INTERACTIVE CONTROL OF ACCESS TO SERVICES AND CAPABILITIES OF A MOBILE DEVICE

BACKGROUND

[0001] The use of wireless communications systems is well known for transmitting information between fixed stations and one or more geographically dispersed mobile receivers. For example, satellite communications systems have been used in the trucking industry for years to provide messaging and location information between fleet owned dispatch centers and their respective tractor-trailer vehicles. Systems exist where a company, hereinafter referred to as a contractee, provides equipment and services which incorporate wireless telephone services. The contractee can bundle equipment and services, including value added applications and/or products and provide, resell, lease or rent them to employees, customers, contractors, etc.

[0002] The contractee may wish to limit the availability of certain ones of the bundled services. Until now, no system or method allowed contractee control of access to bundled services. Up till now, this control was always held by the telecommunications service provider.

[0003] Phone service providers generate much income through providing services to user mobile stations (MS) which route traffic through a mobile switching center (MSC). The MSC provides services and coordination between mobile users and external communications networks. This backbone switch is also a primary billing vehicle of a telecommunications service provider allowing a range of billing schemes based on time of day, demand, volume of data, etc. A need exists to allow mobile communications users, particularly those associated with fleet communications, to control costs and access to certain systems such as ring back tones, three-way calling, call waiting, voice mail, etc. while avoiding the costly billing of the phone company's MSC.

[0004] There has been a long-standing trend toward distributed processing. For instance, attempts are underway to avoid the MSC-the central telco switch. The MSC is problematic for many reasons. For instance, it typically takes up space on

many floors; it has to be cooled, etc. Attempts have been underway to make a packet switch with distributed processing. In this manner, attempts have been made to reduce the footprint (e.g., power consumption, size, computing requirements) while trying to increase processing capacity. Reducing the footprint currently is addressed by spreading functionality over several switches. For instance, it is now common to use what are referred to as intelligent peripherals. As an example, some telecommunications companies handle call traffic by routing calls to one city several hundred miles from base stations connected by fiber optics in another city through a central station. As the trend toward distributed switches and switching continues even functions such as the Home Location Register (HLR) and Visiting Location Register (VLR) that used to be a part of the MSC are now located separate from the MSC.

[0005] A need exists to allow business owners, equipment rentals, etc. to control of access to features by mobile communications equipment such as mobile phones, etc. A need also exists to control of access to features to mobile equipment in an environment with a reduced footprint.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] **FIG. 1** is a diagram depicting the interaction of processes, such as a parent process known as Mobile Feature Control Application (MFCA) within a mobile station (MS).

[0007] **FIG. 2** illustrates the mobile feature control application daemon.

[0008] **FIG. 3** illustrates a communication network including each MS being operable in accordance with that depicted by the diagram of **FIG.1**.

[0009] **FIG. 4** illustrates a block diagram of one aspect of a preferred embodiment, wherein a package of services or service features is associated with a mobile communications terminal (MCT).

[00010] **FIG. 5** illustrates a diagram of another aspect of a preferred embodiment wherein software files or code are downloaded to an MCT in response to a service request

[00011] **FIG. 6** illustrates a diagram showing a system view of one embodiment.

[00012] **FIG. 7** illustrates ATM cell traveling along a virtual path through routers in an ATM to its destination.

[00013] **FIG. 8** illustrates a diagram of one embodiment showing a mobile communications terminal (MCT) carried by vehicle which may be operating in conjunction with a dispatcher controlling a fleet of vehicles.

[00014] **FIG. 9** illustrates a block diagram of an exemplary MCT.

[00015] **FIG. 10** illustrates a diagram of one embodiment, showing an MCT on a truck that can receive code or files downloaded from a package of features in conjunction with an authorization server.

[00016] Applicable reference numerals have been carried forward.

DETAILED DESCRIPTION

[00017] In one preferred embodiment, a system determines authorization for access to one or more services grouped together as a package of services (hereinafter referred to as a package). The package of services replicate the vertical features of a conventional mobile switching center (MSC) which is a telecom switch that provides coordination of call setup and telecom services. The system offers business proprietors, contractors for telecommunication services, and service providers the ability to authorize users, particularly users of mobile communication terminals, access to package services. The implementation of the aforementioned system may be accomplished in one aspect using a mobile feature control application daemon operable in an embedded operating system within a mobile station (MS). The MS as referenced herein may include a mobile phone, a smart phone, a personal digital assistant with wireless capabilities, a desktop computer, a portable computer (e.g., laptop or notebook computer) with wireless capability (802.11 local area network connectivity (e.g. WiFi)), a pager or other personal communications device.

[00018] **FIG. 1** is a diagram depicting the interaction of processes, such as a parent process known as Mobile Feature Control Application (MFCA) **2** within a MS. MFCA **2** listens on a port for service requests 12 from Mobile Operating System (MOS) **4**. For instance, in connection with receiving a service request which results from an incoming command/call **6** to update (modify or control) a feature list

(not shown) in MFCA database **8**, MFCA **2** spawns (as indicated by the arrows from **2** to **10**) a MFCA child process **10** in response to service request **12** initiated by a user or program action. Similarly, more service requests **12** may result in spawning MFCA child processes **10** as show in **FIG. 1**. As a consequence thereof, multi-process handling of incoming service requests may be provided. In one aspect, another type of service request may result from MS entries **14**, e.g. keypad entries (e.g., dialed digits or other ways of entering digital data via keyboard, voice command, biometric indicator, etc.) through hardware interface **16**. In this aspect, MFCA child **10** checks (as indicated by double ended arrows from **10** to **8**) the incoming keypad entries 14 against the allowed features defined in the MFCA database **8**. Presently, this type of functionality is usually defined and implemented on an associated Message Switching Center (MSC) (not shown). Alternatively, the database or a portion of it could be downloaded to the MS and an authorization may be proxied to MFCA **2**, MFCA child process **10** or some other process on the MS for one or more desired features.

