US 20050278448A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2005/0278448 A1

Mazor (43) Pub. Date: Dec. 15, 2005

(54) SYSTEM AND METHOD FOR PIN-TO-PIN NETWORK COMMUNICATIONS

(76) Inventor: **Gadi Mazor**, Ramat Efal (IL)

Correspondence Address:
PILLSBURY WINTHROP LLP
P.O. Box 10500
McLean, VA 22102 (US)

(21) Appl. No.: **10/892,243**

(22) Filed: **Jul. 16, 2004**

Related U.S. Application Data

(60) Provisional application No. 60/488,005, filed on Jul. 18, 2003.

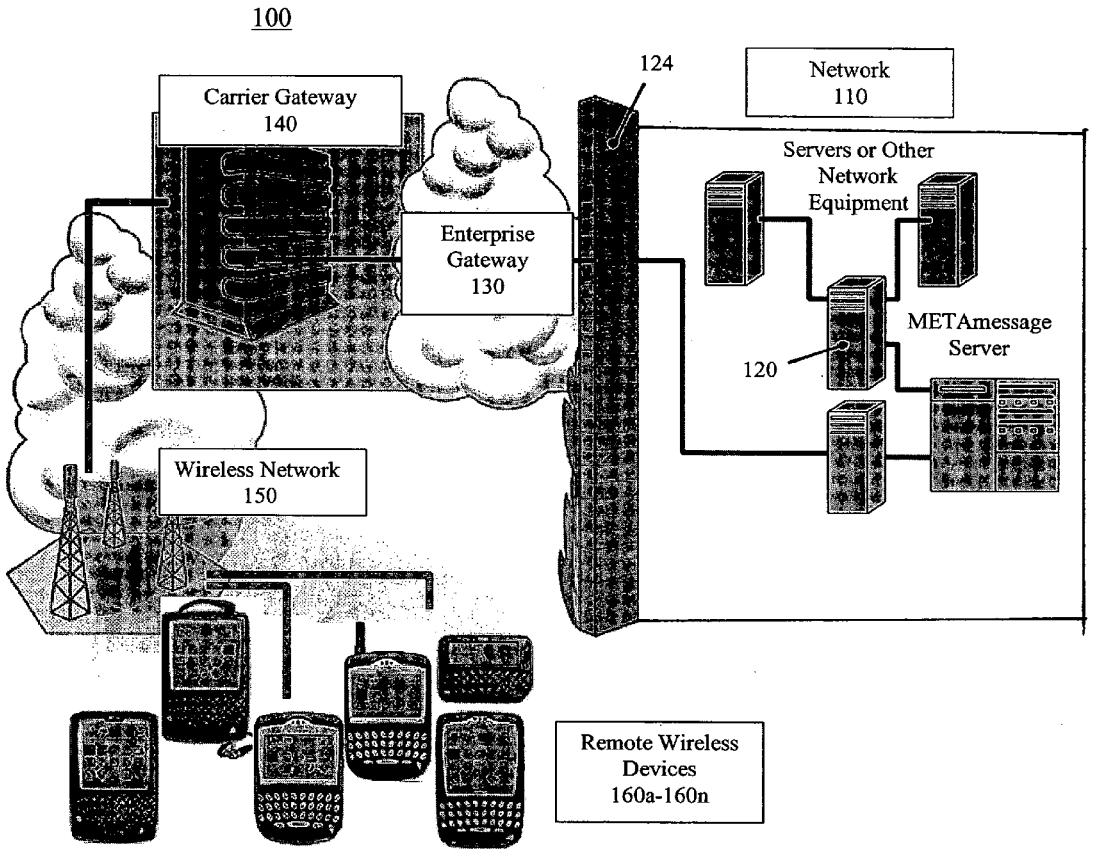
Publication Classification

(51) **Int. Cl.**[7] **G06F 15/16**

(52) **U.S. Cl.** **709/227**

(57) **ABSTRACT**

A system and method is provided for enabling wireless access to a computer network via communication between a remote (client) wireless device and a wireless device physically linked to the computer network. A bank of one or more wireless gateway devices may be cradled and connected to a network server. The wireless gateway devices may then act as a node on the wireless network, and remote wireless devices may send and receive messages to and from the wireless gateway devices using PIN-to-PIN messaging. The wireless gateway devices, when cradled, may communicate with any attached server or other network equipment, and may therefore act as a wireless gateway to the server or other network equipment.



