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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 June 2016 (02.06.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/085582 A1

(51) International Patent Classification:
H04W 48/12 (2009.01) *H04W 84/12* (2009.01)

(21) International Application Number:
PCT/US2015/055740

(22) International Filing Date:
15 October 2015 (15.10.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/083,377 24 November 2014 (24.11.2014) US

(71) Applicant: **THOMSON LICENSING** [FR/FR]; 1-5 rue Jeanne d'Arc, F-92130 Issy-les-Moulineaux (FR).

(72) Inventor: **CRAWLEY, Casimir Johan**; 13471 Winamac Court, Carmel, Indiana 46032 (US).

(74) Agents: **SHEDD, Robert, D.** et al.; Thomson Licensing LLC, 4 Research Way, 3rd Floor, Princeton, New Jersey 08540-6620 (US).

(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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR WLAN DEVICE PAIRING

(57) Abstract: A method for pairing a wireless device with an access point using a push button on the access point includes receiving a request at an access point to join a wireless network and receiving a push button command to pair the wireless device to the access point. The method then inhibits broadcast of all service set identifiers associated with the access point and determines if the wireless device is permitted to pair with the access point. The access point then broadcasts only a service set identifier associated with the wireless device so that erroneous pairings between the access point and the wireless device are prevented.

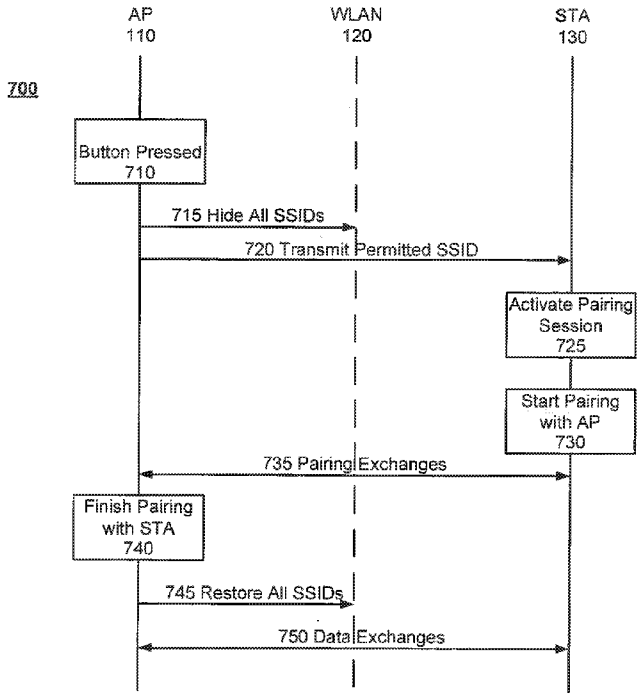

Fig. 4

WO 2016/085582 A1

Published:

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

METHOD AND APPARATUS FOR WLAN DEVICE PAIRING

FIELD

[0001] The present invention relates to the setup and use of wireless networks, specifically the pairing of devices in a WLAN.

BACKGROUND

[0002] Several methods for joining a wireless network already exist. The basic method is the direct sharing of the WiFi™ key. This method has drawbacks: it is complicated and error prone. Moreover it reveals the WiFi™ key. Having those drawbacks in mind, the WiFi™ alliance promoted WiFi™ Protected Setup (WPS) procedures. This is a set of methods that ease the process of entering a WiFi™ network. In one method called the WPS Push Button Configuration (PBC) method, the user presses two buttons, one on the entering (enrollee) device and one on the access point (AP). This method takes time because of a two minute temporization time period. If this temporization is not implemented, the method is known to be vulnerable. Also, an unintended device could join the network if it is in range. It is well known that service set identifiers SSIDs of AP services may be hidden and not transmitted during normal WLAN operation in order to hide such SSIDs from detection and hacking. However, it is a generally accepted practice to transmit all AP SSID information during a WPS PBC procedure. This is performed so that all of the possible SSIDs of an access point are available for a joining or enrolling station STA to access. But, there are risks for the access point network and the remote station in a WPC PBC process. For example, the STA can mistakenly pair with a wrong SSID resulting in the STA not receiving the AP services it desires. An incorrect pairing of an AP and STA could provide connection to an SSID service that is not authorized for the particular STA. An incorrect pairing may simply not allow proper data exchange because of incompatibilities between different AP and STA capabilities. Service failure, interruption of service, and security breaches may result from incorrect pairings. Also, the STA could pair with the wrong AP resulting in a security threat or operation difficulty.

[0003] Solutions to this incorrect pairing problem include transmitting all of the SSIDs during a WPC PBS setup but requiring the STAs to transmit a customer identifier string during the WPS set up so that the AP can recognize and pair only with authorized STAs. This pairing protection scheme PPS insures that unauthorized STBs never connect to AP WLAN

services that are not compatible with the authorization or capabilities of a STA joining the WLAN using the WPS PCB process. However, this solution still does not prohibit STBs that are not customer identifier protected from pairing with lower priority or incorrect APs during the WPC PBC pairing process. The above disadvantages should be overcome and an easier and more secure method is needed to prevent undesired pairing of STAs with APs in a wireless network.

SUMMARY

[0004] This summary is provided to introduce a selection of concepts in a simplified form as a prelude to the more detailed description that is presented later. The summary is not intended to identify key or essential features of the invention, nor is it intended to delineate the scope of the claimed subject matter.