[00019] Database **8**, in one aspect, may include extended markup language (XML) files. Alternatively, database **8** may include other computer language files such as wireless markup language (WML) files, Practical Extraction and Report Language (Perl) files, Binary Runtime Environment for Wireless (BREW) application (app) files, Executables (.EXE files), Java ARchive (JAR) files, Java 2 Platform, Micro Edition (J2ME) files, C++ files, C files, or many more other types of files depending on feature, service, operating system (OS) etc. The files within database 8 may include information pertaining to what services , features, conditions of use, algorithms for determining use, programs, scripts, etc., are made available to the holder of the phone from, for instance, the phone owner, business proprietor, contractor for telecommunication services, or service providers as the case may be. The services or features may relate to information entered in the phone such as biometric data, voice commands or dialed digits (e.g., via keypad), or incoming information transmitted from a remote location such a calls or messages (e.g., short message service (SMS).

[00020] In one preferred embodiment, MFCA **2** listens on a port for service request **12** through mobile operating system (MOS) **4**. Any mobile operating system

that has a multi-threaded multiprocessing architecture may be sufficient. For instance, Symbian™, Win CE™, Rex™, VxWorks™, ThreadX™, or Nucleus™, to name a few, are examples. A well known operating system such as Symbian ™ may be employed. However, in one aspect, MOS **4** is modified to cause all service requests **12** to be sent to MFCA **2**. For instance, authorization from the MFCA prior to feature use might be local to the MS and use an algorithm / script etc... which was downloaded earlier. MFCA **2** in turn spawns a child process, MFCA **10**, that verifies that the service requested authorized for the user of the MS. For instance, in a case where a service request occurs in conjunction with dialed digits from M S user entries **14**, MFCA **10** checks database **8** to determine whether the request is supported by the MS. Child process MFCA **10** accesses database **8** using a XML or WML command call that may, for instance be named "MobileFeatures.MFCA(feature_type,...) corresponding to a MFCA class. Additional methods may be defined as enhancements to provide features on the MS as specified by a fleet owner, etc. For instance, the service request may be for the MS to gain access to SMS messages, Location Based Services (LBS), Call Waiting (CWT), roaming services or any number of other services. The suite of accessible services may be customized on an MS basis, user, location, time or other algorithm thereby controlling access to services on a case by case basis according to given criterion/criteria. Moreover, a provider of services such as a company owner, phone rental service, etc., may service access on a customer, contractor, employee, etc. basis. Services made available to an MS may be added, modified, or deleted through programming port **13** in hardware interface **16.** Programming services/features into an MS may occur in connection with data sent wirelessly to a mobile station from for instance, a fleet owner, MS rental agency, business owner, etc.

[00021] **FIG. 2** illustrates the mobile feature control application daemon. MFCA **2** and its spawned application, MFCA 10, as shown in **FIG. 1**, are included within mobile feature control **3**. MOS **4** handles the operation of a MS. The features and functionality capable of implementation by a MS are downloaded to MOS **4** by, for instance, by an entity intended to control such functionality such as a fleet operator, business owner, etc. In one aspect, database **8** is updated with information indicative

of whether a particular feature or functionality is authorized for MOS **4**. Accessible features for a particular MS may be readily identified by checking the contents of its database **8**. In another aspect, a MS may be provided with a complete or near complete set of features. However, the contents of database **8** (e.g., as specified through XML files), which may be programmed from a location remote from the MS, may determine which features carried out in conjunction with MOS **4** are available to the MS user. As indicated above, service requests (shown by the arrow from MOS **4** to Mobile Feature Control **3**) may result from incoming calls (or messages) or MS user entries such as keypad entries through hardware interface **16**. Such service requests are handled through MOS **4** (as indicated by the arrow from Mobile Feature Control **3** to MOS 4, so that incoming or outgoing signals from a MS indicative of a particular feature, e.g. three-way calling, voice mail, SMS messaging, etc., whether prompted by keypad strokes or incoming calls, are controlled through MOS **4**, providing MOS **4** with the capability as a gate-keeper to available MS features. For instance, perhaps the requested functionality may be programmed into MOS4. However, a given feature may only be available during certain times, e.g. over-seas calling after 9:00 p.m., etc. MOS **4** may cause a MS to display a message on the MS which indicates that a particular feature is not allowed in conjunction with denying access to particular feature that may be sought, for instance, through keypad strokes or buttons. Functionality may be easily programmed into a MS using a development kit that may be available for a mobile operating system. Additionally, a user might enable a function, feature, etc. through password authorization or by filling out a credit card payment page etc...

[00022] In one preferred embodiment of this invention, control of services/features made available to a particular MS may be managed from a remote location using, for example, a web server with feature information embedded in web pages. For a set of Mobile Station (MS) owned by a small company or public agency, such as a police agency, access and control of available features/services may be configured via a secure website.

