US 20090028082A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2009/0028082 A1

(43) Pub. Date: Jan. 29, 2009

Wynn et al.

(54) **SYSTEMS AND METHODS FOR WIRELESS NETWORK SELECTION BASED ON ATTRIBUTES STORED IN A NETWORK DATABASE**

(75) Inventors: **Simon Wynn**, Redwood City, CA (US); **David Fraser**, Oakland, CA (US)

Correspondence Address:
SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
990 Marsh Road
Menlo Park, CA 94025 (US)

(73) Assignee: **Devicescape Software, Inc.**, San Bruno, CA (US)

(21) Appl. No.: **12/240,969**

(22) Filed: **Sep. 29, 2008**

Related U.S. Application Data

(63) Continuation-in-part of application No. 12/240,920, filed on Sep. 29, 2008, which is a continuation-in-part of application No. 11/899,739, filed on Sep. 6, 2007.

(60) Provisional application No. 60/976,344, filed on Sep. 28, 2007, provisional application No. 60/824,756, filed on Sep. 6, 2006.

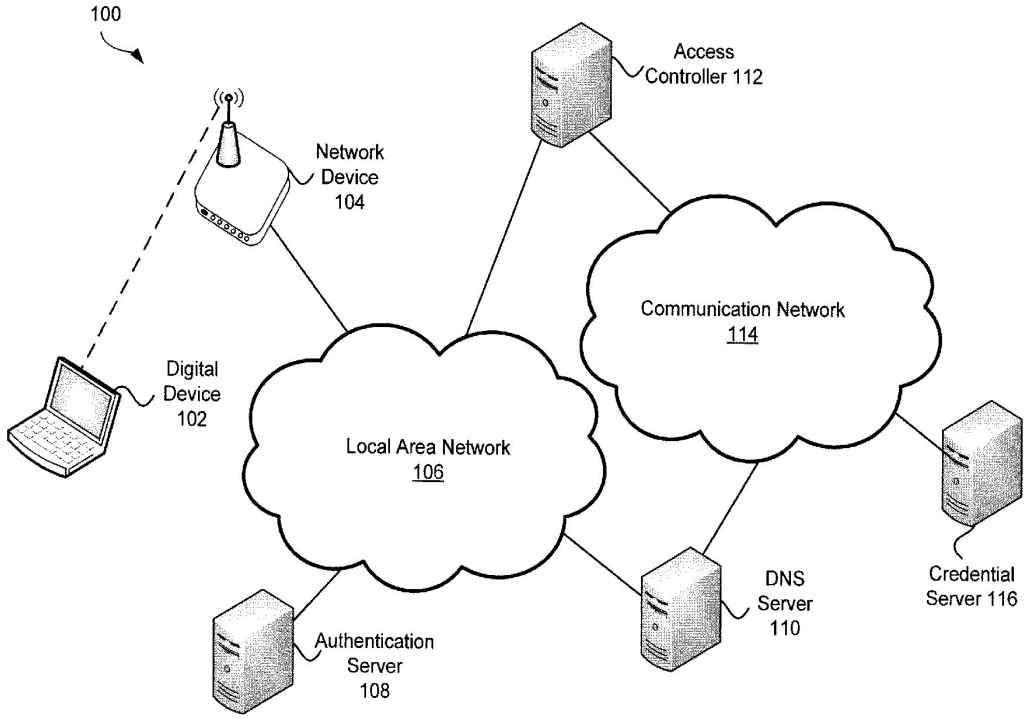
Publication Classification

(51) **Int. Cl.**
H04W 48/18 (2009.01)
H04B 7/00 (2006.01)

(52) **U.S. Cl.** **370/310**

(57) **ABSTRACT**

Systems and methods for wireless network selection based on attributes stored in a network database are disclosed. In some embodiments, a method comprises receiving a network identifier associated with a wireless network, determining if a network profile associated with the network identifier is stored within a network profile database comprising a plurality of network profiles, and if the network profile associated with the network identifier is stored within the network profile database, retrieving the network profile, or if the network profile associated with the network identifier is not stored within the network profile database, initiating the network profile, obtaining an attribute associated with the network device identifier, and storing the attribute within the network profile.



Google Exhibit 1052
Google v. SecCommTech

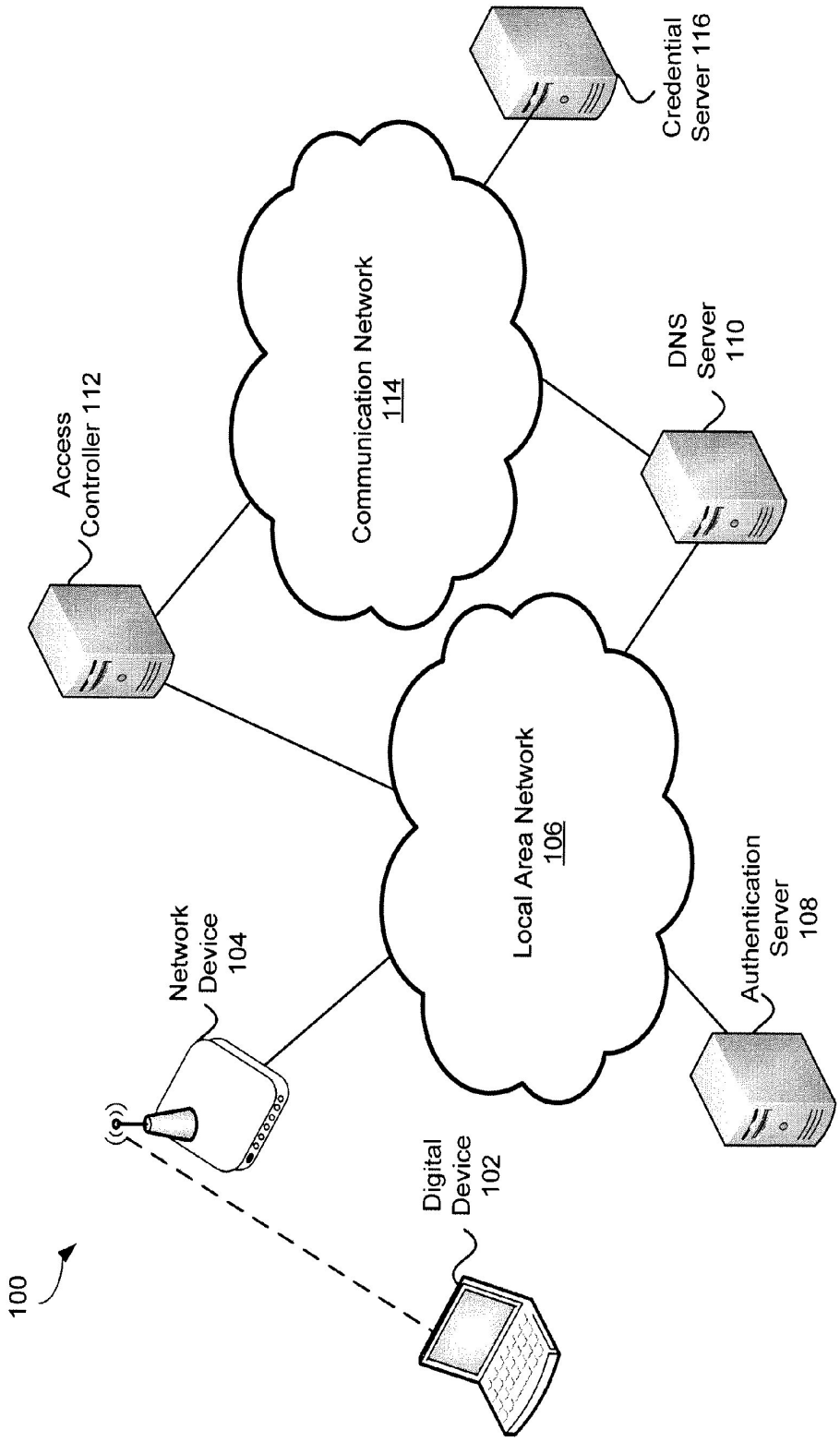

100
Digital Device 102
Network Device 104
Access Controller 112
Local Area Network 106
Communication Network 114
Credential Server 116
DNS Server 110
Authentication Server 108

FIG. 1

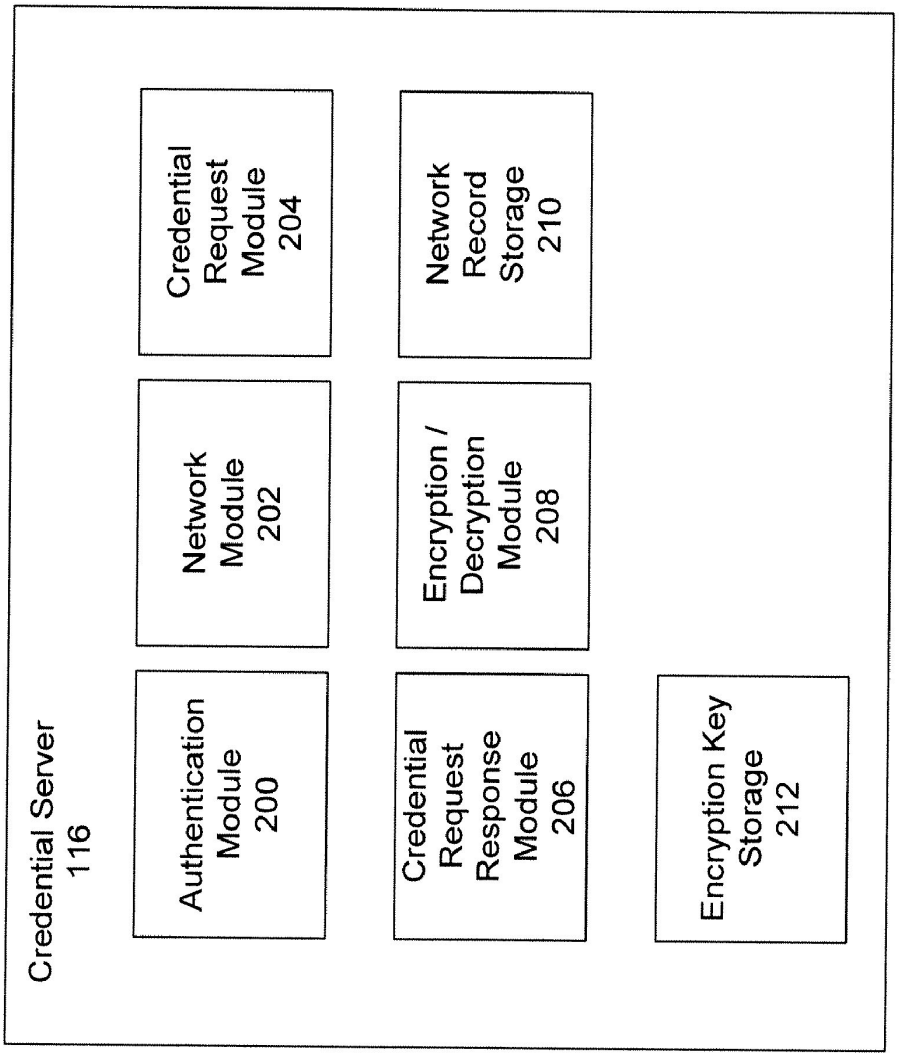

Credential Server
116
Authentication Module
200
Network Module
202
Credential Request Module
204
Credential Request Response Module
206
Encryption / Decryption Module
208
Network Record Storage
210
Encryption Key Storage
212

FIG. 2

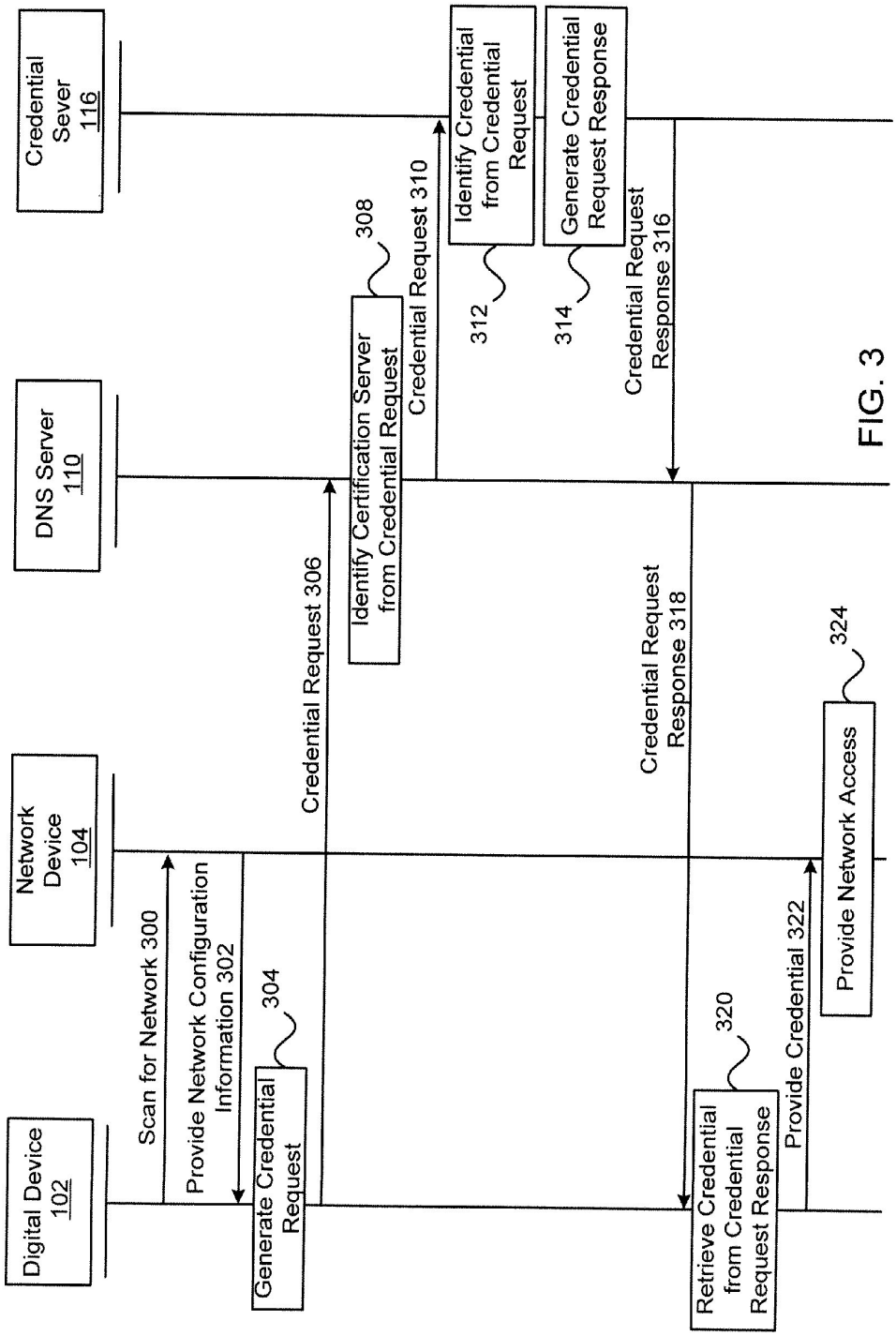

Digital Device 102
Network Device 104
DNS Server 110
Credential Sever 116
Scan for Network 300
Provide Network Configuration Information 302
Generate Credential Request
304
Credential Request 306
Identify Certification Server from Credential Request
308
Credential Request 310
Identify Credential from Credential Request
312
Generate Credential Request Response
314
Credential Request Response 316
Credential Request Response 318
Retrieve Credential from Credential Request Response
320
Provide Credential 322
Provide Network Access
324

FIG. 3

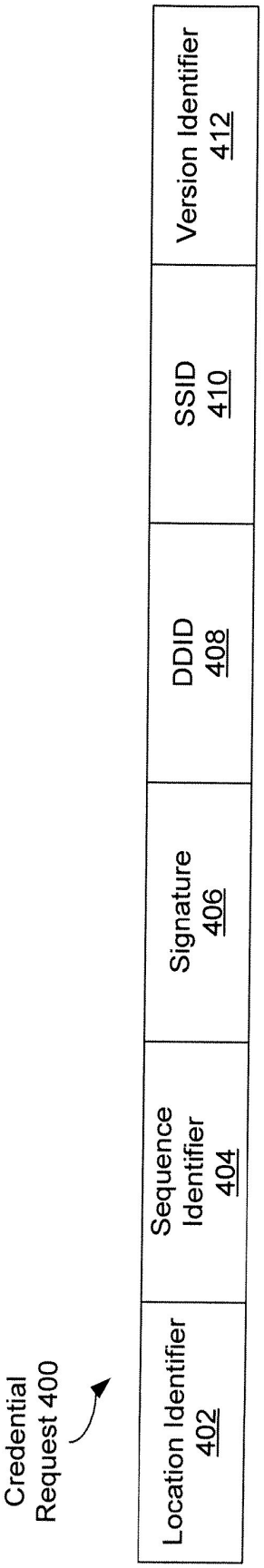

Credential Request 400
Location Identifier 402
Sequence Identifier 404
Signature 406
DDID 408
SSID 410
Version Identifier 412

FIG. 4

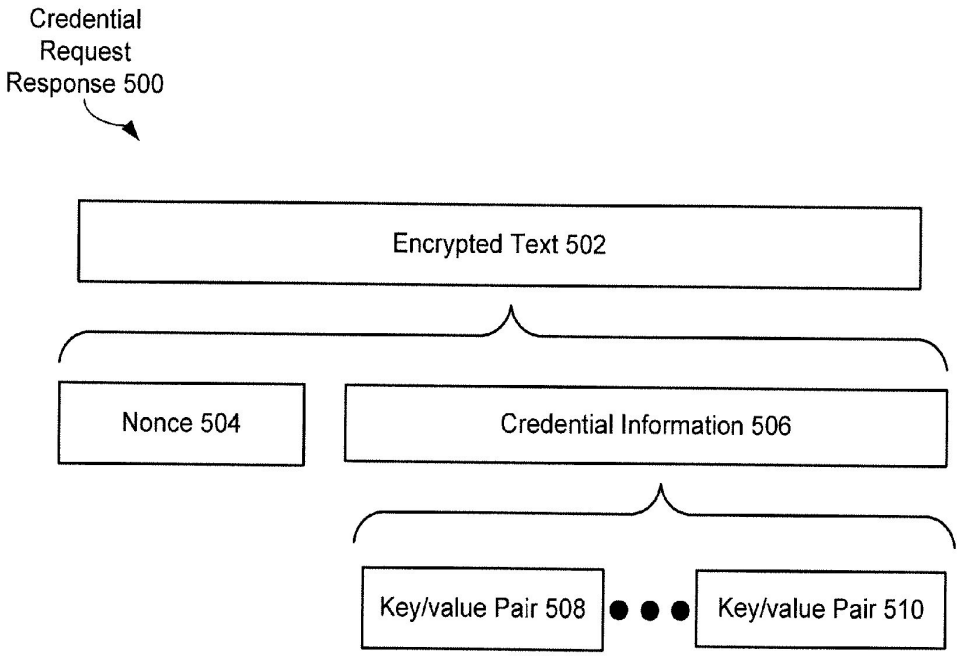

Credential
Request
Response 500
Encrypted Text 502
Nonce 504
Credential Information 506
Key/value Pair 508
Key/value Pair 510