[0005] In one aspect of the invention, a method for pairing a wireless device with an access point using a push button on the access point includes receiving a request at an access point to join a wireless network and receiving a push button command to pair the wireless device to the access point. The access point inhibits the broadcast of all service set identifiers associated with the access point. The access point determines if the wireless device is permitted to pair with the access point. In one embodiment, a media access control address of the wireless device is compared with a list a permitted wireless devices for the determination. If the wireless device is permitted to pair with the access point, a service set identifier associated with the wireless device is broadcast to the wireless device. Pairing of the access with the wireless device is performed. Erroneous pairings are avoided because the only visible service set identifier for the wireless station is the service set identifier that is permitted for the wireless device. After pairing, the wireless device can access the resources of the access point.

[0006] In another aspect of the invention, a method for pairing a wireless device with an access point in a wireless network using a personal computer in communications with the access point includes receiving a selection of a service set identifier from the personal computer. The access point inhibits broadcast of all service set identifiers except for the service set identifier selected for the wireless device by the personal computer. The personal computer provides a logical push button configuration activation and pairing of the access point with the wireless device is accomplished. After pairing, the access point restores the broadcast of all of the service set identifiers. The newly added wireless device can then exchange information between the access point and the wireless device across the wireless network.

[0007] Additional features and advantages of the invention will be made apparent from the following detailed description of illustrative embodiments which proceeds with reference to the accompanying figures. It should be understood that the drawings are for purposes of illustrating the concepts of the disclosure and is not necessarily the only possible configuration for illustrating the disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The foregoing summary of the invention, as well as the following detailed description of illustrative embodiments, is better understood when read in conjunction with the accompanying drawings, which are included by way of example, and not by way of limitation with regard to the claimed invention. In the drawings, like numbers represent similar elements.

[0009] Figure 1 illustrates an example environment in which the current invention may be practiced;

Figure 2 depicts an example signal exchange diagram between an access point and a station according to a first method of the invention;

Figure 3 depicts an example signal exchange diagram between an access point, a personal computer, and a station according to a second method of the invention;

Figure 4 depicts an example signal exchange diagram between an access point and a station according to a third method of the invention;

Figure 5 depicts steps of a first example method according to aspects of the invention;

Figure 6 depicts steps of a second example method according to aspects of the invention;

Figure 7 depicts steps of a third example method according to aspects of the invention; and

Figure 8 illustrates an example access point according to aspects of the invention.

DETAILED DISCUSSION OF THE EMBODIMENTS

[0010] In the following description of various illustrative embodiments, reference is made to the accompanying drawings, which form a part thereof, and in which is shown, by way of illustration, how various embodiments in the invention may be practiced. It is to be

understood that other embodiments may be utilized and structural and functional modification may be made without departing from the scope of the present invention.

[0011] Figure 1 illustrates a system 100 which serves as an example environment for the present invention. An access point (AP) 110 has the capability to control a WLAN 120. The AP can be a router, a gateway, or combination router gateway that can manage the WLAN 120 and provide access to services such as network 160 access. Network 160 can represent available AP resources such as internet access, storage access, LAN access, and the like. Stations 130 and 140 are example remote terminals or stations (STA) that can wirelessly connect to the AP 110 via WLAN 120 to gain access to AP system resources such as network 160. The AP 110 has a physical push button 150 that allows for WiFi™ Protected setup (WPS) Push Button Configuration (PBC) functionality.

[0012] In one embodiment, a personal computer 170 may be connected to the AP, either via RF link or via hardline to provide a user with access and management control of the AP. The configuration of the AP may be setup or modified via the PC 170. Using the PC, WLAN network configurations, such as security and access settings, may be adjusted by a user or system administrator.

[0013] Figure 2 depicts a signaling or activity diagram 200 between the AP 110 and an example remote station, such as the STA 130. Communications between the STA 130 and the AP 110 occur through the wireless local area network WLAN 120. Initially, a pairing session is initiated at activity 205. Here, the STA 130 initiates transmission of a media access control (MAC) address to the AP 110 using signal 210. However, the AP 110 does not respond until the PBC button 150 of Figure 1 is depressed by a system user as in activity 220. After activity 220, the AP 110 hides all SSIDs by turning off the transmission of identifying indicia of the SSIDs related to the AP 110. During this time, remote stations, such as STA 140, which may already be linked to the AP, continue to operate without public identification of SSID names. At activity 230, the AP examines the MAC address of STA 130 to determine of the STA 130 has permission to gain access to the AP 110. It does this by comparing the incoming MAC address with a list of authorized MAC addresses.

[0014] Assuming that the MAC address of STA 130 is acceptable via comparison of the list, then the SSID of the authorized service for the specific MAC address is transmitted. At this point, only the SSID of the authorized service for the MAC address of STA 130 is transmitted via signal 240. The STA 130 is then able to initiate the pairing process at activity 245 by selecting the available SSID that is compatible with the AP 110. The selection of a compatible and authorized SSID is based on the MAC address of the STA and the selection is

limited to only the SSID that was made visible by the AP. The transmission of SSID is enabled via the association of the MAC address of the STA 130 on the list of service associated with that specific MAC address. This selective transmission avoids the STA 130 selecting a wrong or unsuitable SSID.

