



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
61/237,753	08/28/2009		220	RALEP024+		

CONFIRMATION NO. 9155

21912

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

FILING RECEIPT



OC000000037669498

Date Mailed: 09/10/2009

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;
Rob Rightmyer, Santa Clara, CA;
Vladislav Kudelin, Los Altos, CA;

Power of Attorney:

Michael Schallop--44319

If Required, Foreign Filing License Granted: 09/03/2009

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/237,753**

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

Non-Publication Request: No

Early Publication Request: No

Title

ADAPTIVE AMBIENT 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

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).

ADAPTIVE AMBIENT SERVICES

CROSS REFERENCE TO OTHER APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 61/206,354 (Attorney Docket No. RALEP001+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed January 28, 2009, U.S. Provisional Patent Application No. 61/206,944 (Attorney Docket No. RALEP002+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 4, 2009, U.S. Provisional Application No. 61/207,393 (Attorney Docket No. RALEP003+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 10, 2009, U.S. Provisional Patent Application No. 61/207,739 (Attorney Docket No. RALEP004+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed on February 13, 2009, U.S. Provisional Patent Application No. 61/270,353 (Attorney Docket No. RALEP022+) entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING filed on July 6, 2009, and U.S. Provisional Patent Application No. __/ __, __ (Attorney Docket No. RALEP023+) entitled ADAPTIVE AMBIENT SERVICES filed on August 25, 2009, which are incorporated herein by reference for all purposes.

BACKGROUND OF THE INVENTION

[0002] With the advent of mass market digital communications, applications 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), DOCSIS, DSL, and Wi-Fi (Wireless Fidelity) becoming user capacity constrained. In the wireless case, although network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum and cell splitting 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 compared to wireless, wire line user service consumption habits are trending toward very high bandwidth applications and content 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 wireless network architecture for providing adaptive ambient service in accordance with some embodiments.

[0006] **Figure 2** illustrates a wireless network architecture for providing adaptive ambient service including a proxy server in accordance with some embodiments.

[0007] **Figure 3** illustrates a flow diagram for providing adaptive ambient service in accordance with some embodiments.

[0008] **Figure 4** illustrates a flow diagram for providing adaptive ambient service in accordance with some embodiments.

[0009] **Figure 5** illustrates a flow diagram for providing adaptive ambient service in accordance with some embodiments.

[0010] **Figure 6** illustrates a flow diagram for providing adaptive ambient service in accordance with some embodiments.

[0011] **Figure 7** illustrates a flow diagram for providing adaptive ambient service for a surf-out option in accordance with some embodiments.

DETAILED DESCRIPTION

[0012] 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.

[0013] 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.

[0014] In some embodiments, adaptive ambient services for a device (e.g., any type of device capable of communicating with a wireless network) or use of a service on a wireless network are provided. In some embodiments, an ambient experience is the user experience that is available at the time the device is sold in the event the user has not yet signed up for a service plan or the device is not sold with a prepaid service plan or other required service plan. In some embodiments, an ambient service generally refers to a set of application access, network

destinations, sources, and/or traffic control rules to enable an ambient service experience, and, in some embodiments, also includes a set of billing rules to keep an accounting of service usage for different service usages (e.g., various bill by account rules or service usage accounts). For example, the ambient experience can be defined by an ambient service profile, an ambient service plan, the other service usage activity control policies, and/or the ambient service or ambient experience bill-by-account usage accounting and/or billing policies in effect in the network, on the device, on an intermediate networking device, or any combination thereof.

[0015] For example, if a service processor (e.g., on the device, the intermediate networking device, or both) is used in large part to define the ambient service profile, then the initial provisioning and activation settings in the service processor, and possibly a service controller in the network, can define the user service upgrade offering choices, network destination access control possibilities, traffic control policies, mobile commerce transaction capabilities (e.g., which transaction websites, WAP sites or portals the user can access to purchase information, content, music, games and/or eBooks), possibly free news or weather or other modest bandwidth Internet services that are provided free of charge to entice the user into using/upgrading the service or using the transactions or viewing advertisements, what advertisements are displayed to the user or what advertisement based websites the user is exposed to, certain applications may have access while others are blocked (e.g., Internet based text services have access but email downloads do not), or various other example service capabilities related to, for example, any set of application access, destinations, sources, traffic control rules to enable an ambient service experience, and/or a set of billing rules to keep an accounting of service usage for different service usages (e.g., various bill by account rules or service usage accounts). Some specific example embodiments for the type of useful services that can be enabled with the ambient service invention disclosed herein include the following. In some embodiments, a content purchasing service (e.g., books, news, magazines, music, video, games, and mobile applications) is facilitated in which the device access is partially, largely, or entirely limited to the device or network based applications, source/destination addresses, and/or content transfers required to properly implement the service, in which other applications, source/destination addresses and/or content types are partly, largely, or entirely blocked. In some embodiments, such ambient services can have service usage monitoring and accounting that is reported for one or more individual ambient services. For example, the service usage for a

book storefront browsing and download service can be separately accounted for while other services such as a general Internet shopping or auction service, a music service, a picture upload and store/print service, a search and/or advertisement service can also each have individual service usage accounting, or in some cases, groups of services can have aggregate service usage accounting. In some embodiments, an ambient service is provided for the device prior to the time a user has paid for permanent or full time access services, which consists of a service selection platform for allowing the device user to access certain limited network functions and/or resources, and to access those network resources necessary to choose a pay-for-service plan option are provided. In some embodiments, the individual and/or group ambient service usage accounting can be transformed into one or more billing records wherein the service usage for each ambient service is billed to an entity, which can be the business entity that provides the ambient service experience and/or transaction platform, or the end user, or the central service provider, or an MVNO service provider, or a distribution partner, or an OEM, or another entity interested in paying for one or more ambient services.

[0016] In some embodiments, allowing some or all of these services, and blocking or throttling other ambient user service attempts (e.g., unpaid large file size Internet downloads or uploads or movie viewing or other access that would consume bandwidth and cause the ambient service to be a potential source of losses for the service provider) is made possible, for example, by various service profile control capabilities of the service processor and/or the service controller or using various other techniques. In some bill by account embodiments, as discussed herein, in which each service activity can, for example, be separately tracked with the service monitor and other agents and server functions to produce a billing offset that allows categorization and mediation of different billing entities (accounts) provides the capability for the service provider to individually account for the costs of each ambient service element. For example, this allows for business models in which the free access to the end user can be paid for or partially paid for by one or more service provider partners who are billed for service access using the bill by account capabilities (e.g., the transaction partners can pay for user access to their transaction experience and perhaps pay a revenue share for transaction billing, the advertising sponsored website partners pay for their access service share).

[0017] While the service control capabilities of the service processor and the bill by account service cost sharing and transaction revenue sharing in some cases can create a profitable ambient business model, in other cases, the ambient services can be a potential source of losses for the service provider. Accordingly, in some embodiments, the ambient service capabilities can be modified over time to reduce service cost to the service provider or VSP based on a variety of decision factors. For example, the user can have one level of traffic control for a period of time, and if the user has not signed up for service by the end of the period or if the user is no longer in good standing (e.g., based on various service usage criteria) for use of the service, the ambient service access is reduced (e.g., the transmission speed can be reduced or throttled, and/or the total volume of data transmitted can be reduced or throttled, possibly additionally according to time of day parameters and/or network busy state parameters) by changing the service control policy settings in the service processor, and the service level can be further reduced over time if the user continues to not sign up for service or the user does not create much transaction revenue. In some embodiments, this can limit or prevent users from “camping” on free ambient services without generating any meaningful revenue to fund the service, or viewing any advertising to fund the service. In some embodiments, a user can be throttled in such a manner until the user executes a “useful activity” (e.g., a purchase, viewing advertising, answering a questionnaire, signing up for a service, accepting a beta trial, and/or earning valued customer points), and after a useful activity occurs, then the access capabilities of the device are increased. As another example, various recursive throttling algorithms can be utilized to one or more of the service activities offered in ambient service mode so that the user experiences what full speed service is like, and if the user continues consuming appreciable bandwidth with the service activity, then the activity is throttled back to reduce costs until or unless the user selects a pay-for-service plan (or accumulates sufficient service access points as discussed below). In these examples, the service processor or service controller can issue the user a notification explaining that their service is currently free so their usage is being throttled, and if they desire to receive better service, service plan upgrade offers can be delivered to the user interface (UI). In some embodiments, the level of access (e.g., ambient service bandwidth and/or transfer limits, reachable addresses beyond the ambient service and/or bandwidth or transfer limits for open Internet usage and/or email usage, text usage) is increased as the user increases the number of useful activities (e.g., the user accumulates “service access points,”

which are then spent on access activities). It will now be apparent to one of ordinary skill in the art that the various ambient service parameters including various provisioning and activation processes used to provide an ambient service, can also be managed by various virtual service provider (VSP) apparatus and processes. For example, this allows the same service controllers and service processor solutions to be used to define a wide range of ambient experiences for various device groups or user groups that are controlled by different VSPs.

[0018] Similarly, rather than controlling ambient service profile settings using the device assisted services functions and/or VSP functions to control the service controller, service processor, provisioning and activation settings, other embodiments call for the ambient service profile settings to be controlled by various network based service activity control equipment as similarly discussed herein and/or by various intermediate networking devices. Depending on the level of service control and service monitoring sophistication (e.g., advanced DPI, TCP session aware techniques, or other service aware techniques), some, much, most or all of the above described ambient services functionality can be implemented using network based service controls and various VSP management and control techniques. Similarly, in some embodiments, service processor, provisioning and activation settings, and the ambient service profile settings can also be (at least in part) controlled by various intermediate networking devices. In some embodiments, network equipment that can provide ambient service controls include, without limitation, service gateways, routers, charging functions, HLRs, proxy servers.