FIG. 5

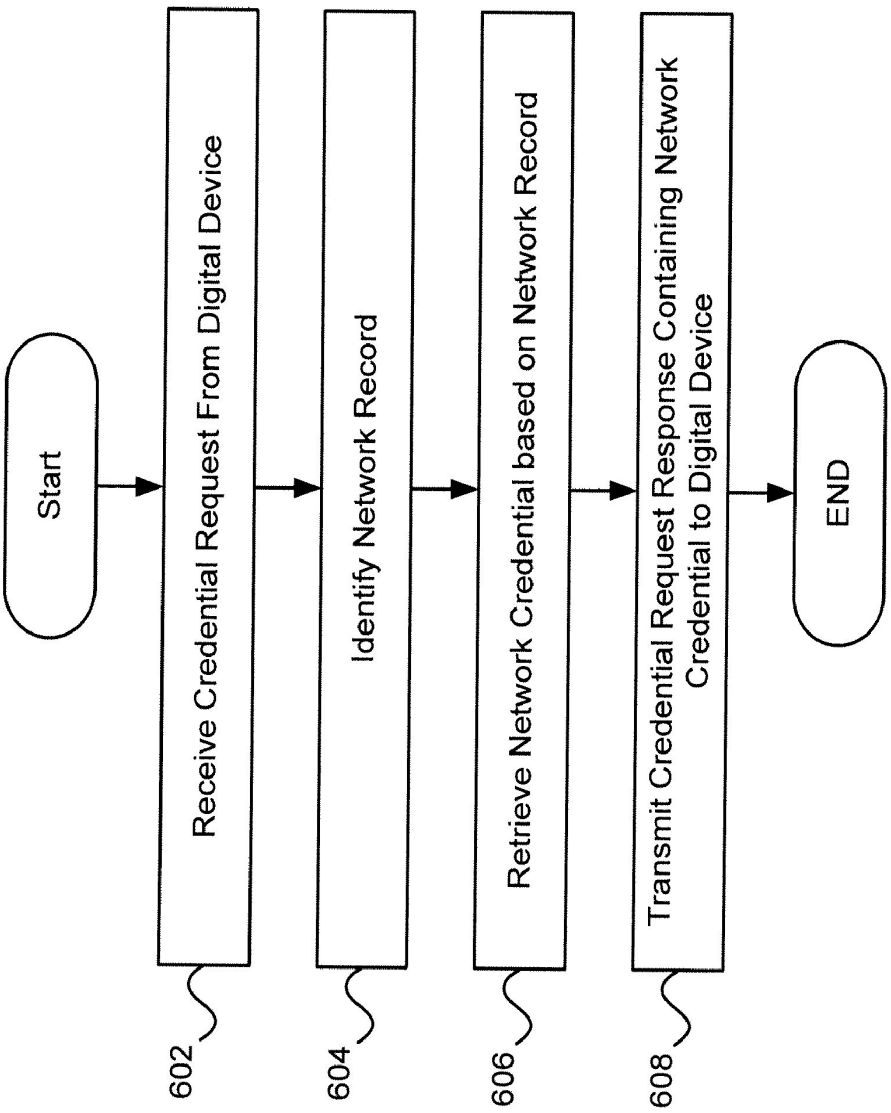

Start
Receive Credential Request From Digital Device
Identify Network Record
Retrieve Network Credential based on Network Record
Transmit Credential Request Response Containing Network Credential to Digital Device
END
602
604
606
608

FIG. 6

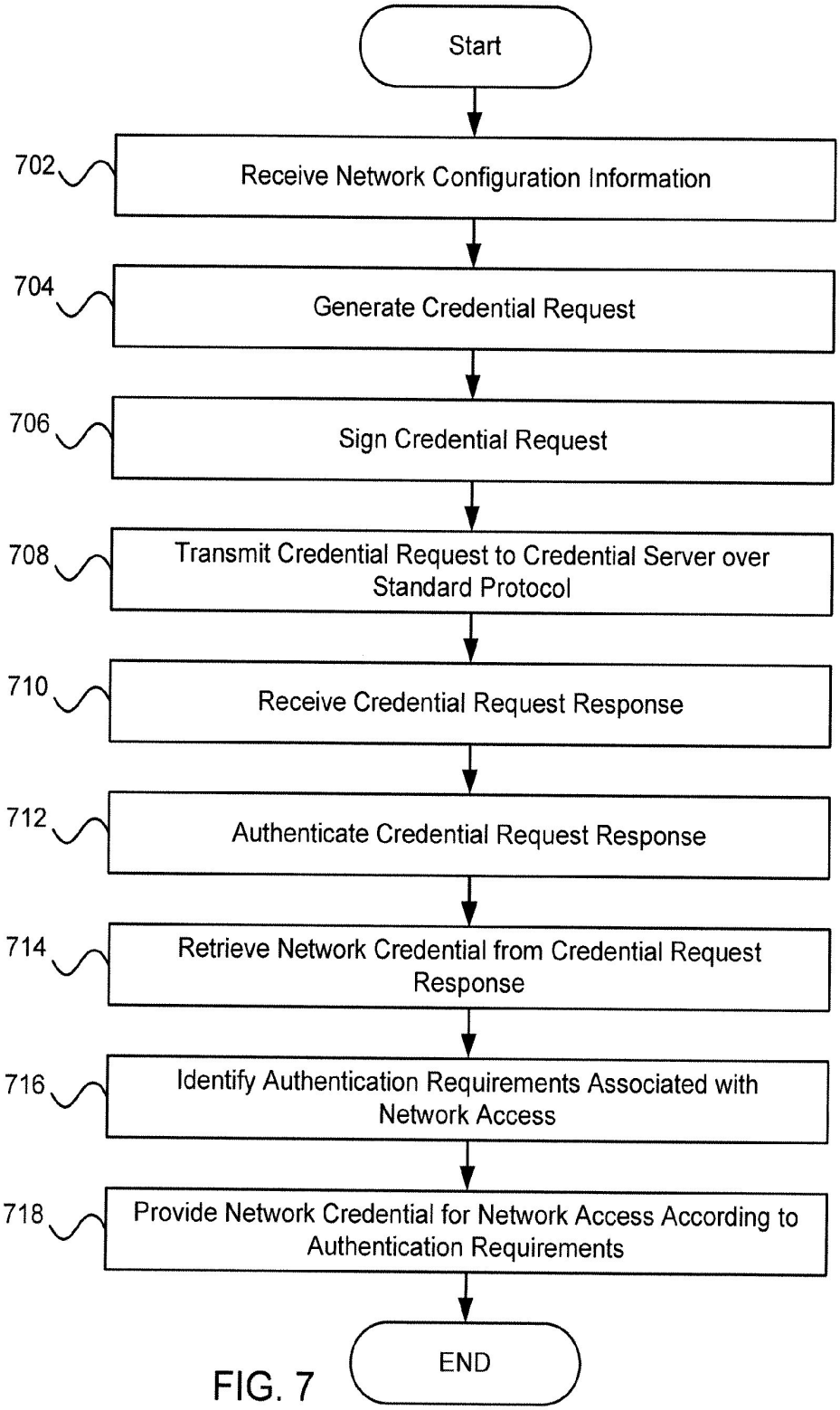

Start
702
Receive Network Configuration Information
704
Generate Credential Request
706
Sign Credential Request
708
Transmit Credential Request to Credential Server over Standard Protocol
710
Receive Credential Request Response
712
Authenticate Credential Request Response
714
Retrieve Network Credential from Credential Request Response
716
Identify Authentication Requirements Associated with Network Access
718
Provide Network Credential for Network Access According to Authentication Requirements
END

FIG. 7

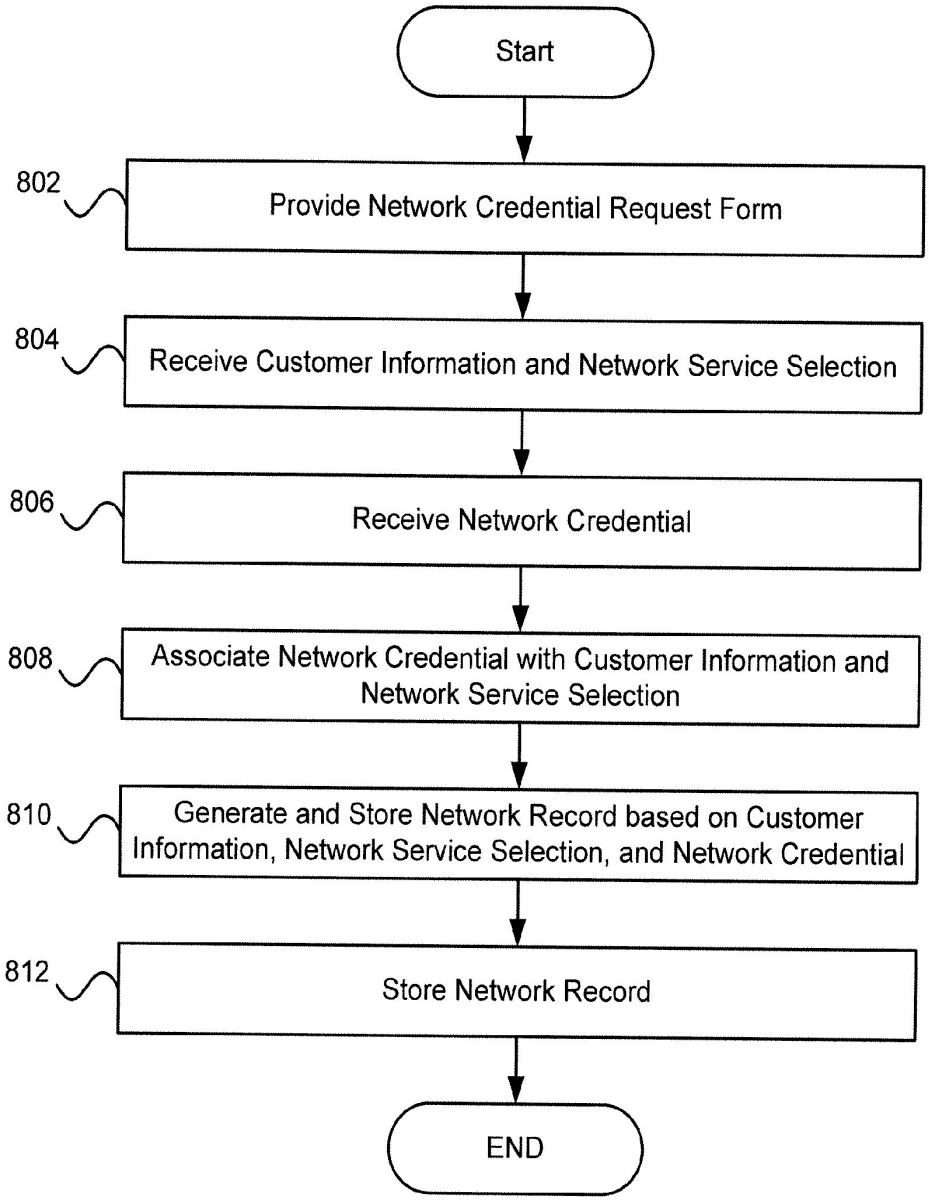

Start
802
Provide Network Credential Request Form
804
Receive Customer Information and Network Service Selection
806
Receive Network Credential
808
Associate Network Credential with Customer Information and Network Service Selection
810
Generate and Store Network Record based on Customer Information, Network Service Selection, and Network Credential
812
Store Network Record
END

FIG. 8

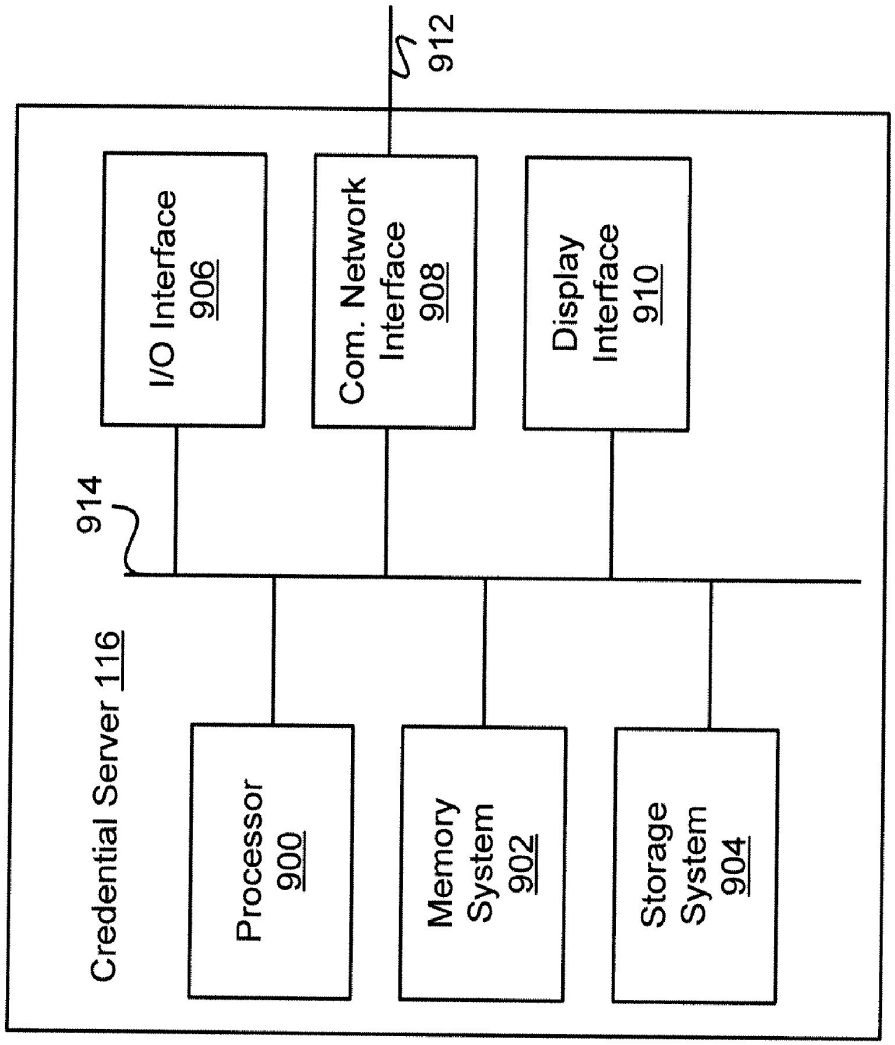

912
I/O Interface
906
Com. Network
Interface
908
Display
Interface
910
914
Credential Server 116
Processor
900
Memory
System
902
Storage
System
904

FIG. 9

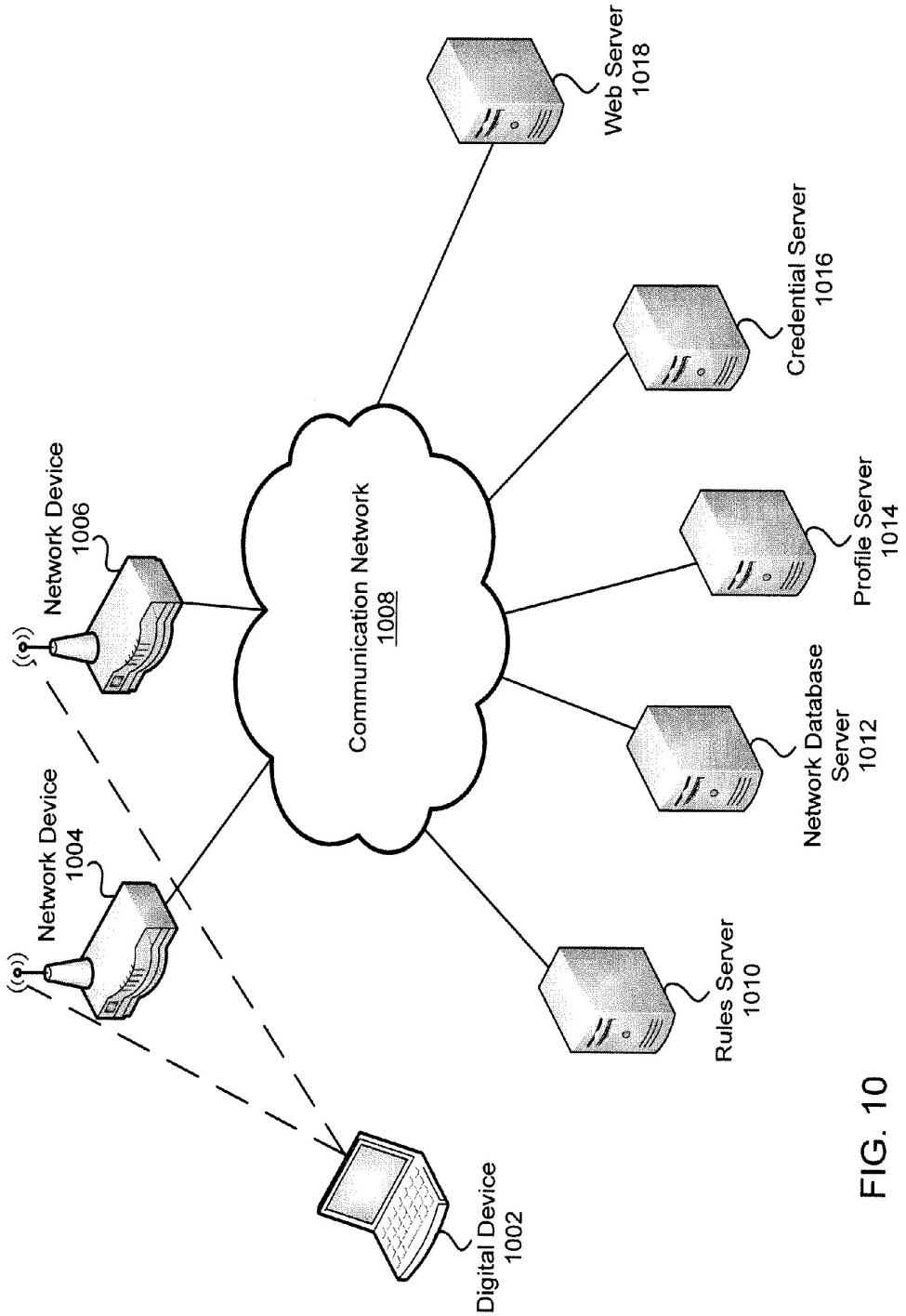

Web Server
1018
Credential Server
1016
Profile Server
1014
Network Database
Server
1012
Rules Server
1010
Communication Network
1008
Network Device
1006
Network Device
1004
Digital Device
1002