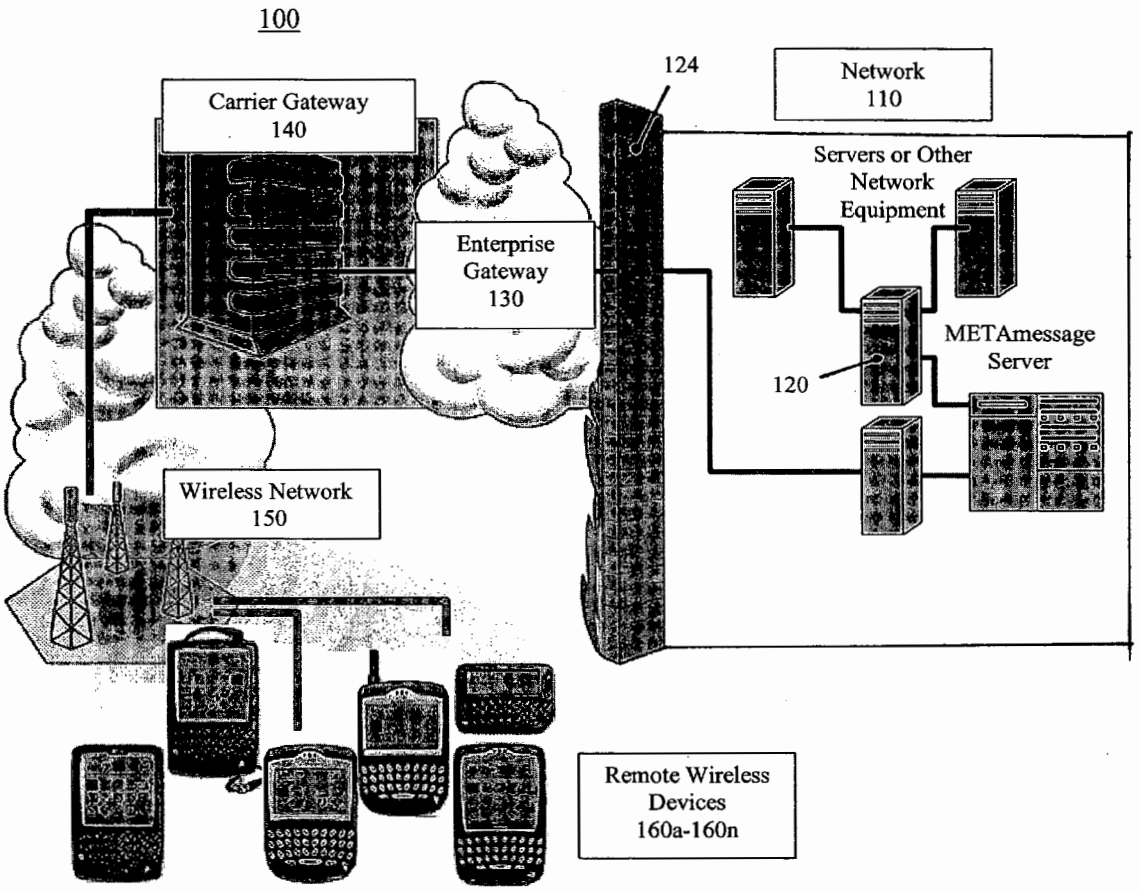

100
124
Network
110
Carrier Gateway
140
Enterprise
Gateway
130
Servers or Other
Network
Equipment
METAmessage
Server
120
Wireless Network
150
Remote Wireless
Devices
160a-160n

