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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 March 2022 (31.03.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/061586 A1

(51) International Patent Classification:
H04W 12/12 (2021.01)

(21) International Application Number:
PCT/CN2020/117152

(22) International Filing Date:
23 September 2020 (23.09.2020)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **ARRIS ENTERPRISES LLC** [US/US]; 3871 Lakefield Drive, Suwanee, Georgia 30024 (US).

(72) Inventor: **LIAO, Zoe**; 8 & 9 Gaoxin South Ninth Ave. Ring Rd, Keji South Road - Building 2, 3F, 4F & 5F, Nanshan District, Shenzhen, Guangdong 518057 (CN).

(74) Agent: **CHINA SINDA INTELLECTUAL PROPERTY LIMITED**; B11th Floor, Focus Place, 19 Financial Street, Xicheng District, Beijing 100033 (CN).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

(54) **Title:** USING AP INFORMATION FOR DETERMINING NETWORK OPERATIONS

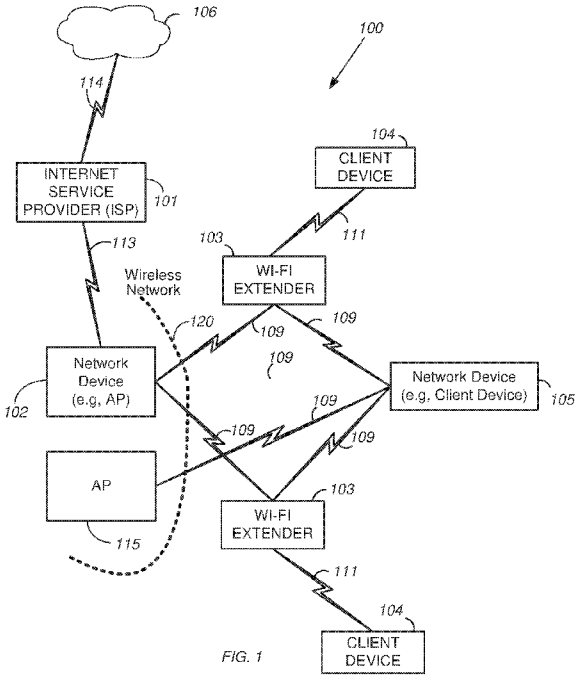


FIG. 1

(57) **Abstract:** A network device for managing a network. The network device analyzes a network to obtain access point (AP) information, determines the AP information meets predetermined criteria, andperforms an operation based on the AP information meeting the predetermined criteria. The network device may be an AP having the same SSID and security mode as the scanned AP. The AP generates a message that is sent to the client device to warn the user to change Wi-Fi configurations, such as using a different SSID, security mode, and password. When the network device is a client device, the client device determines whether a BSSID of an AP is in a blocked AP list or an allowed AP list. The client device may connect with the AP when the BSSID of the AP is in the allowed AP list. The client device may look for another AP when the BSSID is in the blocked list.

[Continued on next page]

WO 2022/061586 A1

TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

USING AP INFORMATION FOR DETERMINING NETWORK OPERATIONS

BACKGROUND

[0001] The subject matter of the present disclosure relates to a network device, such as an access point (AP) or a client device, performing an operation based on AP information of another AP meeting predetermined criteria.

SUMMARY

[0002] Aspects of the present disclosure are drawn to a network device that determines network operations based on access point (AP) information. The network device may be an AP or a client device. A blocked AP list and an allowed AP list are presented to a client device.

[0003] When the network device is an AP, the AP obtains AP information. For example, the AP scans for surrounding APs and obtains the Service Set Identifier (SSID) & security mode of other APs. Next, the AP determines that the first AP information meets predetermined criteria by determining whether a scanned AP has a same SSID and security mode as the scanning AP. The AP then performs an operation based on the AP information of the scanned AP meeting the predetermined criteria. For example, the scanning AP warn the user to change the Wi-Fi configuration of the scanning AP, i.e., use a different SSID, a different security mode, and a different password. The user deletes the Wi-Fi connection configuration of the former SSID saved on the client devices, and use the new configuration to connect to the AP. If an extender is connected to the AP, the BSSIDs of the extender is ignored and removed from the list of scanned APs. Thus, the BSSIDs of the extender do not trigger the warning.

[0004] When the network device is a client device, the client device analyzes a network to obtain first AP information by obtaining a Basic Service Set Identifier (BSSID)of an AP that it may have previously connected with. Next, the client device determines the first AP information meets predetermined criteria by determining whether the AP is in the blocked AP list or in an allowed AP list. When the AP is in the blocked AP list, the client device scans for other APs. When the AP is not in the blocked AP list, the client device continues with consideration of the AP. After Wi-Fi authentication is completed, and before obtaining the IP address, the client device continues to analyze APs that are not in the blocked AP list. When the AP is in the allowed list, the client devices connects with the AP. When the AP is not in the allowed list, a

warning is displayed to the client device to warn the user of the potential danger, and lets the user determine whether to continue. This process is not used with commonly used hotspots.

[0005] Options may be provided for controlling connection with the AP. A "Sure" option may be selected to continue with a previous connection procedure, and to add the BSSID of the AP to the allowed AP list. A "Never" option may be selected to add the BSSID of the first AP to the blocked AP list, and to continue to scan for a third AP. A "Yes for now" option may be selected to continue with the previous connection procedure. A "No for now" option may be selected to ignore the AP for a predetermined time period, and to continue to scan for the other APs.

BRIEF SUMMARY OF THE DRAWINGS

[0006] The accompanying drawings, which are incorporated in and form a part of the specification, illustrate example embodiments and, together with the description, serve to explain the principles of the present disclosure.

[0007] Fig. 1 is a schematic diagram of a system.

[0008] Fig. 2 illustrates broadcasting of SSIDs by APs.

[0009] Fig. 3 is a block diagram of a client device.

[0010] Fig. 4 illustrates a block diagram of a network device.

[0011] Fig. 5 is a flow chart of a method for determining network operations based on access point (AP) information.

[0012] Fig. 6 is a flow chart of a method for determining network operations based on access point (AP) information.

DETAILED DESCRIPTION

[0013] While implementations are described herein by way of example, those skilled in the art will recognize that the implementations are not limited to the examples or figures described. It is understood that the figures and detailed description thereto are not intended to limit implementations to the particular form disclosed but, on the contrary, the intention is to cover modifications, equivalents, and alternatives falling within the spirit and scope as defined by the appended claims. The headings used herein are for organizational purposes and are not meant to be used to limit the scope of the description or the claims. As used throughout this

application, the word "may" is used in a permissive sense (i.e., meaning having the potential to), rather than the mandatory sense (i.e., meaning must). Similarly, the words "include," "including," and "includes" mean "including, but not limited to."

[0014] Wireless networks pose security risks not generally encountered in wired computer networks. For example, unauthorized ("rogue") wireless access points (APs) may be implemented in a network. An unauthorized AP may be used to deny access of a client device to the network, or to attract traffic and obtain sensitive information from users. An unauthorized AP may spoof the SSID, security mode, and password of a legitimate AP. An unauthorized AP may further set parameters such as the power and channel again to spoof those of a legitimate AP in order to minimize the likelihood of being detected.

[0015] The subject matter of the present disclosure determines network operations based on access point (AP) information. The network device may be an AP or a client device. A blocked AP list and an allowed AP list are presented to a client device.

[0016] When the network device is an AP, the AP obtains AP information. For example, the AP scans for surrounding APs and obtains the Service Set Identifier (SSID) & security mode of other APs. Next, the AP determines that the first AP information meets predetermined criteria by determining whether a scanned AP has a same SSID and security mode as the scanning AP. The AP then performs an operation based on the AP information of the scanned AP meeting the predetermined criteria. For example, the scanning AP generates a message that is sent to the client device to warn the user to use a different SSID, a different security mode, and a different password.