FIG. 10

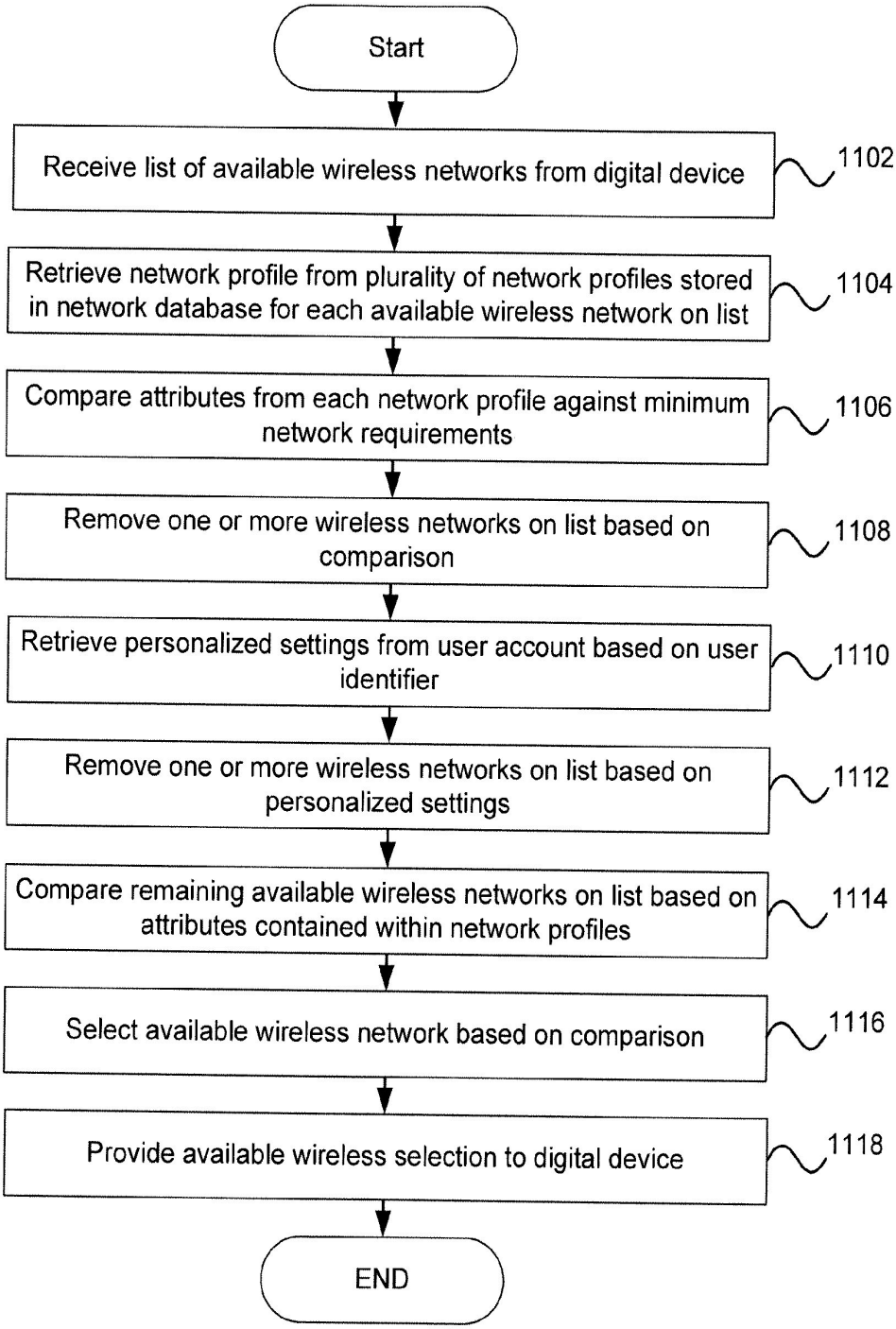

Start
Receive list of available wireless networks from digital device
1102
Retrieve network profile from plurality of network profiles stored in network database for each available wireless network on list
1104
Compare attributes from each network profile against minimum network requirements
1106
Remove one or more wireless networks on list based on comparison
1108
Retrieve personalized settings from user account based on user identifier
1110
Remove one or more wireless networks on list based on personalized settings
1112
Compare remaining available wireless networks on list based on attributes contained within network profiles
1114
Select available wireless network based on comparison
1116
Provide available wireless selection to digital device
1118
END

FIG. 11

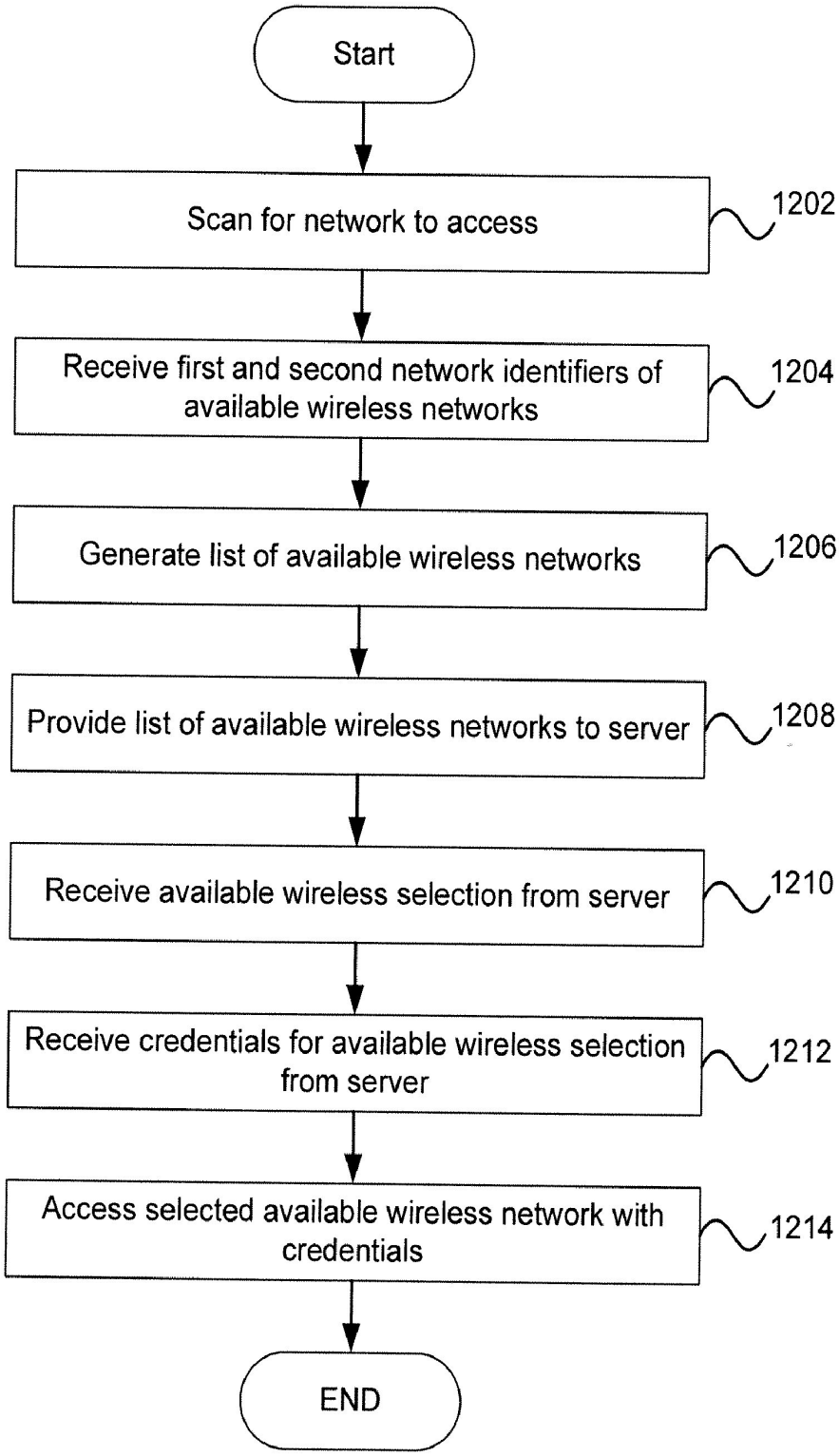

Start
Scan for network to access
1202
Receive first and second network identifiers of available wireless networks
1204
Generate list of available wireless networks
1206
Provide list of available wireless networks to server
1208
Receive available wireless selection from server
1210
Receive credentials for available wireless selection from server
1212
Access selected available wireless network with credentials
1214
END

FIG. 12

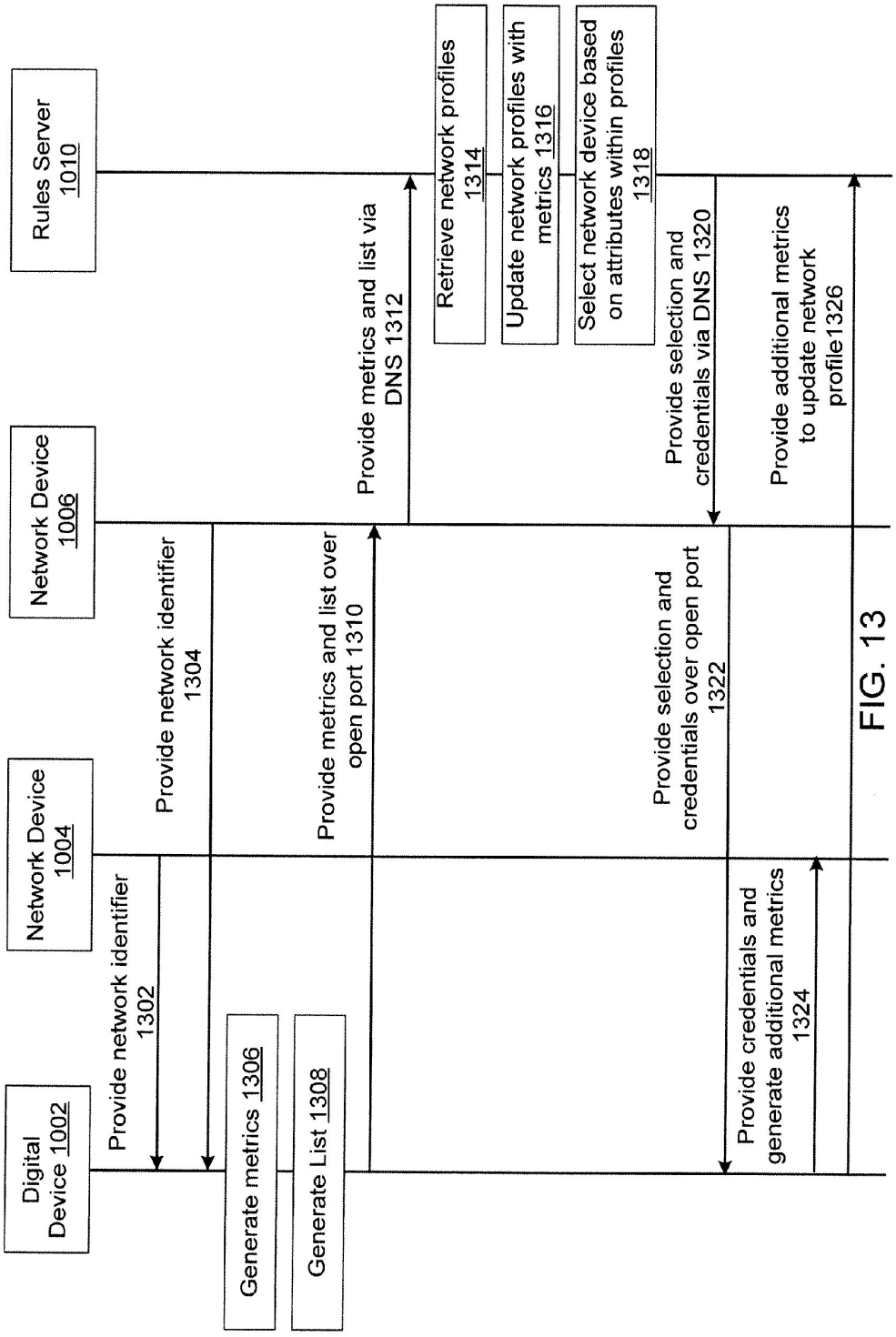

Digital Device 1002
Network Device 1004
Network Device 1006
Rules Server 1010
Provide network identifier 1302
Provide network identifier 1304
Generate metrics 1306
Generate List 1308
Provide metrics and list over open port 1310
Provide metrics and list via DNS 1312
Retrieve network profiles 1314
Update network profiles with metrics 1316
Select network device based on attributes within profiles 1318
Provide selection and credentials over open port 1322
Provide selection and credentials via DNS 1320
Provide credentials and generate additional metrics 1324
Provide additional metrics to update network profile1326

FIG. 13

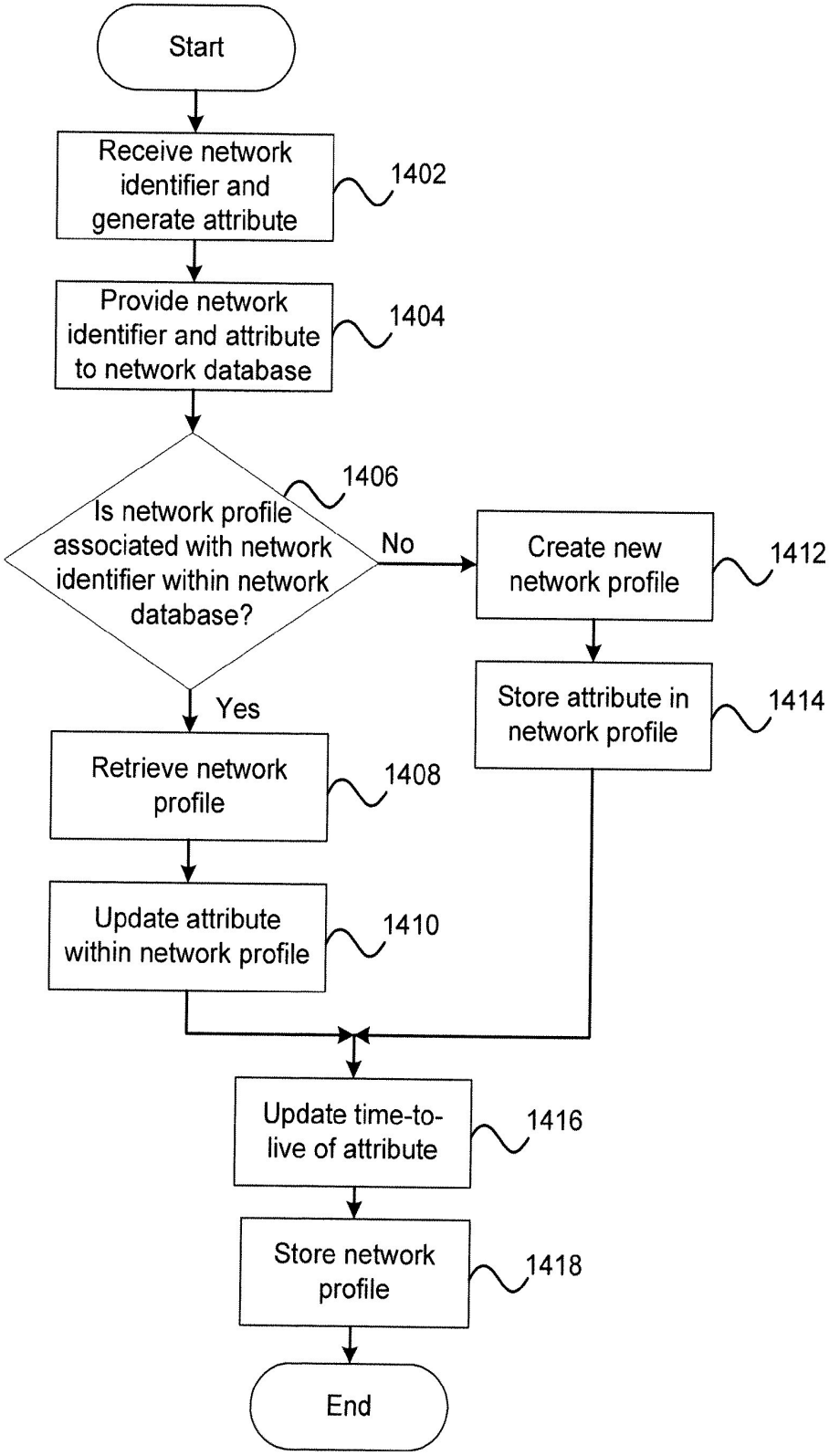

Start
Receive network identifier and generate attribute
1402
Provide network identifier and attribute to network database
1404
Is network profile associated with network identifier within network database?
1406
No
Create new network profile
1412
Store attribute in network profile
1414
Yes
Retrieve network profile
1408
Update attribute within network profile
1410
Update time-to-live of attribute
1416
Store network profile
1418
End

FIG. 14

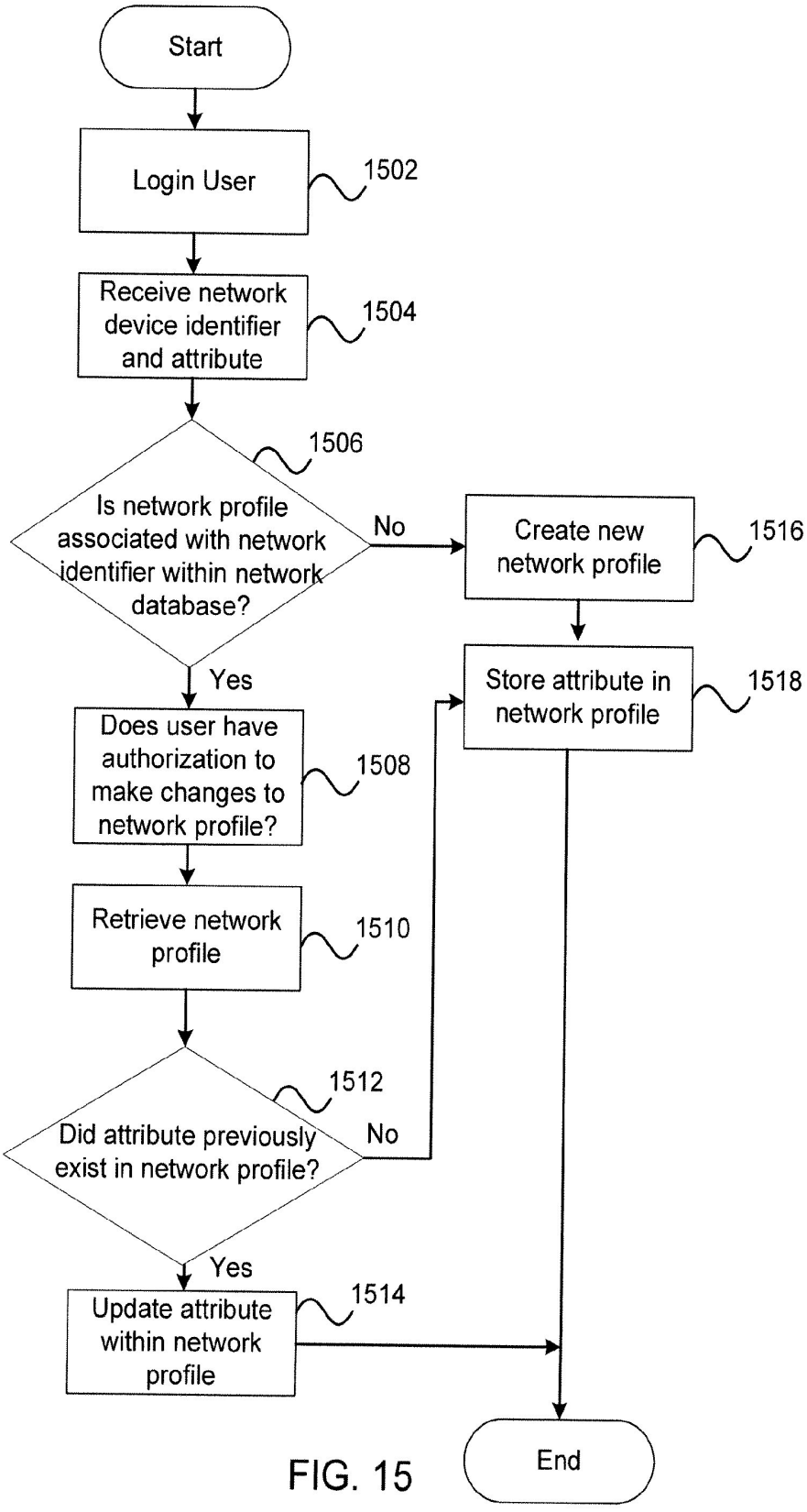

Start
Login User
1502
Receive network device identifier and attribute
1504
1506
Is network profile associated with network identifier within network database?
No
Create new network profile
1516
Yes
Store attribute in network profile
1518
Does user have authorization to make changes to network profile?
1508
Retrieve network profile
1510
1512
Did attribute previously exist in network profile?
No
Yes
Update attribute within network profile
1514
End

