US 20060183461A1

(19) United States

(12) Patent Application Publication

Pearce

(10) Pub. No.: US 2006/0183461 A1

(43) Pub. Date: Aug. 17, 2006

(54) SYSTEM AND METHOD OF MODIFYING POLICY SETTINGS IN AN ELECTRONIC DEVICE

(75) Inventor: **Graham Pearce**, Waterloo (CA)

Correspondence Address:
TORYS LLP
79 WELLINGTON ST. WEST
SUITE 3000
TORONTO, ON M5K 1N2 (CA)

(73) Assignee: **Research in Motion Limited**

(21) Appl. No.: **11/055,489**

(22) Filed: **Feb. 11, 2005**

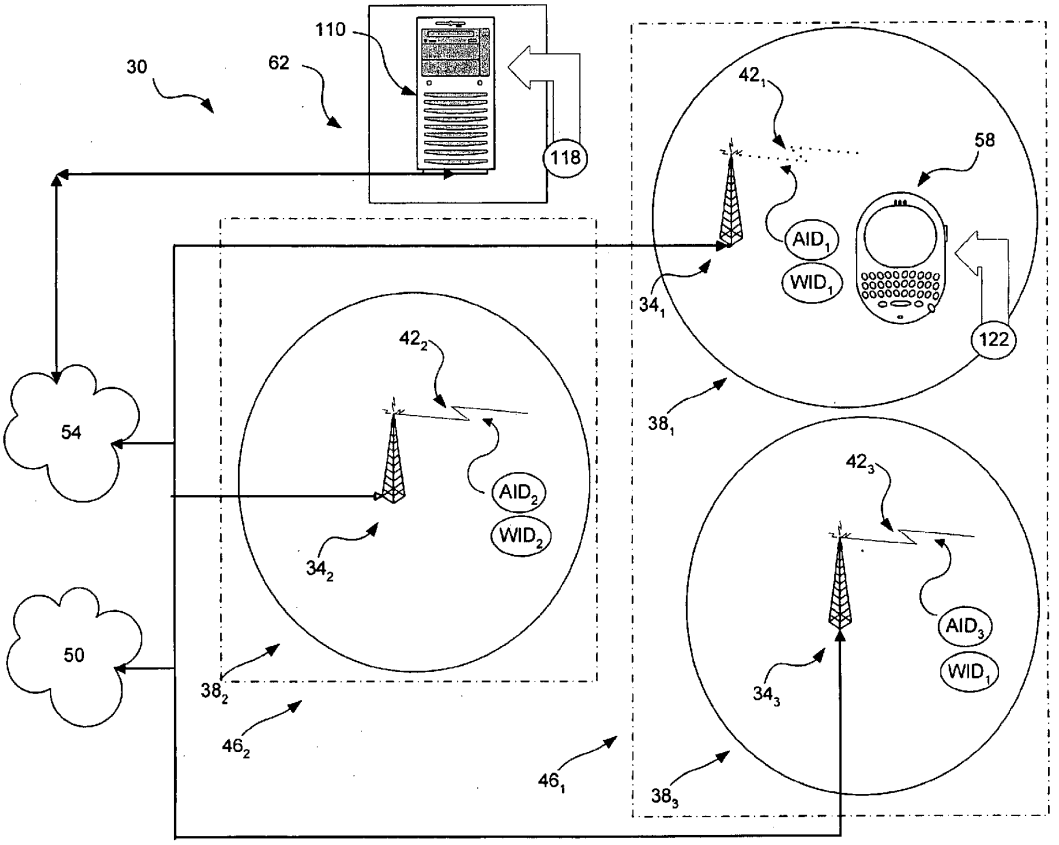
Publication Classification

(51) **Int. Cl.**
H04Q 7/20 (2006.01)

(52) **U.S. Cl.** **455/411**

(57) **ABSTRACT**

The present invention provides a system and method of modifying policy settings in an electronic device. An embodiment includes a plurality of access stations, each capable of wirelessly transmitting across a geographic region. A mobile electronic device, capable of roaming between regions is operable to establish a wireless link with the access stations. The device is owned by an office which sets communication policies determining through which access stations mobile device can place voice calls. This policy is stored on an office server as a database and periodically transmitted to the device as the device makes contact with the office server over the internet. Hence, the device maintains a copy of this policy database. When placing a voice call, the device first determines which access station is serving the region it is located in and then determines whether it is allowed to place a call through that access station using its policy database.



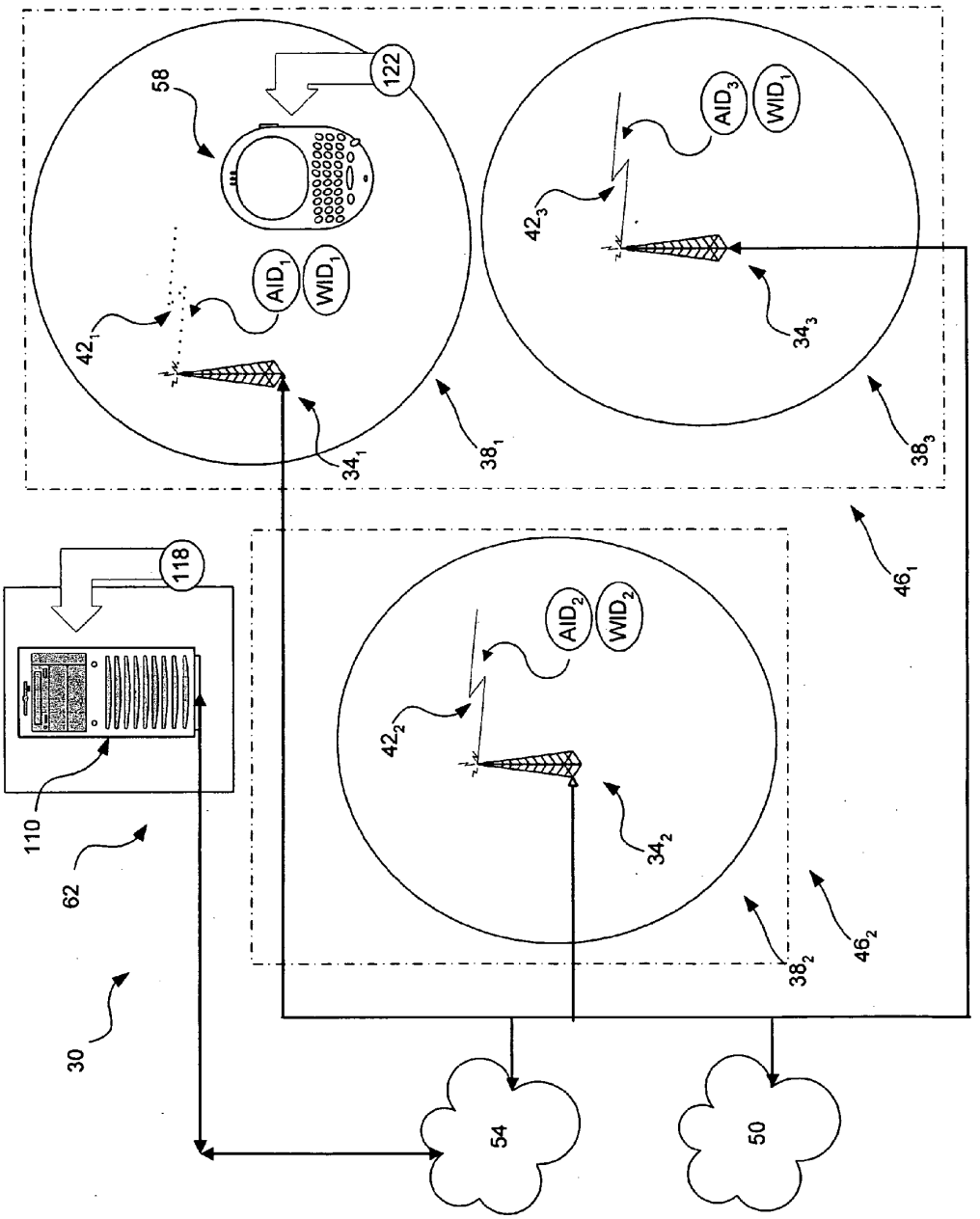
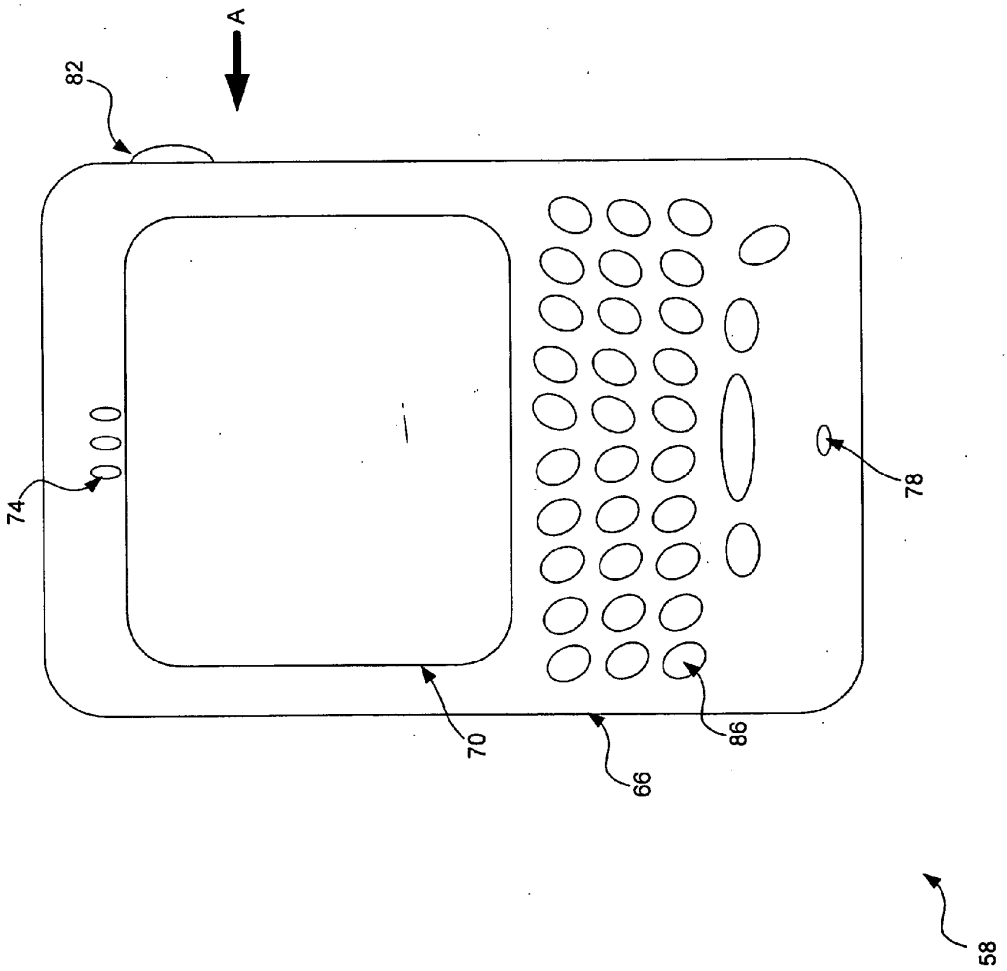