[0015] In the pairing process started by activity 245, pairing exchanges 250 are performed. Such pairing exchanges may include the exchange of public and private encryption keys, such as "Diffie–Hellman–Merkle" key exchanges. As a result of the pairing key exchanges 250 the AP 110 is able to finish the pairing to the STA 130 at activity 255. After the pairing is established, the pairing process is considered complete and all previous transmissions of SSIDs from the AP 110 are restored at signaling 260. Data exchanges between the AP 110 and the newly paired STA 130 may now take place as example data exchanges 265. Note that the WPS PBC method of Figure 2 only involves the interaction of two active machines: the AP 110 and the STA 130 across the WLAN 120. In the Figure 2 signaling diagram, a physical push button 150 is used. However, a logical push button signaling is also possible according to aspects of the invention.

[0016] Figure 3 depicts a signaling or activity diagram 300 between a personal computer 170 (PC), an AP 110, and a STA 130. This signaling scheme involves a logical PBC method instead of a physical PBC method. In Figure 3, the PC 170 is used to select an SSID for a WLAN accessible service for STA 130 that is available via AP 110. The selection of SSID for the STA 130, which has no communicative connection to the WLAN 120, is performed at activity 305. As a result, signal 310 is sent which includes the SSID selection. The signaling 310 is sent from the PC 170 to the AP 110.

[0017] After receipt of the SSID selection of 310, the AP acts with signal 320 to hide all SSIDs except for the selected SSID. Hiding all SSIDs except the selected SSID for STA 130 permits STA 130 to easily select the correct SSID at activity 325. The STA 130 at 325 initiates the pairing activity by selecting the transmitted SSID without having to make a selection from a multitude of SSIDs. Hiding all SSIDs except for the selected SSID for STA 130 guarantees that STA 130 does not connect to an incorrect SSID. In prior systems, STA 130 would have to select which SSID it wanted to pair with because all SSIDs may be transmitted in the WPS PBC process. This can lead to the STA 130 pairing with an incorrect SSID or a STA 310 PBC overlap pairing failure. However, the improved technique represented in Figure 3 ensures that the STA 130 pairs with only the selected and authorized SSID.

[0018] The PC 170 sends a logical push button activation signal to the AP 110 via signal 330. Signal 330 is detected by the AP 110 as a logical button press at activity 335. This activity also initiates pairing signal exchanges 340. Such pairing exchanges may include the exchange of public and private encryption keys, such as "Diffie–Hellman–Merkle" key exchanges. As a result of the pairing key exchanges 340 the AP 110 is able to finish the pairing to the STA 130 at activity 345. After the pairing is established, the pairing process is considered complete and SSID transmissions from the AP 110 are restored at signaling 350. Data exchanges between the AP 110 and the paired STA 130 may now take place as example data exchanges 355.

[0019] Figure 4 depicts a signaling or activity diagram 700 between the AP 110 and an example remote station, such as the STA 130. Communications between the STA 130 and the AP 110 occur through the wireless local area network WLAN 120. At step 710, a physical button on the AP110 is pressed. In one embodiment, the physical button is pressed a number of times, such as three times, to indicate that a specific SSID is to be chosen. In an alternate embodiment, a special physical button is pressed to indicate a specific SSID selection. In either event, the AP 110 interprets the button pressing as the selection of a pre-selected SSID for pairing with STA 130. After the button press activity 710, the AP 110 hides all SSIDs by turning off the transmission of identifying indicia of the SSIDs related to the AP 110. During this time, remote stations, such as STA 140, which may already be linked to the AP, continue to operate without public identification of SSID names.

[0020] At this point, when the SSID names are hidden, only the specific SSID for pairing with STA 130 is transmitted via signal 720. The STA 130 is then able to initiate the pairing process at activity 725 by selecting the only available SSID whose identity is transmitted by the AP 110. The selection of a compatible and authorized SSID is limited to only the SSID that was made visible by the AP. This selective transmission avoids the STA 130 selecting a wrong or unsuitable SSID.

[0021] At step 730, the STA 130 initiates pairing with the AP 110. In the pairing process started by activity 730, pairing exchanges 735 are performed. Such pairing exchanges may include the exchange of public and private encryption keys, such as "Diffie–Hellman–Merkle" key exchanges. As a result of the pairing key exchanges 735 the AP 110 is able to finish the pairing to the STA 130 at activity 740. After the pairing is established, the pairing process is considered complete and all previous transmissions of SSIDs from the AP 110 are restored at signaling 745. Data exchanges between the AP 110 and the newly paired STA 130 may now take place as example data exchanges 750.

[0022] Figure 5 is an example method 400 that uses an improved WPS PBC physical pushbutton according to aspects of the invention. Figure 5 is an example method that utilizes the example signal flow of Figure 2. The method 400 includes a wireless device, such as STA 130, and an access point, such as AP 110. At step 401, the STA 130 activates a pairing request. This request is accomplished via use of a user interface on the STA 130 requesting access to the WLAN 120 via the AP 100. As part of the request, an identity indication of the STA 130 is provided to the AP 110. In one embodiment, the identity indication is a MAC address. This MAC address may be part of a beacon message where the wireless station, seeking to operate on an IEEE 802.11 WLAN, starts transmitting beacon messages to the AP.

[0023] As a result of the request at 401, the AP 110 receives the pairing request and MAC address of the STA 130 at step 405. At step 410, the AP 110 receives a push button configuration control command via an activation of the push button on the AP 110, such as push button 150 of Figure 1. The activation of the push button provides a push button command to the AP 110 to pair the wireless device, such as STA 130, to the AP. Receiving a push button command at the AP includes receiving an indication at the access point that the pairing button, such as button 150 of Figure 1, has been activated.