FIG. 15

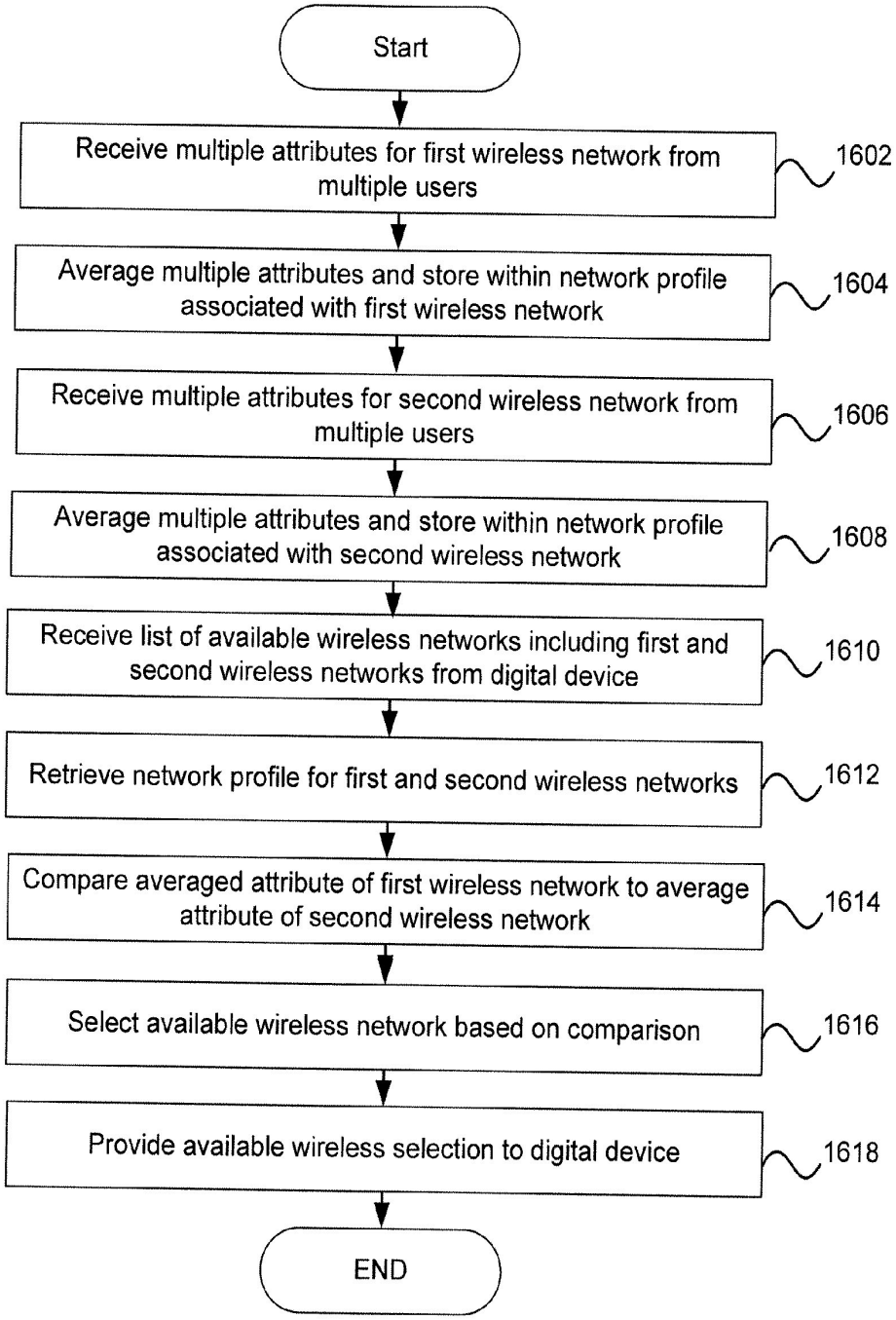

Start
Receive multiple attributes for first wireless network from multiple users
1602
Average multiple attributes and store within network profile associated with first wireless network
1604
Receive multiple attributes for second wireless network from multiple users
1606
Average multiple attributes and store within network profile associated with second wireless network
1608
Receive list of available wireless networks including first and second wireless networks from digital device
1610
Retrieve network profile for first and second wireless networks
1612
Compare averaged attribute of first wireless network to average attribute of second wireless network
1614
Select available wireless network based on comparison
1616
Provide available wireless selection to digital device
1618
END

FIG. 16

SYSTEMS AND METHODS FOR WIRELESS NETWORK SELECTION BASED ON ATTRIBUTES STORED IN A NETWORK DATABASE

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The present application claims benefit of U.S. Provisional Patent Application No. 60/976,344 filed Sep. 28, 2007, and entitled "Systems and Methods for Opportunistic Access to Free and Open Wireless Networks" which is incorporated herein by reference.

[0002] The present application is also a continuation-in-part of U.S. Nonprovisional patent application Ser. No. _____, filed Sep. 29, 2008, entitled "Systems and Methods for Wireless Network Selection" which is a continuation-in-part of U.S. Nonprovisional patent application Ser. No. 11/899,739, filed Sep. 6, 2007, entitled "Systems and Methods for Providing Network Credentials" which claims benefit of U.S. Provisional Patent Application No. 60/824,756 filed Sep. 6, 2006, and entitled "Network Credential Discovery Using DNS," which are all hereby incorporated by reference. The present application is also related to co-pending U.S. patent application Ser. No. 11/899,697, entitled "System and Method for Acquiring Network Credentials," filed Sep. 6, 2007, and co-pending U.S. patent application Ser. No. 11/899,638, entitled "Systems and Methods for Obtaining Network Access," filed Sep. 6, 2007 both of which are incorporated by reference.

BACKGROUND

[0003] 1. Field of the Invention

[0004] The present invention generally relates to accessing communication networks. More particularly, the invention relates to the automatic access of wireless communication networks.

[0005] 2. Description of Related Art

[0006] The increasing use of the networks to access information has resulted in a greater dependence on network communication for a variety of activities. With this dependence comes the growing expectation that network access will be ubiquitous. Network access for mobile users has been particularly enhanced by improvements in wireless technology. Various cellular (e.g. GSM, CDMA and the like), Wi-Fi (i.e. IEEE 802.11), WiMAX (i.e. IEEE 802.16), and other technologies have enabled a wide range of access options for a potential network user. Many wireless access points or "hotspots" are accessible only with local geographic regions—in some cases as small as a specific business or other address. In addition, strategically placed hotspots may provide public or private network access for a diverse group of people.

[0007] The owners or managers of hotspots often require password and the like to enable user access. As a result, a user of multiple hotpots may have to store, remember, or otherwise manage a large number of passwords. Many users may store their passwords on a laptop computer they use to access the hotspot. However, not all devices capable of accessing hotspots are laptop computers; cellular phones, personal digital assistants (PDAs), and many other devices are now capable of wireless access. Unfortunately, users often cannot easily enter the password on the device or store the password within the device. For example, some devices capable of wireless access may not have a keyboard. Even when a device includes a keyboard, the keyboard is often small and may be of limited functionality, especially for users with limited finger dexterity.

[0008] When users store passwords on a laptop computer, the user must first access the laptop computer and store the correct password within the computer. When a password changes, the user is required to update the password within the computer. Additionally, having the username and password stored in the device presents a security problem should the device be lost or stolen.

[0009] Further, users are typically required to enter a password, username, and navigate a website to obtain network access. This process is time consuming and the user may enter the wrong information and be forced to re-enter data.

[0010] When users enter a password manually, they are less apt to remember difficult passwords. As a result, simple password access is susceptible to hacking and may compromise the user's network access, the hotspot, and/or the user's personal information. Moreover, the user's network access may be stolen if the user's simple password is hacked or simply guessed.

[0011] Connecting to wireless networks has traditionally been a complex process for users of wireless devices for other reasons. Typically, the user enters an area where two or more Wi-Fi networks are present, selects the Wi-Fi function on their laptop, and views a series of 'scan results' listing the available Wi-Fi networks. In one example, the listing of available Wi-Fi networks comprises a list of Wi-Fi network SSID identifiers. Users must often identify which Wi-Fi networks do not have encryption or other security mechanisms (e.g., a login page). To add to user frustration, some of the wireless networks may be functional while others may be misconfigured in such a way that renders the network unuseable.

[0012] The user typically makes an arbitrary decision which Wi-Fi network to connect to based on the listing. In making a decision of which Wi-Fi network to connect, the user typically does not know whether the selected Wi-Fi network will provide adequate quality of service or even if the network will be able to provide an IP address via Dynamic Host Configuration Protocol (DHCP).

[0013] Wi-Fi networks, in homes, business and Hotspots can be identified by a human readable name (e.g., the SSID identifier). An example of an SSID identifier might be "My Home Network," or "tmobile." In addition to the SSID identifier, when a secure Wi-Fi network is first connected, various security parameters may need to be entered to configure either the WEP (Wired Equivalency Privacy), WPA (Wi-Fi Protected Access), or other security schemes.

[0014] Many Wi-Fi networks are left "open" with no encryption mechanism. Often this is intentionally done by the owner of the Wi-Fi network to enable easy access without the need for a WEP or WPA network key. However, Wi-Fi networks are also left "open" with no encryption mechanism because the owner is either unaware that the network is open or does not know how to secure the network. As a result, although the Wi-Fi network is "open," the network is not being intentionally shared. Such networks are very convenient for a user of a Wi-Fi enabled device, however, the user may not know that they do not have permission to use an otherwise open network.

[0015] Unfortunately, some countries have instituted laws which make it illegal to access a wireless network that is not purposefully shared. As a result, users may be unaware that an

"open" network is not shared and, as a result, unintentionally commit a criminal act by accessing the network.

SUMMARY OF THE INVENTION

[0016] Exemplary methods and systems for providing network credentials for network access are described. The exemplary method comprises receiving a credential request from a digital device over a network device, identifying a network record based on at least some information within the credential request, retrieving a network credential from a plurality of network credentials based on the network record, and transmitting a credential request response containing the network credential from the plurality of network credentials to the digital device.

[0017] The method may further comprise decrypting the credential request, authenticating the credential request, and encrypting the credential request response. Further, the method may also comprise retrieving an encryption key based on the digital device. The credential request may be received over a standard protocol of the network device. The standard protocol may be DNS.

[0018] The credential request may comprise a location identifier. The method may further comprise receiving a confirmed access response from the digital device.

[0019] An exemplary system for providing network credentials may comprise a credential request module and a credential request response module. The credential request module may be configured to receive a credential request from a digital device over a network device. The credential request response module may be configured to identify a network record based on at least some information within the credential request, retrieve a network credential from a plurality of network credentials based on the network record, and transmit a credential request response containing the network to the digital device.

[0020] An exemplary computer readable medium may have embodied thereon a program. The program may be executable by a processor for performing a method for providing network credentials. The method may comprise receiving a credential request from a digital device over a network device, identifying a network record based on at least some information within the credential request, retrieving a network credential from a plurality of network credentials based on the network record, and transmitting a credential request response containing the network credential from the plurality of network credentials to the digital device.

[0021] Systems and methods for selecting a wireless network are disclosed. In some embodiments, a method comprises receiving a first network device identifier for a first network device and a second network device identifier for a second network device, obtaining a first network profile comprising a first attribute, the first network profile based on the first network device identifier, obtaining a second network profile comprising a second attribute, the second network profile based on the second network device identifier, and selecting either the first network device identifier or the second network device identifier based on an attribute analysis of the first attribute and the second attribute.

[0022] In various embodiments, the first network device identifier and the second network device identifier are received from a digital device by a server. The method may further comprise providing a wireless network selection based on the selection. The method may also further comprise providing a credential request response based on the selection.

[0023] In some embodiments, the network selection identifier comprises the first network device identifier. The network selection identifier may also comprise a sorted list including the first network device identifier and the second network device identifier wherein the list is sorted based on the attribute analysis of the first attribute and the second attribute. An attribute may comprise a performance metric, a shared indicator, and a service identifier.

[0024] The method may further comprise comparing the first attribute and the second attribute to minimum requirements wherein selecting either the first network identifier or the second network device identifier is also based, at least in part, on the comparison of the attributes to the minimum requirements. The method may also further comprise comparing the first attribute and the second attribute to personalized settings wherein selecting either the first network identifier or the second network device identifier is also based, at least in part, on the comparison of the attributes to personalized settings. The method may also further comprise receiving a user identifier and retrieving the personalized settings from a user account based on the user identifier.

[0025] In various embodiments, a system comprises a digital device and a server. The digital device may be coupled to a communication network and configured to transmit a first network device identifier for a first network device and a second network device identifier for a second network device over the communication network. The server may also be coupled to the communication network and configured to receive the first network device identifier and the second network device identifier from the digital device, to obtain a first network profile comprising a first attribute, the first network profile based on the first network device identifier, to obtain a second network profile comprising a second attribute, the second network profile based on the second network device identifier, and to select either the first network device identifier or the second network device identifier based on an attribute analysis of the first attribute and the second attribute.

[0026] A computer readable storage medium may be configured to store instructions, the instructions comprising a method, the method comprising the steps of receiving a first network device identifier for a first network device and a second network device identifier for a second network device, obtaining a first network profile comprising a first attribute, the first network profile based on the first network device identifier, obtaining a second network profile comprising a second attribute, the second network profile based on the second network device identifier, and selecting either the first network device identifier or the second network device identifier based on an attribute analysis of the first attribute and the second attribute.

[0027] Systems and methods for wireless network selection based on attributes stored in a network database are disclosed. In some embodiments, a method comprises receiving a network identifier associated with a wireless network, determining if a network profile associated with the network identifier is stored within a network profile database comprising a plurality of network profiles, and if the network profile associated with the network identifier is stored within the network profile database, retrieving the network profile, or if the network profile associated with the network identifier is not

stored within the network profile database, initiating the network profile, obtaining an attribute associated with the network device identifier, and storing the attribute within the network profile.

[0028] The method may further comprise comparing an attribute from within the network profile to personalized settings, determining if the wireless network associated with the network identifier meets user requirements based on the comparison, and providing a credential request response based on the determination. The method may also further comprise comparing an attribute from within the network profile to minimum requirements, determining if the wireless network associated with the network identifier meets the minimum requirements based on the comparison, and providing a credential request response based on the determination.

[0029] In some embodiments, the method may further comprise comparing an attribute from within the network profile to another attribute from within another network profile stored within the network database and providing a credential request response based on the comparison. The method may also further comprise comparing an attribute from within the network profile to minimum requirements, determining if the wireless network associated with the network identifier meets the minimum requirements based on the comparison, comparing an attribute from within the network profile to another attribute from within another network profile stored within the network database, and selecting the wireless network based, at least in part, on the comparisons.

[0030] The network identifier may be received from a digital device by a server. The network identifier may comprise an SSID identifier and the attribute may comprise a performance metric, a shared indicator, and a service identifier.

[0031] Storing the attribute within the network profile may comprise averaging one or more existing attributes with the obtained attribute and storing the result in the network profile. In some embodiments, storing the attribute within the network profile may comprise performing an algorithm on one or more existing attributes with the obtained attribute and storing the result in the network profile.

[0032] The method may also further comprise updating other network profiles within the network database by updating a shared indicator within each network profile that is associated with an identical attribute. The attribute may be an SSID identifier.

[0033] In various embodiments, a system comprises a digital device and a server in communication with a communication network. The digital device may be configured to provide a network identifier associated with a wireless network over a communication network. The server may be configured to receive the network identifier, determine if a network profile associated with the network identifier is stored within a network profile database comprising a plurality of network profiles, and if the network profile associated with the network identifier is stored within the network profile database, retrieve the network profile, or if the network profile associated with the network identifier is not stored within the network profile database, initiate the network profile, obtain an attribute associated with the network device identifier, and store the attribute within the network profile.

[0034] In some embodiments, a computer readable storage medium is configured to store instructions. The instructions may comprise a method. The method may comprise the steps of receiving a network identifier associated with a wireless network, determining if a network profile associated with the network identifier is stored within a network profile database comprising a plurality of network profiles, and if the network profile associated with the network identifier is stored within the network profile database, retrieving the network profile, or, if the network profile associated with the network identifier is not stored within the network profile database, initiating the network profile, obtaining an attribute associated with the network device identifier, and storing the attribute within the network profile.

BRIEF DESCRIPTION OF THE DRAWINGS

[0035] FIG. **1** is a diagram of an environment in which embodiments of the present invention may be practiced.

[0036] FIG. **2** is a block diagram of an exemplary credential server.

[0037] FIG. **3** is a flow diagram of an exemplary process for providing network access to the digital device.

[0038] FIG. **4** is a block diagram of an exemplary credential request.

[0039] FIG. **5** is a block diagram of an exemplary credential request response.

[0040] FIG. **6** is a flow diagram of the exemplary method for providing network credentials.

[0041] FIG. **7** is another flow diagram of the exemplary method for providing network credentials.

[0042] FIG. **8** is a flow diagram of an exemplary method for receiving and storing network credentials.

[0043] FIG. **9** is a block diagram of an exemplary credential server.

[0044] FIG. **10** is a diagram of another environment in which embodiments of the present invention may be practiced.

[0045] FIG. **11** is a flow diagram of an exemplary process for providing a selection of a wireless network.

[0046] FIG. **12** is a flow diagram of an exemplary process for selecting a wireless network.

[0047] FIG. **13** is a diagram for selecting a wireless network and accessing the selected wireless network.

[0048] FIG. **14** is a flowchart of an exemplary process for updating and storing attributes associated with wireless networks within a network database.

[0049] FIG. **15** is another flowchart of an exemplary process for updating and storing attributes associated with wireless networks within a network database.

[0050] FIG. **16** is a flow diagram of an exemplary process of using a network database in selecting a wireless network.