58
122
AID_1
WID_1
42_1
34_1
38_1
AID_3
WID_1
42_3
34_3
38_3
46_1
118
110
62
30
AID_2
WID_2
42_2
34_2
38_2
46_2
54
50

Fig. 1

Fig. 2



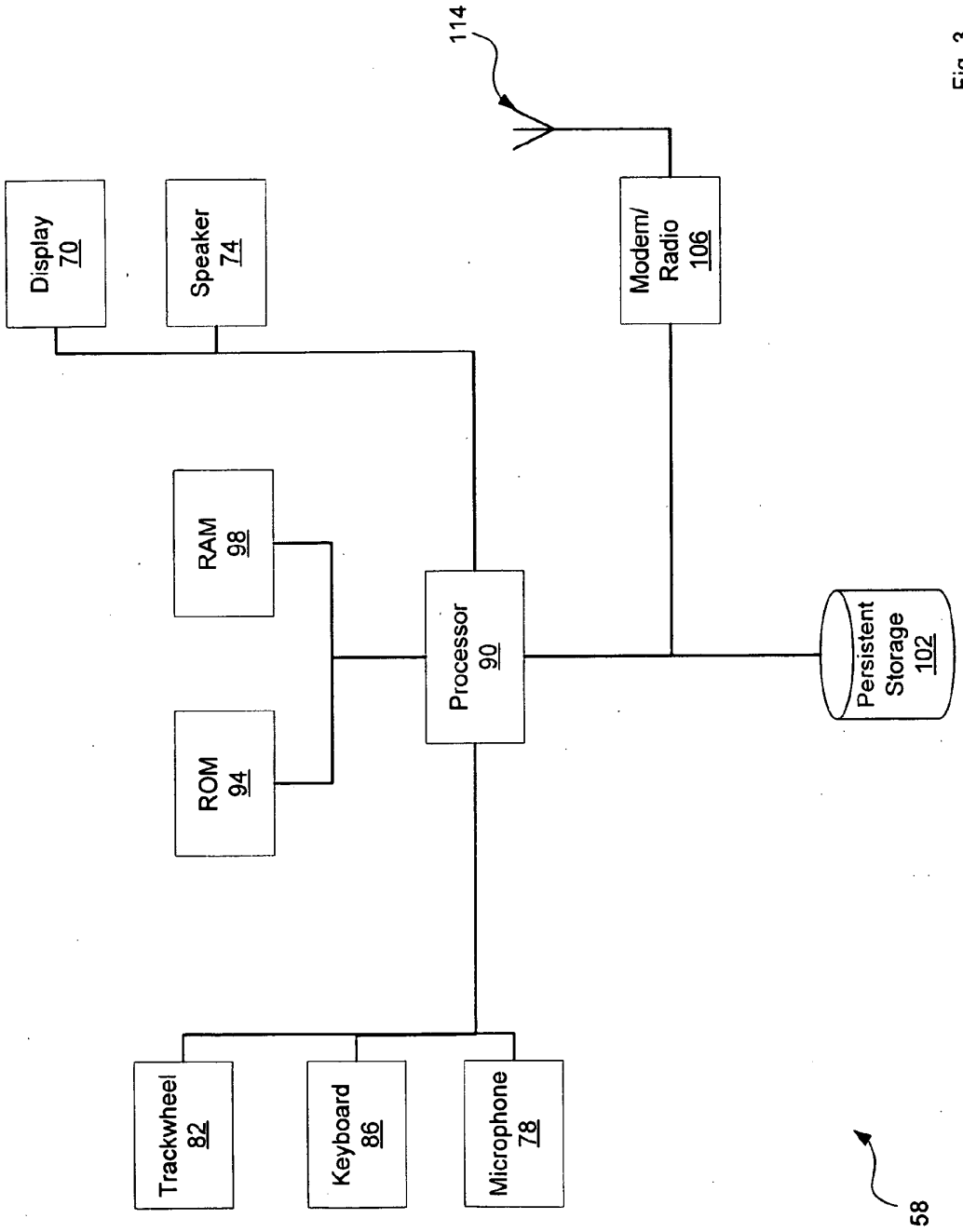

Display
70
Speaker
74
114
Modem/
Radio
106
RAM
98
ROM
94
Processor
90
Persistent
Storage
102
Trackwheel
82
Keyboard
86
Microphone
78
58