[0024] At step 415 the AP acts to inhibit broadcasting of all SSIDs associated with the AP. This inhibition or ceasing of transmission of all SSIDs from the AP provides an indication that the present improved WiFi™ or wireless protected setup (WPS) has commenced. In contrast to a conventional WPS method where all SSIDs may be transmitted, method 400 hides all SSIDs by ceasing the broadcasting of all SSIDs associated with the AP. At step 420 the AP determines if the wireless device, such as a STA is permitted to pair with the AP. This step includes comparing an identifier indicator, such as a MAC address, of the wireless device with a listing of SSIDs and wireless device indicators. Pairing of the wireless device is permitted if the wireless device indicator corresponds to an approved device for AP access on the listing of SSIDs and wireless device indicators.

[0025] If the MAC address of the wireless device is not approved to operate on the SSID of the AP, then step 435 is performed. Step 435 is a step which can indicate, via screen display, LED illumination, printing or logging that pairing of the wireless device with the AP has failed. Then, step 445 is undertaken which restores all of the normally transmitted SSID broadcasts. Returning to step 420, if the AP does permit the MAC address of the wireless device on the SSID, then step 425 is performed. Step 425 broadcasts only the SSID that is associated with the wireless device that seeks access to the AP. This step ensures that the wireless device only sees a compatible and authorized SSID available for pairing. Thus, the

wireless station is prevented from erroneously pairing with a SSID that is not compatible or authorized for pair with the wireless station. Stated another way, the broadcasting of only the selected SSID ensures that the wireless device pairs with only a correct service set identifier.

[0026] At step 430 the AP and wireless device attempt a pairing using the SSID that is broadcast to the wireless station. The pairing process includes exchanging security keys between the AP and the wireless device. In one embodiment, pairing signal exchanges include public and private encryption key exchanges, such as "Diffie–Hellman–Merkle" key exchanges. If the pairing fails, step 435 and 445 are performed. If the pairing succeeds, then step 440 may be performed in which the AP provides an indication, such as display on a screen or an LED, print, or data logging, of the pairing success. Then, step 445 is performed to restore all of the previously broadcast SSIDs associated with the AP. The wireless device and the AP then can exchange data as would be normal for a paired AP and wireless device communicating over a WLAN.

[0027] Figure 6 is an example method 500 that uses an improved WPS PBC logical pushbutton according to aspects of the invention. Figure 6 is an example method that utilizes the example signal diagram of Figure 3. The method 500 includes a terminal, such as personal computer 170, a wireless device, such as STA 130, and an access point, such as AP 110. The PC 170 may have a wired connection to the AP, such as shown in Figure 1, or may be connected via an RF interface, such as via WLAN 120 using a protocol such as IEEE 802.11. At step 505, the PC is provided a selection of an SSID for the wireless station, such as STA 130, so that the wireless station can operate on the WLAN of the AP. A user of the PC can provide the selection of SSID. Thus a request for the addition of the wireless station to an SSID is provided to the AP by the PC. At step 515, the AP hides all SSIDs except for the requested SSID selection made by the PC. Hiding all SSIDs from the pairing wireless device, STA 130, prevents pairing of the wireless device to a service set identifier that is not associated with the wireless device. Stated another way, the broadcasting of only the selected SSID ensures that the wireless device pairs with only a correct service set identifier.

[0028] At step 520, the wireless station activates a pairing request. This pairing request activation can be accomplished using a user interface on the wireless device so that pairing of the wireless device to the AP is initiated. At step 525, the AP receives a logical push button configuration activation signal (logical push button press) from the PC. Receiving a logical push button configuration activation from the PC includes receiving a signal indication from the PC that a logical push button activation is initiated. The AP detects this logical activation signal.

[0029] As a result, at step 530, the AP attempts pairing with the wireless device. Pairing includes exchanging security keys between the AP and the wireless device. In one embodiment, pairing signal exchanges include public and private encryption key exchanges, such as "Diffie–Hellman–Merkle" key exchanges. Also at step 530 the AP can activate wireless pairing session indicators if available. These indicators can be a display, such as a screen display or a LED illumination, a printing, or a logging of pairing activity. At step 535, the AP assesses if the pairing has succeeded. If the pairing did not succeed, then step 545 can indicate a pairing process failure. Such a failure indication can include a display on a screen or an LED, print, or data logging, of the pairing failure. The AP can then restore the broadcasting of all SSIDs via step 550. If the pairing assessment of step 530 is positive, then the AP may indicate, if available an indication of pairing success. Such an indication can include a display on a screen or an LED, print, or data logging, of the pairing success. Once the status of the pairing is known, then the AP performs step 550 by restoring the broadcasting of all active SSIDs of the AP. This signifies the end of the pairing process and the continuation of normal exchanges of data and other information between the access point and the wireless device across the wireless network.

[0030] Figure 7 is an example method 800 that uses an improved physical pushbutton configuration method according to aspects of the invention. Figure 7 is an example method that utilizes the example signal flow of Figure 4. The method 800 includes a wireless device, such as STA 130, and an access point, such as AP 110. In one embodiment, at step 805, successive presses or activations of a physical pairing button on the AP 110 are made in a given time interval. An example time interval is 10 seconds. However other time intervals can also be used such as 5, 15, or 20 seconds. In an alternative embodiment, a special, dedicated push button on the AP 110 may be pressed. Whether the button activations are multiple or are of a single special pushbutton, other than a WPS PBC button for example, the AP 110 is alerted to the fact that a specific SSID is to be used for pairing. This specific SSID may be preselected within the AP 110 so that a specific wireless station, such as STA 130, can be paired with only the AP selected SSID.