DETAILED DESCRIPTION OF THE INVENTION

[0051] Embodiments of the present invention provide systems and methods for providing network credentials. In exemplary embodiments, a credential server receives a request for network credentials from a digital device at a hotspot. The request may be formatted as a standard protocol which is relayed from the hotspot to the credential server. The credential server may identify a network record based on at least some information contained within the request and transmit network credentials associated with the network record to the digital device. The digital device may receive the network credentials and provide them to network device in order to obtain network access.

[0052] In various embodiments, a rules server may identify a preferred network from a plurality of available networks that the digital device may connect based on a variety of

network attributes. In one example, a digital device may scan a physical region for available networks and generate a list of available wireless networks. The list may be provided to a rules server which identifies and retrieves a network profile for each wireless network on the list. The rules server may then compare each network profile (e.g., via attributes contained within each profile) to select a preferred network from the list. The rules server may then transmit the wireless network selection to the digital device which may then access the network.

[0053] In some embodiments, the digital device accesses the selected wireless network using credentials provided by the credential server. In one example, when the rules server selects the preferred wireless network, the rules server (or another server in communication with the rules server) may simultaneously (or nearly simultaneously) provide a credential request response including network credentials associated with the selected wireless network.

[0054] FIG. **1** illustrates a diagram of an environment **100** in which embodiments of the present invention may be practiced. In exemplary embodiments, a user with a digital device **102** enters a hotspot. The digital device **102** may automatically transmit a credential request as a standard protocol over a network device **104**. The credential request may be forwarded to a credential server **116** which, based on the information contained within the credential request, transmits a credential request response back to the digital device **102**. The credential request response contains network credentials which the digital device **102** may provide to the network device **104**, the authentication server **108**, or the access controller **112** to obtain access to the communication network **114**.

[0055] In various embodiments, a hotspot comprises the network device **104**, the authentication server **108**, the DNS server **110**, and the access controller **112** which are coupled to the local area network **106** (e.g., a "walled garden"). The network device **104** may comprise an access point which allows the digital device **102** to communicate with the authentication server **108**, the DNS server **110**, and the access controller **112** over the local area network **106**. The digital device **102** may comprise a laptop, mobile phone, camera, personal digital assistant, or any other computing device. The authentication server **108** is a server that requires network credentials from the digital device **102** before allowing the digital device **102** access the communication network **114**. The DNS server **110** provides DNS services over the local area network **106** and may relay requests to other DNS servers (not shown) across the communication network **114**. The access controller **112** is an access device such as a router or bridge that can allow communication between devices operationally coupled to the network device **104** with devices coupled to the communication network **114**.

[0056] Although the hotspot in FIG. **1** depicts separate servers coupled to the local area network **106**, those skilled in the art will appreciate that there may be any number of devices (e.g., servers, digital devices, access controllers, and network devices) coupled to the local area network **106**. In some embodiments, the local area network **106** is optional. In one example, the authentication server **108**, the DNS server **110**, and the access controller **112** are coupled directly to the network device **104**. In various embodiments, the authentication server **108**, the DNS server **110**, and the access controller **112** may be combined within one or more servers or one or more digital devices. Further, although FIG. **1** depicts wireless access, the digital device **102** may be coupled to the network device **104** wirelessly or over wires (e.g., such as 10 baseT).

[0057] In order to access the communication network **114**, the authentication server **108** may require the digital device **102** to provide one or more network credentials for access to the hotspot. The network credential may comprise, for example, a username and password for an account associated with the hotspot. In alternative embodiments, network credentials other than a user name and password may be utilized.

[0058] According to exemplary embodiments, the digital device **102** may dynamically acquire the network credentials from the credential server **116**. The digital device **102** may send a credential request comprising an identity of the digital device **102** (or the user of the digital device **102**) and details about the network device **104** (e.g., name of the network device **104** or Wi-Fi service provider) to the credential server **116**.

[0059] In one example, when the digital device **102** enters the hotspot, the network device **104** may provide an IP address to which DNS queries may be submitted, for example, via DHCP (Dynamic Host Configuration Protocol). The credential request may be formatted as a standard protocol. In an example, the credential request may be formatted as a DNS request. The credential request may be a text record request (e.g., TXT), which comprises a standard record type such that the network infrastructure (e.g., the access controller **112**) will not block the request. More details regarding the process for acquiring network credentials are provided in co-pending U.S. patent application Ser. No. 11/899,697, entitled "System and Method for Acquiring Network Credentials," filed Sep. 6, 2007, and incorporated by reference herein.

[0060] In some embodiments, the credential request is received by the DNS server **110** which may forward the credential request to the credential server **116** for the network credential. In exemplary embodiments, the credential server **116** may perform a lookup to determine the proper network credential(s) to send back to the DNS server **110** which forwards the network credential back to the requesting digital device **102**. In various embodiments, the proper network credential(s) are sent from the credential server **116** to the digital device **102** over the same path as the transmission of the credential request.

[0061] Although only one DNS server **110** is depicted within FIG. **1**, the credential request may be forwarded through any number of servers, including but not limited to DNS servers, prior to being received by the credential server **116**. In other embodiments, the credential request is forwarded directly from the network device **104** to the credential server **116**.

[0062] In some embodiments, a credential request response from the credential server **116** may comprise the username, password, and/or login procedure information. The login procedural information may comprise, for example, HTML form element names, a submission URL, or a submission protocol. In some embodiments, the network credential response may be encrypted by the credential server **116** using an encryption key associated with the digital device **102** prior to transmission back to the digital device **102**.

[0063] Once the digital device **102** receives the network credential response, the digital device **102** may submit the network credential (retrieved from the network credential response) to the network device **104** in an authentication

response. In exemplary embodiments, the authentication response may be forwarded to an authentication server **108** for verification. In some embodiments, the authentication server **108** may comprise an AAA server or RADIUS server. More details regarding the process for obtaining network access are provided in co-pending U.S. patent application Ser. No. 11/899,638, entitled "System and Method for Obtaining Network Access," filed Sep. 6, 2007, and incorporated by reference herein.

[0064] It should be noted that FIG. **1** is exemplary. Alternative embodiments may comprise more, less, or functionally equivalent components and still be within the scope of present embodiments. For example, as previously discussed, the functions of the various servers (e.g., DNS server **110**, credential server **116**, and authentication server **108**) may be combined into one or two servers. That if, for example, the authentication server **108** and the DNS server **110** may comprise the same server, or the functionality of the authentication server **108**, the DNS server **110**, and the access controller **112** may be combined into a single device.

[0065] FIG. **2** is a block diagram of an exemplary credential server 1I16. The credential server **116** comprises an authentication module **200**, a network module **202**, a credential request module **204**, a credential request response module **206**, an encryption/decryption module **208**, a network record storage **210**, and an encryption key storage **212**. A module may comprise, individually or in combination, software, hardware, firmware, or circuitry.

[0066] The authentication module **200** may be configured to authenticate the credential request and provide security to the credential request response. In various embodiments, the digital device **102** may encrypt or digitally sign the credential request using an encryption key (e.g., a shared encryption key or an encryption key that is a part of a key pair). The authentication module **200** may authenticate the credential request by decrypting the credential request with the proper encryption key retrieved from the encryption key storage **212**. In one example, the digital device **102** generates a hash of the credential request and stores the hash within an encrypted portion of the credential request. The authentication module **200** may decrypt the credential request, generate hash of the credential request response, and compare the generated hash to the hash contained within the credential request for authentication.

[0067] In other embodiments, the digital device **102** may generate a nonce (i.e., a random value) and store the nonce within a portion of the credential request that is digitally signed. The authentication module **200** may decrypt the digital signature to authenticate the credential request and retrieve the nonce. In various embodiments, when the credential request response module **206** generates the credential request response (described hereafter), the authentication module **200** may include the nonce within the credential request response. The authentication module **200** or the encryption/decryption module **208** may then encrypt the credential request response. When the digital device **102** decrypts the credential request response, the digital device **102** may retrieve the nonce from the credential request response and compare the nonce to the nonce that was transmitted within the credential request for further authentication.

[0068] The network module **202** may be configured to receive the credential request and transmit the credential request response over the communication network **114**.

[0069] The credential request module **204** may receive the credential request from the network module **202**. The credential request may be a standard protocol. In one example, the credential request is a UDP protocol (e.g., DNS).

[0070] In exemplary embodiments, the credential request module **204** may retrieve the DDID and the SSID from the credential request. The DDID may identify the digital device **102**, the user of the digital device **102**, and/or the user associated with a network record. The SSID may identify the hotspot or the service provider (i.e., operator) of the hotspot.

[0071] The credential request module **204** or the credential request response module **206** may identify a network record based on the DDID and the SSID. A network record is a record associated (either directly or indirectly (e.g., a relational database)) with the DDID and the SSID. In one example, a network record contains network credentials necessary to provide network access to a digital device **102** associated with the DDID at the hotspot associated with the SSID. Network records may be stored within the network record storage **210**.

[0072] The credential request response module **206** may generate the credential request response. In various embodiments, the credential request response module **206** receives the network credential associated with the DDID and SSID from the network record. In some embodiments, the network credential may comprise a credit card number. In one example, the digital device **102** receives the network credential, retrieves the credit card number, and provides the credit card number to the authentication server **108**. In some examples, the authentication server **108** may then charge a fee to a credit card associated with the credit card number or use the information to confirm the identity of the user prior to granting network access.

[0073] Further, in various embodiments, the network credentials may comprise login procedural information. In one example, the credentials include a username and password which are to be provided within a form (e.g., an authentication form) retrieved from the authentication server **108** by the digital device **102**. In some embodiments, the login procedural information may instruct the digital device **102** to populate specific fields within the form with the network credentials before submitting the completed form to the authentication server **108**. Those skilled in the art will appreciate that there are many ways to provide credentials to the authentication server **108**. The process of providing the credentials to the authentication server is further discussed in co-pending U.S. patent application Ser. No. 11/899,638, entitled "System and Method for Obtaining Network Credentials," filed Sep. 6, 2007.

[0074] The credential request response module **206** or the encryption/decryption module **208** may encrypt the credential request response with an encryption key associated with the DDID or the credential request. In one example, the credential server **116** stores one or more shared encryption keys. Each shared encryption key may be shared by at least one digital device **102**. The credential request response module **206** may encrypt the credential request response with the shared encryption key associated with the digital device **102** (e.g., the shared encryption key may be associated with the DDID). The credential request response module **206** or the encryption/decryption module **208** may also encrypt the credential request with an encryption key that is part of a key pair. There may be many ways in which the encryption/decryption module **208** encrypts the credential request.

[0075] The encryption/decryption module **208** may decrypt the credential request and encrypt the credential request response. As previously discussed, the encryption/decryption module **208** may decrypt the digital signature of the credential request. In one example, the encryption/decryption module **208** decrypts the digital signature based on an encryption key that is associated with the DDID contained within the credential request. The encryption/decryption module **208** may also encrypt the credential request response. In one example, the encryption/decryption module **208** encrypts the credential request response based on an encryption key associated with the DDID (e.g., a shared encryption key or an encryption key that is part of a key pair).

[0076] In various embodiments, the encryption/decryption module **208** may encrypt the network records contained within the network record storage **210** and manage the encryption key storage **212**. The encryption/decryption module **208** may also establish secure communications (e.g., via SSL and HTTPS) with a digital device when storing network credentials. This process is further described in FIG. **7**. In accordance with some embodiments, the encryption/decryption module **208** may be optional.

[0077] The network record storage **210** and the encryption key storage **212** may store network records and encryption keys, respectively. The network record storage **210** and the encryption key storage **212** may comprise one or more databases. In one example, the network record storage **210** may store network records. A network record may comprise a DDID, SSID, and network credentials. The network record may also comprise a username and password for the user to access, alter, update, or store network records within the credential server **116**.

[0078] In various embodiments, the network record may also allow multiple digital devices **102** to use the same network credentials. In one example, the user may own multiple digital devices **102**. Multiple DDIDs, each DDID associated with a different digital device **102**, may be included in the same network record. In some embodiments, multiple devices may be associated with one or more network records, and the one or more network records are associated with a user. As a result, the user may retrieve the network credentials for a hotspot using any number of digital devices **102**. Those skilled in the art will appreciate that there are many ways in which the network records and/or the information contained therein may be stored and organized (e.g., different data structures, databases, records, organizing schemes, and/or methodologies).

[0079] FIG. **3** is a flow diagram of an exemplary process for providing network access to the digital device **102**. When the digital device **102** first enters into a hotspot, the digital device **102** may scan for the local area network **106** in step **300**. As a result of the scan, the network device **104** may provide network configuration information in step **302**. The network configuration information may comprise one or more IP addresses for access to the DNS server **110**.

[0080] In step **304**, a credential request is generated by the digital device **102**. Subsequently, the credential request may be sent to the DNS server **110** in step **306** using one of the IP addresses previously received from the network device **104**.

[0081] Based on the credential request, the credential server **116** is identified by the DNS server **110** in step **308**. In other embodiments, the DNS server I**10** forwards the credential request to the credential server **116**. When the DNS server **110** is unable to locally resolve the DNS request, the credential request is forwarded to another DNS server on the communication network **114** (e.g., over port **53**) which may then forward the credential request to the credential server **116**. The credential request is forwarded, either directly or indirectly through one or more other DNS servers on the communication network **114**, to the credential server **116** in step **310**.

[0082] The credential server **116** identifies the network credential needed based on the credential request in step **312**. For example, the credential request may comprise an identifier (i.e., the DDID) for the digital device **102** as well as an identifier for the hotspot SSID (e.g., the service provider such as an operator). The identifiers may be compared against a table (e.g., network record) of such identifiers by the credential request module **204** or the credential request response module **206** to determine the proper network credential. A credential request response is then generated by the credential request response module **206** in step **314** and relayed back to the DNS server **110** in step **316**. The DNS server **110** forwards the credential request response back to the digital device in step **318**.

[0083] The digital device **102** may then retrieve the network credentials from the credential request response in step **320**. The network credential may then be provided to the network device **104** in step **322**. Upon verifying the network credentials, the network device **104** provides network access to the digital device **102** in step **324**.

[0084] Referring now to FIG. **4**, an exemplary credential request **400** is shown in more detail. According to exemplary embodiments, the credential request module **204** may generate the credential request **400**. In one embodiment, the credential request **400** may be a DNS string having a structure that comprises a location identifier **402**, a sequence identifier **404**, a signature **406**, the DDID **408**, a service set identifier (SSID) **410**, and a version identifier **412**.

[0085] The optional location identifier **402** may indicate a physical or geographic location of the digital device **102**, the network device **104**, the authentication server **108**, or the access controller **112**. In various embodiments, the location identifier **402** may be used by the credential server **116** to track the usage of hotspots, users of the digital device **102**, as well as the digital device **102**.

[0086] The sequence identifier **404** may comprise any number or set of numbers used to correspond to a subsequent request to the credential server **116** to determine if the login is successful. That is, the sequence identifier **404** provides a correlation mechanism by which verification of the login process may be made by the credential server **116**.

[0087] In exemplary embodiments, the signature **406** comprises a cryptographic signature (i.e., digital signature) that is utilized to prevent spoofing. The signature **406** of the request from digital device **102** is verified by the credential server **116**. If the signature **406** is not valid, then the request is rejected by the credential server **116**.

[0088] The DDID **408** comprises an identifier of the digital device **102**. For example, the DDID **408** may comprise a MAC address or any other identifier of the digital device **102**.

[0089] The SSID **410** comprises an identifier of the network access point or Wi-Fi service provider. For example, the SSID **410** may comprise the name of the service provider or the name of the venue operating the network device **104**.

[0090] The version identifier **412** may identify the protocol or format of the credential request **400**. For example, a digital device **102** may generate the credential request **400** and orga-

nize the data in a number of different formats. Each different format may be associated with a different version identifier. In some embodiments, the components of the credential request response module **206** may be updated, reconfigured, or altered over time, which may affect the structure of the credential request **400**. As a result, the credential server **116** may receive a plurality of credential requests **400** which are formatted differently. The credential server **116** may access the required information from each credential request based on the respective version identifier.

[0091] FIG. **5** is a block diagram of an exemplary credential request response. According to exemplary embodiments, the credential request response module **206** may generate the credential request response **500**. In one embodiment, the credential request response **500** may comprise encrypted text **502**. The encrypted text may comprise an optional nonce **504** and credential information **506**. The credential information may comprise key/value pairs **508** through **510**.

[0092] As previously discussed, the credential request response may be formatted as a DNS response comprising encrypted text **502**. The encrypted text **502** includes the network credentials (e.g., username, password, and login procedure information). Although the credential request response **500** is depicted as including encrypted text **502**, the text within the credential request response **500** need not be encrypted.

[0093] The encrypted text **502** may comprise the nonce. The nonce, as previously discussed, may be retrieved from the credential request. Once the credential request response **500** is received by the digital device **102**, the digital device **102** may compare the nonce within the credential request response **500** to the nonce transmitted within the credential request for authentication. Although the nonce is depicted as within the credential request response **500** in FIG. **5**, the nonce is optional.

[0094] The credential information **506** may comprise a username, password, login procedure information, or a combination of these. The credential information **506** may comprise key/value pairs **508** through **510**. Any number of key/value pairs may be within the credential information **506**. The key/value pairs may represent the credential information to be received and translated by the digital device **102**. The credential information **506** is depicted as key/value pairs for exemplary purposes only; the credential information may be within any format not necessarily limited to key/value pairs.

[0095] FIG. **6** is a flow diagram of the exemplary method for providing network credentials. In step **602**, the credential server **116** receives the credential request from the digital device **102**.

[0096] In various embodiments, the credential server **116** decrypts and authenticates the digital signature with an encryption key. The credential server **116** may then identify a network record based on the DDID and the SSID contained within the network record in step **604**. In one example, the credential request response module **206** retrieves one or more network records associated with the DDID within the credential request. The credential request response module **206** then identifies at least one network credential associated with the SSID within the retrieved network record(s).

[0097] In step **606**, the credential request response module **206** retrieves the identified network credential(s) from the selected network record. In one example, the credential request response module **206** identifies a username and password that the user of the digital device **102** must provide to the authentication server **108** to obtain network access. The credential request response module **206** generates the credential request response comprising the network credentials (e.g., username, password) to the digital device **102** in step **608**.

[0098] In some embodiments, the credential request response module **206** may identify login procedural information as part of the network credentials. The credential request response module **206** may retrieve the login procedural information from the network record (e.g., the same network record containing a password associated with the SSID). The login procedural information may contain a form identifier and instructions (e.g., parameters) for the digital device **102** to follow to obtain network access. In one example, the digital device **102** retrieves the form identifier and instructions from the network credential within the credential request response. The digital device **102** may identify forms received from the authentication server **108** and input data based on the form identifier and instructions. In another example, the digital device **102** provides information to the authentication server **108** to obtain network access based on the login procedural information included within the credential request response. The process of providing information to the authentication server **108** is further described in U.S. patent application Ser. No. 11/899,638 entitled "Systems and Methods for Obtaining Network Access", filed Sep. 6, 2007.

[0099] FIG. **7** is another flow diagram of the exemplary method for providing network credentials. The digital device **102** may search and find an available wireless network via the network device **104**. While connecting to the hotspot, the digital device **102** may receive network configuration information in step **702**. Network configuration information may comprise an identifier for the network device **104**, or the DNS server **110**. In one example, the digital device **102** receives a DNS server IP address (e.g., for the DNS server **110**) during the connection process.

