Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2777098 A1 2011/04/14

(21) 2 777 098

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2010/10/08
(87) Date publication PCT/PCT Publication Date: 2011/04/14
(85) Entrée phase nationale/National Entry: 2012/04/10
(86) N° demande PCT/PCT Application No.: CA 2010/001611
(87) N° publication PCT/PCT Publication No.: 2011/041905
(30) Priorité/Priority: 2009/10/09 (US61/250,195)

(51) Cl.Int./Int.Cl. *H04W 12/06* (2009.01),
H04W 48/20 (2009.01)

(71) Demandeur/Applicant:
MANKU, TAJINDER, CA

(72) Inventeur/Inventor:
MANKU, TAJINDER, CA

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : UTILISATION D'UN PREMIER RESEAU POUR COMMANDER L'ACCES A UN SECOND RESEAU
(54) Title: USING A FIRST NETWORK TO CONTROL ACCESS TO A SECOND NETWORK

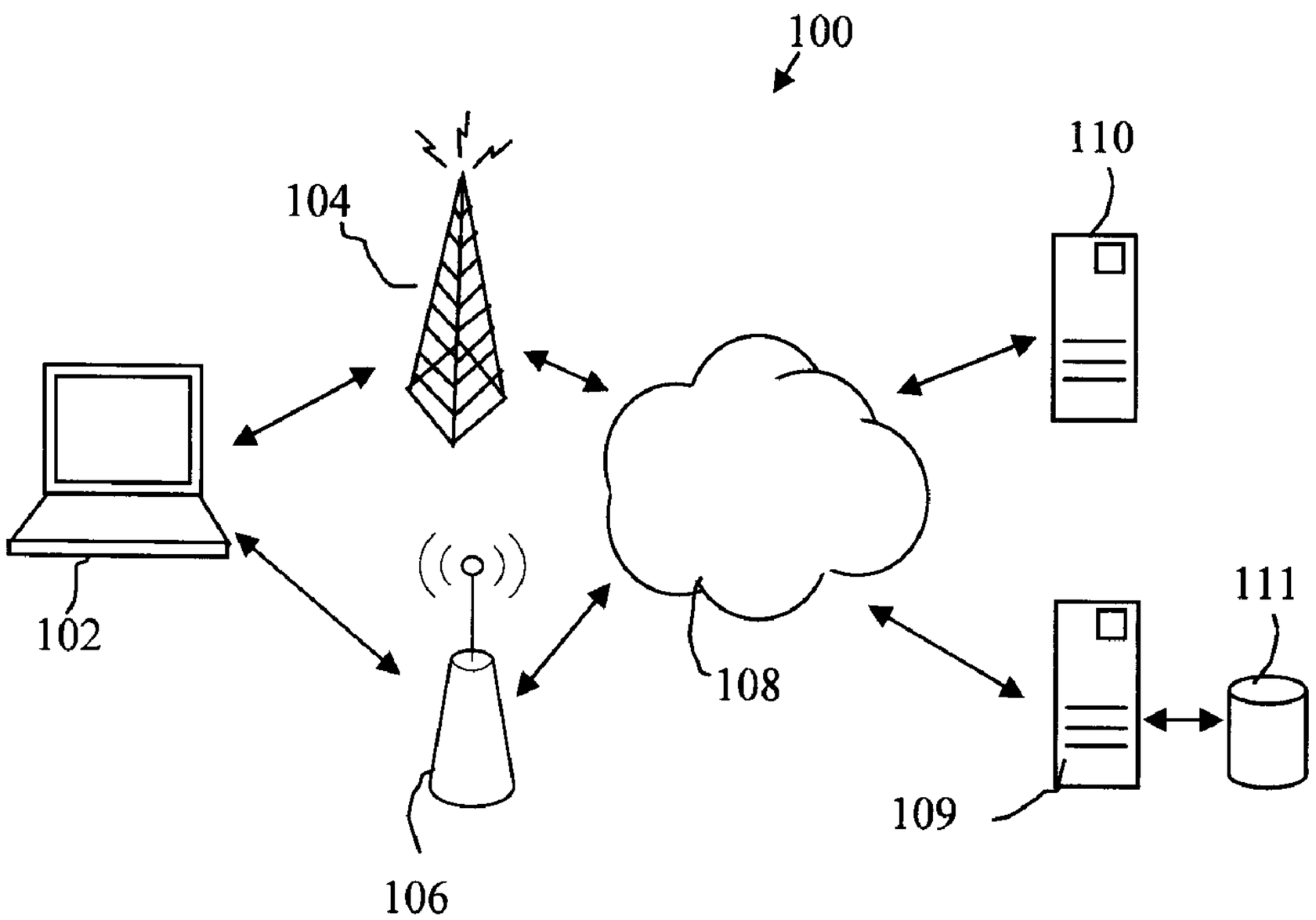

Figure 1

(57) Abrégé/Abstract:
A wireless communication device is configured to be able to communicate via both a first access point and a second access point for using the first access point to obtain validation credentials in order to permit use of the second access point to access a

CA 2777098 A1 2011/04/14

(21) 2 777 098

(13) A1

(57) Abrégé(suite)/Abstract(continued):
network. The wireless communication device comprises a processor; and a non-transitory computer readable medium having stored thereon computer executable instructions. The instructions are operable to: initiate communication with the second access point in order to access a network; obtain an access point identifier from the second access point, the access point identifier for identifying the second access point; transmit the access point identifier to a validation server via the first access point; receive validation credentials from the validation server via the first access point; and use the validation credentials to validate the wireless communication device with the second access point to obtain access to the network.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 April 2011 (14.04.2011)

PCT

(10) International Publication Number
WO 2011/041905 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04W 48/20* (2009.01)

(21) International Application Number:
PCT/CA2010/001611

(22) International Filing Date:
8 October 2010 (08.10.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/250,195 9 October 2009 (09.10.2009) US

(72) Inventor; and
(71) Applicant : **MANKU, Tajinder** [CA/CA]; 263 Lion's Court, Waterloo, ON N2L 6M7 (CA).