[00023] In one embodiment, an MS feature configuration may be managed via wireless methods using an Internet connection to a MS. This permits an embedded application to be downloaded to an MS.

[00024] **FIG. 3** illustrates a communication network **21** including each MS **22** being operable in accordance with that depicted by the diagram of **FIG.1**. Mobile switching center (MSC) **24** provides services and coordination between MS **22** and external networks such as public telephone switching network (PTSN) **24** and public data switching network (PDSN) **26** in connection with MS registrations on a Home Location Register (HLR) **29** and a Visiting Location Register (VLR) **36** in connection with roaming. Communication network **21** includes home system **32** which represents the system for which MS **22** is normally registered. Home system **32** includes MSC **34** and VLR **36**. An MS **22** communicates over-the-air terrestrially via Base Station Controller (BSC) **38** connected to MSC **34** of home system **32**. Home system **32** is connected to PTSN 24 and PDSN **26**. Home Location Register (HLR) **40**, which holds the registrations of MSs registered with home system **32**, is connected to home system **32** and serving system **42**. Serving system **42** includes MSC **44** and Visiting Location Register (VLR) 48. Home and serving systems **32** and **42**, respectively, as well as third party networks (not shown) support and provide plain old telephone service (POTS), voice, data, and/or other services to MS(s) **22** over the entire communication network **21**. Programming the accessibility of features available to MS **22** may be provided by through and/or from remote station **50** which may be operated by a fleet owner, business owner, equipment rental agency, etc. Remote station **50** may include data processing functionality such as a server and memory for maintaining control of MS feature accessibility.

[00025] In another preferred embodiment, a system determines authorization for access to one or more services grouped together as a package of services (hereinafter referred to as a package). The system offers business proprietors, contractors for telecommunication services, and service providers the ability to authorize users, particularly users of mobile stations. A mobile station can comprise a mobile phone, a personal digital assistant with wireless capabilities, a portable computer with wireless capability, a pager or other personal communications device. With reference to **FIG. 4**, which illustrates a block diagram of one aspect of a preferred embodiment, package **52** is associated with mobile communications terminal (MCT) **22**. Services available to MSC **22** from package

52 can be accessed through the provision of software files, codes, etc. from file server **56**. Service providers may provide wireless and wireline service over one or more networks labeled with the appropriate wireless or wireline designation indexed, for example, by A through Z. Authorization server **54** either approves or denies access to a requested service, e.g. voice mail, conference calling, phone network update, etc. Authorization server **54** is ideally located with or under the control of a contractee offering bundled services. Authorization server **54** is programmed to evaluate requests from an MCT **22** for authorization to use one or more of the services and/or service features bundled in package **52**. MCT **22** forwards requests to authorization server 54 through one of the wireline or wireless networks labeled A through Z. Wireless and wireline networks labeled A through Z may be intelligent and/or virtual networks. An intelligent network (IN) provides functionality to be flexibly distributed to a variety of network nodes both on and off of a network. Further, the architecture of the intelligent network may be modified to control the bundle of services in the package. A virtual network may be provided using ones of networks A through Z. A virtual network may be formed by primarily programming in, rather than hard-wiring, an extension of an existing network on an as needed basis. New, "intelligent" network nodes and special network components and also additional functions for extending existing exchanges are introduced into the network. The architecture of the intelligent network is obtained primarily from the operation of a service switching point (SSP), which is introduced as an extension of existing digital local or trunk exchanges, and of service control points (SCP) used as "intelligent" network nodes for setting up connections within.

[00026] Accessing authorization server **54** need not occur through an MSC. Consequently, in other embodiments, the path to authorization server **54** may occur through 802.11 (Wi-Fi), Ethernet virtual interface, Universal Serial Bus (USB), docking station, Ethernet cable, etc.

[00027] A user may be pre-authorized to access certain features, services, etc. both while in or out of contact with authorization server **54**. This aspect is particularly useful for mobiles that will be executing customer or business proprietary features or services while outside of a cellular service area, e.g., geofence, data access, computer assisted repair, etc.

[00028] **FIG. 5** illustrates a diagram further depicting the functionality of the mobile station feature control daemon within MS **22**. In one preferred embodiment, MOS **4** may be modified with an application that is capable of receiving inputs from Mobile Switching Center (MSC) **44** via, for instance, Over-the-Air Parameter Administration (OTAPA) or OTASP using the IS-707 protocol. Mobile Feature Control (MFC) **3**, as described herein, provides an interface to MOS **4** whereby services are verified with each request. If the requested service is not supported as indicated by a feature database then access to that feature is denied. MFC **3** accepts inputs from the MOS **4** that are marked as feature control data. This data is then stored in a feature database such as database **8**.

[00029] It is contemplated that the MFC **3** may be provided via a downloadable software application. The mechanism for downloading the application to MS **22** may vary with the MS. For instance, in some cases, the MFC application will be downloaded from the telecommunications service provider.

[00030] In one embodiment, all dialed digits on MS **22** and service requests are sent to the Mobile Feature Control application (MFCA), not shown, within MFC **3**. The MFCA then compares the requested service to the services allowed in the feature database **8**. The features in database **8** are not accessible for changes by the user of the MS **22**. The features can only be changed by an operator at remote station **50** having access to MS **22**.