[0019] Whether the ambient service monitoring and control apparatus is implemented with device assisted service techniques, network based techniques, or a combination of both, various embodiments disclosed herein provide for adaptive ambient service embodiments that address the dynamic (e.g., non-static) nature of Internet service access needs (e.g., allowable source/destination and/or application lists, blocked source/destination and/or application lists, traffic control policies for each source/destination and/or application).

[0020] Providing an ambient service profile for an ambient service can be complicated by the variable nature of network addresses and offered services such as, for example, the Internet. For example, a central service provider, MVNO provider or VSP may desire to provide ambient service access to a given web site partner's web service, in exchange for a business deal with the

website partner that motivates the service provider to provide the ambient access. In this example, the ambient access is intended to enable access (either wide open or throttled) to the website partner's collection of URLs (and possibly one or more applications) associated with the service, while blocking or differentially throttling access to other network destinations and/or applications not associated with the web site partner services. A problem can arise in this example whenever the website partner changes the addresses and/or domains associated with the website services, because any static access list and access list policies -outs makes a static list impractical. In such cases, the adaptive ambient service embodiments disclosed herein provide a solution to these problems, whether the adaptive ambient access controls and/or traffic controls are implemented with device assisted service apparatus, network based apparatus, or a combination of both.

[0021] As another example, an ambient service profile for a transaction service provider may include that service provider's domain or web site as an allowed destination. However, there may be inline advertisements provided by ad servers and/or partner sites that should also be included in the set of allowed destinations in the ambient service profile, and these may be dynamic or frequently changing. As another example, an ambient service provider may not want to allow access to sites that typically involve relatively high data usage (e.g., streaming and/or downloading of video content), while allowing other sites that result in less bandwidth intensive service usage activities. As another example, during a session a user may attempt to surf out of the ambient service, such as when the user attempts to access a website or service that is not an allowed or pre-approved destination in the ambient service profile (e.g., a search site can be the pre-approved ambient service, but the ambient service partner paying for the search service access may desire to also allow and pay for user click-through to search results and/or advertising offers, or, for example, an ambient shopping service sponsor may desire to also pay for click-through to vendor partners sites to provide a purchase transaction opportunity to the user). Moreover, the defined ambient service profile quickly stagnates as various applications and destinations, for example, change over time or on each request/usage (e.g., new applications become available and/or web site content and link changes occur daily if not hourly and/or are dynamically generated using well known web site techniques). Thus, what is needed is an adaptive technique for providing an ambient service.

[0022] Accordingly, in some embodiments, adaptive ambient services using an adaptive ambient service profile are provided. In some embodiments, a flexible efficient adaptive ambient service control is provided by using an intelligent element in the network that performs one or more of the following functions: (1) beginning with an initial list of allowable ambient service device access behaviors (e.g., addresses/URLs, applications and/or content types, in some cases with a set of traffic control policies that are differentiated as discussed above), (2) as the user accesses the ambient service, determine if the access behavior of the device is within or outside of the desired ambient service access and/or traffic control policies (e.g., determine if the access behavior is properly associated with the desired ambient services and/or service policies), (3) for those access behaviors that are within the desired ambient service policies, expand the list of allowable ambient service device access behaviors to include the new behaviors that are desired (e.g., include new sub-domains, advertising content sources, transaction partner addresses, desired surf-outs), (4) for those device access behaviors that are outside of the desired ambient service policies (e.g., are not associated or beneficially associated with the desired ambient service), expand the list of blocked or differentially throttled ambient service device access behaviors to include the new behaviors that are undesired or less desired. In some embodiments, the intelligent network element used to adapt the ambient service control is included in one or more network equipment functions (e.g., service gateways, routers, charging gateways, HLRs, AAA, base station, service controller). In some embodiments the intelligent network element used to adapt the ambient service control is included in the device and/or intermediate networking device service processor. In some embodiments, the intelligent network element used to adapt the ambient service control is included in a combination of the device (and/or intermediate networking device) and one or more network equipment functions.

[0023] In some embodiments, a flexible and efficient adaptive ambient service is provided using a baseline (e.g., a basic starting point) of an adaptive ambient service profile that includes default or previously defined (e.g., by an ambient service provider, network provider, VSP, or another entity) allowable access list and disallowed access list for the ambient service, such as to various applications, destinations, sources, traffic control rules, and/or bill by account rules or a combination thereof. In some embodiments, the ambient service profile is an automated and a self-evolving service profile using various techniques, such as those described herein.

[0024] In some embodiments, an adaptive ambient service includes providing an ambient service profile. In some embodiments, the ambient service profile includes ambient service allowed access rules and ambient service disallowed access rules. In some embodiments, the ambient service profile further includes ambient service monitored access rules, in which access to, for example, certain applications or destinations is allowed but is considered suspect or unknown, and thus, such access is monitored (e.g., until that application or destination is reclassified under an ambient service allowed access rule or ambient service disallowed access rule). In some embodiments, the ambient service allowed/disallowed/monitored access rules include IP addresses, domains (e.g., URLs for web sites), or any other unique network destination or application or source identifiers. In some embodiments, the ambient service rules provide differentiated traffic control rules. In some embodiments, the differentiated traffic control rules provide differentiated bandwidth and/or total data transfer limits according to traffic control policy elements, such as activities associated with the main ambient service functions (e.g., the main partner website or a transaction service), activities associated with secondary ambient service functions (e.g., a secondary surf-out website or a less desired service activity), activities transferring different content types, activities associated with different applications, activities based on time of day, activities based on network busy state, activities that require higher or lower QOS, and/or other activities.

[0025] In some embodiments, the ambient service allowed access rules and/or ambient service disallowed access rules are pushed to (e.g., published, at predefined times, during low service usage times or periods of low service usage activities, or upon request) the device or the intermediate device (e.g., any type of networking device capable of communicating with a device and a network, such as a femto cell, or any network communication device that translates the wireless data received from the device to a network, such as an access network) from the network (e.g., an element in the network that securely provides such data, such as a service controller for the ambient service). In some embodiments, the ambient service allowed access rules and/or ambient service disallowed access rules are pulled by (e.g., at predefined times, during low service usage times or periods of low service usage activities, or upon request) the device or the intermediate device from the network (e.g., an element in the network that securely provides such data, such as a service controller for the ambient service).

[0026] In some embodiments, the device or intermediate device includes techniques for automatically adapting the service profile based on ambient service usage and thereby updates the ambient service allowed access rules, the ambient service monitored access rules, and/or ambient service disallowed access rules locally. Device access activities that fall into the monitored access rules are those activities which are determined not to be disallowed as yet, and are allowed to take place while the intelligent adaptive service element tests the activities on the monitored access rules list to determine if they belong on the allowed access rules list, should be moved to the disallowed access rules list, or should remain on the monitored access rules list for further testing and/or observation. In this way, a useful and friendly user experience can be maintained as the adaptive ambient service rules undergo “training” to accommodate dynamic changes to the ambient service sites. The device or intermediate device can then periodically provide the updated ambient service allowed access rules, ambient service monitored access rules, and/or ambient service disallowed access rules with the network using various network communication techniques, such as those described above. In some embodiments, the device periodically synchronizes its locally stored ambient service allowed access rules, ambient service monitored access rules, and/or ambient service disallowed access rules with the network using various network communication techniques, such as those described above. In some embodiments, the training for one or more of the three lists occurs on the device. In some embodiments, the training for one or more of the three lists occurs in the network. In some embodiments, the training for one or more of the three lists occurs partly on the device and partly in the network.

[0027] In some embodiments, various techniques are used for providing the adaptive ambient service. Generally, in some embodiments, a requested use of the ambient service is analyzed to determine its association with the ambient service. In some embodiments, service usage traffic patterns are analyzed. In some embodiments, the requested use of the ambient service is determined to be associated or within the ambient service by querying the ambient service. In some embodiments, the requested used of the service is analyzed by testing the requested application, destination, or source. In some embodiments, access for an activity not already on the allowed list or the disallowed list is initially allowed (and in some embodiments, placed on the monitoring list) if the access is associated with a TCP session and/or socket already in progress that is associated with an allowed ambient service. In some embodiments, access for

an activity not already on the allowed list or the disallowed list is initially allowed (and in some embodiments, placed on the monitoring list) if the access is associated with an application already associated with and/or connected to an allowed ambient service. In some embodiments, access for an activity not already on the allowed list or the disallowed list is initially allowed (and in some embodiments, placed on the monitoring list) if the access is associated with a URL referral from an allowed URL. In some embodiments, access for an activity not already on the allowed list or the disallowed list is initially allowed (and in some embodiments, placed on the monitoring list) if the access is associated with a traffic usage pattern that is within certain pre-set parameters.

[0028] In some embodiments, various techniques are used for providing the adaptive ambient service that allows for a surf-out option (e.g., to an advertisement web site or to a web site in a search result, such as a search engine's paid search result or a search engine's organic search result). In some embodiments, a surf-out option is managed using a second set of rules in the ambient service profile for the surf-out option. In some embodiments, initial allowance of a surf-out website access is based on a main ambient website generating the surf-out (e.g. with a user click), or referring the surf-out. In some embodiment, once the main ambient service creates a surf-out that will be accounted to the main ambient service usage accounting, the surf-out website access rules are constructed according to a set of temporary allowance rules. These temporary allowance rules allow the main ambient service partner to sponsor the surf-out without the danger of the surf-out website becoming a permanent allowed ambient service that the main ambient service partner must sponsor indefinitely. The temporary surf-out rules can then consist of one or more of the three access list constructions (allowed, disallowed, monitoring) as discussed above, and similar types of adaptive rules may be applied to create one or more of the lists. Differences with the temporary surf-out rules may include limitations based on total time allowed for access to the surf-out site, rules based on limiting total data transfer or transfer bandwidth, rules on content type, rules on either allowing or disallowing a secondary surf-out (or beyond secondary to third tier etc), allowing or disallowing advertising sources. As with all other ambient access list rules, the surf-out rules can also be modified based on time of day, user priority, user class, user service plan, user useful activity points, and/or network busy state.