(74) Agent: **GOWLING LAFLEUR HENDERSON LLP**; Suite 1600 1 First Canadian Place, 100 King Street West, Toronto, Ontario M5X 1G5 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: USING A FIRST NETWORK TO CONTROL ACCESS TO A SECOND NETWORK

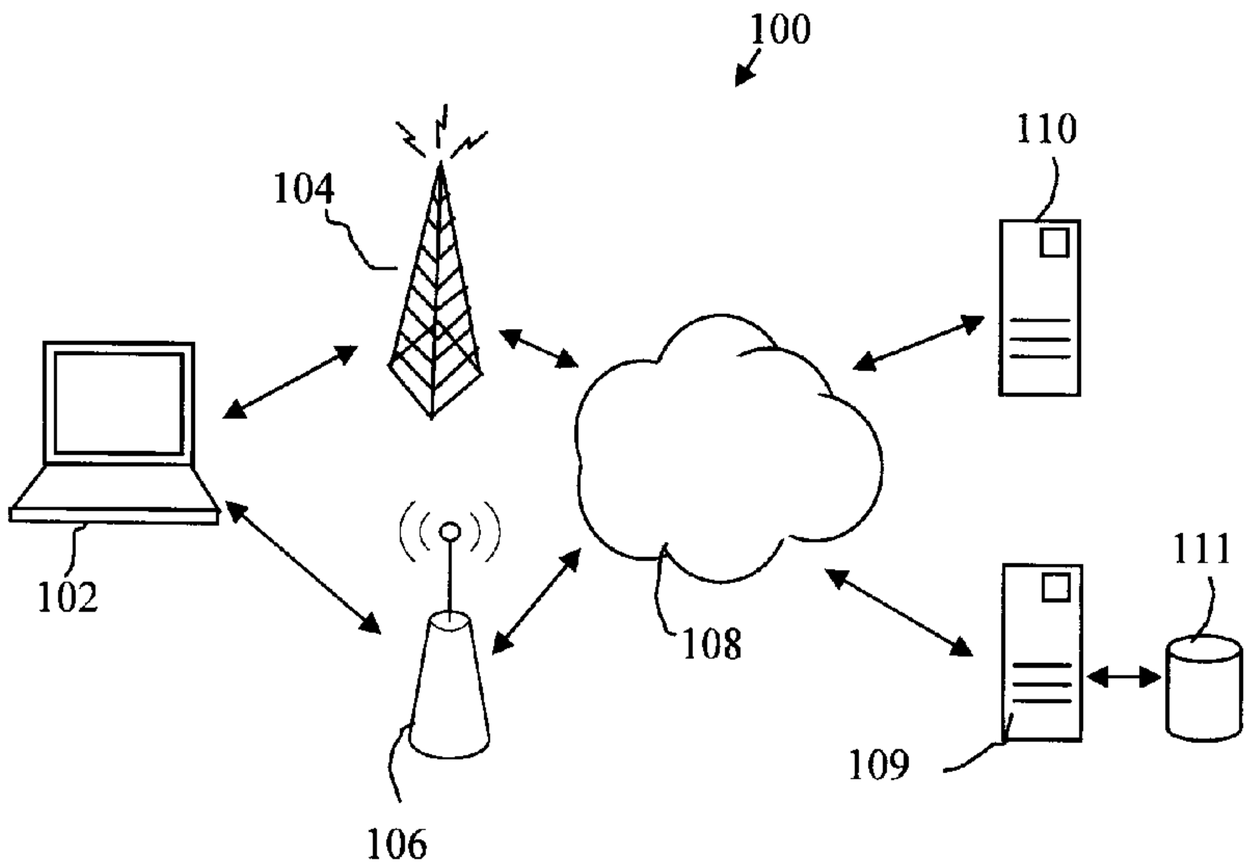

Figure 1

(57) **Abstract**: A wireless communication device is configured to be able to communicate via both a first access point and a second access point for using the first access point to obtain validation credentials in order to permit use of the second access point to access a network. The wireless communication device comprises a processor; and a non-transitory computer readable medium having stored thereon computer executable instructions. The instructions are operable to: initiate communication with the second access point in order to access a network; obtain an access point identifier from the second access point, the access point identifier for identifying the second access point; transmit the access point identifier to a validation server via the first access point; receive validation credentials from the validation server via the first access point; and use the validation credentials to validate the wireless communication device with the second access point to obtain access to the network.

WO 2011/041905 A1

USING A FIRST NETWORK TO CONTROL ACCESS TO A SECOND NETWORK

[0001] The present invention relates generally to a system and method for obtaining access to a network and specifically to the use of a first network to obtain validation credentials to a second network.

BACKGROUND

[0002] The proliferation of the Internet, portable communication devices and wireless networks has lead to the widespread use of communication devices capable of transmitting data as well as voice signals over the air. Most of the communication devices being manufactured provide at least two different wireless technologies to transmit the data; Wireless Wide Area Network (WWAN) technology and Wireless Local Area Network (WLAN) technology.

[0003] An example of a WWAN is cellular technology. Initially cellular service providers provided different data packet radio technology depending on the infrastructure they had already established. For example, cellular service providers running on a Code Division Multiple Access (CDMA) infrastructure introduced Evolution-Data Optimized (EV-DO) to provide data packet transfer. Cellular providers running on a Global System for Mobile Communications (GSM) infrastructure introduced General Packet Radio Service (GPRS) to provide data packet transfer. Currently, the GSM and CDMA infrastructures are running 3G standards. However, as the technology evolves, it appears as if most cellular service providers are moving towards the fourth generation of radio technologies, referred to as Long Term Evolution (LTE). It is expected the cellular technologies will continue to advance and evolve. However, cellular technology is still in its relative infancy and access to bandwidth is still relatively expensive and slow.

[0004] An example of a WLAN is Wi-Fi, which was developed by the Wi-Fi Alliance. Wi-Fi allows local area networks (LANs) to be deployed without wires for client devices, typically reducing the costs of network deployment and expansion. Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host WLANs. Therefore, portable devices such as notebook computers, video game consoles, mobile phones and personal digital assistants can connect to the Internet when within range of a WLAN connected to the Internet. Using Wi-Fi typically provides relatively inexpensive access to bandwidth. However, Wi-Fi networks have limited range.

[0005] Accordingly, a business model has developed providing "hotspots" to allow a user with a Wi-Fi enabled device to access the Internet. Specifically, a hotspot is a site that offers Internet access over a WLAN through the use of a router connected to an Internet service provider. Hotspots typically use Wi-Fi technology to provide the wireless network.

[0006] The hotspot may be offered as a value added service by a business or may be used as a dedicated source of revenue. For example, hotspot service providers like Boingo, T-Mobile, Bell, Rogers, AT&T, iPASS, and the like offer a collection of hotspots across a region. If a subscriber subscribes to a hotspot provider's access program, the customer is provided with an account and corresponding validation credentials. The validation credentials are typically a user name and password. To access the Internet, when the subscriber is at the hotspot, the subscriber launches a web browser, such as Internet Explorer for example. The web browser attempts to access the Internet via the Wi-Fi access point at the hot spot. However, software operating on the Wi-Fi access point intercepts the attempt and prompts the user to enter the validation credentials. If the validation credentials are accepted, the user is given access to the network.

[0007] However, such a system may require the customers to search out specific hotspots to which they subscribe, which may be inconvenient.

[0008] Further, such a system may require that the customers subscribe to multiple hotspot providers to ensure that they have sufficient hotspot coverage, which can be wasteful and expensive.