FIG. 1

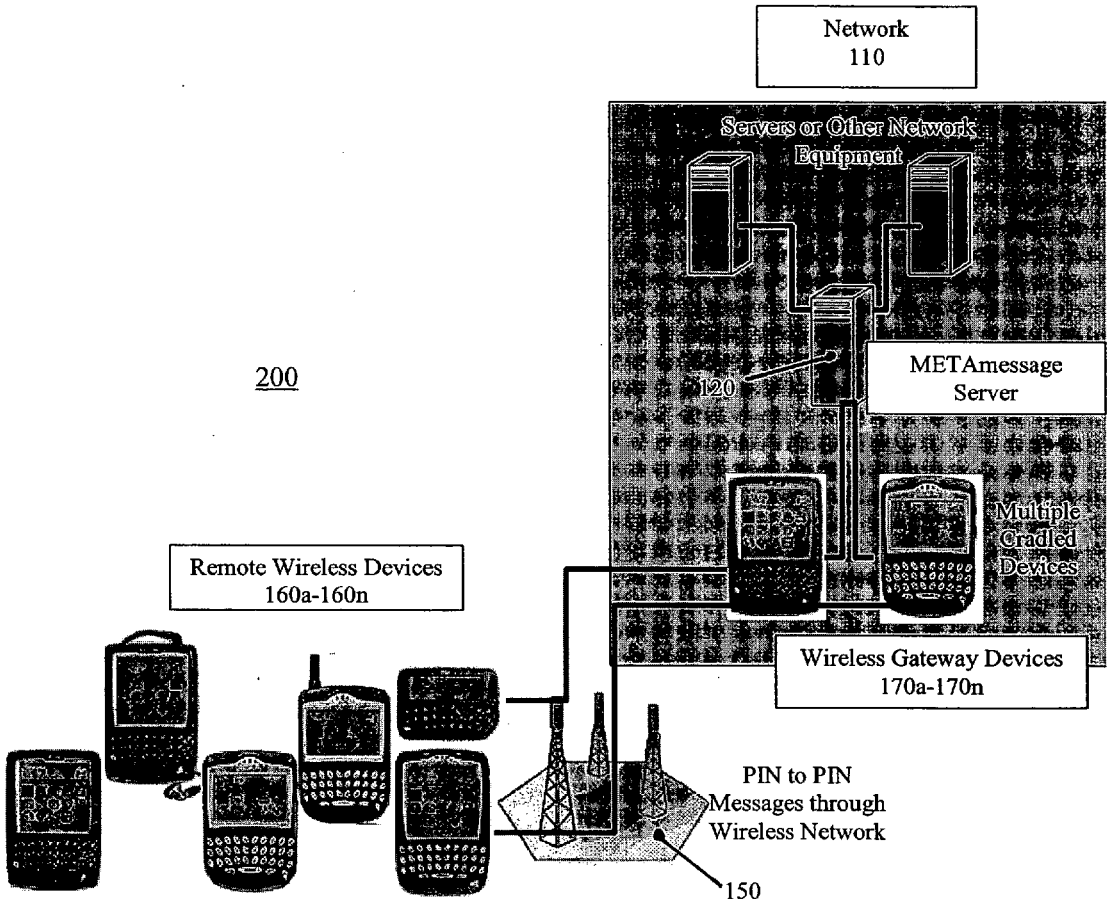

Network
110
Servers or Other Network
Equipment
200
120
METAmessage
Server
Multiple
Cradled
Devices
Remote Wireless Devices
160a-160n
Wireless Gateway Devices
170a-170n
PIN to PIN
Messages through
Wireless Network
150