[0029] In some embodiments, once the content offered to the user is no longer associated with the main ambient service allowed or monitoring access list, the surf-out option can be limited to one or more the following: a limitation on the number of new user actions or choices, a limitation on the number of new web pages or portal pages, a limitation on the number of new URLs or sub-URLs, domains or sub domains, a limitation on the existence or type of advertisements, a limitation on the existence or type or size of certain content, a limitation on the number of new addresses, a limitation on the type of file downloads, a limitation on the number of file downloads, a limitation on the number of new URLs or sub-URLs or domains or sub-domains, a limitation on the activities of a given application, a limitation on the time the surf-out sequence, and/or a limitation on the total data transfer for the surf-out sequence. In some embodiments, once one or more of these established limitations are exceeded, then the surf-out sequence can be disallowed or differentially traffic controlled or throttled in some way. In some embodiments, the differential throttling successively reduces the allowed connection bandwidth for the ambient service surf-out sequence based on length of time from the point where the surf-out sequence branched from the main ambient service allowed or monitored access list, the number of user activities since the surf-out sequence branched from the main ambient service allowed or monitored access list, the number of web pages selected since the surf-out sequence branched from the main ambient service allowed or monitored access list, the total data transferred since the surf-out sequence branched from the main ambient service allowed or monitored access list, the number of new URLs or domains since the surf-out sequence branched from the main ambient service allowed or monitored access list. In some embodiments, after the surf-out activities or sequence is disallowed or differentially traffic controlled or throttled, once the user again utilizes the ambient service in a manner that is directly associated with the main ambient service allowed access list or monitoring access list, and the main ambient service experience again provides a surf-out or click through option for the same or similar surf-out experience, then the ambient surf-out limitations can be reset, removed, somehow reduced or modified so that the user may again continue the same or similar surf-out experience. In some embodiments, the surf-out sequence is stored in an access list so that the surf-out sequence is remembered the next time a similar sequence is selected from the main ambient service allowed or monitoring lists, and there may be differential service allowances applied to the surf-out sequence.

[0030] There are many advantageous application settings, service models and service business models where this type of capability to limit surf-out sequences and, in some cases, to then “refresh” or remove limitations or modify the limitations for the same or a similar surf-out sequence is valuable. An example is provided and one reasonably skilled in the art can appreciate how this can be applied to many more examples. An Internet search service provider can be an ambient service partner who sponsors ambient service access to the search website. A search website is not of much value unless the user can click-through to other web sites offered up in user click through options based on search results. Thus, it is imperative to allow the surf-out option. In some embodiments, the search provider may charge differentially for paid or sponsored search results, banners or click-throughs offered up as part of an ambient service so that the search result sponsor may help to bear the costs of ambient access in the bill by account setting. However, once the user has selected a surf-out option, it is important to make sure the surf-out sequence does not become an unlimited access allowance for the user to then surf the Internet for any purpose since this would result in completely unlimited Internet access which the search service provider and/or the search service sponsors would be billed for. Thus, in some embodiments, it is important to limit the “search sequence tree” so that the “branches” of the surf-out sequence do not progress very far from the main “trunk” of the main ambient service. The surf-out sequence “branches” can be limited in many ways, and the above embodiments are provided as examples, but at this point one skilled in the art will recognize that many more specific embodiments are possible, where a main aspect of many of the embodiments is the ability to identify and allow a surf-out sequence that is not on the main ambient service allowed or monitoring list, establish a process for temporarily allowing certain types of surf-out sequence, and then limiting the surf-out sequence branches.

[0031] In some embodiments, the surf-out option is implemented on a service processor (on a device and/or an intermediate networking device) with device assisted services. In some embodiments, the surf-out option is implemented with a combination of a service processor and a service controller. In some embodiments, the surf-out option is implemented with the various service control and monitoring verification techniques discussed elsewhere.

[0032] In some embodiments, the surf-out option is billed to a main ambient service provider or a secondary ambient service partner (e.g., based on a referring URL, such as that

provided by a search engine for a search result and/or a sponsored search result). In some embodiments, the surf-out option is restricted to the associated user session. In some embodiments, the surf-out option is restriction to the associated application. In some embodiments, the surf-out option is limited by time, data usage, or any other criteria. In some embodiments, the surf-out option is controlled or restricted based on a user's current standing (e.g., good standing). In some embodiments, the user's standing is determined based on various criteria (e.g., purchase behavior, ad click through behavior, user account standing, user browsing behavior, user service data usage, reward points, or any other criteria). In some embodiments, where a search engine is generating the click through for the surf-out, only sponsored search results where the search provider is getting paid for displaying the search result are allowed in the ambient service for search out (and/or in some embodiments only the sponsored search results are displayed at all). In some embodiments, both sponsored search and un-sponsored search are displayed and allowed.

[0033] In some embodiments, there is an identifier communicated from the device (e.g., a unique application identifier, an agent header, such as in an html header, a cookie, such as in an html cookie, or a communication handshake sequence) to the ambient service provider (e.g., a web service or web site) that identifies the device communication traffic as being associated with an ambient service. In some embodiments, the ambient service partner can interpret the identifier to ascertain that the communication is being sponsored within an ambient service model. In some embodiments, once the ambient service partner thus determines that the communication is associated with an ambient service model, any aspect of any combination of the ambient service experience, service interface (e.g., web pages or portal pages) look and feel, service interface (e.g., web pages or portal pages) complexity and/or content, offered content, content resolution, offered advertising, advertising resolution, transaction offers, transaction offer content or resolution, offered service bandwidth, total data transfer delivered, surf-out options, or other aspects of the ambient service experience served up by the ambient service partner may be tailored to optimize the offered ambient service experience. In some embodiments, the ambient service partner will optimize the offered ambient service experience in this way to reduce total bandwidth delivered in cases where the ambient service partner or some other entity is paying for the ambient service access via some aspect of the bill by account embodiments discussed elsewhere.

[0034] In some embodiments, the surf-out option is associated with a token (e.g., in a request header or some other secure or encrypted token or cookie associated with the session request) for an ambient service provider or ambient service partner, so that the surf-out session can be billed to that ambient service provider or ambient service partner, respectively. In such embodiments, the ambient service web site can receive a token request and provided that the website provides a valid token then the access to the ambient service session is allowed. In this way, a highly scalable ambient service system can be provided to any web site service partner who subscribes to the token service. In some embodiments, user information may also be included in the token request to the web site provider, so that the web site provider may determine if the user is worth paying the ambient service access fees for.

[0035] In some embodiments, a token is used to identify, enable, account for and/or establish billing for the ambient service access associated with a main ambient service and not just the surf-out sequences. In general, whenever a token enabled ambient service embodiment is discussed herein, one of reasonable skill in the art will recognize that the token ambient service technology can be utilized for either a main ambient service or an ambient service surf-out sequence.

[0036] In some embodiments, a proxy server is provided, and the ambient service provider monitors, accounts, controls, and/or optimizes the service usage through the proxy server (e.g., using the adaptive ambient service profile and/or any of the techniques described herein). In some embodiments, the proxy server implements the various techniques described herein (e.g., determines if the requested access is within the ambient service profile or belongs on the monitoring or disallowed lists, whether the requested access is compliant with a surf-out option, whether the user is in good standing, whether the requested access is associated with a referring URL, adapts one or more of the three access lists, and/or whether the requested access is associated with a token for an ambient service provider or ambient service provider). For example, in some embodiments, the proxy server manages the secure token protocol for the surf-out option, as described herein. In some embodiments, the proxy server manages the bill by account for the various adaptive ambient service techniques and/or the billing of ambient service providers/partners for the adaptive ambient service provided for the surf-out option, as described herein. Each of these various techniques are discussed in greater detail below.

[0037] In some embodiments, one or more service gateways (or router), in some cases in conjunction with a charging gateway, HLR, AAA server, base station, etc (any combination of these elements being a “gateway embodiment”), is provided, and the ambient service provider monitors, accounts, controls, and/or optimizes the service usage through a gateway embodiment (e.g., using the adaptive ambient service profile and/or any of the techniques described herein). In some embodiments, a gateway embodiment implements the various techniques described herein (e.g., determines if the requested access is within the ambient service profile or belongs on the monitoring or disallowed lists, whether the requested access is compliant with a surf-out option, whether the user is in good standing, whether the requested access is associated with a referring URL, adapts one or more of the three access lists, and/or whether the requested access is associated with a token for an ambient service provider or ambient service provider). For example, in some embodiments, a gateway embodiment manages the secure token protocol for the surf-out option, as described herein. In some embodiments, a gateway embodiment manages the bill by account for the various adaptive ambient service techniques and/or the billing of ambient service providers/partners for the adaptive ambient service provided for the surf-out option, as described herein. Each of these various techniques are discussed in greater detail below.