Fig. 3

Fig. 4

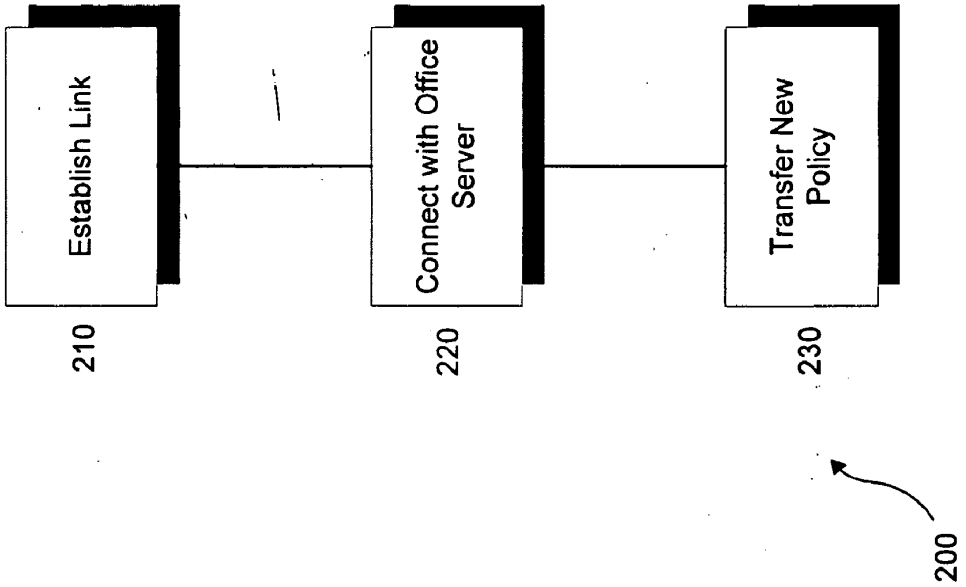
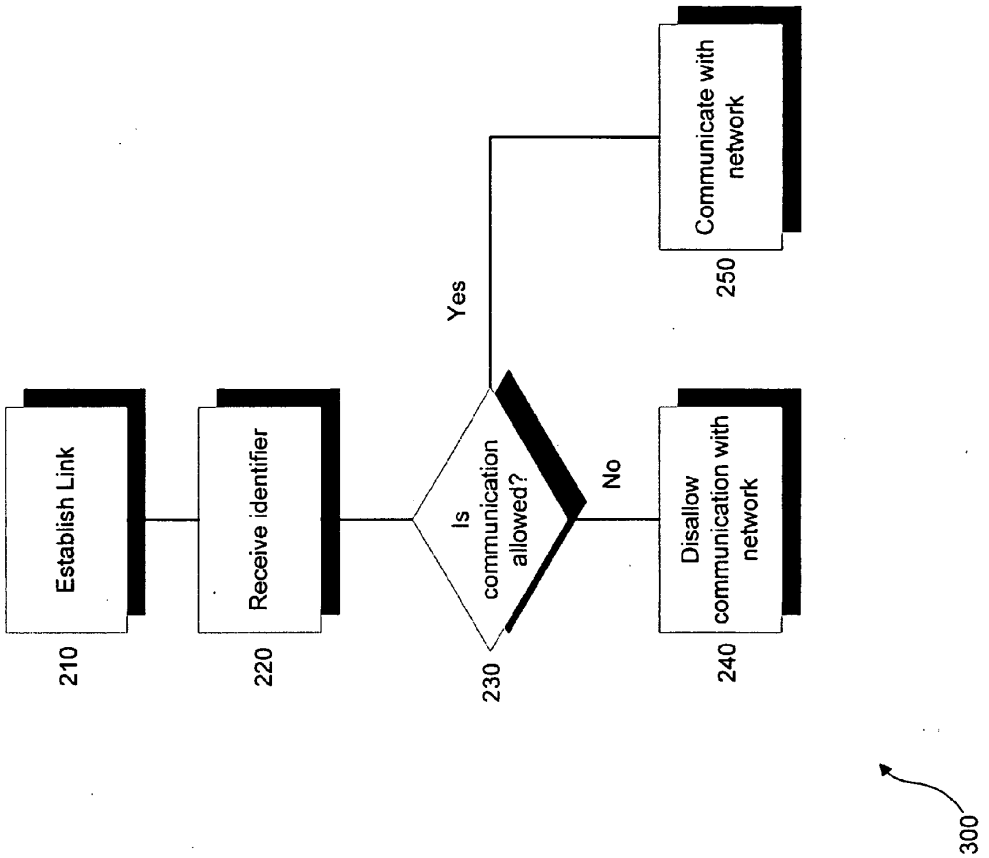

Establish Link
210
Connect with Office Server
220
Transfer New Policy
230
200

Fig. 5


Establish Link
210
Receive identifier
220
Is communication allowed?
230
Yes
No
Communicate with network
250
Disallow communication with network
240
300