[0017] When the network device is a client device, the client device analyzes a network to obtain first AP information by obtaining a Basic Service Set Identifier (BSSID)of an AP that it may have previously connected with. Next, the client device determines the first AP information meets predetermined criteria by determining whether the AP is in the blocked AP list or in an allowed AP list. When the AP is in the blocked AP list, the client device scans for other APs. When the AP is not in the blocked AP list, the client device continues with consideration of the AP. . After Wi-Fi authentication is completed, and before obtaining the IP address, the client device continues to analyze APs that are not in the blocked AP list. When the AP is in the allowed list, the client devices connects with the AP. When the AP is not in the allowed list, a warning is displayed to the client device suggesting that the client device scan for other APs to

connect with. When the AP is not in the allowed list, a warning is displayed to the client device to warn the user of the potential danger, and lets the user determine whether to continue. This process is not used with commonly used hotspots.

[0018] Fig. 1 is a schematic diagram of a system 100.

[0019] As shown in Fig. 1, the system includes a network device 102 connected to the Internet 106 via an Internet Service Provider (ISP) 101. The network device 102 is also connected to different wireless devices such as wireless extenders 103 and client devices 104 and network device 105. Network device 105 may be a client device. Herein, network device 105 will be referred to as client device 105. The system shown in Fig. 1 includes wireless devices (e.g., wireless extenders 103 and client devices 104, 105) that may communicate with network device 102 directly or indirectly via one or more wireless networks 120 (e.g., private, guest, iControl, backhaul network, or Internet of things (IoT) network). Network devices 104, 105 may obtain AP information via beacons or probe responses without being connected to the wireless network 120. Additionally, there could be some overlap between wireless devices (e.g., wireless extenders 103 and client devices 104, 105) in the different networks. That is, one or more network devices could be located in more than one network. For example, the wireless extenders 103 could be located both in a private network for providing content and information to a client device 104, 105 and also included in a backhaul network or an iControl network.

[0020] Starting from the top of Fig. 1, the ISP 101 can be, for example, a streaming video provider or any computer for connecting the network device 102 to the Internet 106. The connection 114 between the Internet 106 and the ISP 101 and the connection 113 between the ISP 101 and the network device 102 can be implemented using a wide area network (WAN), a virtual private network (VPN), metropolitan area networks (MANs), system area networks (SANs), a DOCSIS network, a fiber optics network (e.g., FTTH (fiber to the home) or FTTX (fiber to the x), or hybrid fiber-coaxial (HFC)), a digital subscriber line (DSL), a public switched data network (PSDN), a global Telex network, or a 2G, 3G, 4G or 5G network, for example.

[0021] The connection 113 can further include as some portion thereof a broadband mobile phone network connection, an optical network connection, or other similar connections. For example, the connection 113 can also be implemented using a fixed wireless connection that operates in accordance with, but is not limited to, 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE) or 5G protocols. It is also contemplated by the present disclosure

that connection 113 is capable of providing connections between the network device 102 and a WAN, a LAN, a VPN, MANs, PANs, WLANs, SANs, a DOCSIS network, a fiber optics network (e.g., FTTH, FTTX, or HFC), a PSDN, a global Telex network, or a 2G, 3G, 4G or 5G network, for example.

[0022] The network device 102 can be, for example, a hardware electronic device that may be a combination modem and gateway device that combines the functions of a modem, an access point, and/or a router for providing content received from the content provider (e.g., ISP 101) to network devices (e.g., wireless extenders 103 and client devices 104, 105) in the system. It is also contemplated by the present disclosure that the network device 102 can include the function of, but is not limited to, an Internet Protocol/Quadrature Amplitude Modulator (IP/QAM) set-top box (STB) or smart media device (SMD) that is capable of decoding audio/video content, and playing over-the-top (OTT) or multiple system operator (MSO) provided content.

[0023] The connections 109 between the network device 102, the wireless extenders 103, and client devices 104, 105 can be implemented using a wireless connection in accordance with any IEEE 802.11 Wi-Fi protocols, Bluetooth protocols, Bluetooth Low Energy (BLE), or other short range protocols that operate in accordance with a wireless technology standard for exchanging data over short distances using any licensed or unlicensed band such as the citizens broadband radio service (CBRS) band, 2.4 GHz bands, 5 GHz bands, 6 GHz bands, 60 GHz bands, etc. Additionally, the connections 109 can be implemented using a wireless connection that operates in accordance with, but is not limited to, RF4CE protocol, ZigBee protocol, Z-Wave protocol, or IEEE 802.15.4 protocol. It is also contemplated by the present disclosure that the connections 109 can include connections to a media over coax (MoCA) network. One or more of the connections 109 can also be a wired Ethernet connection.

[0024] The wireless extenders 103 can be, for example, hardware electronic devices such as access points used to extend the wireless network by receiving the signals transmitted by the network device 102 and rebroadcasting the signals to, for example, client devices 104, 105, which may out of range of the network device 102. The wireless extenders 103 can also receive signals from client devices 104, 105 and rebroadcast the signals to the network device 102, or other client devices 104, 105.

[0025] The connections 111 between the wireless extenders 103 and client devices 104, 105 are implemented through a wireless connection that operates in accordance with any IEEE 802.11 Wi-Fi protocols, Bluetooth protocols, Bluetooth Low Energy (BLE), or other short range protocols that operate in accordance with a wireless technology standard for exchanging data over short distances using any licensed or unlicensed band such as the CBRS band, 2.4 GHz bands, 5 GHz bands, 6 GHz bands, 60 GHz bands, etc. Additionally, the connection 111 can be implemented using a wireless connection that operates in accordance with, but is not limited to, RF4CE protocol, ZigBee protocol, Z-Wave protocol, or IEEE 802.15.4 protocol. Also, one or more of the connections 111 can be a wired Ethernet connection.

[0026] Client devices 104, 105 can be, for example, hand-held computing devices, personal computers, electronic tablets, smart phones, smart speakers, IoT devices, iControl devices, portable music players with smart capabilities capable of connecting to the Internet, cellular networks, and interconnecting with other devices via Wi-Fi and Bluetooth, or other wireless hand-held consumer electronic devices capable of executing and displaying content received through the network device 102. Additionally, client devices 104, 105 can be a TV, an IP/QAM STB or an SMD that is capable of decoding audio/video content and playing over OTT or MSO provided content received through the network device 102.

[0027] The connection 109 between the network device 102 and the client device 104, 105 is implemented through a wireless connection that operates in accordance with, but is not limited to, any IEEE 802.11 protocols. Additionally, the connection 109 between the network device 102 and the client device 104, 105 can also be implemented wirelessly through a VPN, WPANs, WLANs, , or a 2G, 3G, 4G or 5G network, for example.

[0028] The connection 109 can also be implemented using a wireless connection in accordance with Bluetooth protocols, Bluetooth Low Energy (BLE), or other short range protocols that operate in accordance with a wireless technology standard for exchanging data over short distances using any licensed or unlicensed band such as the CBRS band, 2.4 GHz bands, 5 GHz bands, 6 GHz bands, 60 GHz bands, etc.. One or more of the connections 10 can also be a wired Ethernet connection.

[0029] A detailed description of the exemplary internal components of the network device 102, the wireless extenders 103, and client devices 104, 105 shown in Fig. 1 will be provided in the discussion of Fig 2. However, in general, it is contemplated by the present

disclosure that the network device 102, the wireless extenders 103, and client devices 104, 105 include electronic components or electronic computing devices operable to receive, transmit, process, store, and/or manage data and information associated with the system, which encompasses any suitable processing device adapted to perform computing tasks consistent with the execution of computer-readable instructions stored in a memory or a computer-readable recording medium.