[0038] **Figure 1** illustrates a wireless network architecture for providing adaptive ambient service in accordance with some embodiments. As shown, Figure 1 includes a 4G/3G/2G wireless network operated by, for example, a central provider. As shown, various wireless devices 100 are in communication with base stations 125 for wireless network communication with the wireless network, and other devices 100 are in communication with Wi-Fi Access Points (APs) or Mesh 702 for wireless communication to Wi-Fi Access CPE 704 in communication with central provider access network 109. In some embodiments, each of the wireless devices 100 includes a service processor 115 (as shown), and each service processor connects through a secure control plane link to a service controller 122. In some embodiments, the network based service usage information (e.g., CDRs) is obtained from one or more network elements. As shown, an MVNO core network 210 also includes a CDR storage, aggregation, mediation, feed 118, a MVNO billing interface 122, and a MVNO billing system 123 (and other network elements as shown in Figure 1). Those of ordinary skill in the art will appreciate that various other network architectures can be used for providing adaptive ambient services, and

Figure 1 is illustrative of just one such example network architecture for which the adaptive ambient service techniques described herein.

[0039] In some embodiments, the various techniques for adaptive ambient services are performed on the device (e.g., device 100) and/or on an intermediate device (e.g., using a service processor 115 and an ambient service profile). For example, the various techniques for adaptive ambient services can be performed on a processor of the device, and the ambient service profile can be securely stored locally on the device using various techniques for secure execution and storage.

[0040] In some embodiments, the various techniques for adaptive ambient services are performed on the device or on the intermediate device with assistance or verification from the network (e.g., a service controller 122 executed on any network element, in which the service controller 122 is in secure communication with the device/intermediate device, including the service processor 115 executed on the device/intermediate device). In some embodiments, adaptive ambient services are performed on the device or on the intermediate device with assistance or verification from the network (e.g., using a service controller for maintaining a centralized set of ambient service allowed access rules and/or ambient service disallowed access rules, and a superset of all ambient service monitored access rules, working cross device population). In some embodiments, the service controller 122 or other network element(s) assist the device for implementing these techniques for adaptive ambient services (e.g., cross device, cross URL/domain usage patterns/monitoring, publishing centralized set of ambient service allowed access rules, ambient service monitored access rules, and/or ambient service disallowed access rules, including, for example, compromised and/or hacked URLs). In some embodiments, the service controller 122 or other network element(s) assist the device for implementing these techniques for adaptive ambient services by verifying the device maintained set of ambient service allowed access rules, ambient service monitored access rules, and/or ambient service disallowed access rules. In some embodiments, the service controller 122 or other network element(s) assist the device for implementing these techniques for adaptive ambient services by verifying the device monitored service usage with CDR service usage using various techniques, for example, such as those described herein. In some embodiments, the service controller 122 or other network element(s) assist the device for implementing these techniques for adaptive

ambient services by verifying the device monitored service usage by IP address (e.g., using CDR by traffic destination).

[0041] In some embodiments the various techniques for adaptive ambient services are performed on the network (e.g., a gateway, router or any other network element using, for example, deep packet inspection (DPI) on the monitored (non-encrypted) network traffic).

[0042] As shown in Figure 1, a CDR storage, aggregation, mediation, feed 118 (e.g., service usage 118, including a billing aggregation data store and rules engine) is a functional descriptor for, in some embodiments, a device/network level service usage information collection, aggregation, mediation, and reporting function located in one or more of the networking equipment boxes attached to one or more of the sub-networks shown in Figure 1 (e.g., central provider access network 109 and/or central provider core network 110), which is in communication with the service controller 122, and a central billing interface 127. As shown in Figure 1, service usage 118 is shown as a function in communication with the central provider core network 110 n. In some embodiments, the CDR storage, aggregation, mediation, feed 118 function is located elsewhere in the network or partially located in elsewhere or integrated with/as part of other network elements. In some embodiments, CDR storage, aggregation, mediation, feed 118 functionality is located or partially located in the AAA server 121 and/or the mobile wireless center/Home Location Register(HLR) 132 (as shown, in communication with a DNS/DHCP server 126). In some embodiments, service usage 118 functionality is located or partially located in the base station, base station controller and/or base station aggregator, collectively referred to as base station 125 in Figure 1. In some embodiments, CDR storage, aggregation, mediation, feed 118 functionality is located or partially located in a networking component in the central provider access network 109, a networking component in the core network 110, the central billing system 123, the central billing interface 127, and/or in another network component or function. This discussion on the possible locations for the network based and device based service usage information collection, aggregation, mediation, and reporting function (e.g., CDR storage, aggregation, mediation, feed 118) can be easily generalized as described herein and as shown in the other figures described herein by one of ordinary skill in the art. Also as shown in Figure 1, the service controller 122 is in communication with the central billing interface 123 (also sometimes referred to as the external billing management

interface or billing communication interface) 127, which is in communication with the central billing system 123. As shown, an order management 180 and subscriber management 182 are also in communication with the central provider core network 110 for facilitating order and subscriber management of services for the devices 100 in accordance with some embodiments.

[0043] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) provides a device/network level service usage information collection, aggregation, mediation, and reporting function. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) collects device generated usage information for one or more devices on the wireless network (e.g., devices 100); and provides the device generated usage information in a syntax and a communication protocol that can be used by the wireless network to augment or replace network generated usage information for the one or more devices on the wireless network. In some embodiments, the syntax is a charging data record (CDR), and the communication protocol is selected from one or more of the following: 3GPP, 3GPP2, or other communication protocols. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) includes a service usage data store (e.g., a billing aggregator) and a rules engine for aggregating the collected device generated usage information. In some embodiments, the syntax is a charging data record (CDR), and the network device is a CDR feed aggregator, and the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) also aggregates CDRs for the one or more devices on the wireless network; applies a set of rules to the aggregated CDRs using a rules engine (e.g., bill by account, transactional billing, and/or any other billing or other rules for service usage information collection, aggregation, mediation, and reporting), and communicates a new set of CDRs for the one or more devices on the wireless network to a billing interface or a billing system (e.g., providing a CDR with a billing offset by account/service). In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates a new set of CDRs for the one or more devices on the wireless network to a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates with a service controller to collect the device generated usage

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

[0044] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs rules for performing a bill by account aggregation and mediation function. In some embodiments, the service controller 122 in communication with the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device generated usage information. In some embodiments, a rules engine device in communication with the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device generated usage information.

[0045] In some embodiments, the rules engine is included in (e.g., integrated with/part of) the CDR storage, aggregation, mediation, feed 118. In some embodiments, the rules engine and associated functions, as discussed herein, is a separate function/device. In some embodiments, the service controller 122 performs some or all of these rules engine based functions, as discussed herein, and communicates with the central billing interface 127. In some embodiments, the service controller 122 performs some or all of these rules engine based functions, as discussed herein, and communicates with the central billing system 123.

[0046] In some embodiments, duplicate CDRs are sent from the network equipment to the billing system 123 that is used for generating service billing. In some embodiments, duplicate CDRs are filtered to send only those CDRs/records for devices controlled by the service controller and/or service processor (e.g., the managed devices). For example, this approach can provide for the same level of reporting, lower level of reporting, and/or higher level of reporting as compared to the reporting required by the central billing system 123.

[0047] In some embodiments, a bill-by-account billing offset is provided. For example, bill-by-account billing offset information can be informed to the central billing system 123 by providing a CDR aggregator feed that aggregates the device based service usage data feed to provide a new set of CDRs for the managed devices to the central billing interface 127 and/or the central billing system 123. In some embodiments, transaction billing is provided using similar techniques. For example, transaction billing log information can be provided to the central billing interface 127 and/or the central billing system 123.

[0048] In some embodiments, the rules engine (e.g., performed by the service usage 118 or another network element, as discussed herein) provides a bill-by-account billing offset. For example, device generated usage information (e.g., charging data records (CDRs)) includes a transaction type field (e.g., indicating a type of service for the associated service usage information). The rules engine can apply a rule or a set of rules based on the identified service associated with the device generated usage information to determine a bill-by-account billing offset (e.g., a new CDR can be generated to provide the determined bill-by-account billing offset). In some examples, the determined bill-by-account billing offset can be provided as a credit to the user's service usage account (e.g., a new CDR can be generated with a negative offset for the user's service usage account, such as for network chatter service usage, or transactional service usage, or for any other purposes based on one or more rules performed by the rules engine).

[0049] As another example, for a transactional service, a first new CDR can be generated with a negative offset for the user's service usage account for that transactional service related usage, and a second new CDR can be generated with a positive service usage value to charge that same service usage to the transactional service provider (e.g., Amazon, eBay, or another

transactional service provider). In some embodiments, the service controller 122 generates these two new CDRs, and the service usage 118 stores, aggregates, and communicates these two new CDRs to the central billing interface 127. In some embodiments, the service controller 122 generates these two new CDRs, and the service usage 118 stores, aggregates, and communicates these two new CDRs to the central billing interface 127, in which the central billing interface 127 applies rules (e.g., performs the rules engine for determining the bill-by-account billing offset).

[0050] In some embodiments, the service controller 122 sends the device generated CDRs to the rules engine (e.g., service usage 118), and the rules engine applies one or more rules, such as those described herein and/or any other billing/service usage related rules as would be apparent to one of ordinary skill in the art. In some embodiments, the service controller 122 generates CDRs similar to other network elements, and the rules (e.g., bill-by-account) are performed in the central billing interface 127. For example, for the service controller 122 to generate CDRs similar to other network elements, in some embodiments, the service controller 122 is provisioned on the wireless network and behaves substantially similar to other CDR generators on the network) as would be apparent to one of ordinary skill in the art.