[0100] In step **704**, the digital device **102** generates the credential request. The credential request may comprise a sequence identifier, DDID, and SSID. In step **706**, the digital device **102** optionally generates a nonce and digitally signs the credential request with an encryption key. The digital device **102** transmits the credential request as a standard protocol in step **708**. The network device **104** may receive and forward the credential request to the communication network **114**. In various embodiments, the network device **104** may provide the credential request to the DNS server **110** which may forward the credential request to the credential server **116**.

[0101] In exemplary embodiments, the credential request module **204** of the credential server **116** receives the credential request. The credential request module **204** may retrieve an encryption key associated with the DDID within the credential server from the encryption key storage **212**. The credential request module **204** may then decrypt the digital signature of the credential request for authentication. The credential request module **204** may further retrieve the nonce and a sequence identifier from the credential request.

[0102] The credential request response module **206** of the credential server **116** may then retrieve a network record associated with the DDID and the SSID from the network record storage **210**. The credential request response module **206** retrieves network credentials from the network record and generates the credential request response. The credential request response may comprise the network credentials and the nonce. The encryption/decryption module **208** may

encrypt the credential request response with an encryption key associated with the DDID retrieved from the encryption key storage **212**. In some embodiments, the credential request response is formatted as a standard protocol (e.g., DNS).

[0103] In step **710**, the digital device **102** receives the credential request response. The digital device **102** subsequently authenticates the credential request response in step **712**. In one example, the digital device **102** decrypts the credential request response with the same encryption key used to digitally sign the credential request. The digital device **102** may further retrieve the nonce within the credential request response and compare the nonce to the nonce transmitted within the credential request for further authentication. If the credential request response is found to be authentic, the digital device **102** retrieves the network credentials from the credential request response in step **714**.

[0104] In step **716**, the digital device **102** identifies the authentication requirements associated with network access. In various embodiments, the digital device **102** determines the correct information and network credentials to provide to the authentication server **108**. In one example, the digital device **102** retrieves one or more network access pages from the authentication server **108**. The digital device **102** may access the correct network access page from the authentication server and automatically make selections. In one example, the digital device **102** may automatically activate selections (e.g., activate buttons within the network access page, check boxes, and select radio buttons).

[0105] For example, the credential request response module **206** may provide instructions to the digital device **102** for the automatic selections within a network access page. As discussed herein, a network access page may comprise one or more web pages, one or more tags, or a combination of both retrieved from the authentication server **108**. In one example, software within the digital device **102** may automatically check all selection boxes within a network access page. The digital device **102** may then uncheck select boxes based on the login procedure information. Those skilled in the art will appreciate that there may be many methods with which selections may automatically be made. In other embodiments, the digital device **102** receives XML tags from the authentication server **108**. The digital device **102** may provide information based on the XML tags and instructions within the login procedural information to the authentication server **108** to obtain network access.

[0106] In step **718**, the digital device **102** provides the network credential to the network device **104** to obtain network access to the communication network **114**. In one example, the credential request response module **206** retrieves one or more forms from the authentication server **108**, populates the forms with one or more network credentials, and provides the completed forms to the authentication server **108**. In another example, the credential request response module **206** provides the network credentials as needed to the authentication server **108**. Once the network credentials are received by the authentication server **108**, the authentication server **108** may allow communication between the digital device **102** and the communication network **114**. In one example, the authentication server **108** commands the access controller **112** to allow the digital device **102** access to the communication network **114**.

[0107] The digital device **102** may subsequently test network connectivity to confirm network access. In one example, the digital device **102** transmits a request to the credential server **116** to determine if the communication network **114** is available. In some embodiments, the query or command contains the sequence identifier previously submitted within the credential request. If network access is successful, the credential server **116** may receive the request and retrieve the sequence identifier. The credential server **116** may then confirm that network access was successful.

[0108] FIG. **8** is a flow diagram of an exemplary method for receiving and storing network credentials. In various embodiments, users may create and store network records within the credential server **116**. For example, the credential server **116** may comprise a credential storage module (not depicted) that provides a graphical user interface (GUI) that allows users to create, store, update, remove, and modify network records.

[0109] In step **802**, the credential server **116** provides the user with a network credential request form. In one example, the credential server **116** provides the network credential request form to a user as one or more web pages over the Internet. The network credential request form is configured to receive the service provider's name (e.g., operator's name) and/or SSID and network credentials.

[0110] The service provider's name may comprise the name of the entity that operates the hotspot, one or more components related to the hotspot (e.g., the network device **104**), or the infrastructure of the local area network **106**. In some embodiments, the service provider's name comprises the name of an organization that manages one or more hotspots for another service provider. In one example, a coffee shop and bookstore may both use a third-party manager to manage the hotspots, even if the hotspots have different service providers. In some embodiments, the network credential request form may be configured to receive the third-party manager's name. In some embodiments, the service provider's name comprises the name of an organization that resells access to a hotspot network (e.g., an aggregator).

[0111] The network credential request form may also receive the SSID as a network service selection. In one example, the network credential request form comprises a pull down menu of different service providers and/or hotspots that the user may select. For example, a user may select "Starbucks" or "San Francisco International Airport" as a hotspot. The user may be given further options to such as geographic locations of the hotspot. The user may also select the service provider. For example, the user may select "T-Mobile" as a service provider. The network credential request form may then allow the user to select among one or more various hotspots associated with T-mobile. The selection(s) may then be stored as a network record. Alternately, a network service identifier associated with the selection(s) is generated as the SSID.

[0112] Further, the network credential request form may receive the network credential from the user. For example, the user may enter a username, password, passcode as network credentials within the network credential request form. In some embodiments, after the network credential request form receives the SSID, the network credential request form determines the type of network credentials required. For example, the network credential request form identifies the information required to access a network at a hotspot at the San Francisco International Airport previously selected by the user. The network credential request form then generates fields or selections to allow the user to enter only the information necessary (e.g., username, password) to obtain network access at the hotspot.

[0113] The credential server **116** may also require the user to register prior to receiving the network credential request form. During registration, the user may be required to agree to terms of service and enter customer information. Customer information comprises a username and a password to access the credential server **116** to store network credentials. Optionally, the customer information may comprise the user's address, contact information, and payment options for the user to use services offered by the credential server **116**.

[0114] In step **804**, the credential server **116** receives the customer information and network service selections over the network credential request form. In step **806**, the credential server may retrieve the network credential. In step **808** the credential server **116** receives the customer information. The credential server **116** associates the network credential with the customer information, network service selection and network credential(s) in step **810** to create a network record. The network record is then stored in step **812**.

[0115] In some embodiments, the user may manually access the credential server **116** via the Internet. In other embodiments, the user may download and install network credential software on the digital device **102**. The network credential software may identify and send the DDID of the digital device **102** to the credential server **116**. In other embodiments, the network credential software may be pre-installed on the digital device **102**. When the digital device **102** first activates the network credential software, the network credential software may identify and send the DDID of the digital device **102** to the credential server.

[0116] The user may input the SSID (e.g., identify the service provider or hotspots) into the network credential software. The user may also input the network credentials within the network credential software. After the network credential software has obtained the DDID, SSID, and network credentials, the network credential software may upload the information to the credential server **116** which stores the information within a network record. In various embodiments, the network credential software may be downloaded from the credential server **116**.

[0117] FIG. **9** is a block diagram of an exemplary digital device. The credential server **116** comprises a processor **900**, a memory system **902**, a storage system **904**, an I/O interface **906**, a communication network interface **908**, and a display interface **910**. The processor **900** is configured to execute executable instructions (e.g., programs). In some embodiments, the processor **900** comprises circuitry or any processor capable of processing the executable instructions.

[0118] The memory system **902** is any memory configured to store data. Some examples of the memory system **902** are storage devices, such as RAM or ROM. The memory system **902** can comprise the ram cache. In various embodiments, data is stored within the memory system **902**. The data within the memory system **902** may be cleared or ultimately transferred to the storage system **904**.

[0119] The storage system **904** is any storage configured to retrieve and store data. Some examples of the storage system **904** are flash drives, hard drives, optical drives, and/or magnetic tape. In some embodiments, the credential server **116** includes a memory system **902** in the form of RAM and a storage system **904** in the form of flash data. Both the memory system **902** and the storage system **904** comprise computer readable media which may store instructions or programs that are executable by a computer processor including the processor **900**.

[0120] The optional input/output (I/O) interface **906** is any device that receives input from the user and output data. The optional display interface **910** is any device that is configured to output graphics and data to a display. In one example, the display interface **910** is a graphics adapter. It will be appreciated that not all digital devices **102** comprise either the I/O interface **906** or the display interface **910**.

[0121] The communication network interface (com. network interface) **908** can be coupled to a network (e.g., the local area network **106** and communication network **114**) via the link **912**. The communication network interface **908** may support communication over an Ethernet connection, a serial connection, a parallel connection, or an ATA connection, for example. The communication network interface **908** may also support wireless communication (e.g., 802.11 a/b/g/n, WiMax). It will be apparent to those skilled in the art that the communication network interface **908** can support many wired and wireless standards.

[0122] In various embodiments, systems and methods are described that enable a digital device to automatically select and access an available wireless network from a plurality of available wireless networks based on rules to achieve a satisfactory quality of service. Such rules could be implemented in the digital device itself, on a server in communication with the digital device, or a combination of both. In various embodiments, a wireless network is a network that allows wireless access between a digital device and a communication network such as the Internet.

[0123] In accordance with some embodiments, a user of a wireless digital device (e.g., digital device capable of Wi-Fi communication) creates an account on a web server and registers one or more digital devices (e.g., computers, laptops, personal digital assistants, and cell phones) with that account. The registered digital devices can be managed and a network record provisioned by a central server (e.g., a profile server or a credential server) via a network communication mechanism, such as HTTP.

[0124] FIG. **10** is a diagram of another environment in which embodiments of the present invention may be practiced. In various embodiments, a user with a digital device **1002** enters an area located near the network devices **1004** and **1006**. In one example, the network devices **1004** and **1006** are separate access points which may each be used to establish communication between the digital device **1002** and the communication network **1008**.

[0125] The digital device **1002** may scan the area surrounding the digital device **1002**, detect the two network devices **1004** and **1006**, and generate a list of available wireless networks with which the digital device **1002** may establish communication. In some embodiments, the list of available wireless networks comprises DDID, SSID, and/or BSID identifiers of the network devices **1004** and **1006**.

[0126] Subsequently, the digital device **1002** provides the list of available wireless networks to a rules server **1010**. In one example, the digital device **1002** provides the list of available wireless networks as a standard protocol over an open port of either the network device **1004** or the network device **1006** to the communication network **1008** and, ultimately, to the rules server **1010**. In another example, the digital device **1002** provides the list of available wireless networks over another network such as a cellular communication network (e.g., via CDMA, GSM, 3G, or EVDO) or other wireless network (e.g., Wi-Fi, Wimax, or LTE network) not depicted.

[0127] The rules server **1010** receives the list of available wireless networks and may retrieve a network profile for each wireless network identified within the list. A network profile is a record that is associated with a wireless network and comprises attributes concerning performance and/or quality of service provided by the associated network. In one example, the rules server **1010** identifies each network within the list and provides the SSID and/or BSID for each network to the profile server **1014**. The profile server **1014** may then provide a network profile (based on the SSID and/or BSID) for each network to the rules server **1010**. In some embodiments, the profile server **1014** retrieves the network profile from a database or other server (e.g., network database server **1012**).

[0128] The rules server **1010** may select a preferred wireless network from the list of available wireless networks based on attributes within the network profiles and/or any attributes received from the digital device **1002**. An attribute is a characteristic of a wireless network. In various embodiments, an attribute includes a performance metric, a shared indicator, or a service identifier. A performance metric of a wireless network is any measure of network performance. In some examples, a performance metric may comprise a latency metric, a bandwidth metric, or a quality of service (QOS) metric. Those skilled in the art will appreciate that a performance metric may include any type of metric that represents performance of a wireless network.

[0129] A latency metric is a measurement that represents time to send a packet of data from the digital device to a server on a network. In some embodiments, the digital device **1002** may send an ICMP "echo request" packet to a server and listen for an ICMP "echo response" reply. The latency metric may comprise an estimate of the round-trip time (generally in milliseconds) and/or include any packet loss. In another example, the latency metric is half of the estimated round-trip time.

[0130] A bandwidth metric is a measurement of the available bandwidth of a wireless network. In one example, the digital device may test available bandwidth by sending a block of data over the wireless network to a server and timing the response.

[0131] A QOS metric is any metric that measures the quality of service of the wireless network, the access device **1004**, the access device **1006**, and/or the communication network **1008**. In one example, the QOS metric represents a reliability of the DHCP which is determined by timing the length of time required to get an IP address. The reliability of the DHCP may comprise a statistical measurement, a probability of receiving an IP address at all, and/or a distribution of time.

[0132] A shared indicator indicates if a wireless network is shared. In some embodiments, the shared indicator may be one of three states including "shared," "not shared," and "unknown". Although the shared indicator may only include a single state (e.g., "not shared"), those skilled in the art will appreciate that the shared indicator can have any number of states. A wireless network with a shared indicator that indicates that the network is "shared" may indicate that the owner of the wireless network intends for others to use the network. One example of a "shared" network may include a wireless network which is intentionally "open" (e.g., unencrypted) for others to use.

[0133] A wireless network with a shared indicator that indicates that the network is "not shared" may indicate that the owner of the wireless network does not desire anyone who does not have express permission to access the network. In one example, wireless networks that are not shared are often intentionally encrypted (e.g., through WEP or WPA) so as to limit access to unauthorized users. Not all networks that are "not shared," however, are encrypted. For example, the owner of the network may misconfigure the network device or, through error, allows a network to be open (i.e., unencrypted) even though the network is not intended to be shared.

[0134] A wireless network with a shared indicator that indicates that the network is "unknown" may indicate that the wireless network may either be "shared" or "not shared." For example, the intent of the owner of an open network may not be known.

[0135] A service identifier may identify one or more services supported by the wireless network. In one example, one or more service identifiers indicate that a wireless network supports VOIP, teleconferencing, and/or video conferencing. The service identifier may identify any kind of service supported by the wireless network. In some embodiments, the service identifier may identify services that are not supported by the wireless network.

[0136] Those skilled in the art will appreciate that the network profile may comprise any number of attributes. Further, those skilled in the art will appreciate that the network profile may comprise only one or more performance metrics, only one shared indicator, or only one or more service identifiers.

[0137] In various embodiments, the rules server **1010** selects one or more wireless networks from the list of available wireless networks based on the attribute analysis. In one example, the rules server **1010** applies rules to the attributes. The rules may comprise minimum requirements, personalized settings, and attribute comparisons. In one example, the rules applied by the rules server **1010** may compare the attributes of one or more wireless networks to one or more minimum requirements. If the attributes for a wireless network are below the minimum requirements, then the wireless network may not be selected or removed from the list of available wireless networks.

[0138] In some embodiments, the rules applied by the rules server **1010** may be based on personalized settings by the user. For example, the user of the digital device **1002** may indicate personalized settings that indicate that the digital device **1002** is only to connect over wireless networks that have been designated as "shared." In this example, the rules server **1010** may select only those wireless networks with an attribute that comprises a shared indicator that identifies the wireless network as "shared."

[0139] In various embodiments, the rules applied by the rules server **1010** may be based on a comparison of the attributes of one wireless network to another. In one example, the attributes may indicate that one wireless network has a greater bandwidth and shorter latency than another. In this example, the rules server **1010** may select one wireless network that has better performance or valuable services in comparison to another. Those skilled in the art will appreciate that there may be any kind of rule used to select or to assist in the selection of a wireless network from the list of available wireless networks.

[0140] More than one rule may be applied by the rules server **1010** in making the wireless network selection. In one example, the rules server **1010** may apply personalized settings of the user before comparing attributes from different wireless networks and making a selection. In another

example, the rules server **1010** may apply minimum requirements to the attributes before comparing the attributes.

[0141] Once the rules server **1010** selects the wireless network based on the comparison of attributes from the network profiles, the rules server l **010** may provide the wireless network selection to the digital device **1002**. A wireless network selection includes one or more identifiers (e.g., network identifiers) that identify at least one wireless network. The wireless network selection may identify a single wireless network or comprise a sorted list of wireless networks which is sorted in order of preference.

[0142] In some embodiments, the rules server **1010** provides credentials (e.g., a credential request response) for the selected wireless network in addition to the wireless network selection to the digital device **1002**. In one example, the rules server **1010** provides the selected wireless network to the credential server **1016** which then provides a credential request response (even though no credential request has been made) for the selected wireless network to the digital device **1002**. In other embodiments, the digital device **1002** receives the wireless network selection and then proceeds to transmit a credential request to the credential server **1016** to receive the credentials as discussed herein.

[0143] Further, in various embodiments, the digital device **1002** attempts to establish a connection based the selected wireless network. If the connection fails, the digital device **1002** may transmit a credential request to the credential server **1016** to retrieve credentials for network access as described herein. The digital device **1002** may provide the credential request to the credential server **1016** over an open port of the network device **1004**. In another example, the digital device **1002** may provide a credential request over any other network including a connection with a different network device or over a cellular connection.

[0144] Although the rules server **1010**, network database server **1012**, profile server **1014**, the credential server **1016**, and the web server **1018** are depicted as separate servers in FIG. **1**, the servers may all be combined as one or more servers. Similarly, the functions of any of the servers may be performed by one of the other servers depicted or any other server.

[0145] Although FIG. **10** depicts multiple servers (e.g., rules server, network database server, profile server, credential server, and web server) for performing the selection of a wireless network from the plurality of available wireless networks, it will be appreciated by those skilled in the art that the selection of the wireless networks may occur within the digital device **1002**. In one example, the digital device **1002** retrieves the scan results listing available wireless networks and selects a wireless network based on configuration preferences. The configuration preferences may be based on one or more locally executed rules, preferred signal strength, or any other attribute or attributes. In another example, the digital device **1002** selects a wireless network that supports a desired service (e.g., VOIP), meets a minimum latency standard, and meets a minimum QOS standard. In another example, the profile server **1014** provides the desired network profiles to the digital device **1002** which performs the analysis to determine the preferred wireless network.

[0146] FIG. **11** is a flow diagram of an exemplary process for providing a selection of a wireless network. In step **1102**, a server (e.g., rules server **1010**, network database server **1012**, profile server **1014**, credential server **1016**, or web server **1018**) receives a list of available wireless networks from the digital device **1002**. In some examples, the list comprises the SSIDs or BSIDs of one or more network devices (e.g., network device **1004** and network device **1006**). The list can comprise any information that identifies a network and/or network device.

[0147] In some embodiments, the server also receives one or more attributes associated with a network and/or network device. In various embodiments, the digital device **1002** measures signal strength, determines available services, or takes a performance metric for one or more networks and/or network devices that are identified on the list of available wireless networks.

[0148] In step **1104**, the server retrieves a network profile from a plurality of network profiles stored in a network database for each available wireless network on the list of available wireless networks. Each network profile may comprise at least one attribute. In some embodiments, not all wireless networks on the list have a network profile. When a network profile for a wireless network on this list is not found, a network profile associated with the wireless network may be then created. If attributes are received from the digital device **1002**, the server may determine which attribute received from the digital device **1002** is associated with which network, network device, and/or network profile.