[0009] Yet further, it is difficult to share validation credentials. Businesses that that employ tens, hundreds or even thousands of employees may only need a few hotspot accounts, since only a few employees will need to access a hotspot and any given time. With the present system, it is difficult to manage the accounts and control who is able to access the hotspots at any given time.

[0010] Accordingly, it is an objective of the present invention to obviate or mitigate at least some of the above-mentioned disadvantages.

SUMMARY

[0011] In accordance with an aspect of the present invention there is provided wireless communication device configured to be able to communicate using both a first access point and a

second access point for using the first access point to obtain validation credentials in order to permit use of the second access point to access a network, the wireless communication device comprising: a processor; and a non-transitory computer readable medium having stored thereon computer executable instructions for execution by the processor, the computer executable instructions operable to: initiate communication with the second access point in order to access a network; obtain an access point identifier from the second access point; transmit the access point identifier to a validation server via the first access point; receiving validation credentials from the validation server via the first access point; and use the validation credentials to validate the wireless communication device with the second access point to obtain access to the network.

[0012] In accordance with a further aspect of the present invention, there is provided a validation server configured to provide validation credentials to a mobile communication device configured to be able to communicate with a network via both a first access point and a second access point , the validation server comprising: a processor; and a non-transitory computer readable medium having stored thereon computer executable instructions for execution by the processor, the computer executable instructions operable to: receive a request from the mobile communication device via the first access point, the request including an access-point identifier for identifying the second access point and subscriber information for identifying a subscriber; retrieve validation credentials from a database and; transmit the validation credentials to the wireless communication device via the first access point for use by the mobile communication device for connecting to the network via the second access point.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] Embodiments of the present invention will now be described by way of example only with reference to the following drawings in which:

Figure 1 is a block diagram of a network infrastructure;

Figure 2 is a flow chart illustrating operation of a mobile communication device;

Figure 3 is a flow chart illustrating operation of a validation server; and

Figure 4 is a block diagram of an alternative network infrastructure.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0014] For convenience, like numerals in the description refer to like structures in the drawings. Referring to Figure 1, a diagram illustrating a network environment is illustrated generally by numeral 100. The network environment 100 comprises a mobile communication device 102, a first access point 104, a second access point 106, a network 108, a validation server 109, and a target server 110. The mobile communication device 102 can connect to the network 108 via one or both of the first network access point 104 or the second network access point 106 in order to communicate with the validation server 109 or web server 110.

[0015] In the present embodiment, the network 108 is a Wide Area Network (WAN) such as the Internet.

[0016] The mobile communication device 102 is a mobile device such as a portable computer, tablet computer, smartphone or a personal digital assistant (PDA). The communication device 102 is configured to be capable of communicating via the first access point 104 and the second access point 106. In the present embodiment, the communication device 102 further includes validation software for communication with the validation server 109 via the first access point 104.

[0017] The first access point 104 is a cellular base station for communicating over a cellular network. As is known in the art, the cellular base station 104 provides a data packet service such as GSM-based High Speed Packet Access (HSPA).

[0018] The second access point 106 is a Wi-Fi access point configured as a hotspot. Accordingly, the Wi-Fi access point 106 includes hotspot software that intercepts an initial request from the communication device 102 to access the Internet 108 via the Wi-Fi access point 106. The hotspot software requires that the communication device 102 submits validation credentials before providing it with access to the Internet 108. Accordingly, the Wi-Fi access point 106 can be viewed as a Local Area Network (LAN) that provides a gateway to the Internet 108.

[0019] The validation server 109 is a server configured to manage validation credentials for a plurality of different users for a plurality of different hotspots. The validation credentials are

stored in a database 111. The amount and type of information may vary, depending on the implementation, as will be apparent to a person of ordinary skill in the art. Further, the validation server 109 and the database 111 are illustrated separately for ease of explanation only. The validation server 109 and the database 111 may be implemented on a single physical machine or by means of a distributed collection of servers and databases, as will be apparent to a person of ordinary skill in the art. Given the sensitive nature of the validation credentials, the validation server 109 and the database 111 will need to be secured appropriately, as will be apparent to a person of ordinary skill in the art.

[0020] The target server 110 is a remote computing device from which the mobile communication device 102 may request information and to which the mobile communication device 102 may transmit information via the Internet 108. The target server 110 may be a web server or may be any other device, such as a mail server, SIP server, and the like, connected to the Internet 108, with which the mobile device 102 wished to communicate.

[0021] Referring to Figure 2 a flow chart showing the general operation of the communication device 102 is illustrated generally by numeral 200. At step 202, a subscriber attempts to use the communication device 102 to access the Internet 108 via the Wi-Fi access point 106 and is prompted by the hotspot software for validation credentials.

[0022] At step 204, the validation software obtains an access point identifier. In the present embodiment, the access point identifier is a Wi-Fi identifier (ID) of the Wi-Fi access point 106. The Wi-Fi ID can be any identifier that sufficiently identifies the Wi-Fi access point for obtaining user credentials. For example, it may be sufficient to obtain an identifier of the service provider managing the Wi-Fi hotspot. Alternatively, it may be necessary to obtain a Service Set Identifier (SSID), or other unique identifier, of the Wi-Fi access point 106 itself.

[0023] At step 206, the wireless communication device 102 transmits the Wi-Fi ID along with subscriber identification information to the validation server 109 using the first network access point 104. At step 208, the wireless communication device 102 receives the validation credentials from the validation server 109 via the first network access point 104.

[0024] At step 210, the validation software communicates the received validation credentials to hotspot software for validating the subscriber. The subscriber is validated and, at step 212 the communication device 102 is permitted by the Wi-Fi access point 106 to use the Wi-Fi access point 106 to connect to the Internet 108.

[0025] Optionally, the status of the connection to the Wi-Fi access point 106 may be monitored as follows. At step 214, once the subscriber has access to the Internet 108, the validation software "pings" the validation server 109 at various intervals via the Wi-Fi access point 106. This ping provides an update to the validation server 109 that the connection to the Wi-Fi access point 106 is being maintained.

[0026] At step 216, the wireless communication device 102 receives an acknowledgment message via the cellular network 104 in response to the ping sent at step 214. At step 218, the acknowledgment message is forwarded, via the Wi-Fi access point 106 verifying that the connection is still active. If the connection appears to be inactive, at step 220 a new connection can try to be re-established. Input from the subscriber to confirm that it is desirable to establish a new connection may be obtained at this point.

[0027] Referring to Figure 3 a flow chart showing the general operation of the validation server 109 is illustrated generally by numeral 300. At step 302, the validation server 109 receives subscriber information and Wi-Fi ID from the wireless communication device 102. At step 304, the validation server 109 verifies the subscriber identification information and the Wi-Fi ID. Validation of subscriber identification is beyond scope of current invention and can be achieved using any known or propriety method in the art, with appropriate security to the task.