[0030] Further, any, all, or some of the computing components in the network device 102, the wireless extenders 103, and client devices 104, 105 may be adapted to execute any operating system, including Linux, UNIX, Windows, MacOS, DOS, and ChromOS as well as virtual machines adapted to virtualize execution of a particular operating system, including customized and proprietary operating systems. The network device 102, the wireless extenders 103, and client devices 104, 105 are further equipped with components to facilitate communication with other computing devices over the one or more network connections to local and wide area networks, wireless and wired networks, public and private networks, and any other communication network enabling communication in the system.

[0031] In Fig. 1, connections 109, 111, 113 may provide beacon and probe responses that may be used to provide network information, such as SSID, supported rates, security rates and modes, etc. A spoofing or rogue AP 115 is shown connected to network device 105. The rogue AP 115 may have spoofed the SSID and other information from an AP, such as network device 102 or wireless extenders 103, which allows the client devices 104, 105 to connect to the AP 115 automatically. The subject matter of this disclosure may be implemented by a network device, which may be a network device 102 (e.g., includes an AP, a gateway, a router, a modem, etc.), or a client device, such as client device 105. When such network device 102 is an AP, network device 102 performs a scan for surrounding APs based on, for example, the mechanisms of a Dynamic Channel Selection feature. Thus, network device 102 may scan all radio channels and find other APs within range, such as AP 115. From the scan, the network device 102 obtains AP information of AP 115, such as the Service Set Identifier (SSID) & security mode of AP 115. Next, the network device 102 determines that the AP information of AP 115 meets predetermined criteria by determining whether AP 115 has the same SSID and security mode as network device 102. The network device 102 then performs an operation based on the AP information of the scanned AP meeting the predetermined criteria. For example, the scanning AP generates a

message that is sent to the client device 104, 105 to warn the user to change the Wi-Fi configurations, e.g., SSID, security mode and password, of the scanning AP 102, and the user would delete the Wi-Fi connection configuration of the old SSID of AP 103 that is saved on client devices 104, 105. The user would then configure the client devices 104, 105 with the new Wi-Fi configurations to connect to AP 102.

[0032] When such network device is a client device, such as client device 105, client device 105 analyzes the network 120 to obtain AP information by obtaining a Basic Service Set Identifier (BSSID) of APs that it may have previously connected with, such as AP 102. Next, the client device 105 determines the AP information of AP 115 meets predetermined criteria by determining whether AP 115 is in a blocked AP list or in an allowed AP list. When AP 115 is in the blocked AP list, the client device 105 scans for other APs in network 120.

[0033] When AP 115 is not in the blocked AP list, client device 105 continues with consideration of AP 115. After Wi-Fi authentication is completed, and before obtaining the IP address, the client device 105 continues to analyze APs that are not in the blocked AP list. When AP 115 is in the allowed list, client device 105 connects with AP 115. When AP 115 is not in the allowed list, a warning is displayed to client device 105 to warn the user of the potential danger, and let the user determine the options to use. This process is not used with commonly used hotspots.

[0034] Fig. 2 illustrates broadcasting of SSIDs by APs 200.

[0035] In Fig. 2, authentic network device (AP) 210, client device 240, and spoofing network device (AP) 270 are shown. An AP, such as AP 210 forms a wireless network, and all nodes or client devices, such as client device 240, connect to AP 210.

[0036] An AP, such as APs 210, 270, are identified by a SSID or service set identifier. The SSID also identifies the name of the network, i.e., Alpha 212, 272. SSID's are assigned by a network administrator, such as a home user for AP 210 and unauthorized user for AP 270, and are usually given easy to remember and descriptive names, i.e., den, living room, John's game room, etc. AP 210 has SSID Alpha 212. AP 270 also has SSID Alpha 272 because AP 270 is a spoofing or unauthorized AP that may be trying to obtain private information from client device 240 by convincing client device 240 that AP 270 is authentic AP 240. APs 240, 270 also have a basic service set ID (BSSID) 214, 274, respectively, which are used to identify the particular AP and its clients on a network. The BSSID is usually the MAC address of the AP. The BSSID 214

of AP 210 is 06:23:6c:42:a1:ef. The BSSID 274 of AP 270 is 02:17:6a:81:2f:d0. AP 210 is shown using Wired Equivalent Privacy (WEP) 216. AP 210 is shown using Wired Equivalent Privacy (WEP) 276.

[0037] As shown in Fig. 2, AP 210 sends broadcast message 220 with SSID 212 that is received by client device 240 and broadcast message 222 with SSID 212 that is received by AP 270. AP 270 sends broadcast message 280 with SSID 272 that is received by client device 240 and broadcast message 282 with SSID 272 that is received by AP 210. AP 210 can recognize that its SSID Alpha 212 is the same as the SSID Alpha 274 of AP 270. AP 210 then generates a message that is sent to the client device 240 to warn the user to change the Wi-Fi configurations, e.g., SSID, security mode and password, of the scanning AP 210; and the user would delete the Wi-Fi connection configuration of the old SSID of AP 210 that is saved on client device 240. The user would then configure the client devices 240 with the new Wi-Fi configurations to connect to AP 210. The use of client device 240 can changes the SSID 212, e.g., to Animal, and change the security mode 216 to the more secure Wi-Fi Protected Access (WPA) or WPA2.

[0038] Client device 240, when connecting to the network, may obtain the BSSID 214 of AP 210 and BSSID 274 of AP 270. The BSSIDs 214, 274 may be obtain from the beacon packet or probe response from which the client device 240 received the SSIDs 212, 272. Client device 240 examines a blocked AP list 250. BSSID 274 of AP 270 is in the blocked AP list250, so the client device 240 scans for other APs. BSSID 214 of AP 210 is not in the blocked AP list, so client device 240 continues with consideration of AP 210. Client device 105 analyzes the allowed AP list 252. The client determines that BSSID 214 of AP 210 is in the allowed list. Thus, client device 210 connects with AP 210. If BSSID 214 of AP 210 was not in the allowed list, a warning is displayed to client device 240 to warn the user of the potential danger, and let the user determine what options to execute.

[0039] Fig. 3 is a block diagram of a client device 300.

[0040] In Fig. 3, client device 300 includes a processor 310, a communication interface 314, memory 320, a display 330, LEDs 350, speaker 354, and microphone 358. Memory 320 may include an operating system 324 and a rogue AP detection application 326. Display 330 may include a system user interface (UI) 334 that the user may use to setup network access for the client device 300. The display 330 may also display an email component 338, a mobile component 342, and a text messaging component 346. Display 330 may also present other

applications and user interfaces. The display 330 may present a connection warning 370. Three options for connection warnings 370 are shown in Fig. 3, but those skilled in the art will recognize that fewer or more options may be implemented. The connection warning may include an indication 372 that that the connection with the current AP is different than APs previously connected to by the client device 300. The connection warning 370 may also display a confirmation UI 374 for the user to confirm whether the client device still wants to connect with the current AP with a yes option 376 and a no option 378. A configuration option menu 380 may be displayed to allow the client device to disable the options with a "Yes" option 382 and a "No" option 384. Other choices may also be provided, such as "Yes for Now and "No for Now." LEDS 350 and speaker 354 may be used to communicate warnings. Microphone 358 allows audio input to the client device 300.

[0041] Fig. 4 illustrates a block diagram of a network device 400.

[0042] Network device 400 may be an AP. In Fig. 4, network device 400 includes a processor 410, a communication interface 414, memory 420, a display 430, a network interface controller 450, LEDS 460 and speaker 462 for provide warnings for a client device not to connect to an AP. Display 430 may present a system UI 434, an email component 438, a mobile component 442, and a text messaging component 446. Memory includes operating system 422, a database of network information 424, and a rogue AP detection application 426. Network interface controller 450 includes the SSID 452 and password 454.

[0043] Fig. 5 is a flow chart of a method 500 for determining network operations based on access point (AP) information.