FIG. 2

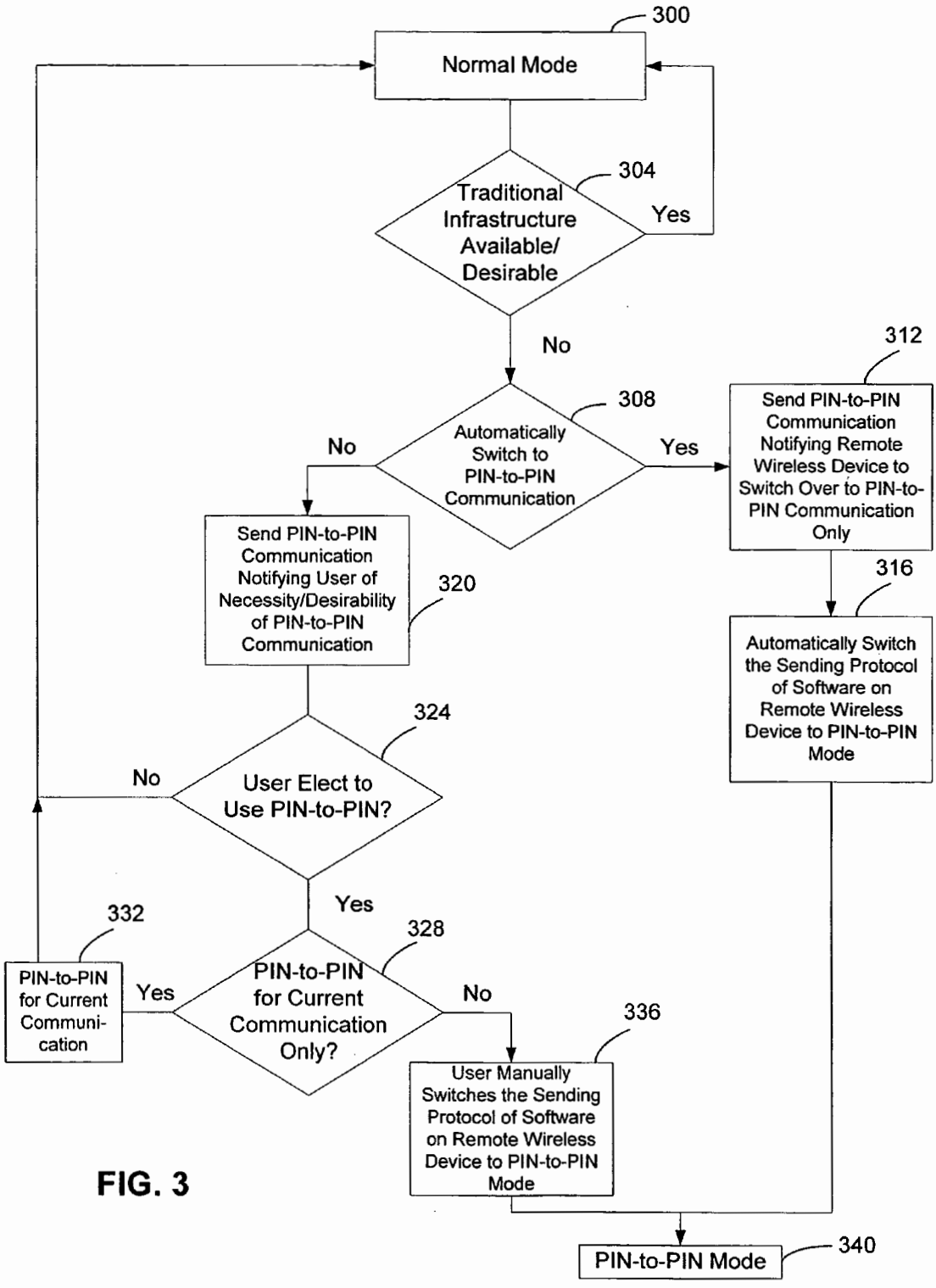

300
Normal Mode
304
Traditional Infrastructure Available/ Desirable
Yes
No
308
Automatically Switch to PIN-to-PIN Communication
No
Yes
312
Send PIN-to-PIN Communication Notifying Remote Wireless Device to Switch Over to PIN-to-PIN Communication Only
316
Automatically Switch the Sending Protocol of Software on Remote Wireless Device to PIN-to-PIN Mode
Send PIN-to-PIN Communication Notifying User of Necessity/Desirability of PIN-to-PIN Communication
320
324
User Elect to Use PIN-to-PIN?
No
Yes
332
PIN-to-PIN for Current Communi-cation
328
PIN-to-PIN for Current Communication Only?
Yes
No
336
User Manually Switches the Sending Protocol of Software on Remote Wireless Device to PIN-to-PIN Mode
PIN-to-PIN Mode
340

FIG. 3

SYSTEM AND METHOD FOR PIN-TO-PIN NETWORK COMMUNICATIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application Ser. No. 60/488,055, filed Jul. 18, 2003, which is incorporated herein by reference.

FIELD OF THE INVENTION

[0002] This invention relates to a system and method for enabling wireless access to a computer network via communication between a remote (client) wireless device and a wireless device physically linked to the computer network.

BACKGROUND OF THE INVENTION

[0003] Wireless computing devices such as, for example, the BlackBerry™ hand-held device by Research in Motion Limited, typically provide users with wireless access to important enterprise information. System infrastructures (or architectures) supporting such devices may generally comprise a wireless network, a carrier gateway, an enterprise gateway (e.g., the BlackBerry™ Enterprise Server or "BES"), and other back-end servers (e.g., Exchange, DB systems, document management systems, etc.), or other components.

[0004] Wireless servers, such as Onset Technology's METAmessage server, may be provided to further enhance the features and functionality of known wireless systems (such as the BlackBerry™ system) by enabling users to access and manage information—data from document management programs, voicemail, SQL/ODBC databases, and CRM/ERP applications, email attachments, network files, web pages, contact information, etc.—from their wireless device.

[0005] In disaster scenarios, such as that of Sep. 11, 2001, various components of a system infrastructure necessary to access important enterprise information from a wireless device may become unavailable. Connectivity to an enterprise may be lost, or back end systems such as BES and Exchange may not function. While wireless devices and wireless networks (e.g., the pager Mobitex and DataTac networks) may operate, as was the case on Sep. 11, 2001, they may still be ineffective if other components of the system infrastructure do not function.

[0006] Certain wireless devices have a dedicated device number or "PIN" which may serve as the device's identifier on a network. PIN's also enable wireless devices on a network to communicate with one another via PIN-to-PIN messaging. This form of communication may occur from device to device through the wireless network, and without the need for a carrier gateway, enterprise gateway, or other system or server. This form of communication may also be quite valuable in the event of a disaster or other scenario if various components of a system infrastructure are comprised. One drawback associated with PIN-to-PIN messaging, however, is that a user must typically know the PIN address of the wireless device of a user that he or she wishes to communicate with. This may be an unlikely occurrence, as most users tend to remember e-mail addresses and/or telephone numbers for contacts, and not the PIN addresses of their wireless devices. These and other drawbacks exist.

SUMMARY OF THE INVENTION

[0007] The invention solving these and other problems relates to a system and method for enabling wireless access to a computer network via communication between a remote (client) wireless device and a wireless device physically linked to the computer network.

[0008] One embodiment of the invention enables users to retrieve the PIN addresses of other wireless devices, as well as interact with designated database systems, file directories, or other back end systems, even if portions of the system infrastructure are unavailable.

[0009] According to an embodiment of the invention, a bank of one or more wireless devices may be cradled and connected to the network, a METAmessage server provided by Onset Technology, Inc., or other back-end server. For convenience, these cradled devices will be referred to herein as "wireless gateway devices." The wireless gateway devices may then act as a node on the wireless network, and remote wireless devices may send and receive messages to and from the wireless gateway devices using PIN-to-PIN messaging. The wireless gateway devices, when cradled, may communicate with any attached server or other network equipment, and may therefore act as a wireless gateway to the server or other network equipment. Accordingly, one or more components of the system architecture that may be unavailable may be bypassed, and a direct link from the devices to the network equipment may be provided.

[0010] According to one embodiment, the addresses of the wireless gateway devices may be stored in a remote wireless device, or may be transmitted in case of emergency to the remote wireless device through a PIN-to-PIN message. The remote wireless device, which typically communicates with the enterprise systems through email or other data channels, may switch to PIN-to-PIN messaging either manually, through operation of the user, or automatically, in response to a received PIN-to-PIN message. The remote wireless device may store multiple addresses of wireless gateway devices, and may send each communication to more than one of those wireless gateway devices, for redundancy purposes. According to one embodiment, multiple METAmessage servers may be provided in different locations, to further make the solution redundant. The wireless gateway devices may be served by different wireless networks, for further redundancy.