[0028] At step 306, the validation server 109 retrieves validation credentials from an account associated with the Wi-Fi ID and the subscriber identification. In the present embodiment, the validation information, subscriber identification and Wi-Fi ID are stored and correlated in the database 111, with appropriate security as is known to a person of ordinary skill in the art. At step 308, the validation information is transmitted securely to the wireless communication device 102. At step 309, the database is updated to indicate that the account is in use.

[0029] Optionally, the status of the connection to the Wi-Fi access point 106 may be monitored as follows. At step 310, a ping is received from the wireless communication device via the Wi-Fi access point 106. At step 312, the validation server 109 transmits an acknowledgment message via the cellular network 104 in response to the ping. At step 314, the acknowledgment message is received, via the Wi-Fi access point 106, verifying that the connection is still active. If the connection appears to be inactive, then at step 316 the database is updated accordingly.

[0030] It will be appreciated that the wireless communication device 102 uses the cellular network 104 to obtain the required validation credentials to access the Wi-Fi access point 106, thereby providing the communication device 102 with access to the Internet 108. By providing the validation software on the communication device 102, the subscriber is not required to manage validation credentials for multiple accounts. Further, the process of accessing the Wi-Fi access point 106 may be entirely transparent to the subscriber, thereby further securing the validation credentials. Yet further, management of multiple accounts can be maintained at a central location, the validation server 109, that has up-to-date information regarding the usage of each of a plurality of accounts.

[0031] The network infrastructure described above facilitates a number of different implementations. For example, in one embodiment, the network infrastructure may be used to manage a plurality of corporate hotspot accounts. A company, or any organization for that matter, may wish to maintain a plurality of hotspot accounts for their employees to access while away from the office. However, it is often unnecessary and, therefore, expensive to maintain an account for each user. Accordingly, only a few are set up to be shared between employees.

[0032] In this embodiment, each employee's subscriber identification is correlated with a group identifier. In the present embodiment this is accomplished by the validation software on the wireless communication device 102. That is, the validation software is configured with information identifying the group identifier and this information is transmitted as part of the subscriber identification information. Alternatively, the validation server 109 may be configured to correlate individual users with a group identifier and therefore, the group identifier need not be transmitted by the wireless communication device 102.

[0033] As part of retrieving the validation credentials at step 306, the validation server 109 retrieves one of a plurality of available accounts associated with the group identifier, verifies that the account is not currently in use, and then updates the database 111 to reflect that the account is in now in use.

[0034] If, however, all of the accounts for the group identifier are in use, then the validation server 109 returns a busy message to the wireless communication device 102. The validation software informs the subscriber, via a graphical user interface (GUI) on the wireless communication device 102, that all of the accounts are in use.

[0035] Alternatively, if all the accounts for the group identifier are in use, the validation server 109 dynamically creates a new account and correlates it with the group identifier. The validation server 109 then transmits the new validation credentials to the wireless communication device 102.

[0036] Thus it will be appreciated that the validation server can be used to manage a plurality of shared account while remaining transparent to the subscribers. This allows groups to easily share accounts between users without tracking which account each group member is using.

[0037] In an alternate embodiment, the network infrastructure 100 may be used to provide the subscriber with a single account, operated by a general hotspot service, that is capable of accessing a plurality of hotspots operated by different service providers. The general hotspot service itself may or may not provide and manage its own Wi-Fi access points 106. However, the general hotspot service would maintain at least a plurality of accounts with a plurality of different service providers. In the present embodiment, the validation server 109 is managed by the general hotspot service. Alternatively, the general hotspot service is managed on a validation server 109 that hosts a plurality of general hotspot services.

[0038] As part of verifying the subscriber identification information and the Wi-Fi ID at step 304, the validation server 109 determines the service provider for the Wi-Fi access point 106 identified by the Wi-Fi ID. The validation server 109 further determines whether or not the service provider is supported by the general hotspot service. That is, does the general hotspot service have accounts registered with the determined service provider. Optionally, the validation

server determines whether the subscriber has subscribed to a level of service that permits access to the determined service provider.

[0039] If the subscriber identification information and the Wi-Fi ID are verified then, as part of retrieving the validation credentials at step 306, the validation server 109 retrieves one of a plurality of available accounts associated with the determined service provider. Further, the validation server 109 verifies that the account is not currently in use and then updates the database 111 to reflect that the account is now in use.

[0040] If, however, if all the accounts for the determined service provider are in use, the validation server 109 dynamically creates a new account with the determined service provider. The validation server 109 transmits the new validation credentials to the wireless communication device 102.

[0041] Alternatively, if all of the accounts for the determined service provider are in use, then the validation server 109 returns a busy message to the wireless communication device 102. The validation software informs the subscriber, via a GUI on the wireless communication device 102, that all of the accounts are in use.

[0042] In yet an alternate embodiment, the network infrastructure 100 may be used to provide "pay-as-you-go" service for Wi-Fi access points 106. Such Wi-Fi access points 106 may include Wi-Fi access points 106 that traditionally provide hotspots, and may include less traditional sources of hotspots, such as small businesses or residences. Referring to Figure 4, in the present embodiment, the validation server 109 further includes an accounting module 402. The accounting module 402 is configured to track the amount of time during which the subscriber is connected to the Wi-Fi access point 106. The connection duration, along with a predefined access rate established by the Wi-Fi access point 106, is used to determine the cost of the connection.

[0043] In the present embodiment, the accounting module 402 interfaces with one or more standard payment modules 404, such as Paypal, Google Checkout, or any online credit card authorization module, as are known in the art. The payment module 404 interfaces with the wireless communication device 102, via either the Wi-Fi access point 106 or the cellular access

point 104, in order to present the subscriber with a GUI to obtain the payment information and provide a summary of the total costs. In the present embodiment, the payment information is obtained before the validation server 109 transmits any validation credentials.

[0044] Accordingly, the present embodiment provides a relatively inexpensive way for small businesses and residences to leverage their own Wi-Fi access points 106 in order to generate revenue.

[0045] In the embodiments described above, the cellular base station 104 is used primarily to obtain the validation credentials, while a bulk of the subsequent communication with the network is transmitted via the Wi-Fi access point 106. In an alternative embodiment, once the connection to the Wi-Fi access point has been established, both the Wi-Fi access point 106 and the cellular base station 104 can be used to transmit data, thereby increasing the bandwidth available to the device. The details of transmitting data using both the Wi-Fi access point 106 and the cellular base station 104 are beyond the scope of the present application and are described in co-pending U.S. Publication No. 20100154044.