[0044] In Fig. 5, method 500 starts (S502), and the network device analyzes a network to obtain access point (AP) information of a first AP (S510). The network device determines that the obtained AP information meets predetermined criteria (S514). The network device performs an operation based on the AP information meeting the predetermined criteria (S518). The method 500 then ends (650).

[0045] Fig. 6 is a flow chart of a method 600 for determining network operations based on access point (AP) information.

[0046] In Fig. 6, method 600 starts (S602), and a determination is made whether network device is an AP or a client device (S622). When the network device is an AP (S626), the AP scans for surrounding APs and obtains SSID and security mode of a scanned AP (S630). The AP

determines the SSID of scanned AP is the same as the SSID of the scanning AP and security mode of scanned AP is the same as security mode of scanning AP (S634). The operation performed by generating a message that is sent to the client device to warn the user to change the Wi-Fi configurations (e.g., SSID, security mode and password) of the scanning AP, delete the Wi-Fi connection configuration of the old SSID of the AP saved on the client device, and then use the new configurations to connect to the AP (S636). The method then ends (S690).

[0047] When the network device is a client device (640), the client is about to connect to a saved SSID (which may be spoofed by the rogue AP (S642. The client device thus determines whether the BSSID of the AP is in the blocked AP list (S644). When the BSSID of the AP is in the blocked AP list (S648), the client device scans for a different AP (S652). When the BSSID of the AP is not in the blocked AP list (S656), the client device continues with the connection procedure with the AP (S660). The client device then determines whether the BSSID of the AP is in the allowed AP list (S664).

[0048] When the BSSID of the AP is in the allowed AP list (S668), the client device continues with connecting to the AP (S672). When the BSSID of the AP is not in the allowed AP list (S676), the client device generates a warning indicating the client device has never connected to the AP and provides options for controlling connection with the AP (S680). The method then ends (S690).

[0049] The processes discussed in this disclosure may be implemented in hardware, software, or a combination thereof. In the context of software, the described operations represent computer-executable instructions stored on one or more computer-readable storage media that, when executed by one or more hardware processors, perform the recited operations. Generally, computer-executable instructions include routines, programs, objects, components, data structures, and the like that perform particular functions or implement particular abstract data types. Those having ordinary skill in the art will readily recognize that certain steps or operations illustrated in the figures above may be eliminated, combined, or performed in an alternate order. Any steps or operations may be performed serially or in parallel. Furthermore, the order in which the operations are described is not intended to be construed as a limitation.

[0050] Embodiments may be provided as a computer program product including one or more non-transitory computer-readable storage media having stored thereon instructions (in compressed or uncompressed form) that may be used to program a computer (or other electronic

device) to perform processes or methods described herein. The computer-readable storage media may include one or more of an electronic storage medium, a magnetic storage medium, an optical storage medium, a quantum storage medium, or the like. For example, the computer-readable storage media may include, but are not limited to, hard drives, floppy diskettes, optical disks, read-only memories (ROMs), random access memories (RAMs), erasable programmable ROMs (EPROMs), electrically erasable programmable ROMs (EEPROMs), flash memory, magnetic or optical cards, solid-state memory devices, or other types of physical media suitable for storing electronic instructions. Further, embodiments may also be provided as a computer program product including a transitory machine-readable signal (in compressed or uncompressed form). Examples of machine-readable signals, whether modulated using a carrier or unmodulated, include, but are not limited to, signals that a computer system or machine hosting or running a computer program may be configured to access, including signals transferred by one or more networks. For example, a transitory machine-readable signal may comprise transmission of software by the Internet.

[0051] Separate instances of these programs can be executed on or distributed across any number of separate computer systems. Thus, although certain steps have been described as being performed by certain devices, software programs, processes, or entities, this need not be the case. A variety of alternative implementations will be understood by those having ordinary skill in the art.

[0052] Additionally, those having ordinary skill in the art readily recognize that the techniques described above can be utilized in a variety of devices, environments, and situations. Although the subject matter has been described in language specific to structural features or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described. Rather, the specific features and acts are disclosed as exemplary forms of implementing the claims.

CLAIMS

What is claimed is:

1. A network device, comprising:

memory; and

a processor configured to execute instructions stored on said memory to cause the network device to:

analyze a network to obtain first access point (AP) information of a first AP;

determine the first AP information meets predetermined criteria; and

perform an operation based on the first AP information meeting the predetermined criteria.

2. The network device of claim 1, wherein the first AP information comprises a first SSID and a first security mode, and the network device is a second AP having second AP information comprising a second SSID and a second security mode, and wherein the processor is further configured to determine the first AP information meets the predetermined criteria by determining that the first SSID is same as the second SSID, and that the first security mode is same as the second security mode.

3. The network device of claim 2, wherein the processor is further configured to perform the operation by generating a warning to inform a client device to use a third SSID, to use a third security mode, and to change a password to establish a connection with the second AP, wherein the generating the warning further comprises at least one of turning LEDs on and off, generating a tone using a speaker, issuing a warning on a system user interface presented on the network device, sending a warning to a mobile component presenting a user interface on the network device, transmitting a call message to a phone, sending a text message, and transmitting an e-mail.

4. The network device of claim 1, wherein the network device comprises a client device and the memory includes a blocked AP list, wherein the processor is further configured to:

before connecting to a saved SSID automatically, determine the BSSID of the first AP is in the blocked AP list and perform the operation by scanning for a third AP.

5. The network device of claim 1, wherein the network device comprises a client device and the memory includes a blocked AP list and an allowed AP list, wherein the processor is further configured to:

determine the BSSID of the first AP is not in the blocked AP list;

perform the operation by continuing with the connection procedure;

determine the BSSID of the first AP is in the allowed list and continue with connecting to the first AP; and

determine the BSSID of the first AP is not in the allowed list and generate a warning when the BSSID of the first AP is not in the allowed list.

6. The network device of claim 5, wherein the processor presents options for warnings when about to connect with the first AP.

7. The network device of claim 6, wherein the processor is further configured to provide options for controlling connection with the first AP by providing:

a "Sure" option to cause the processor to continue with a previous connection procedure, and to add the BSSID of the first AP to the allowed AP list;

a "Never" option to add the BSSID of the first AP to the blocked AP list, and to continue to scan for a third AP;

a "Yes for now" option to continue with the previous connection procedure; and

a "No for now" option to ignore the first AP for a predetermined time period, and to continue to scan for the third AP.

8. A method for managing a network, comprising:

analyzing, by a network device, a network to obtain first access point (AP) information of a first AP;

determining, by the network device, the first AP information meets predetermined criteria; and

performing, by the network device, an operation based on the first AP information meeting the predetermined criteria.

9. The method of claim 8, wherein the first AP information comprises a first SSID and a first security mode, and the network device is a second AP having second AP information comprising a second SSID and a second security mode, and wherein the determining the first AP information meets the predetermined criteria further comprises determining that the first SSID is same as the second SSID, and that the first security mode is same as the second security mode.

10. The method of claim 9, wherein the performing the operation further comprises generating a warning to inform a client device to use a third SSID, to use a third security mode, and to change a password to establish a connection with the second AP, wherein the generating the warning further comprises at least one of turning LEDs on and off, generating a tone using a speaker, issuing a warning on a system user interface in a browser presented on the network device, sending a warning to a mobile component presenting a user interface on the network device, transmitting a call message to a phone, sending a text message, and transmitting an e-mail.

11. The method of claim 8 further comprising providing a blocked AP list, wherein the analyzing the network to obtain the first AP information further comprises before connecting to a saved SSID automatically, determining a BSSID of the first AP is in the blocked AP list, and performing the operation by scanning for a third AP.

12. The method of claim 8 further comprising providing a blocked AP list and an allowed AP list, determining the BSSID of the first AP is not in a blocked AP list, determining the BSSID of the first AP is in the allowed AP list and continuing with connecting to the first AP, determining the BSSID of the first AP is not in the allowed list and generating a warning when the BSSID of the fist AP is not in the allowed list.

