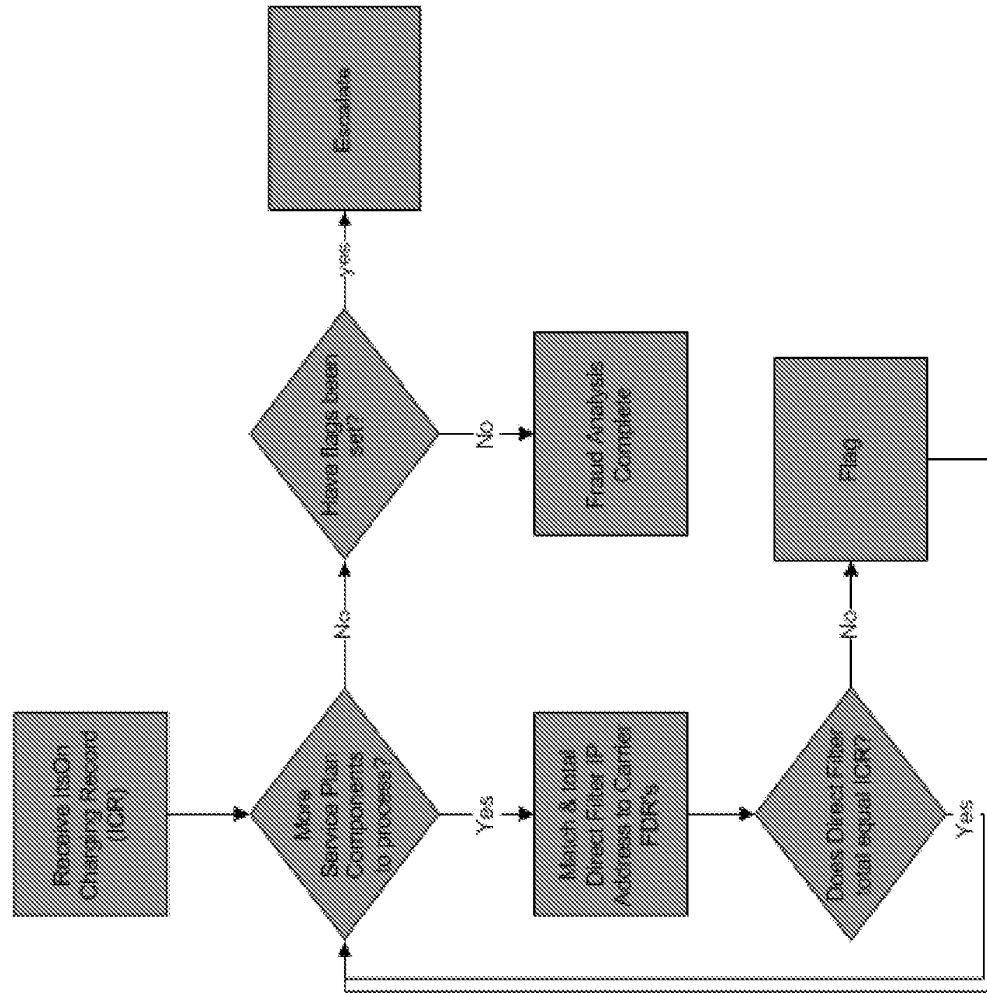
Fraud Sampling

- Analysis of every DCR must be performed on every DCR received
 - If Service Processor is running in secure method/area on device this is sufficient.
- Carrier CDR validation must be performed if Service Processor not secure
 - Based on the specific Service Plan it may be a post process activity
 - Low caps on Services limit liability
 - User will be charged for data, the fine grain mediation will be lost
 - Can be addressed in the contract
 - CDR's may not be available in near/real time
 - Roaming
 - Near-real time CDR validation can be used when DCR validation detects problem
- Carrier FDR validation only needed when fraud audit is required
 - DCR & CDR validation sufficient for all but the most sophisticated fraud attempts

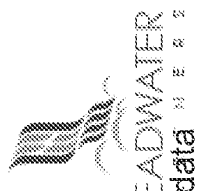
DCR & CDR Fraud Analysis Flow



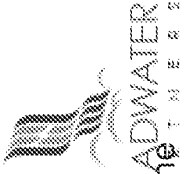
FDR Fraud Analysis Flow



Reconciliation Algorithms for Fraud Detection



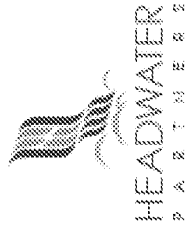
- ~ Traffic based profiling – looking at the average user (maybe by demographic and profiling their data usage by app.
 - ~ Could use a SVN based implementation with boundary analysis to determine if the data and/or app usage is invalid
- ~ App to host based profiling
 - ~ Looking at average app to host/port based profiling. Look at usage of app to host destinations use known fraud and known good profiles to train some kind of AI algorithms to detect future fraud
- ~ Profiling based on connection times and applications for a specific user. For instance if a user is active 9am-1pm and then 6-10pm as connection between 2-5 might be suspicious
- ~ Profiling of data usage and variance statistically across a large user base of same demographic and doing abnormality filtering
- ~ On open web browsing could use Markov chains or similar approaches to predict likely application usage patterns therefore data usage around those apps and see if there is fraud going on
- ~ Could perform inactivity profiling on the device to see if the data usage is similar to a human profile vs. a machine. Same could be performed on the server using CDRs or FDRs, or Start/Stop sessions.
- ~ Analysis on access across devices. If a number of devices are access obscure or lesser know hosts could be fraud or just a set of compromised devices