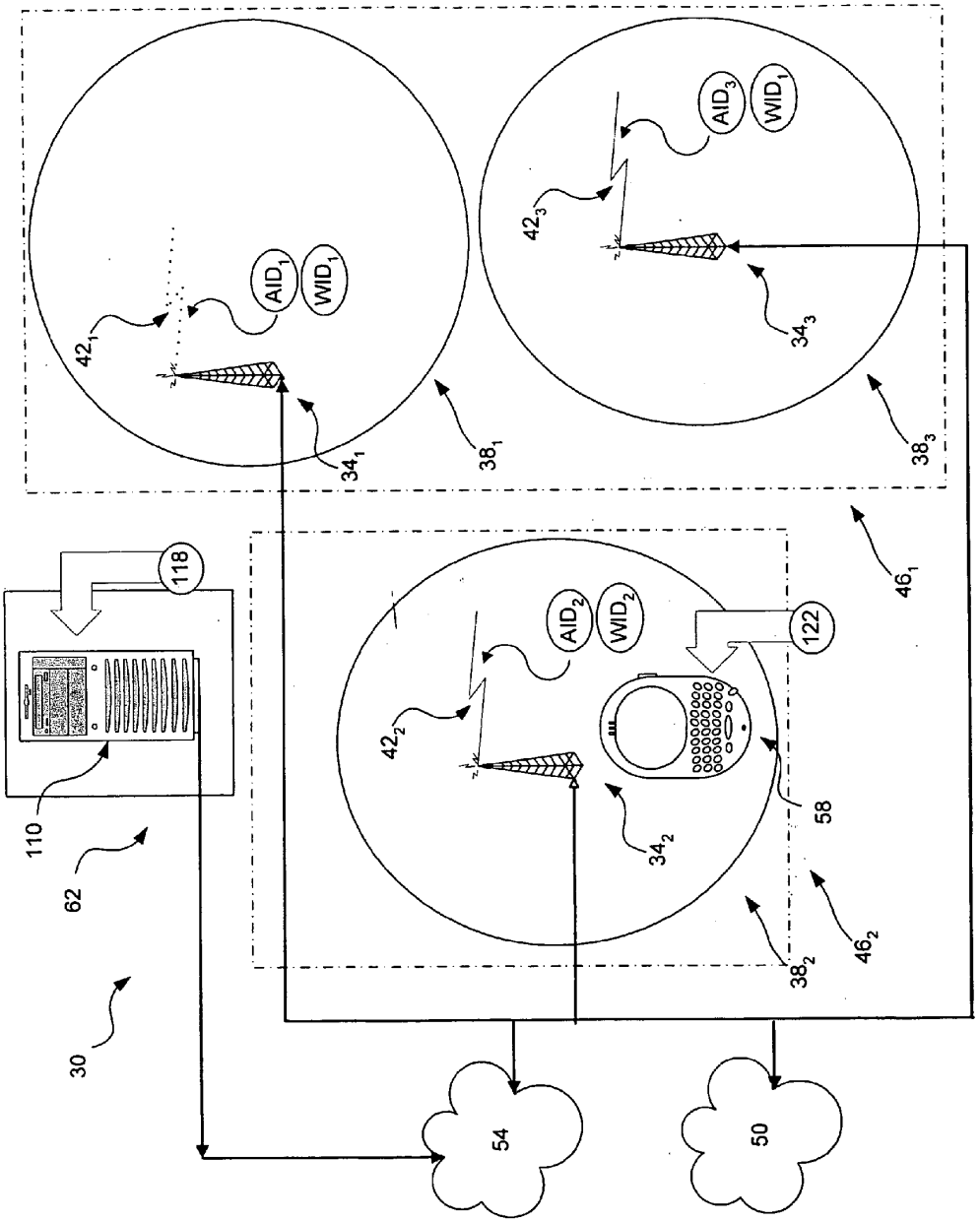

118
110
62
30
42_1
AID_1
WID_1
34_1
38_1
42_3
AID_3
WID_1
34_3
38_3
46_1
42_2
AID_2
WID_2
122
34_2
58
38_2
46_2
54
50

Fig. 6

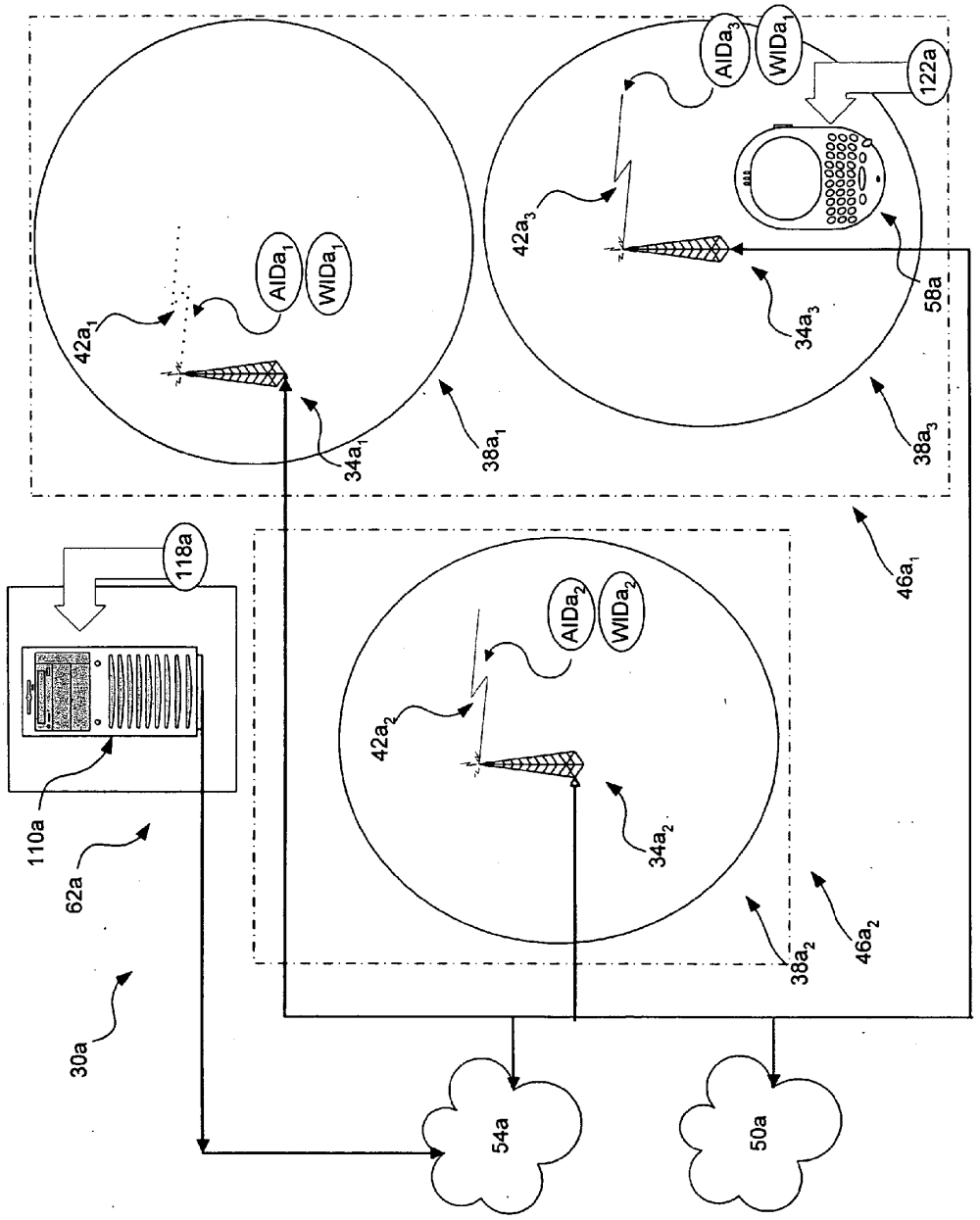

118a
110a
62a
30a
42a1
AIDa1
WIDa1
34a1
38a1
42a3
AIDa3
WIDa1
122a
34a3
58a
38a3
46a1
42a2
AIDa2
WIDa2
34a2
38a2
46a2
54a
50a

Fig. 7

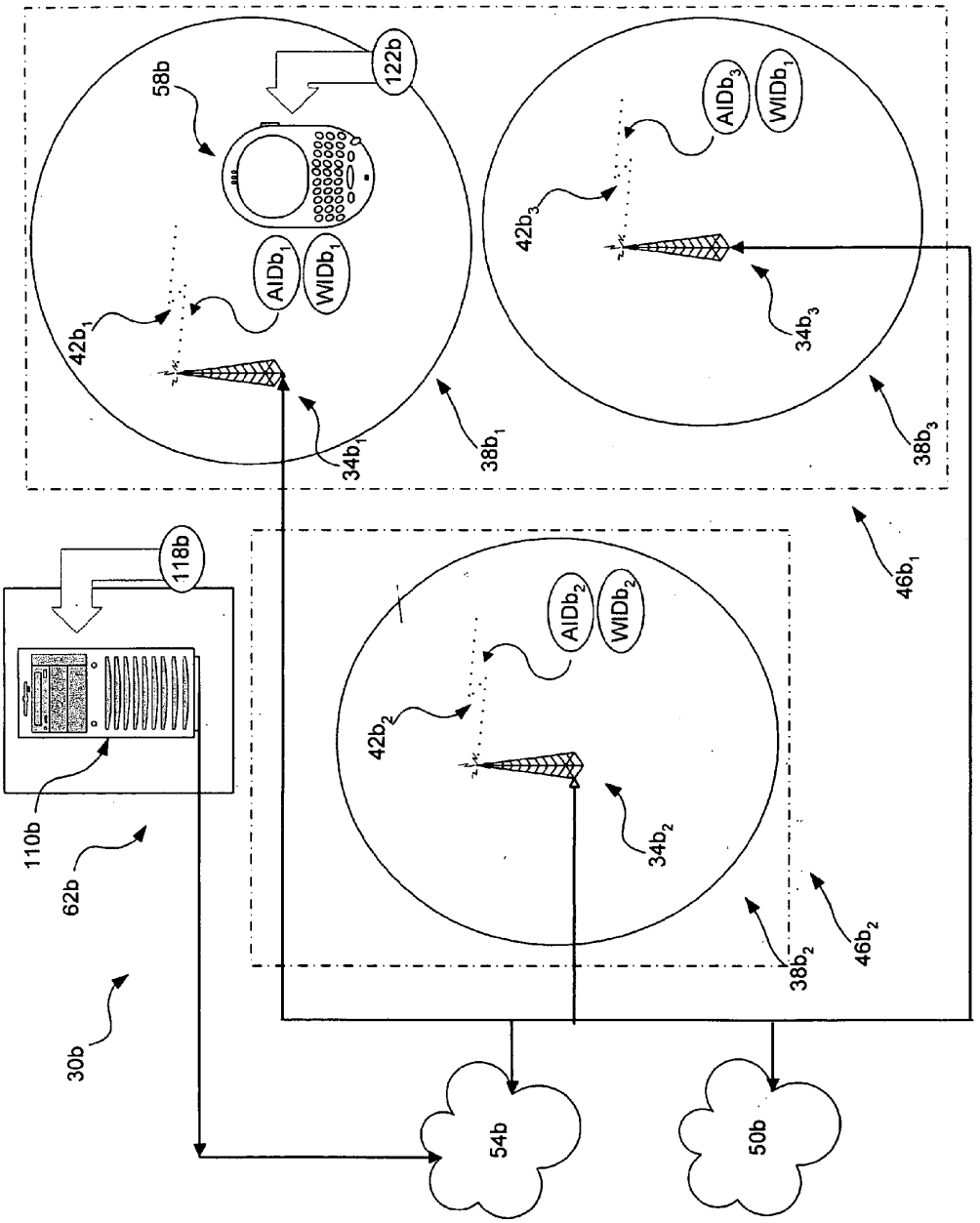

58b
122b
AIDb1
WIDb1
42b1
34b1
38b1
AIDb3
WIDb1
42b3
34b3
38b3
46b1
118b
110b
62b
30b
AIDb2
WIDb2
42b2
34b2
38b2
46b2
54b
50b

Fig. 8

SYSTEM AND METHOD OF MODIFYING POLICY SETTINGS IN AN ELECTRONIC DEVICE

FIELD OF THE INVENTION

[0001] The present invention relates generally to wireless telecommunication and more particularly to a system and method for modifying policy settings in an electronic device.

BACKGROUND OF THE INVENTION

[0002] Mobile electronic devices (MEDs) capable of computing, information storage and communications are increasingly becoming commonplace. MEDs typically integrate the functions of personal information management such as calendaring, data communications such as e-mail and world wide web browsing and telecommunications into a single device. Research In Motion Limited of Waterloo, Ontario, Canada, and PalmOne, Inc. of Milpitas, Calif. USA are two examples of manufacturers of such enhanced wireless electronic devices, and each offer a variety of products in this category.