[0031] At step 810 the AP acts to inhibit broadcasting of all SSIDs associated with the AP. This inhibition or ceasing of transmission of all SSIDs from the AP 110. In contrast to a conventional WPS PBC method where all SSIDs may be transmitted, method 800 hides all SSIDs by ceasing the broadcasting of all SSIDs associated with the AP. Step 815 broadcasts only the SSID that is associated with the wireless device that seeks access to the AP. This step ensures that the wireless device only sees a compatible and authorized SSID available for

pairing. Thus, the wireless station is prevented from erroneously pairing with a SSID that is not compatible or authorized for pair with the wireless station. Stated another way, the broadcasting of only the selected SSID ensures that the wireless device pairs with only a correct service set identifier.

[0032] At step 820 the AP and wireless device attempt a pairing using the SSID that is broadcast to the wireless station. The pairing process includes exchanging security keys between the AP and the wireless device. In one embodiment, pairing signal exchanges include public and private encryption key exchanges, such as "Diffie–Hellman–Merkle" key exchanges. If the pairing fails, step 825 and 835 are performed. If the pairing succeeds, then step 830 may be performed in which the AP provides an indication, such as display on a screen or an LED, print, or data logging, of the pairing success. Then, step 835 is performed to restore all of the previously broadcast SSIDs associated with the AP. The wireless device and the AP then can exchange data as would be normal for a paired AP and wireless device communicating over a WLAN.

[0033] Figure 8 is an example embodiment of an AP, such as that shown in Figure 1, item 110. Here, a connection to a core network 160 is via the network transmitter/receiver interface 602. The core network 160 connection referred to here may include a connection to the internet or other resources which may include servers, remote or cloud memory, or other possible network services. The core network interface 602 connects to the bus interface 604 which allows access to the internal bus 624. Other non-bus implementations are also possible as is well known to those of skill in the art. Present on bus 624 are a storage device 606 which can be used for any general storage such as retrieved or requested data and network management data, parameters, and programs. Such network management and other programs are under the control of controller/processor 608.

[0034] This controller/processor 608 may be a single processor or a multiplicity of processors performing the tasks of network management, user interface control, and resource managements. Control memory 610 can supply program instruction and configuration control for controller/processor 608. The user interface 618 allows a user, network owner, or network manager to see a status of the AP 110. Such indicators may include a display, LEDs, printer interface, or data logging interface. An input/output (I/O) interface 616 allows the AP 110 to connect to a personal computer or other device that can be used to configure and control the AP. The I/O interface 616 may be a hardline interface, such as an Ethernet interface or may operationally be substituted with an RF interface so that the AP 110 can communicate with a PC via a protocol driven interface, such as IEEE 802.XX. Alternately, a remote terminal, such

as PC 160 may also be connected to a WLAN operated by the AP. Other interfaces that are possible via I/O interface 616 are an interactive interface which may include the use of a display device, keyboard, mouse, light pen, and the like.

[0035] AP 110 has a wireless network interface 612 which allows access to and from regular users to the resources of the core network 160. Such an interface includes all elements to control a wireless network, including the use of wireless network protocols such as IEEE 802.XX and the like. The controller/processor 608 of the AP 110 of Figure 6 is configured to provide processing services for the steps of the methods of Figures 4 and 5. For example, the controller processor can provide instruction control to monitor and control the interfaces of the network transmitter/receiver 602, the I/O interfaces 616 and 618, and the WLAN interface 612. Controller/processor 608 directs the flow of information through AP 110 such that the AP activities of signal Figures 2 and 3 are performed as well as the method of Figures 4 and 5.

[0036] The implementations described herein may be implemented in, for example, a method or process, an apparatus, or a combination of hardware and software. Even if only discussed in the context of a single form of implementation (for example, discussed only as a method), the implementation of features discussed may also be implemented in other forms. For example, implementation can be accomplished via a hardware apparatus, hardware and software apparatus. An apparatus may be implemented in, for example, appropriate hardware, software, and firmware. The methods may be implemented in, for example, an apparatus such as, for example, a processor, which refers to any processing device, including, for example, a computer, a microprocessor, an integrated circuit, or a programmable logic device.

[0037] Additionally, the methods may be implemented by instructions being performed by a processor, and such instructions may be stored on a processor or computer-readable media such as, for example, an integrated circuit, a software carrier or other storage device such as, for example, a hard disk, a compact diskette ("CD" or "DVD"), a random access memory ("RAM"), a read-only memory ("ROM") or any other magnetic, optical, or solid state media. The instructions may form an application program tangibly embodied on a computer-readable medium such as any of the media listed above or known to those of skill in the art. The instructions thus stored are useful to execute elements of hardware and software to perform the steps of the method described herein.

Claims:

1. A method for pairing a wireless device with an access point using a push button on the access point, the method comprising:

receiving a request at an access point to join a wireless network;

receiving a push button command to pair the wireless device to the access point;

inhibiting broadcast of all service set identifiers associated with the access point;

determining if the wireless device is permitted to pair with the access point;

broadcasting a service set identifier associated with the wireless device;

pairing the access point with the wireless device;

exchange information between the access point and the wireless device across the wireless network.

2. The method of claim 1, wherein the step of receiving a request comprises the access point receiving an identity indication of the wireless device.