[00031] In other embodiments, in addition to using the mobile feature control application daemon described above, rather than accessing services and features through a MSC, which is typically owned by a telecom service provider, these features and services may be provided through a proprietary asynchronous transfer mode (ATM) network (or asynchronous transfer mode-like network) using the Internet. The ATM network capacity automatically adjusts to meet system needs and bandwidth is allocated on demand.

[00032] **FIG. 6** illustrates a diagram showing a system view of one embodiment which may be used in conjunction with the mobile feature control application daemon described above. With reference to **FIG. 6**, packet switched data network (PDSN) **26** is used to connect ATM router(s) **114**. For instance, ATM router connections may form part of a wide area network (WAN). Each ATM router **114**

contains a route list which specifies the route path of a particular payload type of information. The payload information is formed from native data that an ATM router transfers into a fixed length sequence of data called ATM cells. Generally, an ATM cell is a set of data that is formed by an ATM switch or ATM router as that data enters an ATM network. Package **52** of services is accessed through authorization server **54** which hangs off the ATM network formed by ATM routers **114** which provide connections over the PSDN using the Internet. Control of services and features to a mobile station (not shown) may be controlled by daemon implemented in the mobile station and determined by an entity remote from the mobile station such as a business owner, etc. Data to and from wireless network **117** (e.g. networks A and Z as shown), in one embodiment, is provided through a Session Initiation Protocol (SIP) gateway **118**. SIP is a protocol that allows communication between the Internet and a phone network such as a wireless phone network. For instance, an IP address may translate an IP address to a telephone number and vice versa. Further, SIP may be used as the vehicle that allows instant messaging over the Internet to a wireless phone network, providing bi-directional translation between a wireless phone network and a device connected to the Internet. In other embodiments, gateways based off of the H.323 protocol may be used.

[00033] **FIG. 7** illustrates ATM cell **106** traveling along virtual path **107** through routers **114** with an ATM network to server **109**, its destination. An exploded view of ATM cell **106** is also shown in **FIG. 2**. By convention, each ATM cell **106** contains **5** octets (an 8 bit byte) of header information followed by 48 octets of payload. The header (e.g., User-Network Interface (UNI) header format as shown or network-to-network header interface) includes several fields used by ATM routers and switches to properly route data and to guarantee the necessary quality of service (QoS). The header data identifies the cell, has a logical address that determines the routing, and includes priority and management bits. No error correction is provided beyond the header on the assumption that network traffic will not drop below an acceptable QoS. Information as identified by the Virtual Channel Identifier (VCI) and the Virtual Path Identifier (VPI) is routed to a particular destination specified by the route list for that type of data. The virtual channel is a

single connection across a network that allows ATM cells to be switched to various destinations along virtual paths. ATM creates a fixed channel or route, between two points in connection with data transfer. ATM can be distinguished from, for instance, transmission control protocol/ internet protocol (TCP/IP) wherein data is divided into packets and each packet can take non-fixed routes from source to destination. Consequently, whereas ATM cells specify a particular route from source to destination, TCP/IP can result in packets headed for the same destination to arrive at the destination via different routes. One advantage of ATM over TCP/IP is that the fixed route property of ATM makes it easier to track data and possibly bill for data transferred over a network as compared with TCP/IP. The VCI is a 16-bit field within each ATM cell and it defines the fixed channel on which the ATM cell should be sent. The VPI is an 8 bit field which indicates where an ATM cell is to travel over a network. ATM cells travel in streams through an ATM network in an asynchronous manner. The connection oriented nature of ATM allows a user of the ATM network to enter a stream when an ATM cell is available and not on the basis of fixed time slots. ATM networks typically transfer data at 155.52 and 622.08 Mbs. Cells are randomly assigned to a virtual channel (VC), as identified by the virtual channel identifier, and are multiplexed into the ATM network. Since large amounts of related data may be broken up and contained in more than one ATM cell, data in ATM cells 106 may be reassembled into its native format through a process of Segmentation and Reassembly (SAR), marked by the use of the dotted line shown, in connection with the cell leaving the network and arriving at server **109**, its destination. In **FIG. 7**, features contained in or permitted through a package (not shown), such as ring back tones, three-way calling, call waiting, voice mail, instant messaging (text messaging), etc., which are normally associated with a MSC may be bypassed and handled through an ATM network, formed using router(s) **114**, connected through the Internet. Traffic through a MSC provides a primary billing vehicle of a telephone service provider. By-passing the MSC and proceeding through the Internet may significantly reduce costs attributable to the traditional service provider. Further, quality of service issues may be addressed with more control. In addition to handling package features through an ATM network, the mobile feature control daemon described above allows control of

features as specified by an entity such as a business owner, equipment rental agency, etc.