[0051] In some embodiments, the service controller 122 is provisioned as a new type of networking function that is recognized as a valid and secure source for CDRs by the other necessary elements in the network (e.g., the Service Usage History/ CDR Aggregation and Mediation Server 118). In some embodiments, where the network necessary apparatus will only recognize CDRs from certain types of networking equipment (e.g. RAN Gateway 410 or Transport Gateway 420), then the Service Controller 122 can provide authentication credentials to the other networking equipment that indicate it is one of the approved types of equipment. In some embodiments, the link between the Service Controller 122 and the necessary CDR aggregation and mediation equipment is secured, authenticated, encrypted and/or signed.

[0052] In some embodiments, the CDR storage, aggregation, mediation, feed 118 discards the network based service usage information (e.g., network based CDRs) received from one or more network elements. In these embodiments, the service controller 122 can provide the device based service usage information (e.g., device based CDRs) to the CDR storage,

aggregation, mediation, feed 118 (e.g., the CDR storage, aggregation, mediation, feed 118 can just provide a store, aggregate, and communication function(s)), and the device based service usage information is provided to the central billing interface 127 or the central billing system 123.

[0053] In some embodiments, the device based CDRs and/or new CDRs generated based on execution of a rules engine as described herein is provided only for devices that are managed and/or based on device group, service plan, or any other criteria, categorization, and/or grouping, such as based on ambient service or ambient service provider.

[0054] **Figure 2** illustrates a wireless network architecture for providing adaptive ambient service including a proxy server in accordance with some embodiments. As shown, Figure 2 includes a proxy server 270 in communication with a 4G/3G/2G wireless network operated by, for example, a central provider. In some embodiments, each of the wireless devices 100 includes a service processor 115 (as shown), and each service processor connects through a secure control plane link to a service controller 122. In some embodiments, the network based service usage information (e.g., CDRs) is obtained from Radio Access Network (RAN) gateway(s) 410 and/or transport gateway(s) 420.

[0055] Referring now to the 4G/3G/2G access network as shown in Figure 2, the 4G/3G and 3G/2G base stations/nodes 125 are in communication with a 4G/3G/2G Radio Access Network (RAN) gateway 410 via a radio access network 405, which are in communication with a 4G/3G/2G transport gateway 420 via an access transport network 415. The central provider core network 110 is in network communication with the access transport network 415 (e.g., via a dedicated/leased line, and as shown, via a firewall 124). The Internet 120 is available via a firewall 124 and the transport gateway(s) 420, as shown. Also, as shown, a network apparatus provisioning system 160, order management 180, and subscriber management 182 are in communication with the central provider core network 110. As shown, a AAA server 121, a mobile wireless center/Home Location Register(HLR) 132, a DNS/DHCP 126, and CDR storage, aggregation, mediation, feed 118 are also in communication with the access transport network 415. The central billing system 123 and the central billing interface 127 are shown in communication with the central provider core network 110.

[0056] In some embodiments, the various techniques for adaptive ambient services are performed using the proxy server 270. For example, the ambient service provider can provide the proxy server 270, and the ambient service provider monitors, accounts, controls, and/or optimizes the service usage through the proxy server 270 (e.g., using the adaptive ambient service profile and/or any of the techniques described herein). In some embodiments, the central service provider provides the proxy server 270, and the ambient service provider is provided access to monitor, account, control, and/or optimize the service usage through the proxy server 270 (e.g., using the adaptive ambient service profile and/or any of the techniques described herein).

[0057] **Figure 3** illustrates a flow diagram for providing adaptive ambient service in accordance with some embodiments. At 302, the process for an adaptive ambient service begins. At 304, whether a requested access is within the ambient service profile, such as within the ambient service allowed access rules, the ambient service monitored access rules, and/or ambient service disallowed access rules, is determined. At 306, if the requested access is within the ambient service profile, then the appropriate rule is applied, such as the appropriate ambient service allowed access rule, ambient service monitored access rule, and/or ambient service disallowed access rule. At 308, if not (e.g., the requested access is not within the ambient service profile, such as not categorized within any of the ambient service profile rules), then categorize the requested access as a monitored access. In some embodiments, a requested access that is not otherwise known or categorized in the ambient service profile, is allowed and then monitored (e.g., trusted and then verified through monitoring and other techniques, such as the various other techniques described herein). At 310, if the requested access is categorized as monitored access, then allow the requested access and monitor the requested access. At 312, determine whether the requested access can now be added or blocked based on the monitored access. At 314, if the requested access can now be blocked, then block the requested access and update the ambient service profile accordingly (e.g., add the requested access to the ambient service blocked access rules). Similarly, if the requested access can now be added, then continue to allow the requested access and update the ambient service profile accordingly (e.g., add the requested access to the ambient service allowed access rules). At 316, determine whether to continue to monitor the requested access (e.g., if the requested access is still in progress, and the requested access has not been otherwise categorized as allowed or blocked ambient service access, then continue to

monitor), and if so, continue to monitor the requested access at 318. At 320, the process is repeated for the next requested access. At 322, the process is completed.

[0058] **Figure 4** illustrates a flow diagram for providing adaptive ambient service in accordance with some embodiments. At 402, the process for an adaptive ambient service begins. At 404, whether a requested access is associated with the ambient service is determined. As discussed herein with respect to Figure 4, there are various techniques for testing the association of the requested access with the ambient service. For example, at 406, whether the requested access is within the ambient service profile, such as within the ambient service allowed access rules, the ambient service monitored access rules, and/or ambient service disallowed access rules, is determined. At 408, whether the requested access to an application is tested to determine whether the application is associated with the ambient service and whether the application is currently executing. At 410, whether the requested access is within the same traffic flow as other ambient services traffic is determined (e.g., using various device based, device assisted and/or network based (such as using DPI) traffic monitoring techniques). Various other techniques can also be employed for testing the association of the requested access with the ambient service. For example, incoming traffic can be tagged (e.g., using a referred URL or an HREF or an IMAGE HTML tag); and/or the domain object management (DOM) tree can be analyzed to determine a links model of a requested web page or other techniques can be utilized to determine the links model of the requested web page. As another example, the content of the requested access (e.g., web page content) can be analyzed to determine if it is associated with the ambient service (e.g., using various content relevancy techniques). As another example, a reverse lookup to the requested network destination (e.g., URL, associated domain, sub-domain, ad server domain, or other destination or source) can be determined to test the association of the requested access with the ambient service. At 412, based on the above testing of the association of the requested access with the ambient service, determine whether the requested access can now be added or blocked based on the monitored access. At 414, if the requested access can now be blocked, then block the requested access and update the ambient service profile accordingly (e.g., add the requested access to the ambient service blocked access rules). Similarly, if the requested access can now be added, then continue to allow the requested access and update the ambient service profile accordingly (e.g., add the requested access to the ambient service allowed access rules). At 416, determine whether to continue to test the

association of the requested access with the ambient service (e.g., if the requested access is still in progress, and the requested access has not been otherwise categorized as allowed or blocked ambient service access, then continue to perform the testing analysis), and if so, continue to perform the testing analysis of the requested access at 418. At 420, the process is repeated for the next requested access. At 422, the process is completed.

[0059] **Figure 5** illustrates a flow diagram for providing adaptive ambient service in accordance with some embodiments. At 502, the process for an adaptive ambient service begins. At 504, traffic patterns of ambient service usage are analyzed. As discussed herein with respect to Figure 5, there are various techniques for testing and analyzing the ambient service usage traffic patterns to determine whether the access should be allowed, blocked, or is otherwise deemed suspicious or otherwise not known/categorized, and thus, should be monitored. For example, at 506, expected ambient service usage is compared with the actual ambient service usage (e.g., using various ambient service usage monitoring techniques, as described herein and/or using other techniques). In some embodiments, the expected versus actual ambient service usage is analyzed and can be further categorized as described below. At 508, the ambient service traffic usage is analyzed and categorized. In some embodiments, the ambient service traffic usage is categorized by total traffic, by application, by destination (e.g., URL, domain, sub-domain, or other unique identifier), by traffic flow, by network socket, by time of day, by ambient service profile categorization (e.g., ambient service allowed access, ambient service monitored access, and/or ambient service blocked/disallowed access rules), by web browsing traffic patterns, by content download patterns, and/or using any other categorizations or patterns. In some embodiments, the ambient service traffic usage is aggregated (e.g., across user or user group), and statistical analysis techniques are used to identify categories of allowable or suspect or should be disallowed access service usage requests/patterns (e.g., very infrequently requested access for high data bandwidth ambient service usage may be deemed suspect or automatically categorized as disallowed). At 510, the ambient service traffic usage is correlated with various ambient traffic profiles. For example, buying patterns can be correlated with content download patterns (e.g., a power use categorization versus a seldom/never purchases user categorization can be used to provide different ambient service profiles and/or throttling techniques based on such categorizations for the various ambient service users).

[0060] Various other techniques can also be employed for testing the ambient service usage traffic to provide adaptive ambient services as will now be appreciated by one of ordinary skill in the art in view of the embodiments and examples described herein. At 512, based on the above testing of the association of the requested access with the ambient service, determine whether the requested access can now be added or blocked based on the monitored access. At 514, if the requested access can now be blocked, then block the requested access and update the ambient service profile accordingly (e.g., add the requested access to the ambient service blocked access rules). Similarly, if the requested access can now be added, then continue to allow the requested access and update the ambient service profile accordingly (e.g., add the requested access to the ambient service allowed access rules). At 516, determine whether to continue to test the association of the requested access with the ambient service (e.g., if the requested access is still in progress, and the requested access has not been otherwise categorized as allowed or blocked ambient service access, then continue to perform the testing analysis), and if so, continue to perform the testing analysis of the requested access at 518. At 520, the process is repeated for the next requested access. At 522, the process is completed.