[0003] A typical MED contains a communications interface for establishing wireless communications with telephony and data networks serving different geographic regions. In addition a typical MED contains a microcomputer which controls most of the functionality of the MED and aids in processing of information that the MED is presented with.

[0004] As part of its functionality, a MED is called upon to establish communications with a network through many different network access stations as the user of the MED roams through different geographic regions served by different network access station wireless carrier. Typically, each MED has a designated "home" region served by a "home" wireless carrier. All other regions are roaming regions. The characteristics of services provided when a MED accesses a network through its home region, as opposed to through a roaming region. Such service differences can include reduced connection security, reduced availability of certain types of communications such as bandwidth for data communications, and increased connection fees known as roaming charges. Moreover, the differences in service depends on the roaming region through which a connection is made. For example, availability of digital connections can vary from region to region.

[0005] Variability of service between the home region and the roaming regions can present a significant problem to MED users or employers who pay for the services on behalf of such users. Typically, a user who wants to establish secure connections or avoid roaming charges, for example, monitors his or her location and uses wireless communication only in the roaming regions where secure connections are offered or where no roaming charges are incurred. This requires a knowledge of the geographic region covered and services offered by the each network. Moreover, employers paying for user's services, unlike users, have no way of monitoring individual MED locations and hence rely on individual user's vigilance in order to ensure secure connections or avoid roaming charges.

SUMMARY OF THE INVENTION

[0006] It is an object of the present invention to provide a novel system and method for secure access that obviates or mitigates at least one of the above-identified disadvantages of the prior art.

[0007] An aspect of the invention provides a subscriber device comprising an interface operable to conduct communications over a link with at least one base station in each of a plurality of geographic regions. The device also includes a microcomputer connected to the interface that is operable to maintain a policy associated with each region. The policy defines whether communications between the interface and the at least one base station are permitted for each region. The microcomputer permits the interface to communicate in accordance with the policy.

[0008] The communications can include a plurality of different services. The services can include at least one of voice, emails, internet browsing and text messaging.

[0009] The policy can permit one type of service to be performed in one specific region, while disallowing another type of service in the same specific region.

[0010] The policy can disallow communications in a particular region if the communications within the region are conducted over an insecure link, or are otherwise insecure.

[0011] The policy can disallow communications in a particular region if the communications within the region are conducted over an insecure link, or are otherwise insecure.

[0012] The policy can disallow the communications in at least one of the regions if a financial cost for conducting the communications exceeds a predefined threshold.

[0013] The links can include wireless links that can be based on one or more of CDMA, OFDM, AMPS, GSM, GPRS, bluetooth, infra-red and 802.11.

[0014] The links can include wired links that can be based on Ethernet; USB; Firewire and RS-232.

[0015] Another aspect of the invention provides a method of conducting communications from a subscriber device comprising the steps of:

[0016] i) establishing a link with a base station from the subscriber device;

[0017] ii) receiving an identifier from the base station at the subscriber device;

[0018] iii) determining whether communications with the base station are permitted based on the identifier; and,

[0019] iv) conducting the communications from the subscriber device only if the communications are permitted according to said determining step.

[0020] Another aspect of the invention provides a server for communicating with a plurality of subscriber devices comprising a microcomputer operable to maintain a policy defining whether communications between at least one subscriber station and at least one base station are permitted. The server also an interface for delivering the policy to each of the at least one subscriber device.

[0021] Another aspect of the invention provides a computer readable media operable to store a set of programming

instructions. The programming instructions are for operating a server that is for communicating with a plurality of subscriber devices. The programming instructions are executable on a microcomputer associated with the server. The programming instructions are for rendering the microprocessor operable to maintain a policy defining whether communications between at least one subscriber station and at least one base station is permitted.

[0022] Another aspect of the invention provides a computer readable media operable to store a policy for storage in a subscriber station. The policy defines whether communications between the subscriber station and a particular base station are permitted.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The invention will now be described by way of example only, and with reference to the accompanying drawings, in which:

[0024] **FIG. 1** is a block diagram of a system for modifying communication policy in accordance with an embodiment of the invention;

[0025] **FIG. 2** is a block diagram of the mobile electronic device of **FIG. 1**;

[0026] **FIG. 3** is a block diagram of certain internal components of a mobile electronic device of **FIG. 1**;

[0027] **FIG. 4** is a flowchart depicting a method of updating information in accordance with an embodiment of the invention;

[0028] **FIG. 5** is a flowchart depicting a method of establishing communication according to policy in accordance with an embodiment of the invention;

[0029] **FIG. 6** is another arrangement of the system of **FIG. 1**;

[0030] **FIG. 7** is a block diagram of a system for modifying communication policy in accordance with another embodiment of the invention; and

[0031] **FIG. 8** is a block diagram of a system for modifying communication policy in accordance with an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0032] Referring now to **FIG. 1**, a wireless communication system in accordance with a first embodiment of the invention is indicated generally at **30**. System **30** comprises a plurality of access stations **34** operable to wirelessly transceive across a variety of geographic ranges **38**. In a present embodiment, station **34**, transceives across a first geographic range $\mathbf{38}_1$, station $\mathbf{34}_2$ transceives across range $\mathbf{38}_2$ and station $\mathbf{34}_3$ transceives across geographic range $\mathbf{38}_3$. Access stations **34** communicate wirelessly over a plurality of links **42**. More specifically, station $\mathbf{34}_1$ covers first geographic range $\mathbf{38}_1$ by transmitting and receiving signals through link $\mathbf{42}_1$, station $\mathbf{34}_2$ covers second geographic range $\mathbf{38}_2$ through link $\mathbf{42}_2$ and base station $\mathbf{34}_3$ covers third geographic range $\mathbf{38}_3$ through link $\mathbf{42}_3$. Access stations **34** are operated by different wireless carriers **46**. For example, stations $\mathbf{34}_1$ and $\mathbf{34}_3$ are operated by wireless carrier $\mathbf{46}_1$, whereas station $\mathbf{34}_2$ is operated by wireless carrier $\mathbf{46}_2$. In a present embodiment, system **30** is based on a known voice-based wireless telecommunication such as Global System for Mobile Communications ("GSM") or Advanced Mobile Phone System ("AMPS").

[0033] In system **30**, access stations **34** are also connected to a network **50** and network **54** through a wired connection. In this embodiment network **50** is the public switched telephone network ("PSTN") and network **54** is the Internet, but in other embodiments other types of networks can be employed.

[0034] System **30** also includes a mobile electronic device **58**. Device **58** is owned by office **62** and operated by persons associated with office **62**. As will be described in greater detail below, device **58** is operable to connect to network **50** via a station **34**'s link **42** each time device **58** is located within a range respective to that access station **34**. For example, whenever device **58** is located within geographic range $\mathbf{38}_1$, device **58** can connect to network **50** by linking with access station **34**, through link $\mathbf{42}_1$, and whenever device **58** is located within geographic range $\mathbf{38}_2$, device **58** can connect to network **50** by linking with station $\mathbf{34}_2$ through link $\mathbf{42}_2$.

[0035] Various types of information can be communicated through a link **42**, including voice communications, data communications, etc. In particular, links **42** each carry an wireless carrier identifier WID, that identifies the wireless carrier **46** operating the respective access station **34** that carries that particular link **42**. For example, if device **58** is located within geographic range **381**, or range $\mathbf{38}_3$ device **58** would receive identifier WID_1 through link $\mathbf{42}_1$. In addition, links **42** each carry an access station identifier AID_1 that identifies the access station **34** that carries that particular link **42**. For example, if device **58** is located within geographic range $\mathbf{38}_1$, device **58** would receive identifier AID_1 through link $\mathbf{42}_1$. Furthermore, links **42** carry the phone number (or other unique identifier) associated with each device **58** that connects with an access station **34**. For example, if device **58** is located within geographic range $\mathbf{38}_1$, station **34**, would receive the phone number of device **58** through link $\mathbf{42}_1$. Moreover, links **42** can be based on any number of different wireless communication formats such as analog or digital depending on the type of wireless communication method used. For example, when station **34** employs GSM for wireless communication, link **42** established by that station is a digital link. When station **34** employs AMPS for wireless communication, link **42** established by that station is an analog link. Unlike analog links, which send signals using a continuous stream, digital links transmit the communications in packetized bit streams. Digital links **42** based on GSM offer enhanced security over analog links **42** based on AMPS. Interception and reconstruction of a digital link involves more highly specialized and expensive equipment than an analog link. Moreover, digital links **42** can be encrypted using methods such as stream ciphers, resulting in an encrypted communication between device **50** and access station **34**. In this embodiment link **42**, is a digital link, whereas links $\mathbf{42}_2$ and $\mathbf{42}_3$ are analog links. As such, link $\mathbf{42}_1$ is inherently more secure then links $\mathbf{42}_2$, and $\mathbf{42}_3$.