[0046] As described above, the wireless communication device 102 is configured to communicate using both the first access point 104 and the second access point 106. This can be achieved using a number of different configuration. In a first configuration, the wireless communication device 102 has the radios necessary for accomplishing this task built into the device.

[0047] Alternatively, the wireless communication device 102 only has a built in radio for the second access point 106. A portable radio for communicating with the first access point 104, such as a cellular data stick or cellular telephone with a data plan, is connected to the wireless communication device 102 via a hardware port, such as a Universal Serial Bus (USB) port, or short range radio, such as Bluetooth™.

[0048] Alternatively, the wireless communication device 102 only has a built in radio for the first access point 104. A portable radio for communicating with the second access point 106, such as a Wi-Fi data stick, is connected to the wireless communication device 102 via a hardware port, such as a USB port, or short range radio, such as Bluetooth™.

[0049] Generally speaking, a wireless communication device 102 comprising only a radio for one of the first or second access points 104 and 106 may be paired, either wirelessly or by wire, to another device that provides a radio for the other of the first or second access points 104 and 106.

[0050] Further, although cellular access point 104 is described as being a 3G GSM network, it will be appreciated that it may be mobitex, 2G, CDMA-based EV-DO, LTE, and the like. As will be appreciated by a person of ordinary skill in the art, the type of technology used for the cellular network will likely evolve in the future and such technology may also be used.

[0051] Further, although the previous embodiments describe the Wi-Fi access point 106 primarily as a gateway to the Internet, the Wi-Fi access point may also provide access to a local area network (LAN). For example, if a company often sends it employees to client sites, the employees may need to access the client networks. In such an example, the client can assign the company with one or more accounts and their corresponding validation credentials in order to access their networks. This information can be stored by the validation server 109 and used to validate the employee when the employee attempts to access the client network. As previously discussed, such an implementation provides an added security benefit since the employee never needs to know the validation credentials.

[0052] Yet further, because the account validation occurs at the validation server 109, it is possible to dynamically create accounts and refresh passwords at predetermined or random intervals. Refreshing the password can help limit the subscriber using an account continuously.

[0053] Yet further, although the embodiment described above specifies that the wireless communication device 102 transmits subscriber identification information along with the Wi-Fi ID, it may be possible for the validation server 109 to identify without the wireless communication device 102 explicitly transmitting such information. For example, it may be possible for the cellular network to identify the wireless communication device and transmit the required information to the validation server 109.

[0054] Using the foregoing specification, the invention may be implemented as a machine, process or article of manufacture by using standard programming and/or engineering techniques to produce programming software, firmware, hardware or any combination thereof.

[0055] Any resulting program(s), having computer-readable instructions, may be stored within one or more computer-usable media such as memory devices or transmitting devices, thereby making a computer program product or article of manufacture according to the invention. As such, the terms "software" and "application" as used herein are intended to encompass a computer program existent as instructions on any computer-readable medium such as on any memory device or in any transmitting device, that are to be executed by a processor.

[0056] Examples of memory devices include, hard disk drives, diskettes, optical disks, magnetic tape, semiconductor memories such as FLASH, RAM, ROM, PROMS, and the like. Examples of networks include, but are not limited to, the Internet, intranets, telephone/modem-based network communication, hard-wired/cabled communication network, cellular communication, radio wave communication, satellite communication, and other stationary or mobile network systems/communication links. The client device 102 does not need to be mobile and the first and second access points 104 and 106 do not need to provide a wireless connection to the network.

[0057] A machine embodying the invention may involve one or more processing systems including, for example, CPU, memory/storage devices, communication links, communication/transmitting devices, servers, I/O devices, or any subcomponents or individual parts of one or more processing systems, including software, firmware, hardware, or any combination or subcombination thereof, which embody the invention as set forth in the claims.

[0058] Using the description provided herein, those skilled in the art will be readily able to combine software created as described with appropriate general purpose or special purpose computer hardware to create a computer system and/or computer subcomponents embodying the invention, and to create a computer system and/or computer subcomponents for carrying out the method of the invention.

[0059] Although preferred embodiments of the invention have been described herein, it will be understood by those skilled in the art that variations and combinations may be made thereto without departing from the scope of the appended claims.

CLAIMS:

What is claimed is:

1. A wireless communication device configured to be able to communicate via both a first access point and a second access point for using the first access point to obtain validation credentials in order to permit use of the second access point to access a network, the wireless communication device comprising:

a processor; and

a non-transitory computer readable medium having stored thereon computer executable instructions for execution by the processor, the computer executable instructions operable to:

initiate communication with the second access point in order to access a network;

obtain an access point identifier from the second access point, the access point identifier for identifying the second access point;

transmit the access point identifier to a validation server via the first access point;

receive validation credentials from the validation server via the first access point; and

use the validation credentials to validate the wireless communication device with the second access point to obtain access to the network.

2. The wireless communication device of claim 1 comprising further computer executable instructions operable to transmit subscriber identification information along with the access point identifier.

3. The wireless communication device of claim 1 comprising further computer executable instructions operable to transmit a group identifier along with the access-point identifier, the group identifier identifying a group to which a plurality of accounts for accessing the second access point are established.

4. The wireless communication device of claim 1 comprising further computer executable instructions for monitoring the connection to the second access point, the computer executable instructions operable to:

transmit a ping message to the validation server via the second access point;

receive an acknowledgement message from the validation server via the first access point; and

transmitting the acknowledgement message to the validation server via the second access point.

5. The wireless communication device of claim 1 comprising further computer executable instructions operable to transmit data via both the first access point and the second access point once access to the second access point has been obtained.

6. The wireless communication device of claim 1 wherein the first access point is a cellular base station and the second access point is a Wi-Fi access point.

7. A validation server configured to provide validation credentials to a mobile communication device configured to be able to communicate with a network via both a first access point and a second access point , the validation server comprising:

a processor; and

a non-transitory computer readable medium having stored thereon computer executable instructions for execution by the processor, the computer executable instructions operable to:

receive a request from the mobile communication device via the first access point, the request including an access-point identifier for identifying the second access point and subscriber information for identifying a subscriber;

retrieve validation credentials from a database and;

transmit the validation credentials to the wireless communication device via the first access point for use by the mobile communication device for connecting to the network via the second access point.

8. The validation server of claim 7 wherein the validation credentials are associated with the access-point identifier.

9. The validation server of claim 7 wherein the validation credentials are associated with the subscriber information.

10. The validation server of claim 7 comprising further computer executable instructions operable to update the database once the validation credentials have been retrieved in order to indicate that the validation credentials are in use.

11. The validation server of claim 7 comprising further computer executable instructions operable to verify the subscriber information.

12. The validation server of claim 7 comprising further computer executable instructions operable to

receive a ping message from the mobile communication device via the second access point;

transmit an acknowledgement message to the mobile communication device via the first access point; and

receive the acknowledgement message from the mobile communication device via the second access point.