[00034] **FIG. 8** illustrates a diagram of one embodiment showing mobile communications terminal (MCT) **104** carried by vehicle **116** which may be operating in conjunction with a dispatcher controlling a fleet of vehicles. MCT **104** contains all of the functionality of MS **22** described above and shown in **FIG.s 3, 4** and **5** including the feature control daemon. Services ("services" and "features" as used herein throughout are interchangeable and one includes the other) available to MCT **104** from package **52** can be accessed through the provision of data, software files, codes, etc. Package **52** may also include abilities, applications and services not typically controlled or billed by an MSC, wherein an owner or other party through authorization server **54** maintains control over the use and access of those abilities, applications and services. Authorization server **54** approves or denies a transfer of files, code etc. from package **52** in connection with a plethora of criteria, based on, for instance, the current location of the mobile communication terminal, the time of day, specific end user rights, etc. in addition to approved criteria or commands from remote station **50** (i.e., an entity controlling feature access). This allows remote station **50** the ability to change access rights for MCT **104** as needed and upon request. Ultimate access to services are determined by the feature control daemon (not shown) within MCT **104** as explained above regard to **FIGs. 1, 2 ,4**, and **5**. MCT 104 may contain (not shown) a receiver and transmitter, a communications interface such as a keypad for entering data (e.g. user identification data for package access), and one or more biometric sensors (for the purpose of identifying and/or authorizing users seeking access to a feature contained in package). A biometric sensor may be a fingerprint reader, a retinal scanner or a voice recognition device. MCT **104** may include a full complement of software which only requires activation or authorization from package **52** via activating software or completing software which is downloaded to MCT **104**. Package **52**, itself, may represent a server or one or more locations accessible through ATM network **18**.

[00035] **FIG. 9** illustrates a block diagram of an exemplary MCT **104**. MCT **104** includes central processing unit (CPU) **200**, random access memory (RAM) **221**, read only memory (ROM) **222**, display **223**, user input device **224**, transceiver **225**,

microphone **226**, speaker **227**, Global Positioning System (GPS) receiver **228**, and antenna **229**. ROM **222** is coupled to CPU **200** and stores the program instructions to be executed by CPU **200**. RAM **221** is also coupled to CPU **200** and it stores temporary program data. RAM **221** and ROM **222** may store selected portions of software necessary to implement a package **52** (**FIG. 1**) features. Access software or code downloaded from package **52** and made accessible through mobile feature control **3** implementing a feature control daemon, determine, in connection with programming CPU **200**, a users' ability to use package features. Access and activation rights and other data may be processed by and/or through CPU **200** as gated by the feature control daemon functionality of mobile control feature **3**. By having the necessary software (e.g. codes, programs, scripts or a portion of a program downloaded into RAM **221** or ROM **222**) loaded at MCT **104**, activation of a package feature or deactivation of a package feature can be done quickly, since either only a small amount code need be received in order to change access rights or simply, authorization need only be received in connection with use of the feature control daemon. User input device **224** may include a keypad, a touch pad screen, a track ball, etc. Should such codes, programs, scripts or portions of a program be present, a MFCA need not be accessed during standard operation of MCT **104**. In this case, the code, program, etc. is authorized once, after which the downloaded code/program ,etc. monitors itself during its predetermined lifespan A user (not shown) employs input device **224** to navigate through menus, generate messages, request route information, and other functions. Display **223** is an output device such as a cathode ray tube (CRT), liquid crystal display (LCD), or other user perceptible device. The user may employ display **223** to read decoded messages or other data transmitted from a customer or other unit (such as another MCT) via wireless network **217**.

[00036] In a preferred embodiment, feature access need not be realized through a code, program, script or portion of a program downloaded into a random access memory (RAM) or read only memory (ROM)

[00037] When provided, microphone **226** and speaker **227** may be incorporated in a handset coupled to transceiver **225**. Microphone **226** and speaker **227** may also be more physically separated to enable hands-free communications with the user of

MCT **104**. In this mode, transceiver **225** may include voice activation circuitry that may convert voice into data which is forwarded to CPU **229** for processing. Data is transmitted to CPU **200** via serial bus **231**. Transceiver **225** includes an instruction set necessary to communicate data and voice signals over a wireless network. In one embodiment, transceiver **225** supports code division multiple access (CDMA), wideband CDMA (WCDMA), Universal Mobile Telephone System (UMTS), Global System for Mobile (GSM), Wi-Fi (Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.11), burst tolerance (BT), time division multiple access (TDMA), or Orthogonal Frequency Division Multiple Access (OFDMA) protocols. However other protocols such as time division multiple access and frequency division multiple access may be supported. The wireless network used supports both data and voice signals. Transceiver **225** is coupled to antenna **229** for communicating signals with wireless communication network **117** (shown in **FIG. 6**). When a data signal is received by transceiver **225**, the received data is transferred to CPU **200** via serial bus **231**. The data may include text messages, traffic updates, suggested changes to road navigation, destination, multiple destination order priority, weather, accident, construction or other road network status data, or other information. Use or ability to receive such data may be constrained by a users access rights to package **52** (**FIG. 6**). The data may also include software updates such as package access rights and authorizations for a particular user of MCT **104**. Transceiver **225** may be capable of receiving position and velocity vector signals from on or more of a variety of position-location systems that are known in the art. In one embodiment, CPU **200** may also direct transceiver **225** to receive a GPS signal from a GPS satellite (not shown) and decode the GPS signal to extract position and timing information.

[00038] The downloaded data or code to MCT **104** may be used to enhance or add to package **52** features and functionality to MCT **104**. For example, an entity controlling access to features of MCT **104** may cause the download of useful package **52** features such as accessories or updates to MCT **104**. Alternatively, an entity controlling access may grant a user the ability to access subscription services that provide network based services that are useful in carrying out business, etc.

Further, entertaining features such as images, screen savers, tunes, ring tones, games, or more may be made available to MCT **104**.