13. The method of claim 12, further comprising presenting options for a warning when about to connect with the first AP.

14. The method of claim 13, wherein the presenting options further comprises providing:

a "Sure" option to cause the network device to continue with a previous connection procedure, and to add the BSSID of the first AP to the allowed AP list;

a "Never" option to add the BSSID of the first AP to a blocked AP list, and to continue to scan for a third AP;

a "Yes for now" option to continue with the previous connection procedure; and

a "No for now" option to ignore the first AP for a predetermined time period, and to continue to scan for the third AP.

15. A non-transitory, computer-readable media having computer-readable instructions stored thereon, the computer-readable instructions being capable of being read by a network device, wherein the computer-readable instructions are capable of instructing the network device to perform a method to manage a network, the method comprising:

analyzing, by the network device, a network to obtain first access point (AP) information of a first AP;

determining, by the network device, the first AP information meets predetermined criteria; and

performing, by the network device, an operation based on the first AP information meeting the predetermined criteria.

16. The non-transitory, computer-readable media of claim 15, wherein the network device is a second AP and the first AP information comprises a first SSID and a first security mode of the second AP, wherein the analyzing the network to obtain the first AP information of a first AP further comprises obtaining a second SSID and a second security mode of the first AP, and wherein the determining the first AP information meets the predetermined criteria comprises determining that the first SSID is same as the second SSID, and determining that the first security mode is same as the second security mode.

17. The non-transitory, computer-readable media of claim 16, wherein the performing the operation further comprises generating a warning to inform a client device to use a third SSID, to use a third security mode, and to change a password to establish a connection with the second AP, wherein the generating the warning further comprises at least one of turning LEDs on and off, generating a tone using a speaker, issuing a warning on a system user interface presented on the network device, sending a warning to a mobile component presenting a user interface on the network device, transmitting a call message to a phone, sending a text message, and transmitting an e-mail.

18. The non-transitory, computer-readable media of claim 15 further comprising providing a blocked AP list, before connect to a saved SSID automatically, determining the BSSID of the first AP is in the blocked AP list and performing the operation by scanning for a third AP.

19. The non-transitory, computer-readable media of claim 15, wherein the network device is a client device, the method further comprising storing a blocked AP list and an allowed AP list, determining the BSSID of the first AP is in the allowed AP list and continuing with connect to the first AP, and determining the BSSID of the first AP is not in the allowed AP list and generating a warning.

20. The non-transitory, computer-readable media of claim 19 further comprising presenting options for generating the warning on the client device for the user to use to determine whether to connect to an AP, wherein the presenting options further comprises providing a "Sure" option to cause the network device to continue with a previous connection procedure and to add the BSSID of the first AP to the allowed AP list, a "Never" option to add the BSSID of the first AP to a blocked AP list and to continue to scan for a third AP, a "Yes for now" option to continue with the previous connection procedure, and a "No for now" option to ignore the first AP for a predetermined time period and to continue to scan for the third AP.

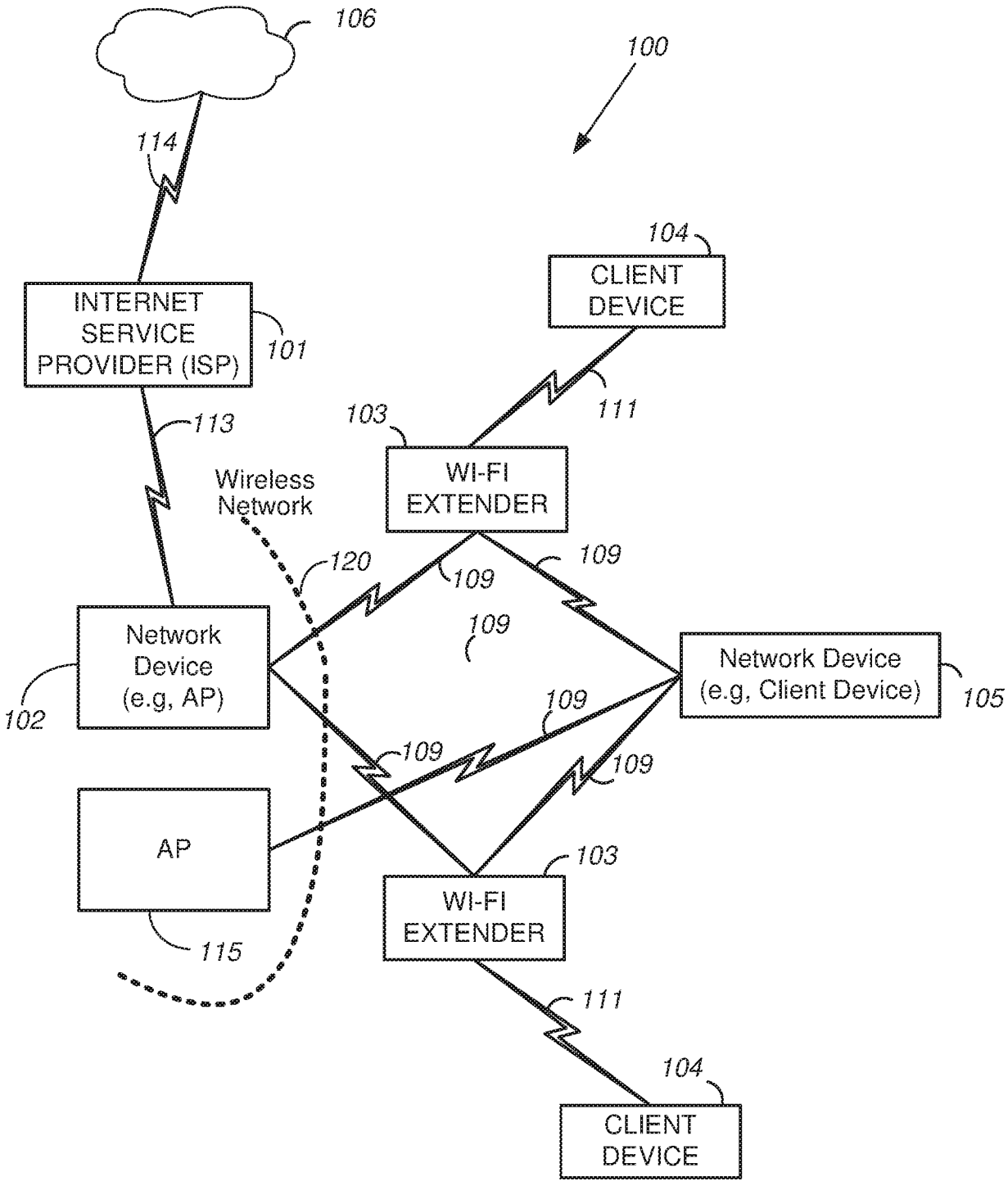

106
100
114
104
CLIENT DEVICE
INTERNET SERVICE PROVIDER (ISP)
101
111
103
113
WI-FI EXTENDER
Wireless Network
120
109
109
109
Network Device (e.g, AP)
Network Device (e.g, Client Device)
105
102
109
109
109
AP
103
WI-FI EXTENDER
115
111
104
CLIENT DEVICE