Additional Embodiments to Secure Sponsored SIM With DAS Enabled

1. Don't zero-rate SIM, require pre-paid or credit card or method for billing to receive a SIM and the service agreement says that if you tamper with device you are billed at a relatively high (less favorable) rate, only provide credit for sponsored or specialized (non-bulk) services via valid SP usage reports, reconciliation of valid SP micro-CDRs against network CDRs occurs in service controller and "benefit of doubt" goes to user, service usage that can not be reconciled is charged to user at agreed upon contract rate. Can offer service this way for non-SP and SP devices. Can still have an experience with non-SP device, but experience is better with SP device.
2. Give out SIM with small usage cap, up cap as micro-CDRs come through, cap increase is determined by reconciliation of valid micro-CDRs against network CDRs in the service controller and "benefit of doubt" goes to user. Usage cap system should be able to respond in a time that is relatively small with respect to minimum time required to burn through cap at max modem data rate. Does not address box of free SIMs problem. Provide credit in reconciliation by either increasing cap or reducing charge against cap. Can offer service this way for non-SP and SP devices. Can still have an experience with non-SP device, but experience is better with SP device.
 - * Additional embodiment detail: can increase cap as soon as we confirm a valid MCDR flow from SP instead of waiting for MCDR usage to offset CDRs – this allows you to stay ahead of usage report delays and make sure a small cap does not shut the guy off before we can mediate out the usage. Detail: can send in the reconciled usage after getting network CDRs, or send credit to increase cap or decrement usage before receiving network CDRs.
3. User agreement that goes with sponsored SIM says that you can only use a certain number (e.g. one) free or sponsored SIM in a given device. Monitor device IMEI or other device credential and SIM credential. Use off-hook or first CDR received condition from network for SIM credential to determine if SP has authenticated and a valid MCDR sequence has been initiated. If a given IMEI or other device credential is burning through more than one free service usage cap with multiple SIMs, then send network a suspend or deny command based on IMEI or other device credential. Can also associate with user if user is providing user credentials somehow as part of device authentication sequence.

Embodiments for Verifying That App Credentials Belongs To An App Group With A Specific App Services Access Policy or Service Plan



- * Device embodiments:
 - App credential checker - signature checker/hash checker for app that is part of the service processor, part of the OS or sits in secure OS execution – first fraud detection layer
 - Confirm app signature/hash with known signature/hash stored in: service controller, download file on device, central authority
 - Check app when it is loaded to confirm that it is the right app
 - Possibly also check app each time it is launched and/or during app operation
 - Report results to Service Controller
 - If app signature/hash is not correct, then suspend, kill, block app
 - If app signature/hash is not correct, then notify service controller
- * Network embodiments:
 - Service controller or equivalent on carrier network maintains data base of valid signatures/hashes and corresponding service policies
 - Distributes to device checker via push or pull
 - Evaluates device checker hash result sent to server
 - App credentials data base or equivalent maintains data base of valid signatures/hashes and corresponding service policies
 - Distributes to device checker via push or pull
 - Evaluates device checker hash result sent to server

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		SERVICE USAGE REPORTING RECONCILIATION AND FRAUD DETECTION FOR DEVICE ASSISTED SERVICES		
First Named Inventor/Applicant Name:		Gregory G. Raleigh		
Filer:		Michael J. Schallop		
Attorney Docket Number:		RALEP041+		
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:	8942290
Application Number:	61418509
International Application Number:	
Confirmation Number:	1496
Title of Invention:	SERVICE USAGE REPORTING RECONCILIATION AND FRAUD DETECTION FOR DEVICE ASSISTED SERVICES
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:	RALEP041+
Receipt Date:	01-DEC-2010
Filing Date:	
Time Stamp:	13:59:09
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$220
RAM confirmation Number	131
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 1.21 (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)	RALEP041plus_Provisional_Coversheet.pdf	1000017 444797bdbc4477277adca797ba60e1aab239df86	no	3
Warnings:					
Information:					
2	Specification	RALEP041plus_App.pdf	1182154 2287318ce76149d60623483989666974a769c4cf	no	40
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	29202 14faf5122a5fd5a02353ae4cbb2873c544e94041	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			2211373		
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.					