[00039] Wireless equipment systems providing equipment management solutions, such as GlobalTRACS® by QUACOMM Incorporated, automatically collect, organize and transmit vital information concerning how equipment is being used, how much equipment is being used as well as the location of that equipment. This information is especially useful to entities renting, distributing, contracting or owning equipment-particularly construction equipment. An equipment management solution system can control equipment use. This type of information can be reported by a sensor tracking, for instance, usage hours and/or time of day use of a system or a piece of equipment. Further, the equipment management solution system may provide global positioning system (GPS)-based equipment location information including data indicating when a piece of equipment has moved outside of a pre-set boundary. For instance, authorization of use of equipment by certain operators may be of a more limited nature than others. With reference to **FIG. 10**, which illustrates a diagram of one alternative embodiment, the functionality of hardware/software **300** associated with MCT **104** on truck **116** representative of a piece of monitored equipment on truck **116** can be governed by code or files downloaded from package **52** in conjunction with authorization server **54**. In one alternative embodiment, the code or files downloaded from package **52** occurs in connection with receipt of authorization from a feature control daemon in connection with authorization server **54** through a wireless communications network **117** that includes one or more base stations **302** and through ATM network **318**. In addition to having feature access determined by access rights granted through a feature control daemon, it is contemplated that MCT **104** may also make requests for authorization to authorization server **54** or to remote station **50** (i.e., an entity controlling feature access) through ATM network **318**. Downloaded codes and/or files may enable use of one or more services available to a user of MCT **104** in package **52** such as activation or configuration of sensor **305** for a particular purpose. This purpose may, for instance, serve to activate or deactivate a particular security device or alarm system. For instance, should a user of MCT **104** require additional programming codes or files to deactivate a security feature of sensor **305**,

then file server **319** may provide the required information through wireless communication network **117** in connection with authorization of a user through authorization server **54** through ATM network **318** connected through PDSN **26**. Alternatively, MCT **104** can obtain, without the necessity to download additional files or codes, package **52** information through wireless communication network **117** and ATM network **318** to activate a function on sensor **338** of trailer **339**. For instance, sensor **305** may receive information sufficient to allow activation or detection of security, safety or inventory related features.

[00040] Wireless communications network **117** may include a satellite network including satellite **30**, a cellular telephone network or other wireless voice and/or data communications network. MCT **104** may be mounted in a vehicle or be part of a mobile device optimally geographically located within the operational boundaries of the wireless network **117**.

[00041] With reference still to **FIG. 10**, network management center (NMC) **348** is coupled to a plurality of MCTs **104** via wireless network **117**. NMC **348** acts as a central routing station for communications between MCTs **104** and one or more customers **350**, dispatch centers **52**, other designated office(s), shippers, consignees, governmental authorities, family members,(all shown generally designated by **54**) etc. NMC **348** may be coupled to customers **350**, dispatch center **352** and designees **54** by the Internet, dialup connection, wireless communication system, local area network or preferably through the Internet using ATM network **318**. NMC **348** is coupled to wireless communication network **117** via wireless connections, dedicated communication lines such as a T1 or T3 line, via a plain old telephone service (POTS) via the Internet or over the Internet through ATM network **18**. Features from package **52** can be provided to the various entities coupled to NMC **348** in connection with access provided by authorization server **54**. In another embodiment, NMC **348** is co-located with at least a portion wireless communication network **117**. For example, NMC **348** could be co-located with a satellite earth transmission/reception station. The communication link between NMC **348** and MCT **104**, is commonly referred to as a forward link, while signals from MCT **104** to NMC **348** are sent on a reverse link. Data communicated on the forward link may include geographical location information, delivery and vehicle status, encoded

voice communications from another MCT **104** and directions, instructions, road status information, and voice communications from NMC **348**. Further, package features can be provided to MCT **104** on the forward link. NMC **348** may cause the receipt of access information through feature control daemon **3** in MCT **104** as determined by entities such as customer **350** and/or dispatch center **352** (responsible for dispatching vehicles according to customer needs) and/or designee **354**. In a preferred embodiment all communication needs are served while avoiding MSCs (not shown), allowing communications to be more easily controlled and costs to be minimized.

[00042] One concept addressed by the foregoing involves reducing the time in connecting a call while requesting access from an authorization server. Switches are often judged by how many calls can be processed per hour. With increased call attempts, a service provider wants to start billing a customer as soon as possible. Billing generally starts at the time a call is connected. The foregoing described feature control daemon running as a background process in a mobile station (mobile communications terminal) can perhaps make billing happen sooner by allowing distributed, multiprocessing and parallel processing at the MS (MCT). For instance, at the same time a connection is being made to a MS (MCT), authorization from an authorization server may be simultaneously sought. Further, the daemon may be running during a call attempt and also simultaneously find the appropriate routes to complete the call as access to a service is being sought through a network.

[00043] In an alternative methodology, a user may request access to a particular feature. The request is routed to authorization server which may grant the users authorization to use the feature. Thereafter, a program, script, code, dynamic Link Library (DLL) or partial program is downloaded to the mobile device (MS, MCT, etc.) which provides access to the desired service or feature, etc. From that point forward, there is no need for to involvement of an MFCA processor further request of an authorization server. Alternately, the program, script, code, dll or partial program may contain an internal disabler that deletes, suppresses or otherwise inhibits the use of the service or feature based on time, hours used, time paid for, etc. without requiring the assistance of an MFCA or an authorization server.