3. The method of claim 2, wherein the identity indication is a medium access control address as part of a beacon message.

4. The method of claim 1, wherein receiving a push button command comprises receiving an indication at the access point that a pairing button has been activated.

5. The method of claim 1, wherein inhibiting broadcast of all service set identifiers further comprises providing an indication that a wireless protected setup has commenced.

6. The method of claim 1, wherein determining if the wireless device is permitted to pair with the access point further comprises:

comparing an identifier indicator of the wireless device with a listing of service set identifiers and wireless device indicators, wherein pairing of the wireless device is permitted if the wireless device indicator is on the listing.

7. The method of claim 1, broadcasting a service set identifier associated with the wireless device comprises broadcasting only a service set identifier that is associated with the wireless device.

8. The method of claim 1, wherein pairing the access point with the wireless device comprises exchanging security keys.

9. The method of claim 1, further comprising indicating, on the access point, a condition of successful pairing.

10. An access point that pairs with a wireless device, the access point comprising:

a wireless interface for receiving a request to join a wireless network;

a processor, connected to memory, that functions to control the wireless interface for pairing with the wireless device;

a pushbutton interface for detecting commencement of a pairing action, wherein when depressed, causes the processor inhibit broadcast of all service set identifiers associated with the access point;

wherein after the processor determines that the wireless device is associated with a service set identifier, the processor causing the wireless interface to broadcast only the service set identifier associated with the wireless device, the processor further acting to pair the access point with the wireless device using the service set identifier.

11. The access point of claim 10, wherein the processor broadcasting only the service set identifier associated with the wireless device ensures that the wireless device pairs with only a correct service set identifier.

12. A method for pairing a wireless device with an access point in a wireless network using a personal computer in communications with the access point, the method comprising:

receiving a selection of a service set identifier from the personal computer;

inhibiting broadcast of all service set identifiers except the received service set identifier;

receiving a logical push button configuration activation from the personal computer;

pairing the access point with the wireless device;

restoring broadcast of all of the service set identifiers; and

exchanging information between the access point and the wireless device across the wireless network.

13. The method of claim 12, wherein inhibiting broadcast of all service set identifiers except the received service set identifier acts to ensure that the wireless device pairs only with the selected service set identifier.

14. The method of claim 12, wherein inhibiting broadcast of all service set identifiers except the received service set identifier prevents pairing of the wireless device to a service set identifier that is not associated with the wireless device.

15. The method of claim 12, wherein receiving a logical push button configuration activation from the personal computer initiates pairing the access point with the wireless device.

16. The method of claim 12, wherein pairing the access point with the wireless device comprises exchanging security key information.

17. An access point that pairs with a wireless device using a personal computer in communications with the access point, the access point comprising:

a wireless interface for receiving a request to join a wireless network;

an input and output interface that couples the personal computer to the access point, the input and output interface receiving a selection of a service set identifier from the personal computer;

a processor, connected to memory, that functions to control the wireless interface for pairing with the wireless device, the processor controlling the wireless interface to inhibit broadcast of all service set identifiers except for the received service set identifier from the personal computer;

wherein the access point receives from the personal computer a logical push button configuration activation, thereafter the processor acts to control the wireless interface to pair the access point with the wireless device;

thereafter the processor causing the wireless interface to restore broadcasting of all of the service set identifiers.

18. The access point of claim 17, wherein the processor controlling the wireless interface to inhibit broadcast of all service set identifiers except for the received service set identifier from the personal computer ensures that the wireless device pairs with only a correct service set identifier.

19. A method for pairing a wireless device with an access point using a push button on the access point, the method comprising:

receiving a push button command to pair the wireless device to the access point;

inhibiting broadcast of all service set identifiers associated with the access point;

broadcasting a service set identifier associated with the wireless device;

pairing the access point with the wireless device;

exchange information between the access point and the wireless device across the wireless network.

20. The method of claim 19, wherein receiving a push button command comprises receiving an indication at the access point that a pairing button has been activated multiple times.

21. The method of claim 20, wherein the pairing button has been activated multiple times in a fixed time interval.

22. The method of claim 1, wherein inhibiting broadcast of all service set identifiers further comprises providing an indication that a wireless protected setup has commenced.