[0036] Referring now to **FIG. 2**, device **58** is shown in greater detail. Device **58** is based on the computing environment and functionality of a personal digital assistant with wireless voice telephony capabilities. However, it is to be understood that device **58** can be based on the construction and functionality of any mobile electronic device that can be connected to a wireless network as well. Such devices include cellular telephones or laptops computers connected

to wireless networks. In a present embodiment, electronic device **58** includes, a housing **66**, which frames an LCD display **70**, a speaker **74**, a microphone **78**, a trackwheel **82**, and a keyboard **86**. Trackwheel **82** can be inwardly depressed along the path of arrow "A" as a means to provide additional user-input. It will be understood that housing **66**, can be made from any suitable material as will occur to those of skill in the art.

[**0037**] Referring now to **FIG. 3**, a block diagram of certain internal components within device **58** are shown. Device **58** is based on a microcomputer that includes a processor **90**. Processor **90** is connected to a read-only-memory ("ROM") **94**, which contains a plurality of applications executable by processor **90** that enables device **58** to perform certain functions. Processor **90** is also connected to a random access memory unit ("RAM") **98** and a persistent storage device **102** which is responsible for various non-volatile storage functions of device **58**. Processor **90** can send output signals to various output devices including display **70** and speaker **74**. Processor **90**, can also receive input from various input devices including microphone **78** and keyboard **86**. Processor **90** is also connected to a modem and radio **106**. Modem and radio **106** are operable to connect device **58** to wireless access stations **34** in range of device **58**, in the usual manner, via an antenna **114**.

[**0038**] Referring back to **FIG. 1**, office server **110** is a computing device, (such as a personal computer, a server, or the like) that is typically comprised of hardware suitable for server type functions, and includes a central processing unit, random access memory, hard-disk storage and a network interface for communicating over network **54**. Office server **110** stores the office connection policy ("CP") database **118**, used for determining which access stations **34** a device **58** can link with in order to connect to a network. Table I shows the initial settings of an example CP database **118** of office **62** for device **58** when it attempts to connect to network **50**, namely when a wireless voice call is being made.

TABLE I

Example record of a CP Database 118 of Office 62
Record # 1

Field 1 Device Identifier	Field 2 Access Station Identifier	Field 3 Policy for Voice Calls
555-555-5555	AID_1	Allow Communication
	AID_2	Allow Communication
	AID_3	Allow Communication

Table I shows one record, labelled Record 1, which reflects information corresponding to device **58**. It should now be apparent that database **118** can include additional records for any additional devices **58** that are included in system **30**.

[**0039**] Describing Table I in greater detail, Field 1 contains the unique identifier of device **58**, in this case its phone number "555-555-5555". Field 2 contains a list of unique identifiers, AID_1 associated with access stations **34**. Field 3 contains the communications policy of office **62** for each access station **34**, in this case simply the decision to either "Allow Communication", or "Disallow Communication". In this case a communication is allowed through access stations AID_1, AID_2 and AID_3. (It should now be apparent that other communications policies (rather than "allow" or "disallow" communication) can be stored in CP databases **118**, and **122**. For example, the communication policy stored may be to limit the length of the call when device **58** is in range of some access stations and allow limitless calls when in range of others. It should also be apparent that a combination of policies can also be used.)

[**0040**] By the same token, device **58** also includes CP database **122** that includes data corresponding to the information stored in CP database **118**. The initial settings of CP database **122** are shown in Table II.

TABLE II

Example of a CP Database 122 of Device 58

Field 1 Access Station Identifier	Field 2 Policy for Voice Calls
AID_1	Allow Communication
AID_2	Allow Communication
AID_3	Allow Communication

Field 1 of database **122** corresponds to Field 2 of database **118**, and Field 2 of database **122** corresponds to Field 3 of database **118**. Because initially, when the user first acquires the device from office **62**, device database **122** has the same content as the office database **118**.

[**0041**] The policy, as described by CP database **118**, is set by office **62** and updated by office **62** from time to time as needed. For example, office **62** may desire that device **58** should place wireless calls through network **50** only when a digital link is available between an access station **34** and device **50** to reduce the chances that the wireless portion of the call is intercepted. According to this policy office **62** would not want device **58** to connect to network **50** through access stations $\mathbf{34}_2$ or $\mathbf{34}_3$ since stations $\mathbf{34}_2$ $\mathbf{34}_3$ only provide an analog link $\mathbf{42}_2$ $\mathbf{42}_3$ based on AMPS which is highly susceptible to interception. Thus, policy database **118** would be updated to reflect the new policy as shown in Table III.

TABLE III

Example record of an Updated CP Database 118 of Office 62
Record # 1

Field 1 Device Identifier	Field 2 Access Station Identifier	Field 3 Policy for Voice Calls
555-555-5555	AID_1	Allow Communication
	AID_2	Disallow Communication
	AID_3	Disallow Communication

Notice that Field 3 associated with AID_2 has been changed to "Disallow Communication" to reflect the new policy that device **58** should not connect to network **50** through access station $\mathbf{34}_2$.

[0042] At this point device database **122** no longer contains the same policies as office database **118**. Office **110** is operable to update CP database **122** of device **58** by communicating with device **58** when device **58** connects to network **54**.

[0043] Referring to **FIG. 4**, a method for updating policy database **122** is indicated generally at **200**. In order to assist in the explanation of the method, it will be assumed that method **200** is operated using system **30**, and that device **58**, as shown in **FIG. 1**, is located in range $\mathbf{38}_1$. Furthermore, the following discussion of method **200** will lead to further understanding of system **30** and its various components. (However, it is to be understood that system **30** and/or method **200** can be varied, and need not work exactly as discussed herein in conjunction with each other, and that such variations are within the scope of the present invention).

[0044] Referring back to **FIG. 4**, at step **210** a link is established. As an example of how step **210** can be performed, device **58** establishes link $\mathbf{42}_1$ with station $\mathbf{34}_1$ which is serving the range $\mathbf{38}_1$. Moving to step **220**, a connection is made with an office server. Continuing with the example, when step **220** is performed device **58** will use link **42**, established at step **210** to connect to network **54**, and through network **54**, will eventually make a connection to office server **110**.

[0045] Method **200** will then advance from step **220** to step **230**, at which point the new policy is transferred. Continuing with the example, database **122** is updated by transferring the new policy to device **58**. The updated CP database **122** is shown in Table IV.

TABLE IV

Example of an Updated CP Database 122 of Device 58

Field 1 Access Station Identifier	Field 2 Policy for Voice Calls
AID_1	Allow Communication
AID_2	Disallow Communication
AID_3	Disallow Communication

[0046] To summarize the example, database **122** originally held the contents of Table II, but upon performance of method **200** using the specific example, database **122** now holds the contents of Table IV. Thus, a policy administered from office **62** has remotely changed base stations **34** that are accessible by device **58** from all access stations **34** down to access station $\mathbf{34}_1$.

[0047] Referring now to **FIG. 5**, a method for placing a wireless call through network **50**, according to CP database **122**, is indicated generally at **300**. In order to assist in the explanation of the method, it will be assumed that method **300** is operated using system **30** and that device **58**, as shown in **FIG. 1**, is located in range $\mathbf{38}_1$. Furthermore, the following discussion of method **300** will lead to further understanding of system **30** and its various components. (However, it is to be understood that system **30** and/or method **300** can be varied, and need not work exactly as discussed herein in conjunction with each other, and that such variations are within the scope of the present invention.)

[0048] Referring back to **FIG. 5**, at step **310** a link is established. As an example of how step **310** can be performed, device **58** establishes link $\mathbf{42}_1$ with station $\mathbf{34}_1$ which is serving range $\mathbf{38}_1$. Moving to step **320**, an identifier is received. Continuing with the example, when step **320** is performed device **58** receives the identifier associated with an access station **34**. In this case, the identifier is AID_1 which is the identifier of access station $\mathbf{34}_1$.