[0011] According to an embodiment of the invention, a user of a remote wireless device may have access to any information on the METAmessage (or other) server, or on any devices connected to it. As one example, a fax server provided with (or connected to) the METAmessage server, or even just a fax card, may provide the additional functionality of enabling users to print any of the information to any fax machine. This further enhances the solution to support lengthy documents that may not be easily read on the remote wireless device.

[0012] These and other objects, features, and advantages of the invention will be apparent through the detailed description of the preferred embodiments and the drawings attached hereto. It is also to be understood that both the foregoing general description and the following detailed description are exemplary and not restrictive of the scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] **FIG. 1** illustrates a wireless system infrastructure (or architecture) supporting communication from wireless devices to an enterprise or other network through carrier and enterprise gateways.

[0014] **FIG. 2** is an exemplary illustration of a system architecture for enabling PIN-to-PIN communication between remote wireless devices to facilitate continued transmission of information during or after a disaster or disruptive event, according to an embodiment of the invention.

[0015] **FIG. 3** illustrates a flowchart of processing according to the invention, in one regard.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0016] With regard to **FIG. 1**, a system infrastructure **100** (or architecture) is illustrated for supporting one or more remote wireless devices (**160***a*-**160***n*). A remote wireless device (**160***a*-**160***n*) may include any device capable of sending and receiving information through a wireless network including, but not limited to, a Blackberry,™ personal digital assistant (PDA), pager, laptop, cell phone, or other wireless device. System infrastructure **100** may comprise a wireless network **150** (e.g., the pager Mobitex or DataTac networks, etc.), a carrier gateway **140**, an enterprise gateway **130** (e.g., the BlackBerry™ Enterprise Server), and a computer network **110** (e.g., a corporate or other network). In some embodiments, a firewall **124** may be provided to prevent unauthorized access to or from computer network **110**.

[0017] Computer network **110** may further comprise one or more "back-end" servers (e.g., a Microsoft Exchange server), database systems, document management systems, or other servers or components. As an example, a wireless server **120**, such as Onset Technology's METAmessage server, may be provided to enable users to access and manage information—data from document management programs, voicemail, SQL/ODBC databases, and CRM/ERP applications, email attachments, network files, web pages, contact information, etc.—from their respective wireless device (**160***a*-**160***n*).

[0018] In the event that system infrastructure **100** is disrupted (e.g., there is a loss of ability to communicate with "back-end" servers through carrier gateway **140** and/or enterprise gateway **130**), an embodiment of the invention enables remote wireless devices (**160***a*-**160***n*) themselves to be used to facilitate communication with back end servers or other network equipment.

[0019] According to an embodiment of the invention illustrated in **FIG. 2**, an exemplary illustration of a system infrastructure **200** (or architecture) is provided for enabling wireless access to computer network **110** via communication between remote wireless devices (**160***a*-**160***n*) and one or more wireless gateway devices (**170***a*-**170***n*) physically linked to computer network **110**.

[0020] In one implementation, PIN-to-PIN messaging may be used to bypass one or more components of system infrastructure **200**. As recited above, PIN-to-PIN messaging refers to the transmission of information from one remote wireless device (e.g., **160***a*-**160***n*) to another (e.g., **160***a*-**160***n*-or-**170***a*-**170***n*) over a wireless network **150**. This communication may be accomplished through the use of dedicated PIN identifiers (or addresses) associated with wireless devices. PIN identifiers may comprise any indicator that serves to identify a particular wireless device on a wireless network. Wireless network **150** may comprise any known network including, but not limited to, Mobitex, Data Tac, or GPRS. Those having skill in the art understand that the nature of wireless devices is such that any particular wireless device may act as both a transmitter or a receiver.

[0021] PIN-to-PIN messages are not limited to those sent over the BlackBerry™ pager network (e.g., Mobitex and DataTec). They may include other types of messages that are sent from one device to another device, bypassing the carrier to enterprise link. For example, SMS messages used by cell phones are also PIN-to-PIN messages.

[0022] According to an embodiment of the invention, PIN-to-PIN messaging may be used to bypass traditional network infrastructure via one or more wireless gateway devices (**170***a*-**170***n*). Similar to remote wireless devices (**160***a*-**160***n*), a wireless gateway device (**170***a*-**170***n*) may include any device capable of sending and receiving information through a wireless network including, but not limited to, a Blackberry,™ personal digital assistant (PDA), pager, laptop, cell phone, or other wireless device.

[0023] According to an embodiment, a wireless gateway device (**170***a*-**170***n*) may be connected to one or more components of computer network **110** via a cradle or other similar mechanism. A cradle may comprise any device capable of physically connecting the circuitry of one electronic device (e.g., a wireless gateway device **170***a*-**170***n*) to the circuitry of another electronic device (e.g., a wireless server **120**). In one implementation, wireless server **120** may be serially connected to one or more cradled wireless gateway devices (**170***a*-**170***n*). Wireless server **120** may further either host or connect to any number of other servers, databases, or information sources such as, for example, a contact information database, emergency procedure files, or other enterprise applications.