13. The validation server of claim 7 comprising further computer executable instructions operable to obtain a group identifier, the group identifier identifying a group to which a plurality of accounts for accessing the second access point are established.

14. The validation server of claim 13, wherein the group identifier is the subscriber information.

15. The validation server of claim 13, wherein the group identifier is received in addition to the subscriber information.

16. The validation server of claim 13 comprising further computer executable instructions operable to determine the group identifier based on the subscriber information.

17. The validation server of claim 13 wherein the computer executable instructions operable to retrieve the validation credentials from the database comprise instructions operable to:

identify a plurality of accounts associated with the group identifier, each account having corresponding validation credentials;

determine an available account from the plurality of accounts, and

retrieve the validation credentials for the available account.

18. The validation server of claim 13 comprising further computer executable instructions operable to establish a new account if no available accounts can be determined.

19. The validation server of claim 7 comprising further computer executable instructions operable to:

communicate with an accounting module to monitor a duration of a connection between the mobile communication device and the second access point; and

interface with a payment module to obtain payment for the mobile communication device accessing the second access point based on the duration of the connection.

20. The validation server of claim 7 wherein the first access point is a cellular base station and the second access point is a Wi-Fi access point.

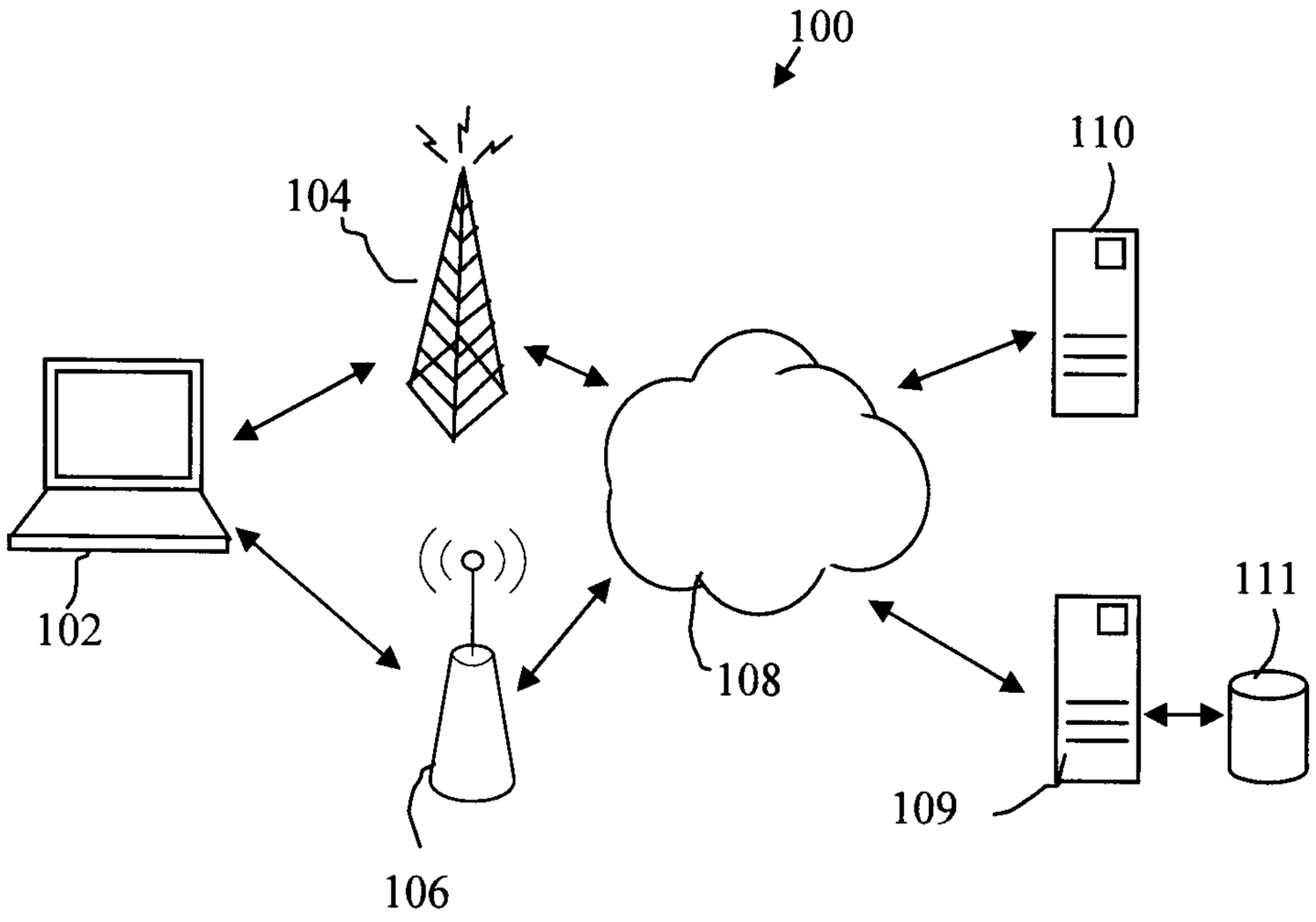

Figure 1

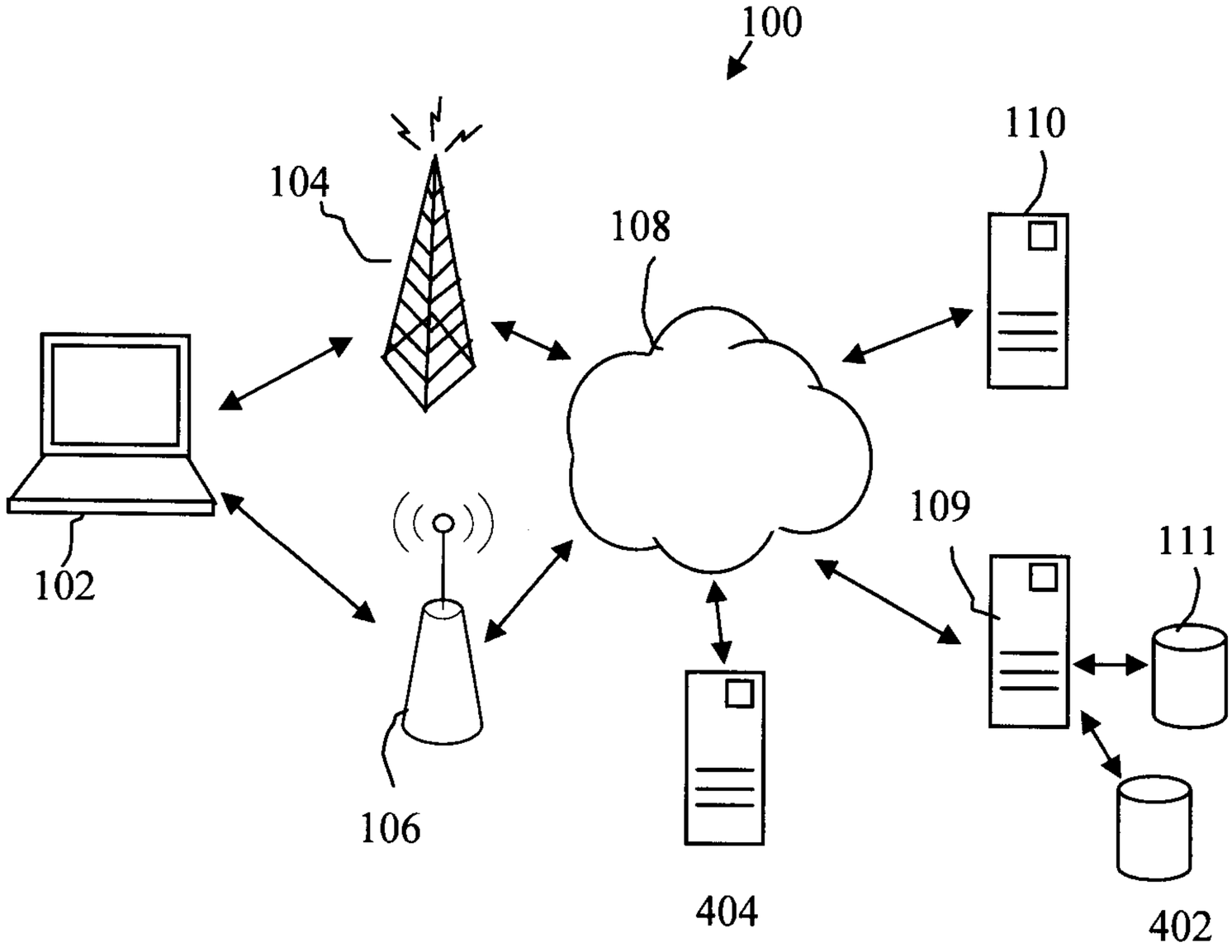

Figure 4

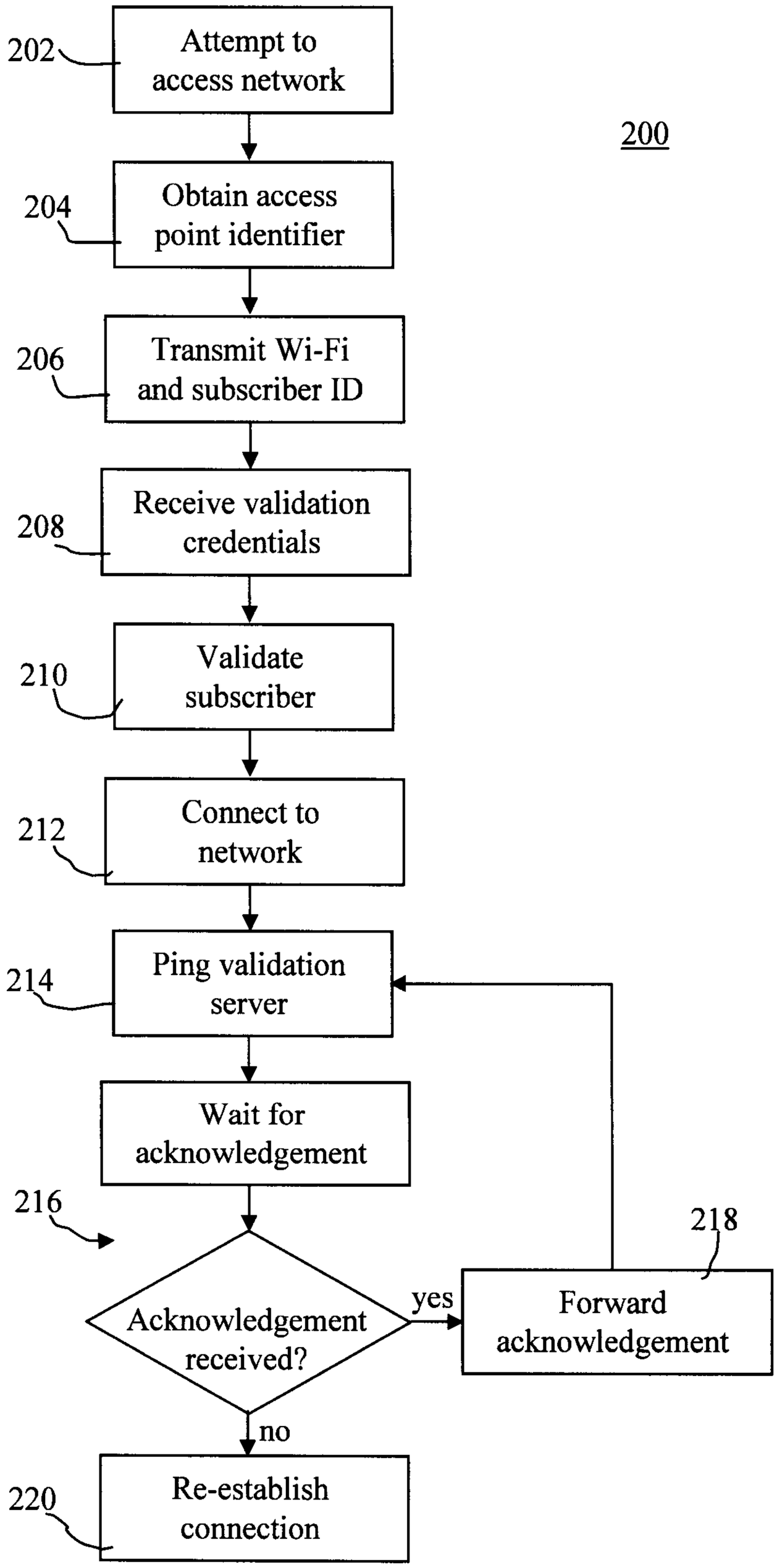
200
202
Attempt to access network
204
Obtain access point identifier
206
Transmit Wi-Fi and subscriber ID
208
Receive validation credentials
210
Validate subscriber
212
Connect to network
214
Ping validation server
Wait for acknowledgement
216
Acknowledgement received?
yes
218
Forward acknowledgement
no
220
Re-establish connection