FIG. 1

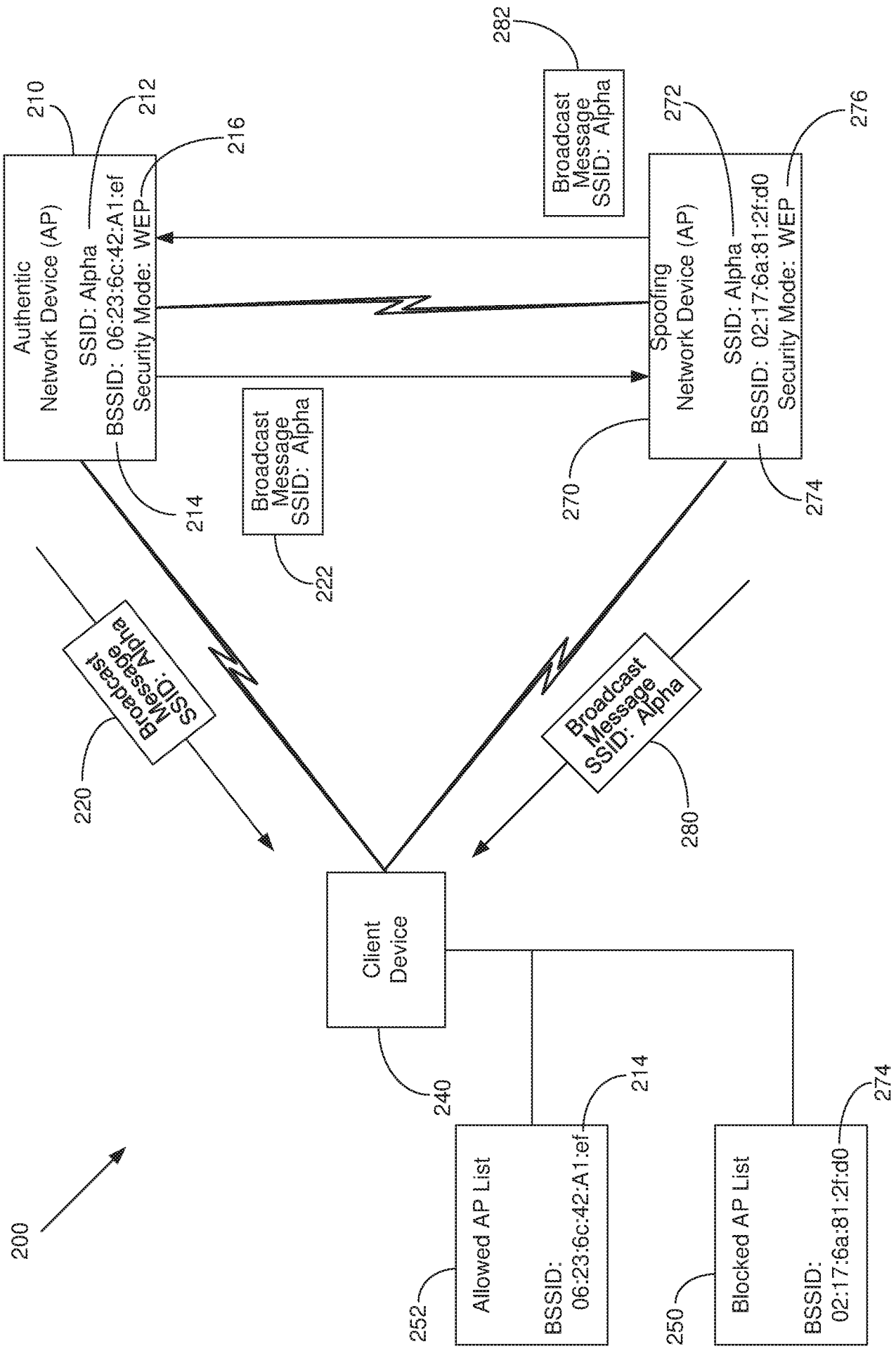

200
Authentic Network Device (AP)
SSID: Alpha
BSSID: 06:23:6c:42:A1:ef
Security Mode: WEP
210
212
216
214
Spoofing Network Device (AP)
SSID: Alpha
BSSID: 02:17:6a:81:2f:d0
Security Mode: WEP
272
276
270
274
282
Broadcast Message SSID: Alpha
Broadcast Message SSID: Alpha
222
Broadcast Message SSID: Alpha
220
Broadcast Message SSID: Alpha
280
Client Device
240
Allowed AP List
BSSID: 06:23:6c:42:A1:ef
252
214
Blocked AP List
BSSID: 02:17:6a:81:2f:d0
250
274

FIG. 2

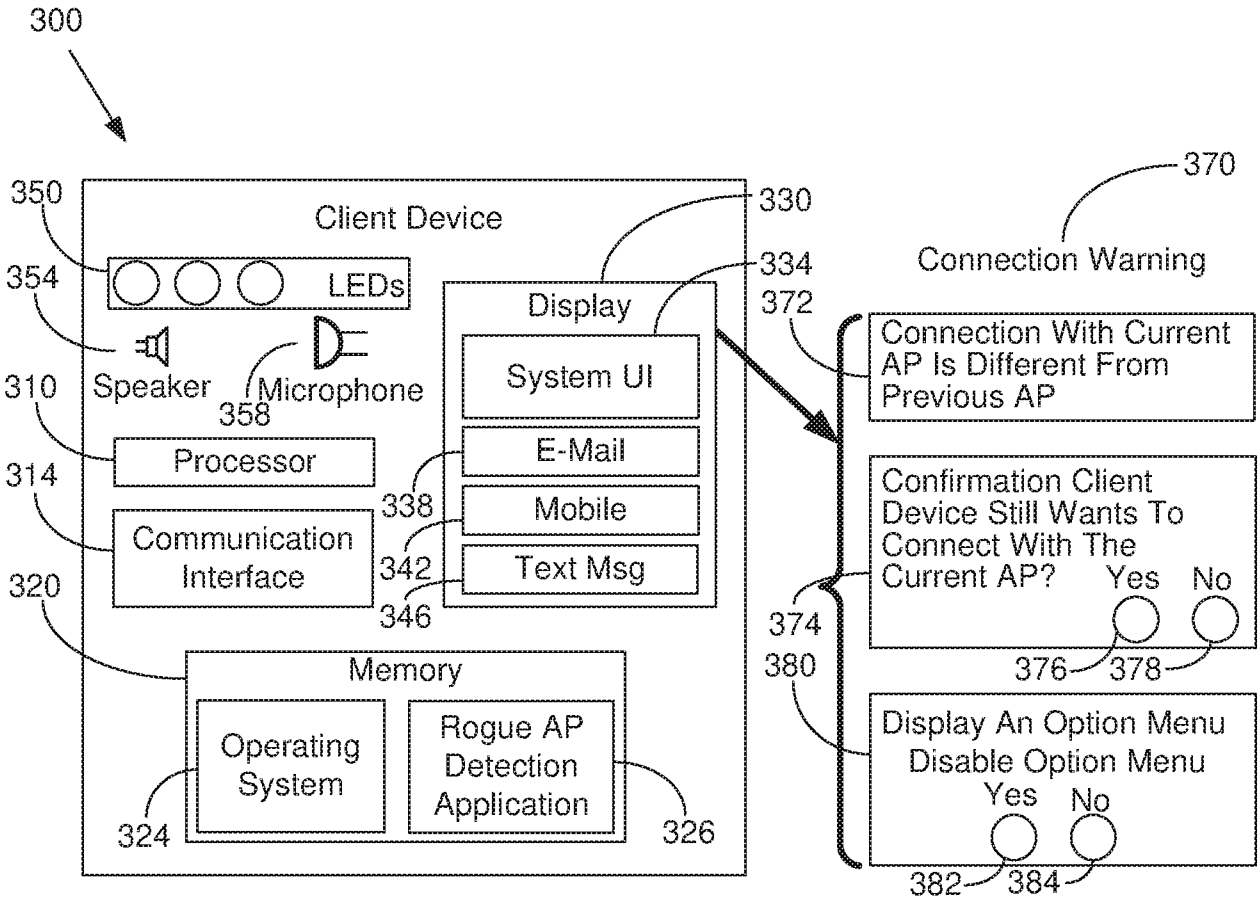

300
350
Client Device
330
370
Connection Warning
354
LEDs
Display
334
372
System UI
Connection With Current AP Is Different From Previous AP
Speaker
Microphone
358
310
Processor
E-Mail
314
338
Mobile
Communication Interface
342
Text Msg
Confirmation Client Device Still Wants To Connect With The Current AP?
Yes
No
320
346
374
380
Memory
Operating System
Rogue AP Detection Application
Display An Option Menu
Disable Option Menu
Yes
No
324
326
376
378
382
384