[0024] According to an embodiment of the invention, wireless server **120** may comprise a METAmessage server provided by Onset Technology, Inc. As recited above, a METAmessage server may enhance the features and functionality of known wireless systems (such as the BlackBerry™ system) by enabling users to access and manage information—data from document management programs, voicemail, SQL/ODBC databases, and CRM/ERP applications, email attachments, network files, web pages, contact information, etc.—from their wireless device.

[0025] To increase the reliability of PIN-to-PIN messaging, and/or PIN-to-PIN access to computer network **110** (or to another network or enterprise), multiple wireless gateway devices (**170***a*-**170***n*) may be cradled and used for transmitting information to and from remote wireless devices (**160***a*-**160***n*) in the event that one or more of the wireless gateway devices (**170***a*-**170***n*) becomes inoperable or inaccessible. Further, multiple wireless servers **120** (or other servers) with accompanying wireless gateway devices may be placed in multiple locations to increase the redundancy of the system. Redundancy may be yet further increased by using multiple wireless networks **150** for the transmission of PIN-to-PIN

messages between remote wireless devices (**160***a*-**160***n*) and wireless gateway devices (**170***a*-**170***n*). If the wireless networks of one or more wireless gateway devices become inoperable, inaccessible, or otherwise unavailable, for any reason, wireless gateway devices operating on other wireless networks may take their place.

[**0026**] Having provided an overview of various embodiments of system infrastructure **200**, a description of the various features and functionalities of the invention with regard to PIN-to-PIN messaging, and/or PIN-to-PIN access to a computer network or networks will now be described. It should be understood that wireless server **120**, remote wireless devices (**160***a*-**160***n*), wireless gateway devices (**170***a*-**170***n*), or other servers or components of system infrastructure **200** may include various software modules to accomplish the functionalities described herein. In other embodiments, as would be appreciated, the functionalities described herein may be implemented in various combinations of hardware and/or firmware, in addition to, or instead of, software.

[**0027**] According to an embodiment of the invention, users of remote wireless devices (**160***a*-**160***n*) may elect whether to use the PIN-to-PIN function of the device for either PIN-to-PIN messaging or PIN-to-PIN access to a component (e.g., a server) of computer network **110**. If this function is elected, a user needs to know or should be able to conveniently access the PIN address of a target device or system component.

[**0028**] In one embodiment, if PIN-to-PIN messaging is desired or needed to bypass unavailable components of system infrastructure **200**, wireless gateway devices (**170***a*-**170***n*) may send initial PIN-to-PIN messages to remote wireless devices (**160***a*-**160***n*) to provide the devices with the PIN identifiers (or addresses) for one or more of wireless gateway devices (**170***a*-**170***n*). The initial PIN-to-PIN messages may also be used to alert users of the need (e.g., in case of an emergency) to switch to PIN-to-PIN communication. PIN addresses of one or more wireless gateway devices (**170***a*-**170***n*) needed for access to computer network **110** may also be stored on the remote wireless devices (**160***a*-**160***n*) and may be updated wirelessly from wireless server **120** (e.g., a METAmessage server) or from another server.

[**0029**] According to an embodiment of the invention, when one or more components of a traditional infrastructure (e.g., carrier gateway **140** or enterprise gateway **130** of system infrastructure **100** in **FIG. 1**) becomes unavailable, PIN-to-PIN communication may be initiated manually by the users of remote wireless devices (**160***a*-**160***n*).

[**0030**] In an alternative embodiment of the invention, remote wireless devices (**160***a*-**160***n*) may be automatically switched to PIN-to-PIN communication through, for example, a PIN-to-PIN message sent by wireless server **120** or other server. Client software on remote wireless devices (**160***a*-**160***n*) may monitor incoming messages and, when such a switching message arrives, switch the sending (or other communications) protocol of the device to PIN-to-PIN mode.

[**0031**] In some embodiments of the invention, a "notification" module may be located on wireless server **120** or on another server of computer network **110**. The notification module may store the PIN addresses of one or more remote wireless devices (**160***a*-**160***n*) and wireless gateway devices (**170***a*-**170***n*) on the network. The notification module may also facilitate notification to remote wireless device users that PIN-to-PIN communication is necessary (e.g., if one or more components of the system infrastructure becomes unavailable).

[**0032**] The notification module may also facilitate the distribution and maintenance of wireless gateway PIN addresses to remote wireless devices (**160***a*-**160***n*). Furthermore, the notification module may facilitate an automatic "switch" of remote wireless devices from normal communication to a PIN-to-PIN communication mode. The PIN addresses of remote wireless devices (**160***a*-**160***n*) and wireless gateway devices (**170***a*-**170***n*) may be changed or updated in the event that devices of any kind are added to, or removed from, the system. The notification module may also facilitate the determination of wireless gateway device availability.