[0149] In step **1106**, the server compares attributes from each network profile against minimum requirements. In one example, the server compares latency metrics from all network profiles in the list (if available) against a minimum latency metric. The server may also compare attributes received from the digital device **1002** against the minimum requirements. In step **1108**, the server removes one or more wireless networks from the list of available wireless networks and/or wireless network profiles based on the comparison(s). For example, any wireless network with a latency metric that falls below the minimum latency metric may not be selected. In other embodiments, a wireless network with a latency metric that falls below the minimum latency metric may receive a weighted value that will be compared to other wireless networks to assist in the selection process.

[0150] In some embodiments, the user of the digital device **1010** determines the minimum requirements. In other embodiments, the minimum requirements may be selected for the user (e.g., by an administrator).

[0151] In step **1110**, the server retrieves personalized settings for a user. The personalized settings may be sent by the user to the server. In some embodiments, the user has an account with the web server **1018** which contains the personalized settings. In one example, the server receives a user identifier along with the list of available wireless networks. The server then accesses the user's account and receives the personalized settings which are then applied to the attributes of the network profiles associated with a wireless network on the list. In various embodiments, users may configure personalized settings (e.g., the "aggressiveness") at which a digital device **1002** may connect to a wireless network. Such configurations could include:

[0152] (a) Connect to anything open regardless of shared indicator;

[0153] (b) connect to anything open except those with default manufacturer SSIDs (e.g., "linksys") that likely indicate the owner simply left the access point open out of the box and is unaware how to configure security functions;

[0154] (c) connect to anything open that the profile server **108** has seen (or stored information regarding the Wi-Fi network); or

[0155] (d) connect to anything open with a shared indicator of "shared," or has been marked as shared by some other means.

Those skilled in the art will appreciate that there may be many personalized settings.

[0156] In step **1112**, the server removes one or more wireless networks from the list or network profiles based on the personalized settings. For example, the personalized settings may indicate that the user only wishes to connect to wireless networks that support videoconferencing and maintain a user defined QOS requirement. The server may then remove any wireless networks from the list of available wireless networks based on the attributes either from the network profiles or recently received from the digital device **1002** that do not meet the user's personalized settings.

[0157] In some embodiments, the personalized settings may then be taken into account either before or after comparison of attributes from the network profiles. In one example, personalized settings indicate that the user does not wish to connect to a wireless network that is not designated as "shared" or providing certain services. In one example, the rules server **1010** either does not retrieve the network profiles associated with networks that do not provide the necessary service and/or does not compare attributes associated with those networks. In other embodiments, the digital device **1002** applies personalized settings to results (e.g., the wireless network selection) received from the rules server **1010** before accessing a preferred wireless network.

[0158] In step **1114**, the server compares the attributes of the remaining wireless networks on the list. In various embodiments, the server will apply a weight and normalize one or more of the attributes (e.g., metrics) from within the network profiles. In some embodiments, older attributes may be removed or weighed less than other attributes that are newer. In one example, any metric that is over one week old may receive less weight than a similar newer metric. In another example, a metric that is over one month old may be removed from the network profiles or not considered in the comparison. Those skilled in the art will appreciate that not all attributes or information from within the network profiles may be taken into account in the comparison.

[0159] Each network profile may comprise any number of attributes. In one example, the rules server **1010** makes a wireless network selection based on comparing a metric from two different network profiles. In some embodiments, the rules server **1010** selects a wireless network based on a comparison between two similar metrics (i.e., the latency metric from the first network profile is compared to the latency metric from the second network profile). Those skilled in the art will appreciate that the rules server **1010** may select a wireless network based on comparisons between two similar recently received metrics or a recently received metric and another within a network profile.

[0160] In other embodiments, the rules server **1010** selects a wireless network based on a comparison of two dissimilar metrics (i.e., the latency metric from the first network profile is compared to a bandwidth metric from the second network profile). The rules server O**10** may execute an algorithm to weigh and normalize similar and/or dissimilar metrics or attributes in order to make a comparison for selecting the appropriate wireless network. In one example, the rules server **1010** compares a latency metric in the first network profile to a bandwidth metric in the second network profile. The rules server **1010** may execute an algorithm to weigh and normalize the metrics. The algorithm may weigh the latency metric more than the bandwidth metric since latency may have a greater impact on network performance.

[0161] An attribute or metric may receive different weights depending on any number of factors. For example, a latency metric may receive a given weight when the metric falls within an acceptable range, otherwise the latency metric may be significantly less weight. A metric recently received from the digital device **1002** may receive greater weight than a metric of a similar type within a network profile. Those skilled in the art will appreciate that there are many ways to compare similar and/or dissimilar performance and/or qualitative metrics.

[0162] In step **1116**, the server selects a wireless network based on the comparison of attributes. The wireless network selection may comprise a single preferred wireless network or a list of wireless networks sorted in order of preference. In one example, the rules server **1010** identifies the most preferred network, the second most preferred network, and so on. The rules server **1010** then provides the wireless network selection to the digital device **1002** in step **1118**.

[0163] In various embodiments, the rules server **1010** only compares metrics that are recently received from the digital device **1002**. In one example, two latency metrics are received from the digital device **1002**. Each latency metric is associated with a separate wireless network identified on a list of available networks. In this example, the rules server **1010** may select a wireless network based on a comparison of the two attributes.

[0164] FIG. **12** is a flow diagram of an exemplary process for selecting a wireless network. In step **1002**, the digital device **1002** enters into an area with two wireless networks and the digital device **1202** scans for networks to access. In step **1204**, the digital device **1002** receives a first and a second network identifier of available wireless networks. As discussed herein, the first and second network identifiers may comprise BSIDs, SSIDs, or any other network identifiers. For example, the first network identifier may comprise a BSID and the second network identifier may comprise an SSID identifier. In another example, the first network may provide multiple identifiers including a BSID and an SSID while the second network provides only an SSID. In this example, the first network identifier may comprise both the BSID and the SSID of the first network device while the second network identifier is only an SSID of the second network device.

[0165] In step **1206**, the digital device **1002** generates a list of available wireless networks. For example, the digital device **1002** may generate a list comprising the first network identifier and the second network identifier. The list is then provided to a server in step **1208**.

[0166] In step **1210**, the digital device **1002** receives a wireless network selection from the server. The wireless network selection may comprise an identifier that identifies the selected wireless network or identifies the network device associated with the selected wireless network (e.g., a BSID and/or SSID of the network device). In various embodiments, the wireless network selection may comprise a list of wireless networks sorted by preference. The list may comprise two or more identifiers that identifies a selected wireless network or network device.

[0167] In step **1212**, the digital device **1002** receives credentials for the wireless network selection from the server. In some embodiments, the credentials are received from the same server that received the list of available wireless networks from the digital device **1002**.

[0168] In various embodiments, the digital device **1002** receives the wireless network selection from the server and then provides a credential request to receive the credentials for the desired network. In one example, the digital device **1002** provides the credential request in the same manner that the digital device **1002** provided the list of available wireless networks (e.g., over an open port of a network). In some embodiments, the preferred network does not require credentials or the credentials are stored locally on the digital device **1002**.

[0169] In step **1214**, the digital device **1002** accesses the selected wireless network with the credentials. The process of applying the credentials to a login page or the like is discussed herein.

[0170] In various embodiments, the digital device **1002** may provide the list of available wireless networks to the server over an open port of a network device in a manner similar to providing a credential request discussed herein. In other embodiments, the digital device **1002** may provide the list to the server over another network. In one example, the digital device **1002** generates a list of available Wi-Fi networks and provides the list over a cellular network (e.g., EVDO or 3G network). In this example, the wireless network selection may be returned to the digital device over the cellular network and then the digital device **1002** may attempt to access the preferred Wi-Fi network.

[0171] In another example, the digital device **1002** accesses one wireless network. The digital device **1002** can then provide a list of the available wireless networks to the server. The server may return the wireless network selection to the digital device **1002**. If the preferred wireless network is not the network that the digital device **1002** has originally accessed, then the digital device **1002** may drop the connection and access the preferred wireless network.

[0172] Although FIGS. **10-12** contemplate a server receiving a list of available wireless networks, determining a wireless network selection, and providing the selection to the digital device **1002**, those skilled in the art will appreciate that a server is not necessary. In one example, the digital device **1002** generates a list of available wireless networks and then retrieves any available information regarding the networks on the list (e.g., from locally stored network profiles, from one or more network devices, from a local or remote database, and/or retrieving information from another network such as the Internet). The digital device **1002** may then make comparisons based on what attributes associated with the networks are available to make a selection or generate a prioritized list. The digital device **1002** may then access the selected wireless network.

[0173] In various embodiments, the digital device **1002** may generate and provide attributes regarding one or more networks to update the network profiles. In one example, the digital device **1002** determines the quality of the signal, bandwidth, or any other metrics and provides those metrics along with the list of available wireless networks to a server. In another example, as the digital device **1002** accesses a selected wireless network, measures attributes, and provides the attributes update metrics within a network profile. Attributes (e.g., latency metrics, bandwidth metrics, and QOS metrics) may be taken by the digital device **1002** at any time and used to update the network profiles.

[0174] FIG. **13** is a diagram for selecting a wireless network and accessing the selected wireless network. In various embodiments, the network device **1004** and network device **1006** provide a first and second network identifiers to the digital device **1002** in steps **1302** and **1304**. In step **1306**, the digital device **1002** generates metrics (i.e., attributes) by taking measurements regarding wireless networks associated with the network device **1004** and network device **1006**. In some examples, the metrics may include latency, strength of signal, or QOS metric.

[0175] In step **1308**, the digital device **1002** generates a list of available wireless networks which may include the network identifier from the network device **1004** as well as the network identifier from the network device **1006**. In some embodiments, the digital device **1002** may also comprise personalized settings which may indicate a preference between the two network identifiers or eliminate one or both of the network identifiers. In one example, the personalized settings indicate that only open networks that do not have a default manufacturer SSID (e.g., "linksys") may be accessed. In this example, if the network identifier from the network device **1004** indicates a default manufacturer SSID, the digital device **1002** may not include that network identifier for the network device **1004** in the list of available wireless networks.

[0176] In some embodiments, if the digital device **1002** cannot generate a list identifying at least two or more networks, the digital device **1002** does not send the list. In one example, if the digital device **1002** can only identify one available wireless network that meets the user's requirements, then the digital device **1002** may attempt to access the wireless network directly or send a credential request for to a server to retrieve any necessary credentials for access.

[0177] In step **1310**, the digital device **1002** provides the attributes and the list of available wireless networks over an open port (e.g., port **53**) of the network device **1006** which acts like a proxy in providing the attributes and list of available networks to the rules server **1010**. In other embodiments, the digital device **1002** provides the attributes and the list over an open port of the network device **1004**. Alternately, the digital device **1002** may provide the attributes and the list over separate networks (e.g., the attributes over an open port of one of the network devices and the list over a cellular network). In step **1312**, the network device **1006** acts as a proxy by providing the attributes and list via DNS to the rules server **1010**.

[0178] In step **1314**, the rules server **1010** retrieves network profiles. In one example, the rules server **1010** retrieves the network identifiers from the list and retrieves network profiles associated with the network identifiers.

[0179] In step **1316**, the rules server **1010** (or profile server **1014**) updates attributes within the network profiles with the attributes received from the digital device **1002**. In one example, a new latency metric from the digital device **1002** is used to update the network profile associated with the network identifier from the network device **1004**. A time-to-live value associated with the attribute may also be updated to indicate that the new latency metric is recent.

[0180] In step **1318**, the rules server **1010** selects a network device based on comparing the attributes from within the network profiles. In some embodiments, the rules server **1010** also applies personalized settings from the digital device **1002** or from an account associated with the digital device **1002** (e.g., via the web server **1018**) before making a selec-

tion. The rules server **1010** may prepare a prioritized list of the two network devices from the list provided by the digital device **1002**. The list is prioritized based on which of the two network devices provides the most desirable service based on the metrics from the network profiles.

[0181] In step **1320**, the rules server **1010** provides the wireless network selection and credentials via DNS back to the network device **1006** to function as a proxy to send the information to the digital device **1002**. In one example, the rules server **1010** selects the network device **1004**. The rules server **1010** may retrieve credentials for the network device **1004** based on the network identifier of the network device **1004**. For example, the rules server **1010** may provide a credential request to the credential server **1016**. The credential server **1016** may provide a credential request response containing necessary credentials to the rules server **1010** which then sends both the credentials received from the credential server **1016** as well as the wireless network selection to the digital device **1002**.

[0182] In step **1322**, then network device **1006** provides the network selection and the credentials over the open port to the digital device **1002**. In step **1324**, the digital device **1002** provides the credentials to access the network device **1004** and generates additional attributes regarding the network (i.e., take additional measurements). Once a connection is established, the new attributes are provided to the rules server **1010** or profile server **1014** to update the network profile associated with the network device **1004** in step **1326**. In one example, the digital device **1002** may measure the time required to establish the connection with the network device **1004**. The time required to establish the connection may then be used to update attributes in a network profile. If a connection is not established or fails, that information may also be provided to update the associated network profile.

[0183] In some embodiments, if the network connection with the selected network fails, the digital device **1002** may re-attempt to make the connection. If multiple attempts to make the connection fail, information regarding the failure is sent to update the associated network profile. The digital device **1002** may then attempt to make a connection with another network device (e.g., the network device **1006**). In some embodiments, the digital device **1002** re-scans the area, generates a new list of available networks which may not include the network that the digital device **1002** failed to connect. The new list may be sent to the rules server **1010** to receive a new wireless network selection and the process may repeat.

[0184] In some embodiments, the rules server **1010** provides a prioritized list of available wireless networks sorted by preference. In one example, the rules server **1010** provides a prioritized list of three networks to the digital device **1002**. The digital device **1002** may then attempt to access the first wireless network on the prioritized list. If the digital device **1002** is unable to connect to the first wireless network, then the digital device **1002** may proceed to attempt to connect to the next network on the list. Those skilled in the art will appreciate that the prioritized list may contain all, one, or some of the wireless networks identified in the list of available wireless networks. For example, the rules server **1010** may not identify wireless networks which are known to provide poor performance, do not provide desired service (e.g., VOIP service), and/or are otherwise blacklisted.

[0185] In various embodiments, the user of the digital device **1002** may override the wireless network selection to access any wireless network. In one example, the user chooses the priority of available wireless networks. In some embodiments, the user may configure the digital device **1002** or configure an account with the web server **1018** to include personal preferences that may reorder or otherwise alter a prioritized list of wireless networks from the rules server **1010**. For example, the list of available wireless networks may be altered based on user preferences by the digital device **1002** or the web server **1018** prior to being provided to the rules server **1010**.

[0186] In some embodiments, in addition to one or more open Wi-Fi networks, there may also be one or more encrypted Wi-Fi networks in a given location. A digital device **1002** may connect to an open Wi-Fi network and transmit the SSID of other Wi-Fi networks, including encrypted Wi-Fi networks, to the rules server **1010** via a network communication protocol such as HTTP.

[0187] The rules server **1010** may then determine, based on personalized settings or other rules, that an available encrypted Wi-Fi network is the preferred choice for a network connection. The rules server **1010** may transmit the necessary encryption keys to the digital device **1002** over the current open Wi-Fi network connection and send instructions to the digital device **1002** to switch to the encrypted Wi-Fi network.

[0188] In various embodiments, a network database may be used to centralize information regarding many different networks. A network database may store a plurality of network profiles. Each network profile within the network database may be associated with a separate network. In some examples, the network profile is associated with a separate network by an BSID, DDID, SSID, or other identifier. Each network profile may comprise attributes from one or more users.

[0189] As more digital devices access new and existing wireless networks, attributes (e.g., metrics and other information) may be collected and stored within the network profiles of the network database. The attributes from many digital devices that access the same wireless network may be weighted and/or averaged to produce an attribute with a higher probability that the attribute will match expected future network performance. Further, users may contribute information or attributes directly (e.g., indicating that a network is shared) to more accurately characterize the wireless network.

[0190] As attributes associated with available wireless networks are gathered and organized, the quality of selections of wireless networks based on the attributes from the network database may increase. For example, a latency metric from a single user's experience with a wireless network may not be representative of the performance of the network. However, a latency metric that is formed from averaging the latency metrics received from twenty separate users who use the same wireless network may be a very accurate indicator of future performance. As more attributes and information is gathered on an increasing number of wireless networks and stored within the network database, the quality and service of wireless networks may be measured. As a result, a digital device may automatically access a wireless network and receive an expected or at least a minimum level of performance.

[0191] FIG. **14** is a flowchart of an exemplary process for updating and storing attributes associated with wireless networks within a network database. Digital devices may scan or receive attributes regarding different network devices and/or networks. These attributes may be provided to a network

database where the information will be stored and aggregated with other attributes for the same network. The digital device may provide that attributes to the network database in many ways. For example, the digital device may provide the attributes to the network database over an open port of a network device. Alternately, the digital device may provide the attributes to the network database through a cellular network or any kind of network.

[0192] The digital device may provide attributes to the network database at any time. In one example, the digital device provides the attributes to the network database prior to logging into a wireless network (e.g., as a standard protocol over an open port). In another example, the digital device may transmit one or more attributes along with a list of available wireless networks as discussed in FIG. **13**. Further, attributes may be collected by the digital device while using a wireless network. In one example, the digital device may be logged into a wireless network for two or more hours. During that time, the digital device may take a latency metric every ten minutes. Similarly, during that time, the digital device may take a bandwidth metric or measure a QOS metric. The attributes may be sent at any time to the network database which may analyze and/or store the attributes.

[0193] In step **1402**, a digital device **1002** receives a network identifier and generates an attribute associated with the network identifier. In one example, the network identifier is a BSID of the wireless network. The attribute may comprise a performance metric, shared indicator, or service identifier. In one example, the digital device **1002** measures a bandwidth metric of a wireless network associated with the network identifier.

[0194] In step **1404**, the digital device **1002** provides the network identifier and attribute to a server to store the attribute within the network database. The digital device **1002** may provide the attribute to the network database as the attribute becomes available. Alternatively, the digital device **1002** may provide one or more attributes to the network database at predetermined intervals or at a given time. Those skilled in the art will appreciate that the digital device **1002** may be configured by a user or an administrator to control how and when the digital device **1002** generates attributes or tests the network to generate one or more attributes. Further, the user or administrator may configure how and when the digital device **1002** provides the attributes to the network database.

[0195] The server may be any kind of server (e.g., a rules server **1010**, network database server **1012**, profile server **1014**, credential server **1016**, or web server **1018**). In one example, the profile server **1014** receives the network identifier and attribute from the digital device **1002**. The profile server **1014** may determine if a network profile associated with the network identifier is within the network database in step **1406**. In one example, the profile server **1014** queries the network database server **1012** for a network profile associated with the network identifier. The network database server **1012** may control the network database.

[0196] If the network profile exists, then another user or administrator has identified or had experience with the wireless network associated with the network identifier. If the network profile does not exist, then the network database may not have previously received an attribute for the wireless network associated with the network identifier. If the network profile exists, the network profile is retrieved in step **1408**. In one example, the network database server **1012** provides the requested network profile to the profile server **1014**.