FIG. 3

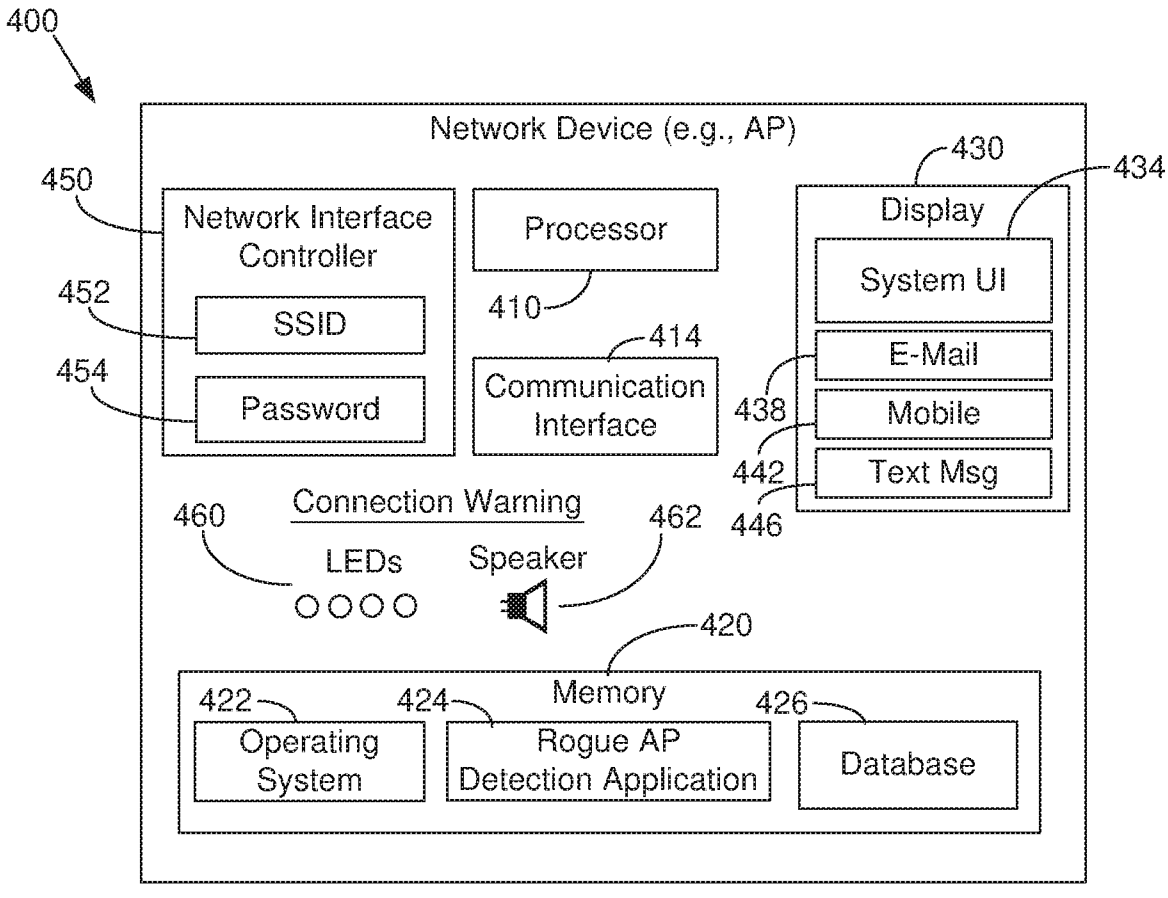

400
Network Device (e.g., AP)
430
434
450
Network Interface Controller
Processor
Display
System UI
452
SSID
410
414
454
Password
Communication Interface
E-Mail
438
Mobile
442
Text Msg
446
460
Connection Warning
462
LEDs
Speaker
420
Memory
422
424
426
Operating System
Rogue AP Detection Application
Database

FIG. 4

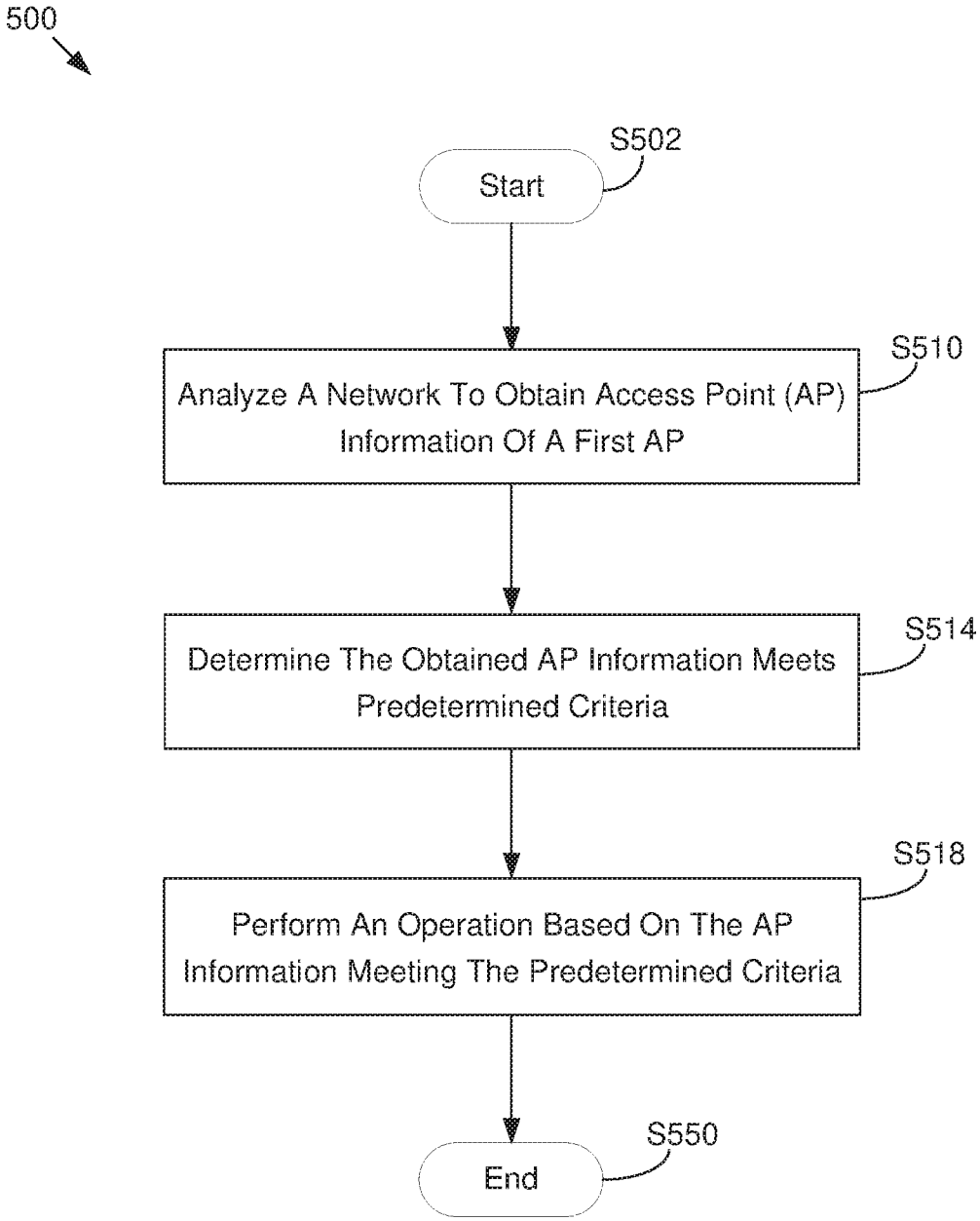

500
S502
Start
S510
Analyze A Network To Obtain Access Point (AP) Information Of A First AP
S514
Determine The Obtained AP Information Meets Predetermined Criteria
S518
Perform An Operation Based On The AP Information Meeting The Predetermined Criteria
S550
End