[**0033**] According to one embodiment, remote wireless devices (**160***a*-**160***n*) may enable users to choose the wireless gateway devices (**170***a*-**170***n*) with which to communicate. Alternatively, the remote wireless devices (**160***a*-**160***n*) may automatically select particular wireless gateway devices (**170***a*-**170***n*) according to their type and/or availability, the type and/or availability of the wireless network **150**, or other criteria. Remote wireless devices (**160***a*-**160***n*) may send single communications to an enterprise or other network through multiple wireless gateway devices simultaneously, further increasing system redundancy.

[**0034**] It should be understood from the various embodiments described above that for either PIN-to-PIN messaging or PIN-to-PIN access to a component (e.g., a server) of computer network **110**, a user should be able to conveniently access the PIN address of a target device or system component. As such, in various embodiments, PIN addresses may be stored on either one or more of wireless server **120** (e.g., a METAmessage server) or other servers of computer network **110**, on one or more of wireless gateway devices (**170***a*-**170***n*), or in the address books (or other directory files) stored on remote wireless devices (**160***a*-**160***n*). As recited above, in those embodiments wherein PIN addresses are stored on remote wireless devices (**160***a*-**160***n*), the addresses may be updated wirelessly from wireless server **120** (e.g., a METAmessage server) or from another server, from wireless gateway devices (**170***a*-**170***n*), or even from other remote wireless devices (**160***a*-**160***n*). Alternative configurations may be implemented.

[**0035**] According to one embodiment, a PIN look-up feature may be provided enabling users to automatically update the address books of their remote wireless device with PIN addresses. A user may send a request with a partial name or initials (or other information) for a contact for which information is desired, and either wireless server **120**, wireless gateway devices (**170***a*-**170***n*), or other system servers or components may then reply with the desired contact information, and/or an option to update the user's handheld address book. Multiple matches may be accommodated by enabling a user to choose from a list of possible matches. If an identified contact has a PIN registered on the network, the PIN may be included with the contact information. In various implementations, access to contact information may be dependent upon on a user's network access rights, or subject to a security protocol.

[0036] According to an embodiment of the invention, a PIN update feature may be enabled. With Automatic PIN Updating, a user may request PIN's for every user on the network. An administrator may configure wireless server **120** (or other server) to either update only existing address book entries for a user, or to update existing entries and add entries that exist on the network but that are not yet in the user's address book.

[0037] According to an embodiment of the invention, PIN-to-PIN archiving functionality may be provided. As an example, administrators in sensitive sectors often disable PIN-to-PIN messaging due to regulations requiring that all messages such as e-mail be recorded or archived. In such instances, handheld wireless devices may be left unused in an emergency if the email server or other network infrastructure were down. According to an embodiment, wireless server **120** (or another system component) may enable administrators to archive PIN-to-PIN messages as a default protocol under normal conditions such that, in an emergency, the feature is enabled and handhelds are available for emergency communications. Upon sending a PIN message, content including "To:, CC:, and BCC:" information may be copied and sent via e-mail to a pre-determined address selected by an administrator or other individual. The message may then be processed with whatever method or tool that is configured by the administrator.

[0038] According to an embodiment of the invention, a "message blast" feature may be enabled. In an emergency, messages often have to go out to special categories of workers. As an example, one notification may be transmitted to all office managers, while another message may be sent to field personnel, etc. Since these individuals may utilize a variety of devices (e.g., BlackBerry handhelds using email or PIN-to-PIN messaging, pocket PC's, cell phones, desktop PC's, even fax machines), wireless server **120** (e.g., a METAmessage server) may enable, for example, a BlackBerry user to send one message to many addressees regardless of their device. The user may have access to three types of groups: a group of addresses created by an administrator; an existing BlackBerry Address Book group; and, a manually entered group. After selecting a group, a user may compose and send a message.

[0039] According to an embodiment of the invention, an "instant conference call" feature may be enabled for those users whose remote wireless device (**160***a*-**160***n*) is voice-enabled. This feature may enable a user to quickly set up a conference call by choosing from a list of pre-defined groups on, for example, their BlackBerry handheld, by selecting participants from the address book, or by entering new numbers. Working with either a local or hosted voice gateway, wireless server **120** may call and connects the intended participants, including the initiating user.

[0040] In addition to the foregoing description, **FIG. 3** illustrates a flowchart of processing according to the invention, in one regard. The following operations may be accomplished using all or some of the of the system components described in detail above, and may incorporate all of the features and functionality of the invention as set forth in the foregoing description and accompanying drawing figures.

[0041] In an operation **300**, a wireless system infrastructure (or architecture) supporting communication from wireless devices to an enterprise or other network through carrier and enterprise gateways, for example, may be functioning normally.

[0042] In an operation **304**, a determination may be made as to whether the wireless system infrastructure (or architecture) is available and functioning properly. If the system is functioning properly, it may be said to be in a "normal mode." If, however, it is determined in operation **304** that an emergency or other event (or series of events) has resulted in one or more components of the wireless system infrastructure (or architecture) becoming unavailable, or if use of the wireless system infrastructure is undesirable, a determination may be made, in an operation **308**, as to whether remote wireless devices may be automatically switched to PIN-to-PIN communication.