[0049] Method **300** then advances from step **320** to step **330**, at which point a determination is made as to whether communication is permissible. In this example, the office policy is examined to determine whether communications through access station $\mathbf{34}_1$ are permitted. To perform this step, device **58** examines the office policy regarding wireless calls associated with identifier AID_1 in CP database **122**. In this case, the policy associated with AID_1 is "Allow Communication". Accordingly, step **350** is performed next and communication is established. Accordingly, in this example, device **58** places a wireless call through network **50**.

[0050] Referring to **FIG. 6**, device **58** now moves to range $\mathbf{38}_2$, served by access station $\mathbf{42}_2$. In order to place a wireless call using device **58**, according to CP database **122**, method **300** is performed a second time.

[0051] Referring back to **FIG. 5**, at step **310** a link is established. As an example of how step **310** can be performed during this second performance of method **300**, device **58** establishes link $\mathbf{42}_2$ with station $\mathbf{34}_2$ which is serving range $\mathbf{38}_2$. Moving to step **320**, an identifier is received. Continuing with the example, when step **320** is performed device **58** receives the identifier associated with access station **34**. In this case, the identifier is AID_2 which is the identifier of access station $\mathbf{34}_2$.

[0052] Method **300** then advances from step **320** to step **330**, at which point a determination is made as to whether communication is permissible. In this example, the office policy is examined to determine whether communications through access station $\mathbf{34}_2$ are permitted. To perform this step, device **58** examines the office policy regarding wireless calls associated with identifier AID_1 in CP database **122**. In this case, the policy associated with AID_2 is "Disallow Communication", as shown in Field 2 of Table IV. Accordingly, step **340** is performed next and communication is not permitted. Accordingly, in this example device **58** is prevented from placing a call.

[0053] Referring now to **FIG. 7**, a system for secure access in accordance with another embodiment of the invention is indicated generally at **30*a***. System **30*a*** is substantially the same as system **30**, and like elements in system **30*a*** bear the same reference as like elements in system **30**, except followed by the suffix "a". System **30*a*** differs from system **30** in that in system **30*a*** different policy databases are used.

[0054] In this embodiment, office **62*a*** desires that device **58*a*** place wireless calls through network **50*a*** only using wireless carrier $\mathbf{46}a_1$ since wireless carrier $\mathbf{46}a_1$ offers cheaper connections than other carriers **46*a***. According to this policy, office **62*a*** would not want device **58*a*** to connect to network **50*a*** through access station $\mathbf{34}a_2$ since station $\mathbf{34}a_2$ is operated by wireless carrier $\mathbf{46}a_2$. CP database **118*a*** reflecting this policy is shown in Table V.

TABLE V

Example record of an Updated CP Database 118a of Office 62a Record # 1		
Field 1 Device Identifier	Field 2 Wireless Carrier Identifier	Field 3 Policy
555-555-5555	WID_1	Allow Communication
	WID_2	Disallow Communication

Notice that Field 3 associated with WID_2 is set to "Disallow Communication" to reflect the new policy that device **58***a* should not connect to network **50***a* through wireless carrier **46***a*$_2$. Such a policy that limits communications according to carrier could be desired for a number of reasons, such as reducing or controlling roaming charges, such that a particular device **58***a* can only perform communications in a home region. Other criteria for setting policies that reside in device **58***a* which define access stations **34***a* that are accessible to device **58***a* will now occur to those of skill in the art.

[**0055**] By the same token, device **58***a* also includes a CP database **122***a* that includes data that corresponds with the information stored in connection policy database **118***a*. Contents of CP database **122***a* is updated by performing method **200**, shown in **FIG. 4** in substantially the same manner as database **122** in system **30**. The updated CP database **122***a* is shown in Table IV.

TABLE VI

Example of an Updated CP Database 122a of Device 58a	
Field 1 Wireless Carrier Identifier	Field 2 Policy for Voice Calls
WID_1	Allow Communication
WID_2	Disallow Communication

[**0056**] Referring back to **FIG. 7**, device **58***a* is in range **38***a*$_2$, served by access station **42***a*$_3$. In order to place a wireless call using device **58***a*, according to CP database **122***a*, method **300** is performed.

[**0057**] Referring back to **FIG. 5**, at step **310** a link is established. As an example of how step **310** can be performed, device **58***a* establishes link **42***a*$_3$ with station **34***a*$_3$ which is serving range **38***a*$_3$. Moving to step **320**, an identifier is received. Continuing with the example, when step **320** is performed device **58***a* receives the identifier associated with wireless carrier **46***a*. In this case, the identifier is $WIDa_1$ which is the identifier associated with wireless carrier **46***a*$_1$, operating access station **34***a*$_3$.

[**0058**] Method **300** then advances from step **320** to step **330**, at which point a determination is made as to whether communication is permissible. In this example, the office policy is examined to determine whether communications through access stations operated by wireless carrier **46***a*$_1$ are permitted. To perform this step, device **58***a* examines the office policy regarding wireless calls associated with identifier $WIDa_1$ in CP database **122***a*. In this case, the policy associated with $WIDa_1$ is "Allow Communication", as shown in Field 2 of Table VI. Accordingly, step **350** is performed next and communication is established. Accordingly, in this example, device **58***a* places a wireless call through network **50***a*.

[**0059**] Referring now to **FIG. 8**, a system for secure access in accordance with another embodiment of the invention is indicated generally at **30***b*. System **30***b* is substantially the same as system **30**, and like elements in system **30***b* bear the same reference as like elements in system **30**, except followed by the suffix "b". System **30***b* differs from system **30** in that in system **30***b* all links **42** are digital and that different policy databases are used.

[**0060**] In system **30***b* office **62***b* employs CP database **118***b* which is substantially the same as CP database **118** but has additional fields used for determining which access stations **34***b* a device **58***b* can link with in order to connect to different networks when using different applications (e.g. voice calls, web browsing, and e-mail). For example, an additional field is used for determining which access stations **34***b* a device **58***b* can link to in order to connect to e-mail through the Internet (network **54***b*). A further field is used for determining which access stations are linkable for surfing the web through the Internet (network **54***b*). Table VII shows an example of database **118***b* of office **62***b* for device **58***b*.

TABLE VII

Example record of a Connection Policy Database 118b of Office 62b				
Field 1 Device Identifier	Field 2 Access Station Identifier	Field 3 Policy for Voice Calls	Field 4 Policy for E-mail Through The Internet	Field 5 Policy for Web-surfing Through The Internet
555-555-5555	AID_1	Allow Communication	Allow Communication	Disallow Communication
	AID_2	Allow Communication	Allow Communication	Disallow Communication
	AID_3	Allow Communication	Disallow Communication	Allow Communication

Table VII shows one record, labelled Record 1, which reflects information corresponding to device **58***b*. It should now be apparent that database **118***b* can include additional records for any additional devices **58***b* that are included in system **30***b*, or additional fields for additional applications available on device **58***b*.

[**0061**] Describing Table VII in greater detail, Fields 1 through 3 contain the same information as CP database **118**, shown in Table I. Field 4 contains the communications policy of office **62***b* for each access station **34***b*, in this case simply the decision to either "Allow Communication", or "Disallow Communication", to be used when device **58***b* attempts to check e-mail through network **54***b*. In this case, device **58***b* can only check e-mail when connected to network **54***b* through access stations $\mathbf{34}b_1$ and $\mathbf{34}b_2$. Note also that device **58***b* is permitted to place voice calls through any of the access stations **34***b*.

[**0062**] Continuing with the description of Table VII, Field 5 contains the communications policy of office **62***b* for each access station **34***b*, in this case simply the decision to either "Allow Communication", or "Disallow Communication", to be used when device **58***b* attempts to surf the web through network **54***b*. In this case device **58***b* can surf the web only through access stations $\mathbf{34}b_3$. (It should now be apparent that other communications policies (rather than "allow" or "disallow" communication) can be stored in CP databases **118***b*, and **122***b*. For example, a communication policy may limit the data bandwidth when device **58***b* is in range of some access stations **34***b* and allow limitless bandwidth when in range of others. It should also be apparent that a combination of policies can also be used.)