[00044] Although the invention herein has been described with reference to particular embodiments, it is to be understood that these embodiments are merely illustrative of the principles and applications of the present invention. For instance, although the mobile devices referenced herein having been described in connection to access associated with a mobile device, it is also intended that feature access may depend on the identity of a user of a mobile device. Therefore, in connection with the identity of the user, access to features and/or services may vary. It is therefore to be understood that numerous modifications may be made to the illustrative embodiments and that other arrangements may be devised without departing from the spirit and scope of the present invention as defined by the appended claims.

[00045] **WHAT IS CLAIMED IS:**

CLAIMS

1. A smart phone comprising:

a transceiver;

a processor connected to said transceiver;

memory connected to said processor;

a feature control daemon operable to store feature control authorization information in said memory.

2. A smart phone as recited in claim 1 wherein said feature control daemon is further operable to wirelessly receive authorization information through said transceiver.

3. A smart phone as recited in claim 1 wherein said authorization information consists of files selected from XML files, WML files, DLL files, exe files, binary files, JAR files, Perl files, BREW app., files C++ files, C files, C# files, other data, script or executables known to said smart phone, or a combination thereof.

4. A smart phone as recited in claim 1 where said feature control daemon includes a mobile feature control application operable to spawn one or more additional mobile feature control application being operable to interrogate said memory for feature control information granting access to one or more features.

5. A smart phone as recited in claim 1 further including a mobile operating system wherein said mobile operation system permits smart phone access to features authorized in connection with feature control information stored in said memory.

6. A smart phone as recited in claim 1 further including a mobile operating system and an interface operable to receive inputs, said mobile operating system being operable to implement features approved for access through said feature control daemon in connection with inputs received by said interface.

7. A smart phone as recited in claim 1 further including a mobile operating system and an interface operable to receive inputs, said mobile operating system being operable to implement features previously approved for access through use of said feature control daemon in connection with inputs received by said interface using previously downloaded XML files, WML files, DLL files, exe files, binary files, JAR files, Perl files, BREW app., files C++ files, C files, C# files, other data, script or executables known to said smart phone, or a combination thereof.

8. A method of control access to services for a mobile station comprising:

receiving a service request;

spawning a application to evaluate said service request by determining whether the service is supported by the mobile station as indicated by stored authorizations in a database within said mobile station;

directing a mobile operating system to access said service in connection with said application determining authorization to access said service.

9. A method as recited in claim 8 wherein said mobile operating system is an operating system selected from the group consisting of Symbian™, Win CE™, Rex™, VxWorks™, ThreadX™, or Nucleus™ Operating Systems.

10. A method as recited in claim 8 wherein keypad inputs to a mobile station are interpreted as a service request.

11. A method as recited in claim 8 wherein predetermined data received by a mobile station is interpreted as a service request.

12. A method as recited in claim 11 wherein said predetermined data is received from a source consisting of a network management center or an authorization server.

13. A method as recited in claim 8 wherein one consisting of an application, a portion of an application or an application enabler is downloaded to a mobile station over-the-air.

14. A method as recited in claim 8 wherein said stored authorizations are contain in files consisting of files selected from XML files, WML files, DLL files, exe files, binary files, JAR files, Perl files, BREW app., files C++ files, C files, C# files, other data, script or executables known to said mobile station, or a combination thereof.

15. A mobile station including:

a transceiver;

a processor connected to said transceiver;

memory connected to said processor;

and a downloadable software application, said software application being operable to provide access to features by a user of said mobile station.

16. A mobile station as recited in claim 15 wherein said downloadable software application is further operable to determine access to features by a mobile station in connection with examining authorization information stored in said memory.

17. A mobile station as recited in claim 15 wherein access to features by said mobile station is based upon one consisting of position, time, data collected, prior activities, device capabilities, identity of a user of the mobile station, or a combination thereof.

18. A mobile communications terminal comprising:

a processor;

a memory including software operable to implement a package of features;

a feature control daemon;

a transceiver coupled to said processor, said transceiver being operable to send and receive data through a wireless communications network coupled to a network, said processor being operable to access package features, for a mobile communications terminal user, provided through said wireless communications network and said network in connection with said feature control daemon providing authorization to access said package features.

19. A mobile communications terminal as recited in claim 18 wherein said processor is permitted use of said package features in connection with programming received by said transceiver from a remote station.

20. A mobile communications terminal as recited in claim 18 wherein said processor is denied use of said package features in connection with said feature control daemon failing to provide authorization.

21. A mobile communications terminal as recited in claim 18 wherein said package of features is selected from the group consisting of ring back tones, three-way calling, call waiting, voice mail, text messaging long distance calling, caller ID, picture messages, multimedia features, non-telephone applications and features, business applications, database access or a combination thereof.

22. A mobile communications terminal as recited in claim 18 further including a mobile operating system and an interface operable to receive inputs, said mobile operating system being operable to implement features previously approved for access through use of said feature control daemon in connection with inputs received by said interface using previously downloaded XML files, WML files, DLL files, exe files, binary files, JAR files, Perl files, BREW app., files C++ files, C files, C# files, other data, script or executables known to said smart phone, or a combination thereof.