[0061] **Figure 6** illustrates a flow diagram for providing adaptive ambient service in accordance with some embodiments. In some embodiments, a combination of various techniques are used for providing adaptive ambient services, such as those described below with respect to Figure 6. In some embodiments, a subset of these various techniques are employed using various combinations of such techniques or individual techniques. At 602, the process for an adaptive ambient service begins. At 604, whether a requested access is associated with the ambient service is determined (e.g., as similarly described above with respect to Figure 4). At 606, the ambient service usage is analyzed (e.g., as similarly described above with respect to Figure 5). At 608, the ambient service is queried to verify the requested access (e.g., if the requested access is not in the ambient service profile or otherwise suspicious or covered by a monitored access rule, then the ambient service can be queried for more information as to whether this requested access is associated with the ambient service usage or should otherwise be allowed). In some embodiments, various requested accesses can be allowed for certain users or for certain requests to allow for monitoring or testing but denied for other users/requests. In some embodiments, the device or intermediate device based ambient service profile settings (e.g., local ambient service profile rules, categorizations, settings, and/or other data) are provided

to the ambient service provider for further analysis and to correlate various access requests with the ambient service (e.g., monitored access requests can be confirmed as approved or not, that is associated with the ambient service or otherwise permissible, or not, as deemed by the ambient service provider using various techniques). At 610, the source of the requested access is analyzed. In some embodiments, the source of the requested access is itself tested using various techniques (e.g., search engine/web crawler techniques or DOM techniques to determine whether certain web based requests are associated with the ambient service; or to verify with a secondary source such as an ad server; or to verify ownership of certain network domains by the ambient service provider or associated advertiser).

[0062] Various other techniques can also be employed for providing adaptive ambient services as will now be appreciated by one of ordinary skill in the art in view of the embodiments and examples described herein. At 612, based on the above testing of the association of the requested access with the ambient service, determine whether the requested access can now be added or blocked based on the monitored access. At 614, if the requested access can now be blocked, then block the requested access and update the ambient service profile accordingly (e.g., add the requested access to the ambient service blocked access rules). Similarly, if the requested access can now be added, then continue to allow the requested access and update the ambient service profile accordingly (e.g., add the requested access to the ambient service allowed access rules). At 616, determine whether to continue to test the association of the requested access with the ambient service (e.g., if the requested access is still in progress, and the requested access has not been otherwise categorized as allowed or blocked ambient service access, then continue to perform the testing analysis), and if so, continue to perform the testing analysis of the requested access at 618. At 620, the process is repeated for the next requested access. At 622, the process is completed.

[0063] **Figure 7** illustrates a flow diagram for providing adaptive ambient service for a surf-out option in accordance with some embodiments. At 702, the process for an adaptive ambient service begins. At 704, whether a requested access is associated with the ambient service is determined. As discussed herein with respect to Figure 7, there are various techniques for testing the association of the requested access with the ambient service. For example, at 706, whether the requested access is within the ambient service profile, such as within the ambient

service allowed access rules, the ambient service monitored access rules, and/or ambient service disallowed access rules, is determined. At 708, whether the requested access to an application is tested to determine whether the application is associated with the ambient service and whether the application is currently executing. At 710, whether the requested access is within a surf-out option is determined (e.g., using surf-out option based techniques, as described herein). At 712, based on the determination of the association of the requested access with the ambient service (e.g., using various association techniques, as described herein), determine whether the requested access can now be added or blocked based on the monitored access. At 714, if the requested access can now be blocked, then block the requested access and update the ambient service profile accordingly (e.g., add the requested access to the ambient service blocked access rules). Similarly, if the requested access can now be added, then continue to allow the requested access and update the ambient service profile accordingly (e.g., add the requested access to the ambient service allowed access rules). At 716, determine whether to continue to test the association of the requested access with the ambient service (e.g., if the requested access is still in progress, and the requested access has not been otherwise categorized as allowed or blocked ambient service access, then continue to perform the testing analysis), and if so, continue to perform the testing analysis of the requested access at 718. At 720, the process is repeated for the next requested access. At 722, the process is completed.

[0064] 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.

[0065] WHAT IS CLAIMED IS:

CLAIMS

1. A system, comprising:
a processor of a communications device configured to:
implement an ambient service profile for assisting control of the communications
5 device use of an ambient service on a network, wherein the ambient service profile
includes a plurality of service policy settings, and wherein the ambient service profile is
associated with an ambient service plan that provides for initial access to the ambient
service with limited service capabilities prior to activation of a new service plan;
monitor use of the first service based on the ambient service profile; and
10 adapt the ambient service profile based on ambient service usage;
a memory of the communications device coupled to the processor and configured to
provide the processor with instructions.
2. The system recited in claim 1, wherein the ambient service profile is implemented by a
proxy server.
- 15 3. The system recited in claim 1, wherein the ambient service plan allows for access to the
ambient service with limited service capabilities that are limited based on one or more of the
following: period of time, network address, service type, content type, application type,
bandwidth, and data usage.
4. The system recited in claim 1, wherein the ambient service plan is a low cost or free trial
20 service plan that is bundled or provided as an option for purchase at a point of sale of the
communications device.
5. The system recited in claim 1, wherein the communications device is activated prior to a
point of sale of the communications device, and the ambient service plan is associated with the
communications device during activation.
- 25 6. The system recited in claim 1, wherein the ambient service plan is associated with the
communications device during one or more of the following: a manufacture of the
communications device, a distribution of the communications device, or a point of sale of the
communications device.

7. The system recited in claim 1, wherein the ambient service plan includes an option to purchase a new service plan for the communications device, wherein the new service plan includes additional service capabilities.

8. The system recited in claim 1, wherein the ambient service profile is programmable by one or more of the following: a manufacturer, a service provider, a distributor, a virtual service provider, and a device manager.

9. The system recited in claim 1, wherein the ambient service is a transaction based service, wherein service usage for the ambient service by the communications device is not billed, and wherein electronic commerce based transactions performed using the communications device are billed as transaction based charges.

10. The system recited in claim 1, wherein the ambient service is a transaction based service, wherein electronic commerce based transactions performed using the communications device are billed as transaction based charges, and wherein a portion or all of service usage costs are billed to one or more of the following: an advertiser, a transaction provider, a mobile virtual network operator, a virtual service provider, and an ambient service provider.

11. The system recited in claim 1, wherein the communications device is a mobile communications device, and the first service includes one or more Internet based services.

12. The system recited in claim 1, wherein the communications device is a mobile communications device, and the first service includes one or more Internet based services, and wherein the mobile communications device includes one or more of the following: a mobile phone, a PDA, an eBook reader, a music device, an entertainment/gaming device, a computer, laptop, a netbook, and a home networking system.

13. The system recited in claim 1, wherein the communications device includes a modem, and the processor is located in the modem.

14. The system recited in claim 1, wherein the first service policy includes one or more of the following: access control settings, traffic control settings, billing system settings, user notification with acknowledgement settings, user notification with synchronized service usage information, user privacy settings, user preference settings, authentication settings, admission

control settings, application access settings, content access settings, transaction settings, and network or device management communication settings.

15. The system recited in claim 1, wherein the implementation of the first service profile is verified based on one or more of the following: device based service usage information and
5 network based service usage information.

16. The system recited in claim 1, wherein the processor of the communications device is further configured to:

determine whether a requested access should be allowed based on the ambient service profile;

10 determine whether a requested access should be blocked based on the ambient service profile; and

determine whether a requested access should be allowed and monitored based on the ambient service profile.

17. The system recited in claim 1, wherein the processor of the communications device is
15 further configured to:

determine whether a requested access should be allowed based on the ambient service profile;

determine whether a requested access should be blocked based on the ambient service profile; and

20 determine whether a requested access should be allowed and monitored based on the ambient service profile,

wherein the ambient service profile includes a surf-out option.

18. The system recited in claim 1, wherein the processor of the communications device is further configured to:

25 modify the ambient service profile based on updates received from the network.

19. The system recited in claim 1, wherein the processor of the communications device is further configured to:

monitor a requested access based on the ambient service profile; and

adapt the ambient service profile based on the monitored access, wherein the ambient service profile includes a set of ambient service allow access, ambient service monitor access, and ambient service block access rules.

20. The system recited in claim 1, wherein the processor of the communications device is
5 further configured to:

monitor a requested access based on the ambient service profile using one or more of the following techniques: determine whether the requested access is associated with the ambient service, analyze ambient service usage, query the ambient service to verify the requested access, and test the source of the requested access; and

10 adapt the ambient service profile based on the monitored access, wherein the ambient service profile includes a set of ambient service allow access, ambient service monitor access, and ambient service block access rules.

21. A method, comprising:

15 implementing an ambient service profile for assisting control of the communications device use of an ambient service on a network, wherein the ambient service profile includes a plurality of service policy settings, and wherein the ambient service profile is associated with an ambient service plan that provides for initial access to the ambient service with limited service capabilities prior to activation of a new service plan;

20 monitoring use of the first service based on the ambient service profile; and
adapting the ambient service profile based on ambient service usage.