Figure 2

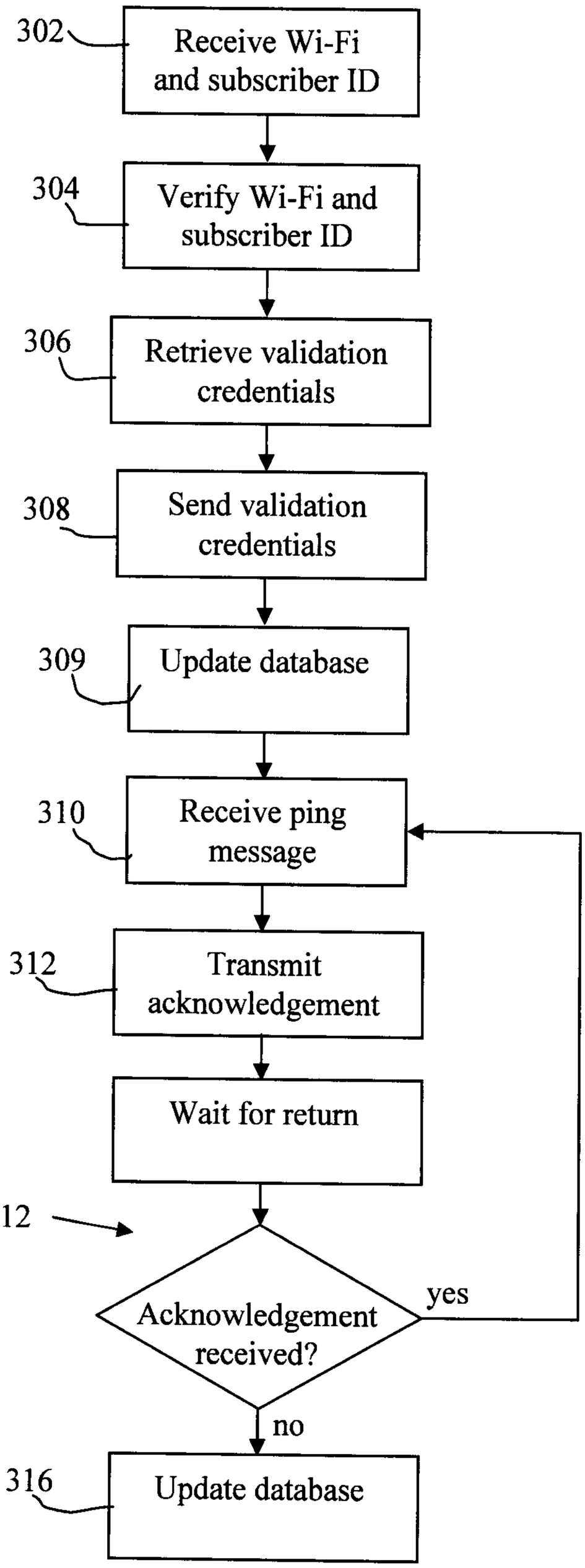
302
Receive Wi-Fi and subscriber ID
304
Verify Wi-Fi and subscriber ID
300
306
Retrieve validation credentials
308
Send validation credentials
309
Update database
310
Receive ping message
312
Transmit acknowledgement
Wait for return
312
Acknowledgement received?
yes
no
316
Update database

Figure 3

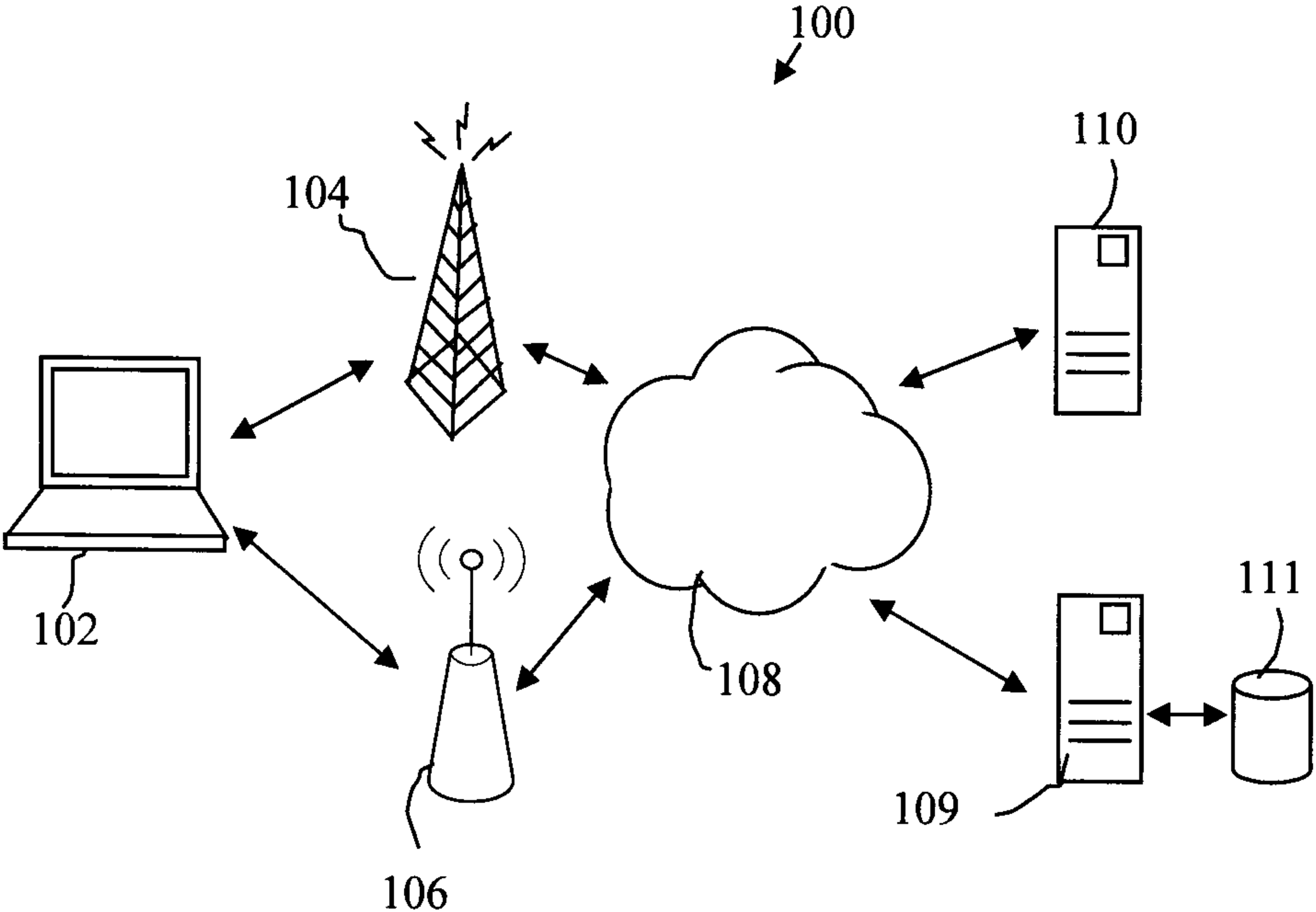

Figure 1