FIG. 5

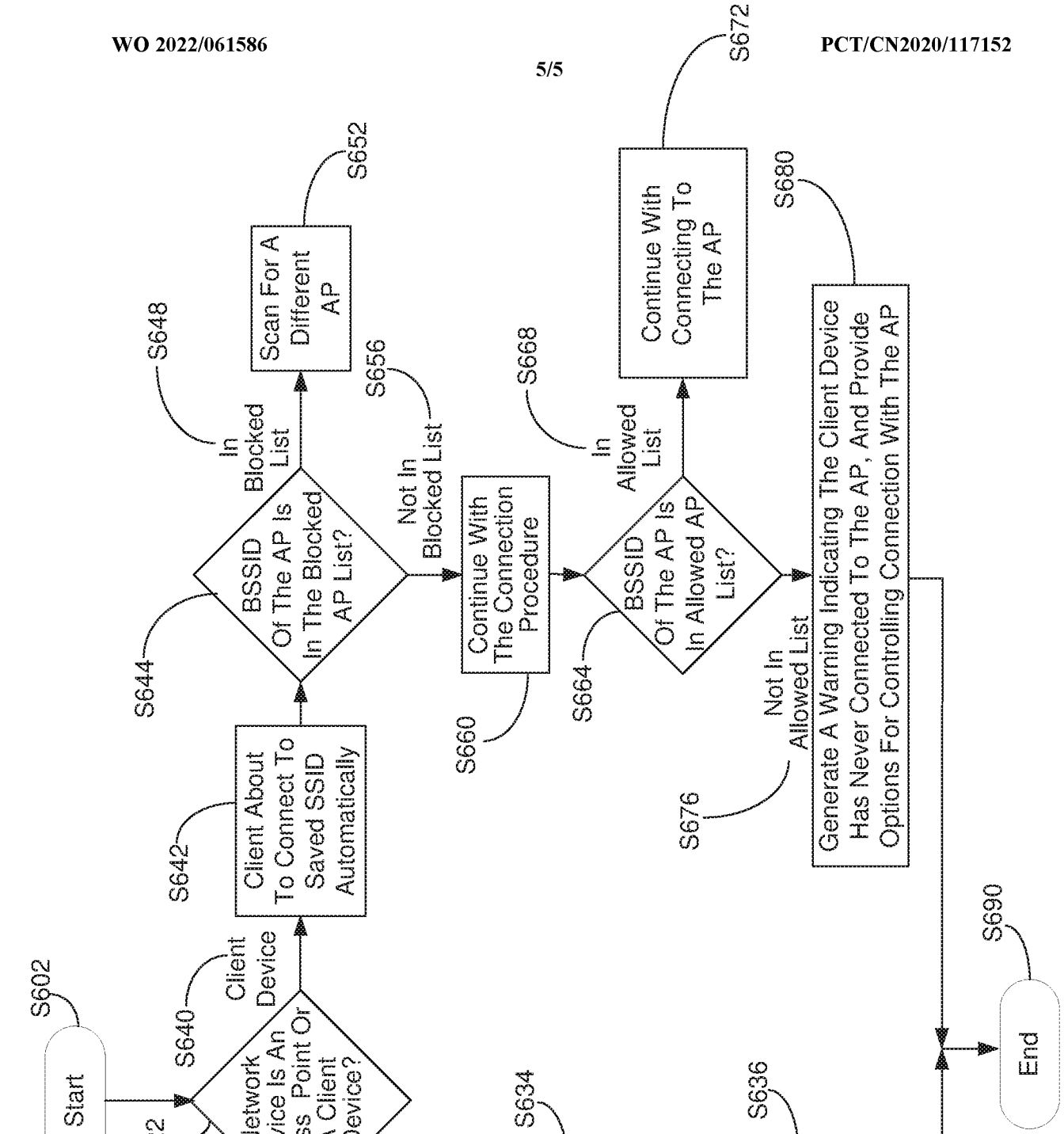

600
Start
S602
Network Device Is An Access Point Or A Client Device?
S622
Client Device
S640
AP
S626
Client About To Connect To Saved SSID Automatically
S642
AP Scans For Surrounding APs And Obtains SSID & Security Mode Of A Scanned AP
S630
BSSID Of The AP Is In The Blocked AP List?
S644
In Blocked List
S648
Not In Blocked List
S656
Scan For A Different AP
S652
Predetermined Criteria Met By SSID Of Scanned AP Being The Same As The SSID Of Scanning AP And Security Mode Of Scanned AP Being The Same As Security Mode Of Scanning AP
S634
Continue With The Connection Procedure
S660
BSSID Of The AP Is In Allowed AP List?
S664
In Allowed List
S668
Not In Allowed List
S676
Continue With Connecting To The AP
S672
Generating A Message That Is Sent To The Client Device To Warn The User To Change The Wi-Fi Configurations, Delete The Wi-Fi Connection Configuration Of The Old SSID Of The AP Saved On The Client Device, And Use The New Configurations To Connect To the AP
S636
Generate A Warning Indicating The Client Device Has Never Connected To The AP, And Provide Options For Controlling Connection With The AP
S680
End
S690

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/117152

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/12(2021.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPTXT;USTXT;VEN;WOTXT;CNABS;CNKI;CNTXT;3GPP:access point, same, rogue, unauthorized, spoofing, unsafe, malicious, scan, detection, BSSID, SSID, AP, blocked, black, white, allowed, list

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2019036951 A1 (SEEDGEN CO LTD) 31 January 2019 (2019-01-31) description paragraphs [0038]-[0100],and figures 1-5	1-20
X	CN 103327484 A (SHENZHEN GONGJIN ELECTRONIC CO) 25 September 2013 (2013-09-25) description paragraphs [0009]-[0022],and figure 1	1-3,8-10,15-17
X	EP 2600648 A1 (BRITISH TELECOMM) 05 June 2013 (2013-06-05) description paragraphs [0015]-[0074], and figures 1-6	1, 8,15
X	CN 106851646 A (BEIJING HONGSHAN RUIDA TECH CO LTD) 13 June 2017 (2017-06-13) description paragraphs [0029]-[0060], and figures 1-2	1-3,8-10,15-17
A	US 2012304297 A1 (CHUNG JAEHOet al.) 29 November 2012 (2012-11-29) the whole document	1-20
A	CN 106792707 A (MAIPU COMM TECHNOLOGY CO LTD) 31 May 2017 (2017-05-31) the whole document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 June 2021	**10 June 2021**
Name and mailing address of the ISA/CN **National Intellectual Property Administration, PRC** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer **BAO,Hongxia** Telephone No. **86-010-62411324**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/117152

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2019036951	A1	31 January 2019	CN	109309657	A	05 February 2019
				KR	20190012775	A	11 February 2019
				KR	101999148	B1	11 July 2019
				US	10609564	B2	31 March 2020
CN	103327484	A	25 September 2013		None		
EP	2600648	A1	05 June 2013	WO	2013079905	A2	06 June 2013
				WO	2013079905	A3	23 October 2014
				US	2014325615	A1	30 October 2014
				EP	2789146	A2	15 October 2014
				US	9603021	B2	21 March 2017
CN	106851646	A	13 June 2017		None		
US	2012304297	A1	29 November 2012	KR	101453521	B1	24 October 2014
				KR	20120129741	A	28 November 2012
				US	8898783	B2	25 November 2014
CN	106792707	A	31 May 2017		None		