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

25 implementing an ambient service profile for assisting control of the communications device use of an ambient service on a network, wherein the ambient service profile includes a plurality of service policy settings, and wherein the ambient service profile is associated with an ambient service plan that provides for initial access to the ambient service with limited service capabilities prior to activation of a new service plan;

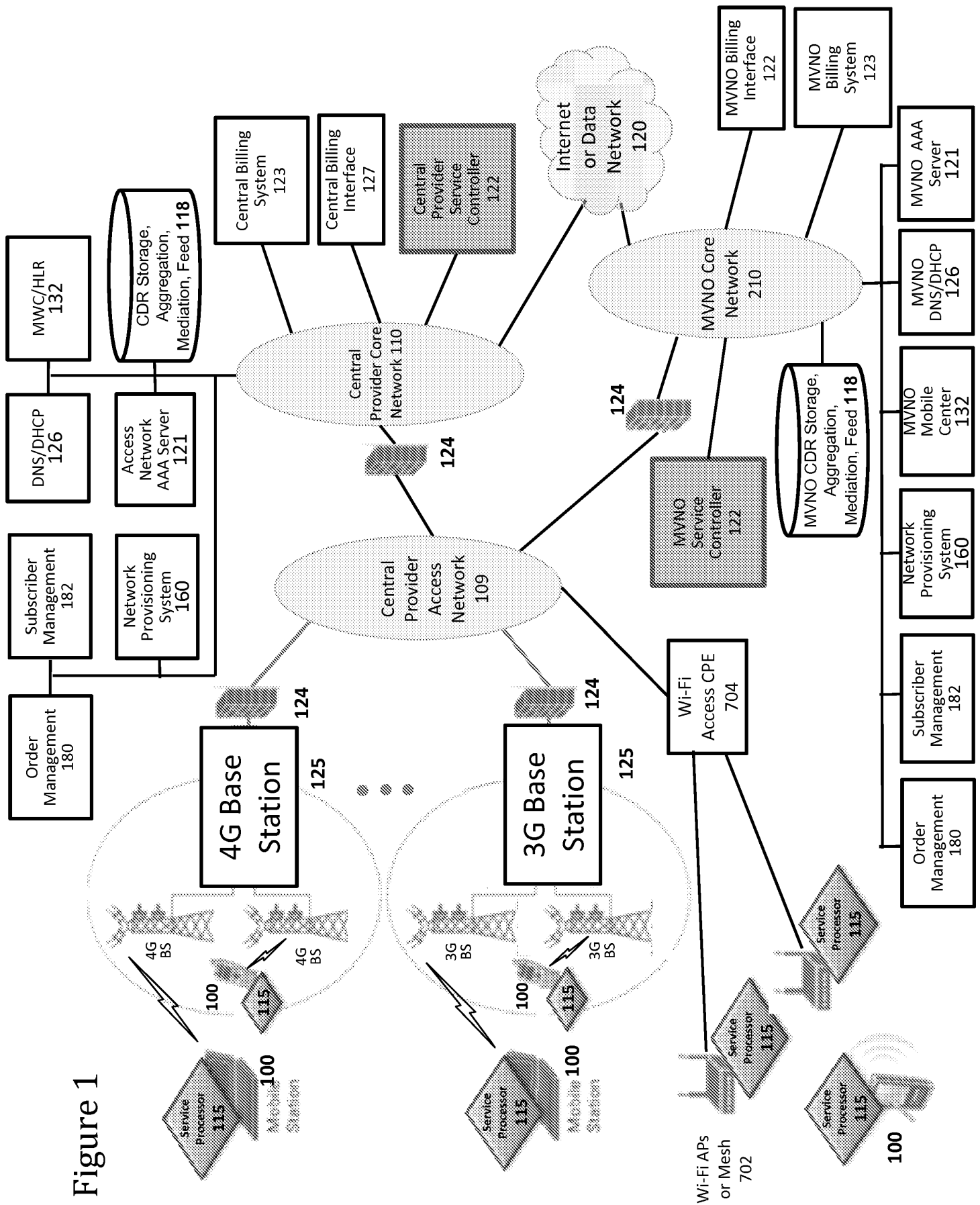
30 monitoring use of the first service based on the ambient service profile; and
adapting the ambient service profile based on ambient service usage.

ADAPTIVE AMBIENT SERVICES

ABSTRACT OF THE DISCLOSURE

[0066] Adaptive ambient services are provided. In some embodiments, an adaptive ambient service includes providing an ambient service profile. In some embodiments, an ambient service includes implementing an ambient service profile for assisting control of the communications device use of an ambient service on a network, in which the ambient service profile includes a plurality of service policy settings, and in which the ambient service profile is associated with an ambient service plan that provides for initial access to the ambient service with limited service capabilities prior to activation of a new service plan; monitoring use of the first service based on the ambient service profile; and adapting the ambient service profile based on ambient service usage.