[**0063**] Device **58***b* also includes a CP database **122***b* that includes data that corresponds with the information stored in connection policy database **118***b*. CP database **122***b* is updated by performing method **200**, shown in **FIG. 3** in substantially the same manner as CP database **122** in system **30**. The updated CP database **122** is shown in Table VIII.

TABLE VIII

Example of a CP Database 122b of Device 58b

Field 1 Access Station Identifier	Field 2 Policy for Voice Calls	Field 3 Policy for E-mail Through The Internet	Field 4 Policy for Web-surfing Through The Internet
AID_1	Allow Communication	Allow Communication	Disallow Communication
AID_2	Allow Communication	Allow Communication	Disallow Communication
AID_3	Allow Communication	Disallow Communication	Allow Communication

[**0064**] Field 1 of database **122***b* corresponds to Field 2 of database **118***b*, Field 2 of database **122***b* corresponds to Field 3 of database **118***b*, Field 3 of database **122***b* corresponds to Field 4 of database **118***b* and Field 4 of database **122***b* corresponds to Field 5 of database **118***b*.

[**0065**] Referring back to **FIG. 8**, which gives an example arrangement, device **58***b* is range $\mathbf{38}b_1$, served by access station $\mathbf{34}_1$. When device **58***b* attempts to access e-mail, method **300** is performed again to determine the permissibility of the e-mail access. Performance of method **300** using system **30***b* is substantially the same as the performance of method **300** using system **30** except that Field 3 of database **122***b* is used to determine the policy as opposed to using Field 2 to determine the policy for voice calls. In this example, the e-mail policy associated with access station **34***b*, (as identified by $AIDb_1$) is to allow communications. Thus, device **58***b* will be able to access e-mail. When device **58***b* attempts to surf the web, on the other hand, performance of method **300** will disallow access to the web since the policy associated with web surfing in region $\mathbf{38}_1$ (specified by the first row of Field 4 of Table VIII) is to disallow communication.

[**0066**] While only specific combinations of the various features and components of the present invention have been discussed herein, it will be apparent to those of skill in the art that subsets of the disclosed features and components and/or alternative combinations of these features and components can be utilized, as desired. For example, although GSM and AMPS are wireless communication methods contemplated, it should now be apparent that other wireless communication methods such as the Code Division Multiple Access ("CDMA") for digital connections and the Total Access Communication System ("TACS") for analog connections are all within the scope of the invention. Other methods include General Packet Radio Service ("GPRS"), and Orthogonal Frequency Division Multiplexing ("OFDM"), amongst others.

[**0067**] In another variation, database **122** in system **30** can be updated through a direct connection between device **58** and office server **110**. It should now be apparent that this direct connection can take the form of a wired connection such as a Universal Serial Bus ("USB") connection, a cross-linked peer to peer Ethernet connection, or a wireless connection such as a Bluetooth connection, an infrared (IR) connection, or a peer to peer IEEE 801.11 (e.g. 802.11b, 802.11g or other 802.11 variants) connection. In yet another variation, database **122** could be updated through a Local Area Connection ("LAN") to which both device **58** and office server **110** are connected.

[**0068**] In another variation, different criteria other than location of device **58** can be used for enabling, disabling or otherwise varying the communication capabilities of device **58**. For example, time can be used as a determinant of communication capabilities. Accordingly, device **58** and certain applications performing on device **58**, such as e-mail, could be allowed to communicate during certain periods of time such as daytime, and certain other applications, such as voice calls, could be able to communicate during other time periods such as night time. These policies can be designed, for example, to take advantage of periods during which certain services are offered at reduced costs by wireless carriers. Thus, office **62** can set up a policy database **118** which allows voice calls only during evenings and weekends when voice calls are cheaper. As another example, policies can be set up to choose between different wireless carriers when each region is served by multiple carriers. So, for example, if a region **38** is served by 2 access stations **34**, device **58** can determine which access station to use consulting the communications policy (namely during the performance of method **300**). Accordingly, when there is a choice of carriers, policies could be designed to select more secure, less expensive or otherwise more desirable wireless carrier over those carriers that are less secure, more expensive or otherwise less desirable.

[**0069**] In yet another variation, device CP database **122** could be updated using different methodologies. For

example, the transfer of CP database **118** could be made selectively, transferring the database only when a difference is found between CP database **118** and **122**. It should now be apparent that a variety of different methods could be employed for determining a difference. For example, each field of database **118** can be compared to the equivalent fields in database **122** to determine whether there are any differences. Alternatively, sizes of the database files or the date of modification of these files could be compared. Moreover, the comparison can be done either by office server **110**, device **58** or some other computer trusted with maintaining synchronized CP databases between the office and the roaming devices. All these methods, and other methods for determining whether a CP database should be transferred to device **58** are within the scope of this invention.

[**0070**] In other variations, the policy can be stored in forms other than a database such as a lookup table. Moreover, the policy can be stored at a computer other than the office server. For example, the policy can be stored on routers and other dedicated computing devices. Also, the policy could be stored on a computer or other electronic device which is operated by an entity other than the office that operates the mobile devices.

[**0071**] While portions of the foregoing description may individually reference systems **30**, **30***a*, **30***b* and **30***c*, it should now be apparent that all or parts of each of these systems can be combined as appropriate or otherwise desired. Accordingly, those of skill in the art will recognize that when certain references are made to one of these systems, and/or its components, such teachings can also be applicable to other ones of those systems.

[**0072**] The above-described embodiments of the invention are intended to be examples of the present invention and alterations and modifications may be effected thereto, by those of skill in the art, without departing from the scope of the invention which is defined solely by the claims appended hereto.

1. A subscriber device comprising:

an interface operable to conduct communications over a link with at least one base station in each of a plurality of geographic regions; and,

a microcomputer connected to said interface and operable to maintain a policy associated with each said region; said policy defining whether communications between said interface and said at least one base station are permitted for each said region; said microcomputer permitting said interface to communicate in accordance with said policy.

2. The device of claim 1 wherein said communications include a plurality of different services.

3. The device of claim 2 wherein said services include at least one of voice, emails, internet browsing and text messaging.

4. The device of claim 2 wherein said policy permits one of said services in a specific region and disallows another one of said services in said specific region.

5. The device of claim 1 wherein said policy is disallows said communications in at least one of said regions if said communications within said region are insecure.

6. The device of claim 1 wherein said policy is disallows said communications in at least one of said regions if a cost for conducting said communications exceeds a predefined threshold.

7. The device of claim 1 wherein said links include wireless links that can be based on one or more of CDMA, OFDM, AMPS, GSM, GPRS, bluetooth, infra-red and 802.11.

8. The device of claim 1 wherein said links includes wired links that can be based on Ethernet; USB; Firewire and RS-232.

9. A method of conducting communications from a subscriber device comprising:

establishing a link with a base station from said subscriber device;

receiving an identifier from said base station at said subscriber device;

determining whether communications with said base station are permitted based on said identifier; and,

conducting said communications from said subscriber device only if communications are permitted.

10. The method of claim 9 wherein said communications include a plurality of different services.

11. The method of claim 10 wherein said services include at least one of voice, emails, internet browsing and text messaging.

12. The method of claim 10 wherein said determining step includes determining whether one of said services in a specific region associated with said base station is allowed.

13. The method of claim 10 wherein said determining step policy disallows said communications with at least one of said base stations if communications within said base station are insecure.

14. The method of claim 10 wherein said determining step is disallows said communications in at least one of said regions if a cost for conducting said communications exceeds a predefined threshold.

15. The method of claim 9 wherein said link is a wireless link based on one or more of CDMA, OFDM, AMPS, GSM, GPRS, bluetooth, infra-red and 802.11.

16. The method of claim 9 wherein said link is a wired link based on Ethernet; USB; Firewire and RS-232.

17. A server for communicating with a plurality of subscriber devices comprising:

a microcomputer operable to maintain a policy defining whether communications between at least one subscriber station and at least one base station is permitted; and,

an interface for delivering said policy to each of said at least one subscriber station.

18. A computer readable media operable to store a set of programming instructions; said programming instructions for operating a server that is for communicating with a plurality of subscriber devices; said programming instructions executable on a microcomputer associated with said server; said programming instructions for rendering said microprocessor operable to maintain a policy defining whether communications between at least one subscriber station and at least one base station is permitted.

19. A computer readable media operable to store a policy for storage in a subscriber station; said policy defining whether communications between a subscriber station and said at least one base station are permitted.

* * * * *