[0043] If it is determined in operation **308** that remote wireless devices should automatically be switched to PIN-to-PIN communication, a PIN-to-PIN communication may be sent by a server, wireless gateway device, or other server or device to a user's remote wireless device in an operation **312**. Client software on the remote wireless device may monitor incoming messages and, when such a switching message arrives, switch the sending (or other communications) protocol of the device to PIN-to-PIN mode (**340**) in an operation **316**.

[0044] By contrast, if it is determined in operation **308** that an automatic switch to PIN-to-PIN mode may not be required, a PIN-to-PIN communication may be sent by a server, wireless gateway device, or other server or device to a user's remote wireless device, in an operation **320**, notifying the user of the necessity or desirability of enabling PIN-to-PIN messaging or PIN-to-PIN access to a component (e.g., a server) of computer network.

[0045] In an operation **324**, a determination may be made by a user as to whether to initiate PIN-to-PIN communication. If a user elects to initiate PIN-to-PIN communication, a determination may be made in an operation **328** as to whether PIN-to-PIN messaging or other PIN-to-PIN communication may be used only for a current communication (e.g., a user needs to send one e-mail message).

[0046] If it is determined, in operation **328**, that PIN-to-PIN messaging or other PIN-to-PIN communication is to be used only for a current communication, then such a communication may occur in an operation **332**. By contrast, if it is determined that PIN-to-PIN communication should be enabled for a longer period of time, PIN-to-PIN communication may be initiated manually by a user in an operation **336**.

[0047] Other embodiments, uses and advantages of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. The specification should be considered exemplary only, and the scope of the invention is accordingly intended to be limited only by the following claims.

What is claimed is:

1. A method for communicating between a wireless device and a computer network that bypasses one or more components of a traditional wireless communication infrastructure, the method comprising:

cradling one or more wireless gateway devices to one or more servers or other pieces of equipment on a computer network;

sending information between the computer network and a remote wireless device via a wireless communication between one or more cradled wireless gateway devices and the remote wireless device.

2. A system for communicating between a wireless device and a computer network that bypasses one or more components of a traditional wireless communication infrastructure, the system comprising:

a remote wireless device; and

a cradled wireless gateway device in wireless communication with said remote wireless device, and coupled to the computer network, wherein said remote wireless device transmits info to and receives info from the computer network via the cradled wireless gateway device.

3. A method for enabling wireless access to a computer network by a remote wireless terminal device by enabling communication between the remote wireless terminal device and a wireless gateway client device that is physically connected to the computer network, the method comprising:

physically connecting one or more wireless gateway client devices to the computer network;

sending information from the computer network to the remote wireless terminal device via a wireless communication link between the one or more wireless gateway client devices and the remote wireless terminal device.

4. The method of claim 3, wherein the remote wireless device has a PIN and each of the wireless gateway client devices has a PIN, and upon the occurrence of predetermined events, one or more wireless gateway client devices communicates its PIN to the remote wireless terminal device to enable subsequent communication between the devices via the PINs.

5. The method of claim 3, wherein the remote wireless terminal device can access resources on the computer network via the wireless gateway client device.

6. The method of claim 5, wherein the resources include one or more of database systems and file directories.

7. The method of claim 3, wherein the wireless gateway client devices, when physically connected to the computer network, act as a node on the network, and remote wireless terminal devices may send and receive messages to and from the wireless gateway devices using PIN-to-PIN messaging.

8. The method of claim 3, wherein the wireless gateway client devices act as a node on the wireless network and communicate with one or more server or other network device.

9. The method of claim 8, wherein the wireless gateway client devices bypasses one or more components of the network architecture that may be unavailable, and provides a direct link from the remote wireless terminal devices to network equipment.

10. The method of claim 4, wherein the addresses of the wireless gateway devices may be stored in the remote wireless device, or may be transmitted in case of emergency or under other specified conditions to the remote wireless device through a specific PIN-to-PIN message.

11. The method of claim 3, wherein under one set of operating conditions, the remote wireless terminal device communicates with the computer network through email or other data channels and under at least another set of operating conditions may switch to PIN-to-PIN messaging either manually, through operation of the user, or automatically, in response to a PIN-to-PIN message sent to it.

12. The method of claim 4, wherein the remote wireless terminal device may store multiple addresses of wireless gateway client devices, and may send each communication to more than one of those wireless gateway devices, for redundancy purposes.

13. The method of claim 3, wherein the computer network includes one or more METAmessage servers, and the step of communicating includes communication through a METAmessage server.

14. The method of claim 13, wherein more than one METAmessage server is connected to the computer network in different locations to provide further redundancy.

15. The method of claim 14, further comprising the step of serving different wireless gateway client devices by different wireless networks to provide further redundancy.

16. The method of claim 13, wherein the method enables access to any information on the METAmessage server or devices connected to it.

17. The method of claim 13, wherein the method enables access to any information on a fax server associated with the METAmessage server.

18. The method of claim 3, wherein the method enables the remote wireless devices to operate in either a PIN-to-PIN Mode or a Normal Mode.

* * * * *