[0197] The profile server **1014** may then update an existing attribute already within the network profile with the newly received attribute in step **1410**. In one example, a latency metric may already exist within the network profile. The older latency metric may be averaged with the new attribute to form a new latency metric that is then stored within the network profile. If an attribute of the same type as the received attribute does not already exist within the network profile, the attribute may be stored within the network profile. For example, the recently received attribute may be a service identifier that indicates that the network supports VOIP. If no such attribute exists within the network profile, the service identifier is then stored within the network profile.

[0198] Those skilled in the art will appreciate that attributes may be combined by any kind of algorithm. In various embodiments, each quantitative attribute (e.g., performance metric) may be weighted based on any number of factors. In one example, individual quantitative attributes for the same metric are all stored within a network profile. The profile server **1012** may execute an algorithm that weighs each individual quantitative attribute based on the number of individual attributes and/or when the attributes were received (older attributes are weighted less than newer attributes). As the number of attributes for each type is received, the accuracy of a weighted representation (e.g., an weighted average) may increase.

[0199] If the network database server **1012** finds that the network profile did not previously exist, the network database server **1012** or the profile server **1014** may create a new network profile associated with the network identifier. The profile server **1014** may then store the attribute within the network profile in step **1414**.

[0200] In various embodiments, the digital device **1002** enters into an area with five wireless networks. The digital device **1002** may generate a list of available wireless networks comprising network device identifiers for all five networks. If any of the five networks have not been previously identified, the network database server **1012** (or any serve) may automatically create a new network profile for each network not previously identified.

[0201] In step **1416**, the profile server **1012** optionally updates a time-to-live characteristic of the attribute. The time-to-live characteristic is a predetermined time that may affect the weight of the attribute in an algorithm and/or may be a deadline from which the attribute is considered expired. In one example, an attribute may be weighted less as the attribute get older (e.g., received two to three weeks before the current time). In some embodiments, when an attribute is thirty days old, the attribute is automatically expired. In one example, an expired attribute may be removed from the network profile automatically. In another example, the attribute may continue to exist in the network profile but is either ignored or weighted very lightly in comparison to newer or "fresher" attributes of the same type.

[0202] In some embodiments, a weighted average of all attributes of a certain type (e.g., the last twenty latency metrics associated with a single wireless network received over the last two weeks) is also associated with a time-to-live characteristic. If the average is not updated, the average itself may be weighted in a manner consistent with the stale

attributes. In some embodiments, averages may expire based on the time-to-live characteristic if the average is not updated regularly.

[0203] In step **1418**, the profile server **1014** or the network database server **1012** stores the network profile within the network database.

[0204] In another example metrics are provided by the digital device **1002** to update one or more network profiles. In one example, a wireless network is recently upgraded to support VOIP. In this example, the digital device **1002** may detect the new capability and provide a service identifier that indicates this capability to the rules server **1010**. The rules server **1010** may retrieve and update a network profile from the profile server **1014** to indicate the new capability. The updated network profile may then be stored within the network database.

[0205] In various embodiments, attributes received from a digital device **1002** may be stored within a plurality of network profiles associated with different network device identifiers. In one example, an attribute comprises a physical location of the network and/or network device identifier. If the digital device **1002** provides a list of available wireless networks, and the location of one of the wireless networks is known, then the network database server **1012** may conclude that all networks on the list of available wireless networks must also be in the same general location. As a result, the network database server **1012** may create or update attributes in all network profiles associated with the list to specify a location even if one or more of those wireless networks are otherwise encrypted (e.g., WEP or WPA).

[0206] A server (e.g., the profile server **1014**, the credential server **1016**, or the web server **1018**) may also be able to determine the location of the digital device **1002**. In one example, the profile server **1014** receives a BSID from the digital device **1002**. The profile server **1014** may refer to a database of locations for different BSIDs to determine the location of the user. In another example, the profile server **1014** may query a GPS unit in the digital device **1002** or a GPS unit within the network device associated with the network device identifier to receive location information. In yet another example, the location of the digital device **1002** may be determined by using an IP address of the digital device **1002**. The location attribute for all wireless networks in the area may then be updated to indicate the general location of related wireless networks or network devices.

[0207] In some embodiments, the location of the user may be determined or retrieved from a network profile in order to identify the general physical location of the user. The general physical location of the user can be used to update attributes of networks in the user's area as discussed. In various embodiments, a location directory of available wireless networks may be created. In one example, a graphical user interface allows a user to interact (e.g., via a web site) with a location database thereby allowing the user to browse a directory of available wireless networks and their respective locations. Further, the directory may indicate one or more attributes or functions of attributes. In one example, the directory identifies the expected latency of one or more wireless networks as well as the location, service offered, and whether the wireless network is intentionally shared.

[0208] Further, targeted advertising may be directed to the digital device **1002** depending on the location of the user or the user's proximity to goods and services. In various embodiments, a database of locations of wireless networks may be generated. Access to the database may then be sold to advertisers to create or direct advertisements.

[0209] FIG. **15** is another flowchart of an exemplary process for updating and storing attributes associated with wireless networks within a network database. In various embodiments, an owner of a wireless network, user of a digital device **1002**, and/or administrator may log onto a web server **1018** to create, update, or access one or more network profiles. In one example, network owners registered with the web server **1018** have the ability to add information and/or attributes within a network profile regarding their own network. For example, the user may indicate that, although the network is open, it is not to be shared (e.g., storing a shared indicator that indicates that the wireless network is "not shared" within the network profile). Alternately, the user may designate their network as "shared." Further, the user may indicate what services may be used over the network (e.g., by the performance of the network is suitable for VOIP or online conference calling but not online video conferencing). The user may also provide information regarding the location of their network device and other network devices in the area.

[0210] In another example, a user of a digital device **1002** registered with the web server **1018** may add attributes regarding wireless networks they have experience with. For example, a user of a digital device **1002** may log onto the web server **1018** to store a shared indicator that indicates a local coffee-shop network is "shared." In some embodiments, the user of the digital device **1002** may be authorized to store an attribute to all network profiles of all coffee shops of the same chain to indicate that their networks are "shared." In other embodiments, an administrator of the coffee-shops or an administrator of the network database may store a shared indicator indicating that all of the wireless networks offered by coffee-shops of the chain are "shared."

[0211] In step **1502**, the web server **1018** logs in a user. The user may log in or register with the web server **1018** over a network such as the Internet. In one example, the user browses to a web page to enter a username or password. In some embodiments, the connection between the user and the web server **1018** are encrypted before or after the user logs in.

[0212] In various embodiments, any user with a digital device **1002** capable of wireless access may have the option to register with the web server **1018**. In some embodiments, the user is authenticated to confirm authorization. Owners of networks may have the option to change the attributes of their own network but not the attributes of any other networks. Administrators, on the other hand, may have the authorization to change attributes associated with a plurality of networks.

[0213] In step **1504**, the web server **1018** receives a network device identifier and an attribute from the user or administrator. In some embodiments, the network device identifier is associated with a single wireless network. In one example, the network device identifier is a BSID identifier of a network device. In other embodiments, the network device identifier is associated with a plurality of wireless networks. For example, the network device identifier may be an SSID identifier such as "Starbucks" The SSID identifier may be shared by many network devices. In this example, every wireless network at a Starbucks coffee shop may have the same SSID identifier.

[0214] In step **1506**, the web server **1018** determines if a network profile associated with the network identifier is within a network database. In some embodiments, the network database is local to the web server **1018**. In other embodiments, the network database server **1012** comprises

the network database. In one example, the web server **1018** provides a request for one or more network profiles that are associated with the network device identifier to the network database server **1012**. In another example, the web server **1018** may query the network database directly or provide a request to the network database server **1012** to determine if the network profile exists.

[0215] If the network profile exists, then the web server **1018** or the network database server **1012** determines if the user has authorization to the changes to the network profile in step **1508**. In some embodiments, the network profile comprises or is associated with security settings that indicate if the user or administrator has rights to access, view, or modify the network profile. In one example, the web server **1018** confirms the authorization of the user with the security settings. Assuming the user is authorized, the network profile is retrieved in step **1510**. If the user is not authorized, the web server **1018** may provide a message indicating that the user is unauthorized to perform the requested action.

[0216] In step **1512**, the web server **1018** determines if the attribute already exists in the network profile. In other words, the web server **1018** determines the type of attribute (e.g., a shared indicator, service identifier, or QUO metric) received from the user and determines if that type of attribute is already present. If the type of attribute is already present then the web server **1018** may update the attribute within the network profile in step **1514**. As discussed previously, if the attribute is quantitative, the web server **1018** may average or perform a weighted algorithm on the different attributes. The result may then be stored within the network profile. In some embodiments, many attributes from the same network device indicator may be averaged or otherwise transformed by one or more algorithms and the results stored within the respective network profile.

[0217] If the attribute is not quantitative, then the existing attribute may be replaced by the new value. For example, the owner of a network may have previously indicated that the network is "shared." The owner may log into the web server **1018**, and request that the network profile for their network be updated to indicate that the network is no longer shared (e.g., replace the shared indicator indicating "shared" with a shared indicator indicating "not shared"). In another example, an administrator may be aware of a chain restaurant that offers free wireless access. The administrator may log onto the web server **1018** and request that all of the network profiles for the chain restaurant be updated to indicate that the networks are "shared."

[0218] If the network profile does not exist in the network database, than the web server **1018** or network database server **1012** creates a new network profile in step **1516**. In some embodiments, the web server **1018** checks to determine if the user is authorized to create a new network profile. The attribute associated with the network device identifier is then stored within the network profile in step **1518**. Similarly, if an existing network profile retrieved did not have the same type of attribute as the one received form the user, the attribute is stored in the retrieved network profile.

[0219] It will be appreciated by those skilled in the art, that although FIG. **15** is discussed with respect to the web server **1018** and the network database server **1012**, the functions described herein may be performed by any server. For example, the functions described in FIG. **15** may be performed by a single server. Alternately, different servers than those described in FIG. **15** may perform the different described functions.

[0220] In various embodiments, the web server **1018** may store personalized settings. In one example, a digital device user creates a user account on web server **1018** and stores the personalized settings. The personalized settings, as described herein, may be used by the rules server **1010** in selecting wireless networks for the user's digital device **1002**. For example, when the user's digital device **1002** provides a list of available wireless networks to the rules server **1010** as well as a user identifier. The rules server **1010** may check with the web server **1018** if there are any personalized settings associated with the user identifier. If personalized settings exist, then the rules server **1010** may apply one, some, or all of the personalized settings to eliminate undesirable wireless networks and/or assist in the wireless network selection process.

[0221] FIG. **16** is a flow diagram of an exemplary process of using a network database in selecting a wireless network. By collecting the attributes into a network database from different users (as discussed in FIGS. **14** and **15**), the rules server **1010** may provide accurate wireless network selections with an increased likelihood of meeting a desired level of performance.

[0222] In step **1602**, the profile server may receive multiple attributes for a first wireless network from multiple users. In on example, many users access the same wireless network (e.g., a wireless network at a busy airport). Each digital device may provide attributes to a server such as the profile server **1014**. The attributes may be collected over a long period or time or nearly simultaneously.

[0223] In step **1604**, the server, such as the profile server **1014** averages the multiple attributes and stores the average within a network profile associated with the first wireless network. In some embodiments, the server retrieves a network profile associated with the first wireless network. The server may then perform an algorithm, including a function that averages attributes of a similar type (e.g., latency metric or bandwidth metric). The result may be stored in the network profile of the first wireless network.

[0224] In step **1606**, the server receives multiple attributes for a second wireless network from multiple users. The second wireless network may be located in the same area as the first wireless network. In step **1608**, the server may average the multiple attributes and store the average within a network profile associated with the second wireless network. Similar to step **1604**, in some embodiments, the server retrieves a network profile associated with the second wireless network. The server may then perform an algorithm, including a function that averages attributes of a similar type and store the result in the network profile of the second wireless network.

[0225] In step **1610**, the server receives a list of available wireless networks including the first and second wireless networks from a digital device **1002**. In one example, the digital device **1002** scans for available wireless networks and receives network device identifiers for the first and second wireless networks. The list of available wireless networks comprising the two network device identifiers may be provided to a server such as the rules server **1010**.

[0226] In step **1612**, the server retrieves a network profile for the first and second wireless networks. For example, the server may retrieve the first and second network profiles based on the two network device indicators within the list of available wireless networks. The first and second network

profiles comprise the results of the multiple attributes received from steps **1602** and **1604**. The first and second network profiles may be retrieved from a network database comprising a plurality of network profiles.

[0227] In step **1614**, the server compares the averaged attribute of the first wireless network to the average attribute of the second wireless network. In taking many attributes of a similar type from many users, the results of the averaging function or algorithm tend to be more accurate and, therefore, may be representative of an expected level of performance of the wireless networks. Similarly as the expectations of performance are more accurate, the comparison of these attributes in the aggregate may also product more accurate results.

[0228] In step **1616**, the server selects an available wireless network based on the comparison. For example, by comparing the averaged attributes of the first wireless network to the average attributes of the second wireless network, the selection of wireless network with the best performance can be made with a higher confidence. As a result, as more users add more attributes to network profiles within the network database, current and increasingly accurate information may be used to help users find and utilize the high quality wireless networks. In step **1618**, the server may provide the network wireless selection to the digital device.

[0229] In various embodiments, the attributes of the different wireless networks may also indicate the usage and/or quality of the wireless networks. The attributes may also indicate the services used. This information may then be analyzed and/or offered to various businesses and services. In one example, a potential business may wish to know the current usage of wireless networks in hotels, airports, and restaurants. Another business may wish to know which services are most popular in certain locations or are most popular with networks associated with a certain kind of business (e.g., convention centers). Similarly, businesses may be interested in eliminating unpopular services or wireless networks that fall below a usage threshold.

[0230] The above-described functions and components can be comprised of instructions that are stored on a storage medium such as a computer readable medium. The instructions can be retrieved and executed by a processor. Some examples of instructions are software, program code, and firmware. Some examples of storage medium are memory devices, tape, disks, integrated circuits, and servers. The instructions are operational when executed by the processor to direct the processor to operate in accord with embodiments of the present invention. Those skilled in the art are familiar with instructions, processor(s), and storage medium.

[0231] The present invention is described above with reference to exemplary embodiments. It will be apparent to those skilled in the art that various modifications may be made and other embodiments can be used without departing from the broader scope of the present invention. Therefore, these and other variations upon the exemplary embodiments are intended to be covered by the present invention.

1. A method comprising:

receiving a network identifier associated with a wireless network;

determining if a network profile associated with the network identifier is stored within a network profile database comprising a plurality of network profiles; and

if the network profile associated with the network identifier is stored within the network profile database, retrieving the network profile;

if the network profile associated with the network identifier is not stored within the network profile database, initiating the network profile, obtaining an attribute associated with the network device identifier, and storing the attribute within the network profile.

2. The method of claim **1**, further comprising:

comparing an attribute from within the network profile to personalized settings;

determining if the wireless network associated with the network identifier meets user requirements base on the comparison; and

providing a credential request response based on the determination.

3. The method of claim **1**, further comprising:

comparing an attribute from within the network profile to minimum requirements;

determining if the wireless network associated with the network identifier meets the minimum requirements base on the comparison; and

providing a credential request response based on the determination.

4. The method of claim **1**, further comprising:

comparing an attribute from within the network profile to another attribute from within another network profile stored within the network database; and

providing a credential request response based on the comparison.

5. The method of claim **1**, further comprising

comparing an attribute from within the network profile to minimum requirements;

determining if the wireless network associated with the network identifier meets the minimum requirements base on the comparison;

comparing an attribute from within the network profile to another attribute from within another network profile stored within the network database; and

selecting the wireless network based, at least in part, on the comparisons.

6. The method of claim **1**, wherein the network identifier is received from a digital device by a server.

7. The method of claim **1**, wherein storing the attribute within the network profile comprises averaging one or more existing attributes with the obtained attribute and storing the result in the network profile.

8. The method of claim **1**, wherein storing the attribute within the network profile comprises performing an algorithm on one or more existing attributes with the obtained attribute and storing the result in the network profile.

9. The method of claim **1**, wherein the network identifier comprises an SSID identifier.

10. The method of claim **1**, wherein the network identifier comprises a BSSID identifier.

11. The method of claim **1**, wherein the attribute comprises a performance metric, a shared indicator, and a service identifier.

12. The method of claim **1**, further comprising updating other network profiles within the network database by updating a shared indicator within each network profile that is associated with an identical attribute.

13. The method of claim **12**, wherein the attribute is an SSID identifier.

14. A system comprising:

a digital device configured to provide a network identifier associated with a wireless network over a communication network;

a server configured to receive the network identifier, determine if a network profile associated with the network identifier is stored within a network profile database comprising a plurality of network profiles, and if the network profile associated with the network identifier is stored within the network profile database, retrieve the network profile, or if the network profile associated with the network identifier is not stored within the network profile database, initiate the network profile, obtain an attribute associated with the network device identifier, and store the attribute within the network profile.

15. The system of claim **14**, wherein the server if further configured to compare an attribute from within the network profile to personalized settings, determine if the wireless network associated with the network identifier meets user requirements base on the comparison; and provide a credential request response based on the determination.

16. The system of claim **14**, wherein the server if further configured to compare an attribute from within the network profile to minimum requirements, determine if the wireless network associated with the network identifier meets the minimum requirements base on the comparison, and provide a credential request response based on the determination.

17. The system of claim **14**, wherein the server if further configured to compare an attribute from within the network profile to another attribute from within another network profile stored within the network database and provide a credential request response based on the comparison.

18. The system of claim **14**, wherein the server if further configured to compare an attribute from within the network profile to minimum requirements, determine if the wireless network associated with the network identifier meets the minimum requirements base on the comparison, compare an attribute from within the network profile to another attribute from within another network profile stored within the network database, and select the wireless network based, at least in part, on the comparisons.

19. The system of claim **14**, wherein the server configured to store the attribute within the network profile comprises the server configured to average one or more existing attributes with the obtained attribute and store the result in the network profile.

20. The system of claim **14**, wherein the server configured to store the attribute within the network profile comprises the server configured to perform an algorithm on one or more existing attributes with the obtained attribute and storing the result in the network profile.

21. The system of claim **14**, wherein the network identifier comprises an SSID

22. The system of claim **14**, wherein the network identifier comprises a BSSID identifier.

23. The system of claim **14**, wherein the attribute comprises a performance metric, a shared indicator, and a service identifier.

24. The system of claim **14**, wherein the server if further configured to update other network profiles within the network database by updating a shared indicator within each network profile that are associated with an identical attribute.

25. The system of claim **24**, wherein the attribute is an SSID identifier.

26. A computer readable storage medium configured to store instructions, the instructions comprising a method, the method comprising the steps of:

receiving a network identifier associated with a wireless network;

determining if a network profile associated with the network identifier is stored within a network profile database comprising a plurality of network profiles; and

if the network profile associated with the network identifier is stored within the network profile database, retrieving the network profile;

if the network profile associated with the network identifier is not stored within the network profile database, initiating the network profile, obtaining an attribute associated with the network device identifier, and storing the attribute within the network profile.

* * * * *