Figure 1



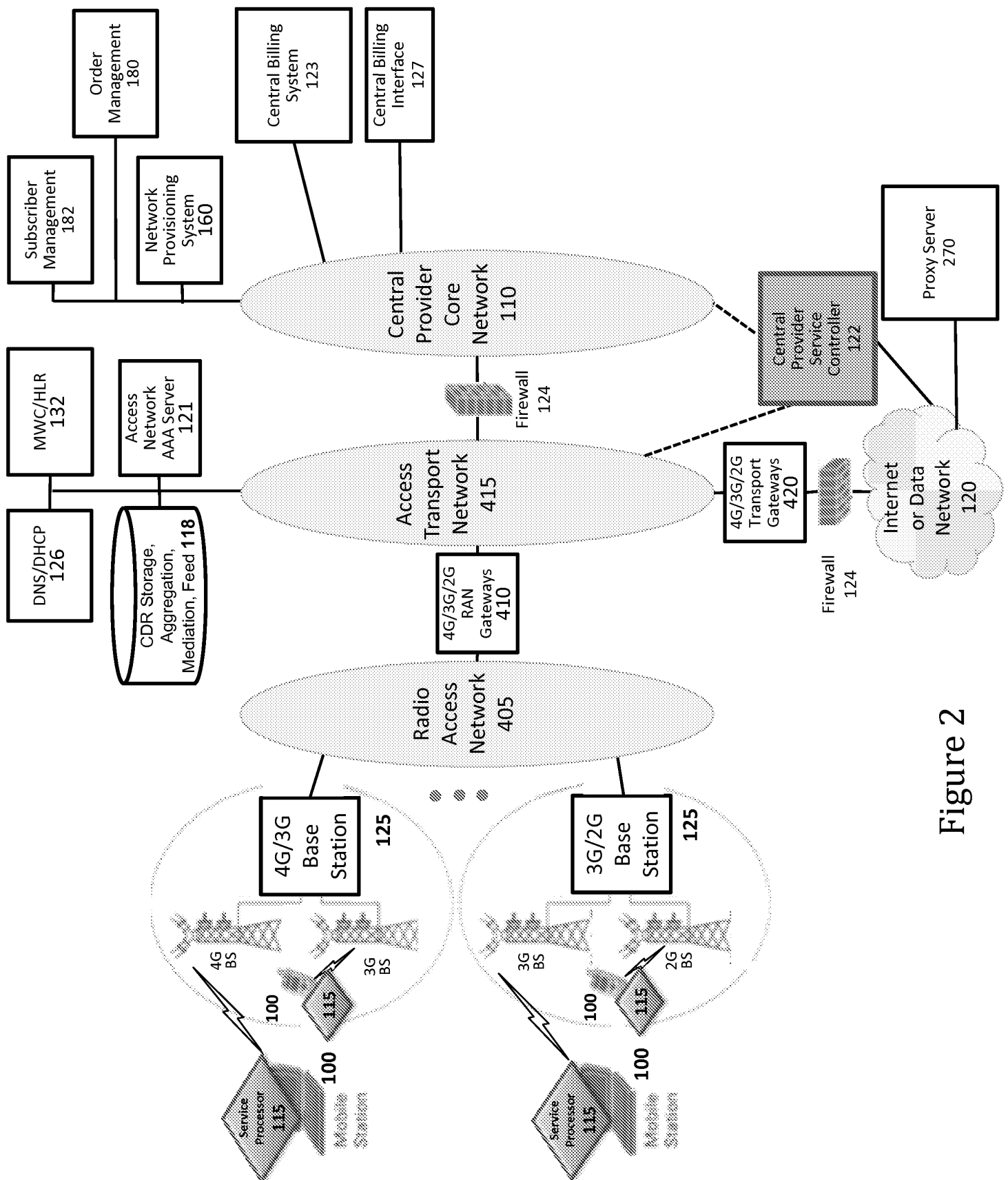


Figure 2

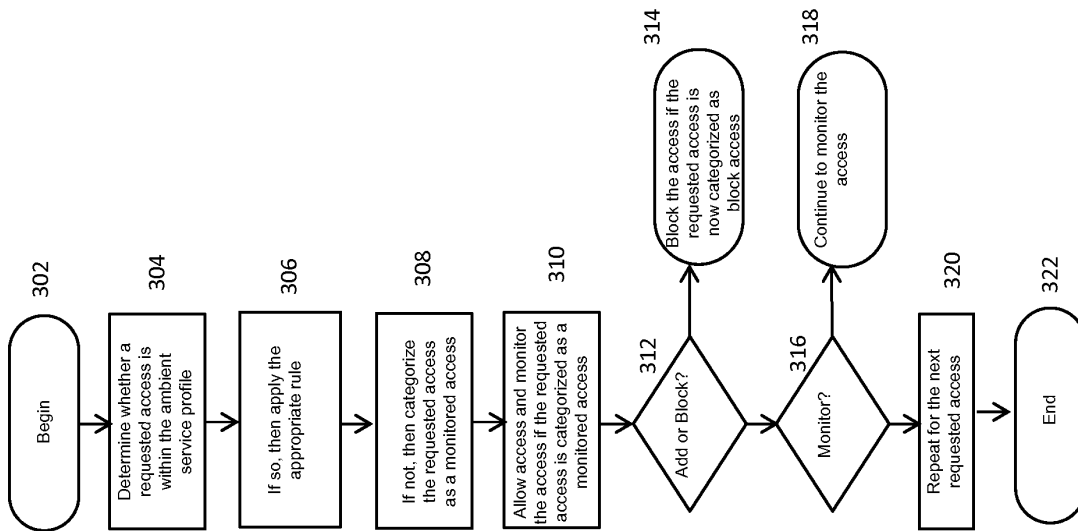


Figure 3

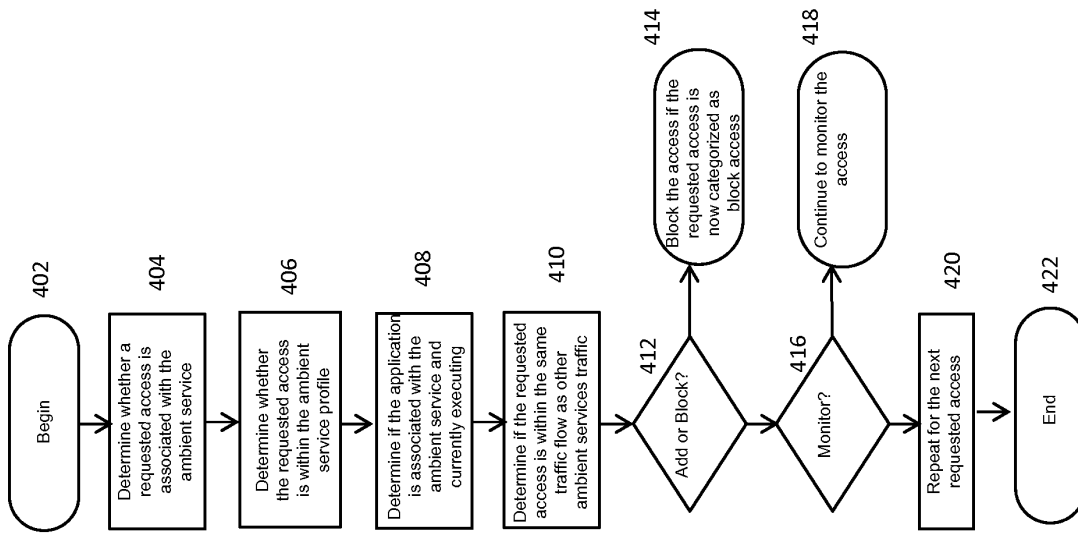


Figure 4

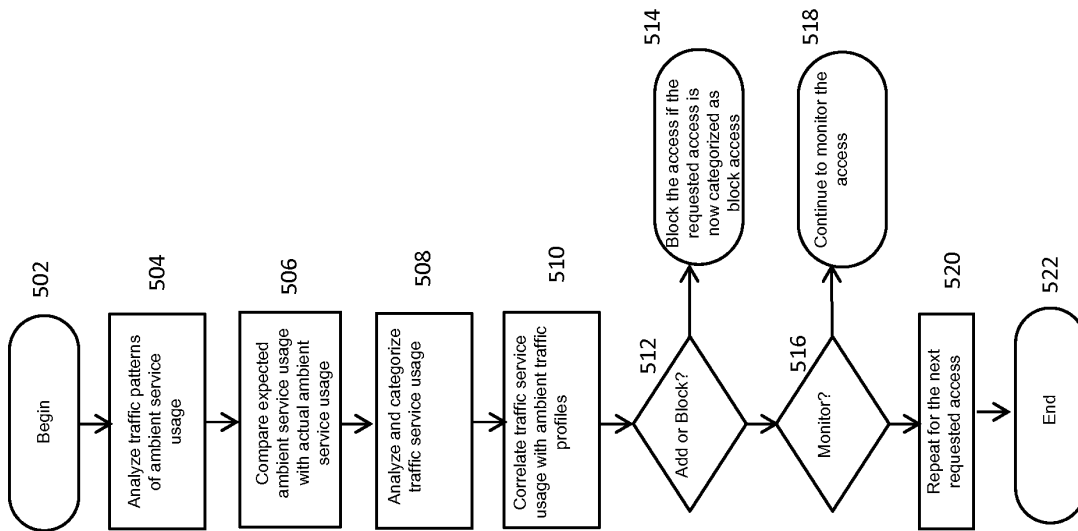


Figure 5

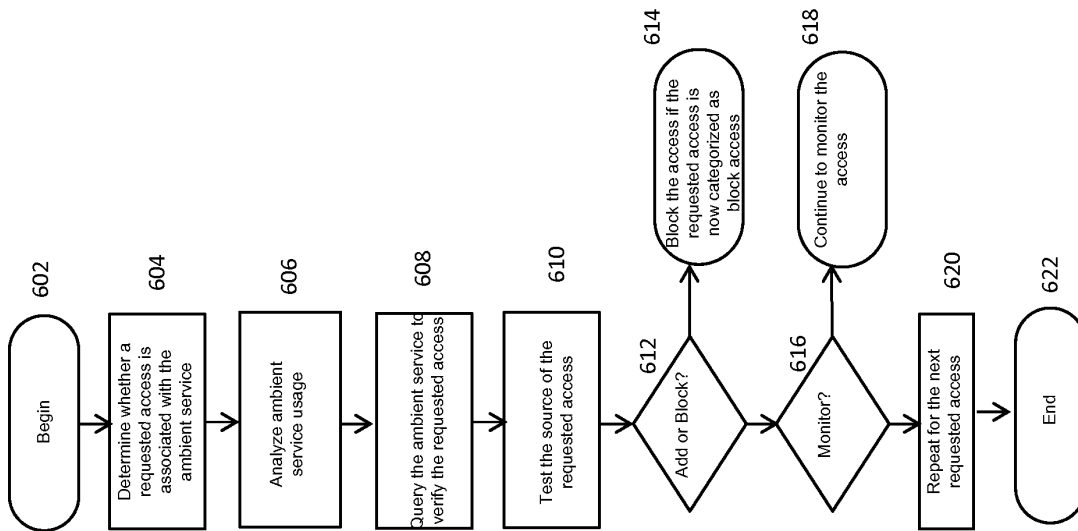


Figure 6

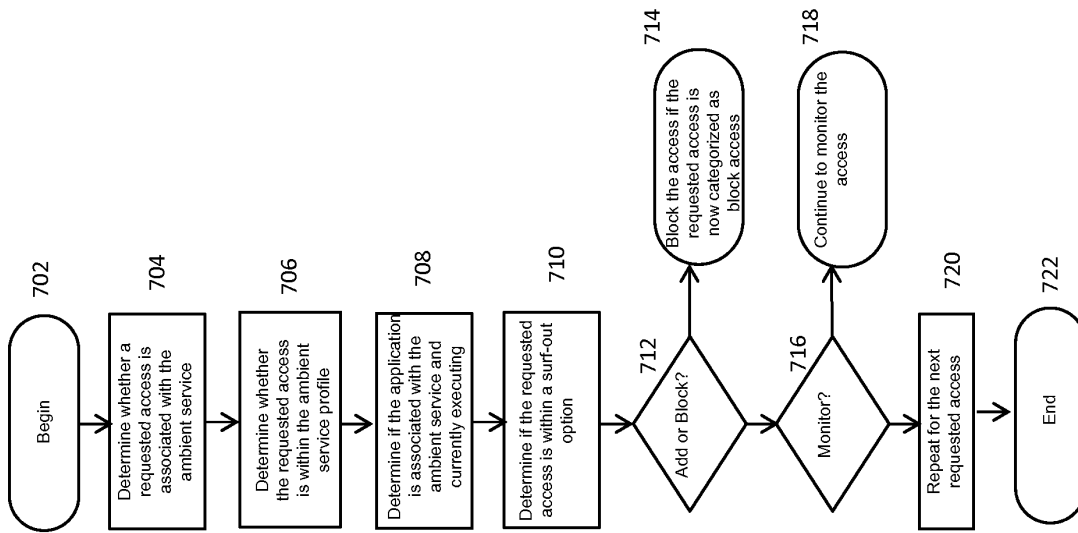


Figure 7

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

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

Inventor 2

Given Name	Middle Name	Family Name	City	State	Country i
Rob		Rightmyer	Santa Clara	CA	US

Inventor 3

Given Name	Middle Name	Family Name	City	State	Country i
Vladislav		Kudelin	Los Altos	CA	US

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

ADAPTIVE AMBIENT SERVICES

Attorney Docket Number (if applicable)

RALEP024+

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)	2009-08-28
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 another 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.

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		ADAPTIVE AMBIENT SERVICES		
First Named Inventor/Applicant Name:		Gregory G. Raleigh		
Filer:		Michael J. Schallop/Veronica Pula		
Attorney Docket Number:		RALEP024+		
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:	5972033
Application Number:	61237753
International Application Number:	
Confirmation Number:	9155
Title of Invention:	ADAPTIVE AMBIENT 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:	RALEP024+
Receipt Date:	28-AUG-2009
Filing Date:	
Time Stamp:	12:31:55
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$220
RAM confirmation Number	7389
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		RALEP024plus_APP.pdf	166704	yes	36
			bb7c7db4c58ff6b32db90b4fa2d83a89188e68b6		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	31	
	Claims		32	35	
	Abstract		36	36	
Warnings:					
Information:					
2	Drawings-only black and white line drawings	RALEP024plus_Figures.pdf	644563	no	7
			b2f4754de38f902b7b2f5dd2bf042595a1671364		
Warnings:					
Information:					
3	Provisional Cover Sheet (SB16)	RALEP024plus_Provisional_Coversheet_Efile.pdf	1018028	no	3
			aed45f27bf9bbbd009b831a6d703f41a9961202c		
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	29237	no	2
			164506048ca65ffc4ef1d6be85c229c08c490ebf		
Warnings:					
Information:					
Total Files Size (in bytes):			1858532		

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.