23. A mobile communications terminal as recited in claim 18 wherein said network includes a plurality of routers connected together through the Internet.

24. A mobile communications terminal as recited in claim 18 wherein said network is connected within one consisting of a packet switched data network or a data switched network.

25. A mobile communications terminal as recited in claim 18 wherein said wireless network is selected from networks consisting of CDMA, WCDMA, UMTS, GSM, 802.11, BT, TDMA, or OFDMA networks.

26. A mobile communications terminal as recited in claim 18 further including an interface used to identify a user for communication with an authorization device through said transceiver.

27. A mobile communications terminal as recited in claim 26 wherein said interface includes a biometric sensor selected from the group consisting of a fingerprint reader, a retinal scanner, a voice recognition device or a combination thereof.

28. A mobile communications terminal as recited in claim 26 wherein said interface includes data entry devices consisting of a keypad, a touch pad screen, a track ball or a combination thereof.

29. A mobile communication terminal as recited in claim 18 wherein said network is an ATM network

30. A method of doing business as recited in claim 18 wherein said package of features is provided through a subscription service.

31. A method of doing business wherein said mobile communications terminal as recited in claim 18 is provided access to a package of features through said network exclusive of a MSC.

32. A method of providing a package of services to a mobile station through a wireless network comprising:

receiving authorization code through a wireless network coupled to an ATM network in order to access features of a package authorized for a user; and

accessing features of said package, authorized by a feature control daemon within said mobile station, through said wireless network coupled to said ATM network.

33. A method of providing a package of services through a wireless network as recited in claim 32 wherein said features of said package are accessed without routing through a mobile switching center which is under the proprietary ownership of another entity.

34. A method as recited in claim 33 wherein said features of said package are accessed using 802.11 connections.

35. A method as recited in claim 33 wherein proprietary ownership includes ownership through being an affiliate, subsidiary, or division of said another entity.

36. A method of providing a package of services through a wireless network as recited in claim 32 wherein said features of said package are selected from the group consisting of ring back tones, three-way calling, call waiting, voice mail, text messaging or a combination thereof.

37. A method of providing a package of services through a wireless network as recited in claim 32 wherein said features of said package and said services include features and services that are not directly tied to phone calls.

38. A mobile communications system comprising:

a wireless communications network:

an ATM network coupled to said wireless communications network;

a authorization device connected to said ATM network; and

a package of features accessible through said authorization device, said authorization device being operable to provide authorization for use of features by a mobile communication terminal in connection with directives received from an entity remote from the mobile communication terminal.

39. A mobile communications system as recited in claim 38
wherein said wireless communications network is coupled to a plurality of mobile communications terminals.

40. A system as recited in claim 39 wherein selected authorized users of said mobile communications terminals are able to access features of said package without communications routing through a mobile switching center that is under the proprietary ownership of another entity.

41. A system as recited in claim 38 wherein said proprietary ownership includes ownership through being an affiliate, subsidiary, or division of said another entity.

42. A system as recited in claim 38 wherein said package of features is selected from the group consisting of ring back tones, three-way calling, call waiting, voice mail, text messaging, other features or a combination thereof.

43. A system as recited in claim 38 wherein said ATM network includes a plurality of routers connected together through the Internet.

44. A system as recited in claim 38 wherein said access device is an authorization server.

45. A system as recited in claim 38 wherein said ATM network is connected within a packet switched data network.

46. A system as recited in claim 38 wherein said ATM network is connected within a data switched data network.

47. A system as recited in claim 38 wherein said wireless communications network consists of a network selected from CDMA, WCDMA, UMTS, GSM, 802.11, BT, TDMA, or OFDMA networks

48. A system as recited in claim 38 wherein said authorization device grants access to said package of features in connection with criteria controlled by an entity remote from said mobile communications terminal, selected from a current location of the mobile communication terminal, a time of day, specific end user rights, download of data, scripts executables source code or a combination thereof.

49. A mobile device comprising:

a transceiver;

a processor connected to said transceiver;

memory connected to said processor;

a feature control daemon operable to store feature control authorization information in said memory.

50. A mobile device as recited in claim 49 wherein said feature control daemon is further operable to wirelessly receive authorization information through said transceiver.

51. A mobile device as recited in claim 49 wherein said authorization information consists of files selected from XML files, WML files, DLL, exe, binary, JAR, Perl, BREW app., C++ files, C files, C# files, or other data, script or executable know to the device, or a combination thereof.

52. A mobile device as recited in claim 49 where said feature control daemon includes a mobile feature control application operable to spawn one or more

additional mobile feature control application being operable to interrogate said memory for feature control information granting access to one or more features.

53. A mobile device as recited in claim 49 further including a mobile operating system wherein said mobile operation system permits smart phone access to features authorized in connection with feature control information stored in said memory.

54. A mobile device as recited in claim 49 further including a mobile operating system and an interface operable to receive inputs, said mobile operating system being operable to implement features approved for access through said feature control daemon in connection with inputs received by said interface.

55. A mobile device as recited in claim 49 further including a mobile operating system and an interface operable to receive inputs, said mobile operating system being operable to implement features previously approved for access through use of said feature control daemon in connection with inputs received by said interface, by using previously downloaded XML files, WML files, DLL, exe, binary, JAR, Perl, BREW app., C++ files, C files, C# files, or other data, script or executable know to the device, or a combination thereof.