23. The method of claim 1, wherein pairing the access point with the wireless device comprises exchanging security keys.

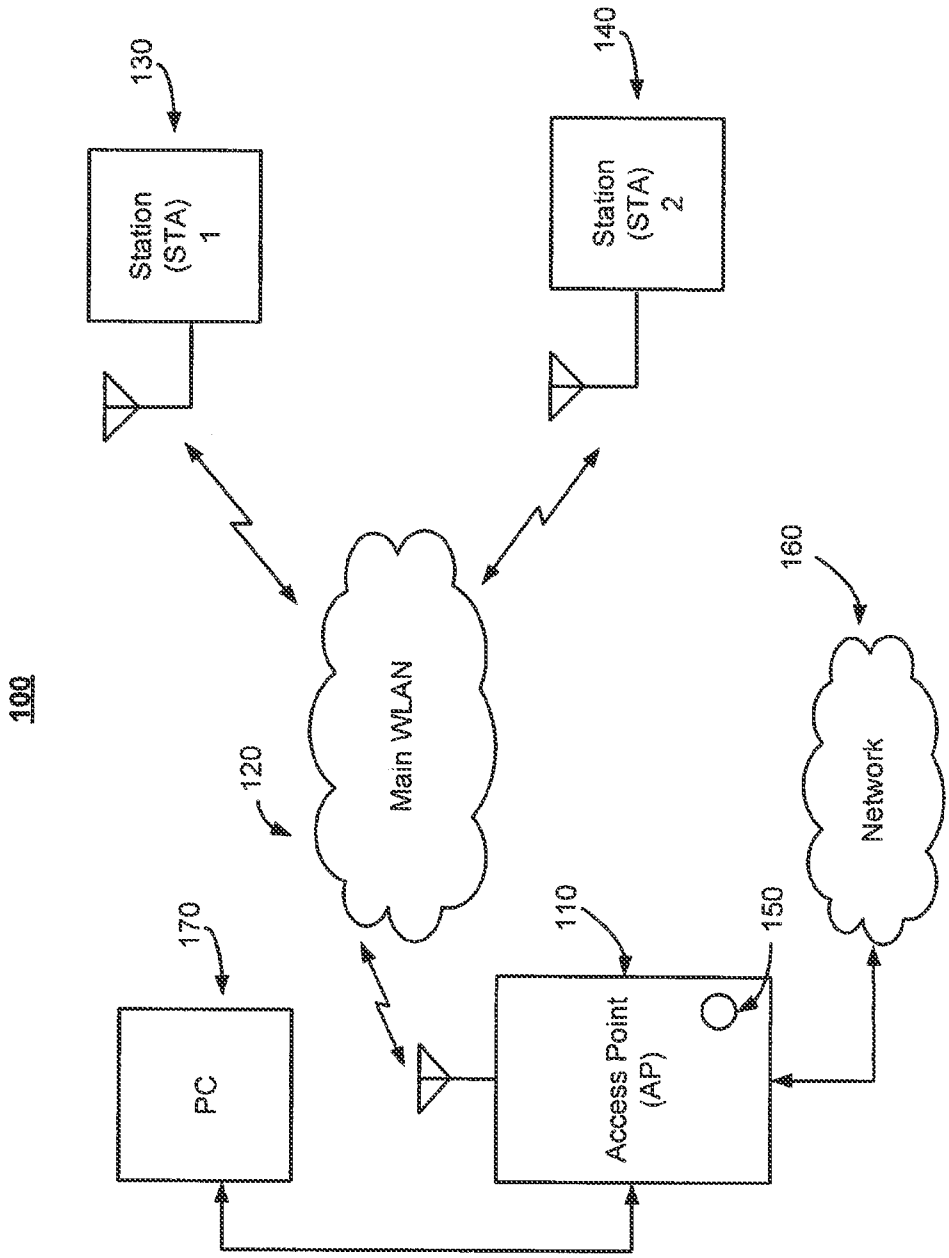
100
130
Station (STA) 1
140
Station (STA) 2
120
Main WLAN
160
Network
170
PC
110
Access Point (AP)
150

Fig. 1

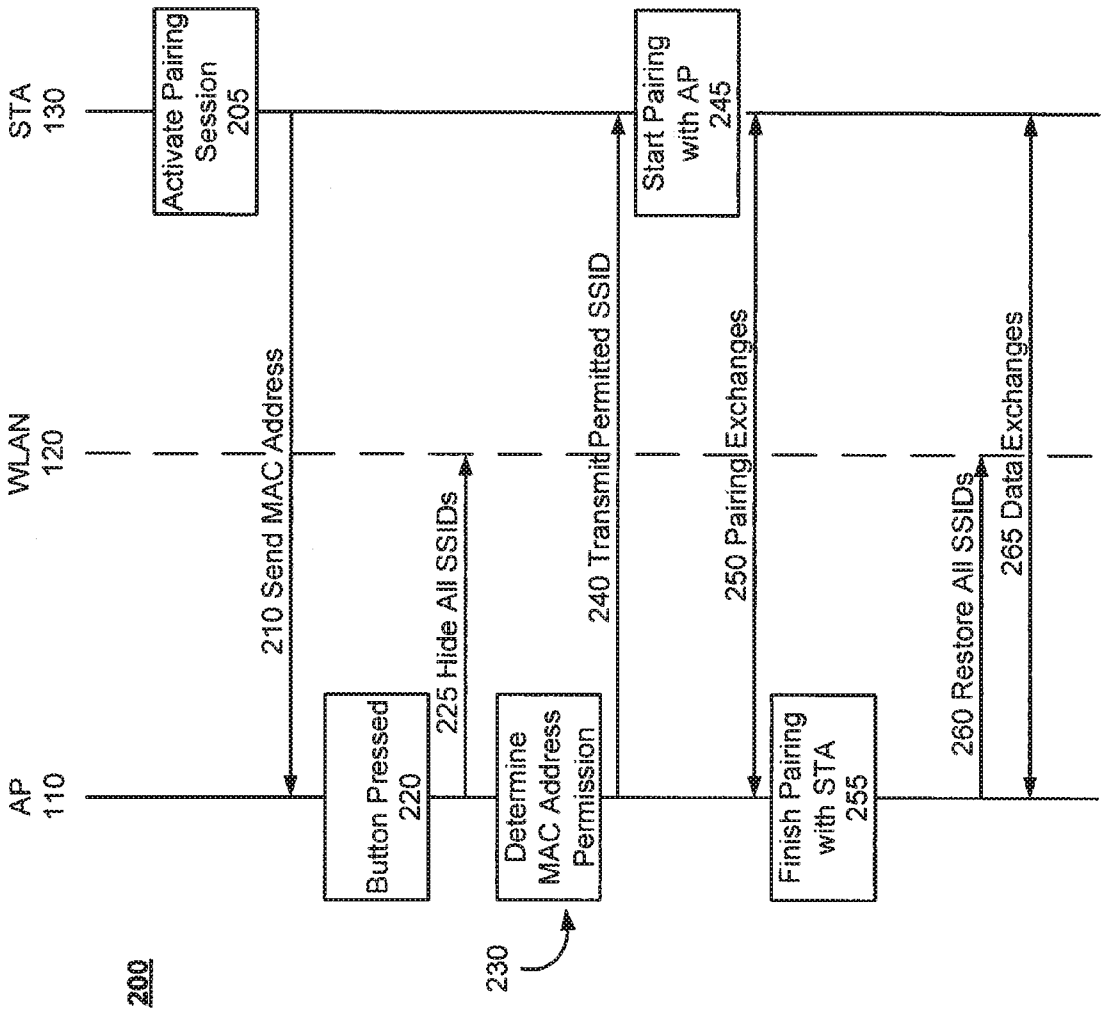
200
AP 110
WLAN 120
STA 130
Activate Pairing Session 205
210 Send MAC Address
Button Pressed 220
225 Hide All SSIDs
Determine MAC Address Permission
230
240 Transmit Permitted SSID
Start Pairing with AP 245
250 Pairing Exchanges
Finish Pairing with STA 255
260 Restore All SSIDs
265 Data Exchanges

Fig. 2

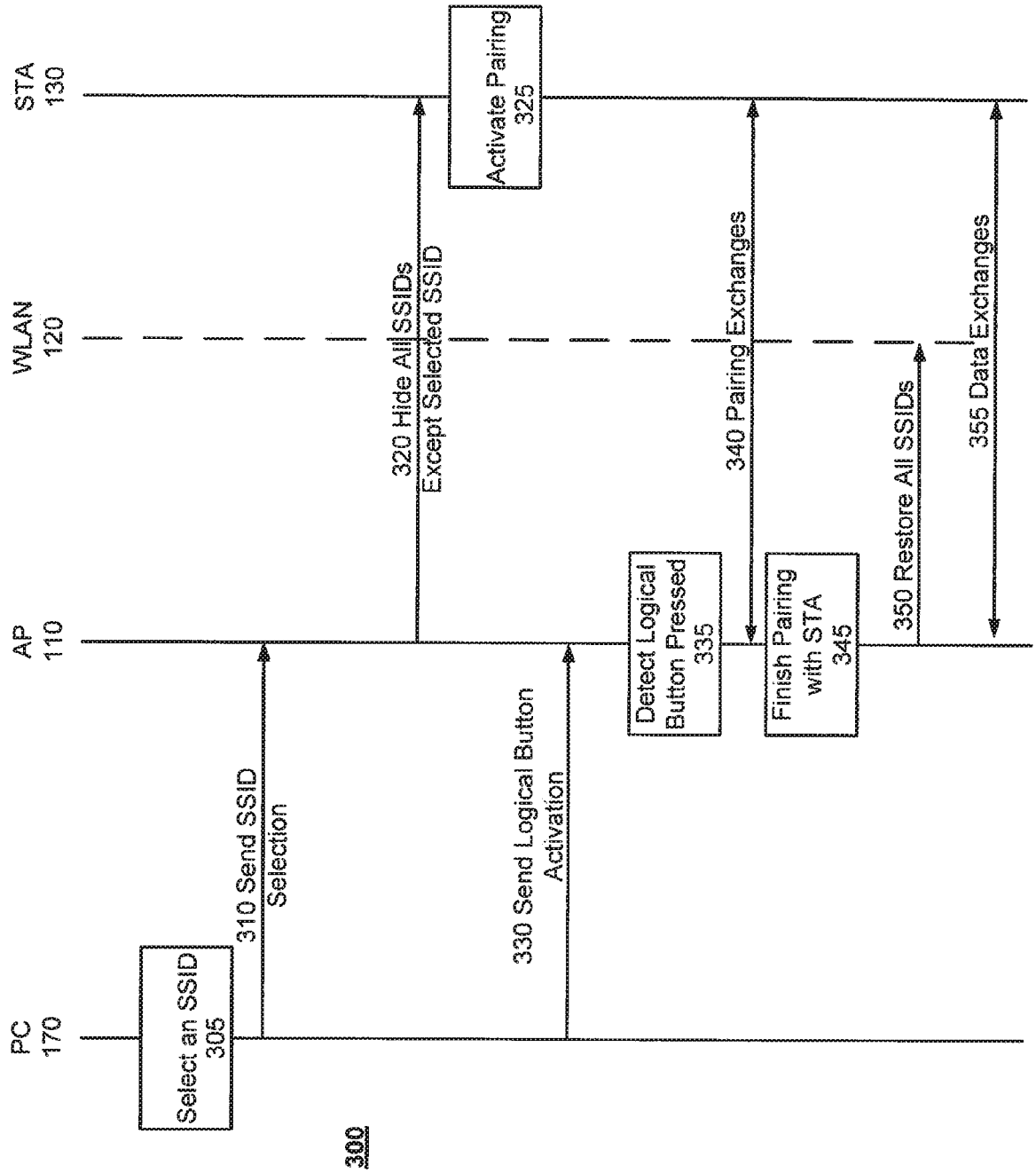
PC
170
AP
110
WLAN
120
STA
130
Select an SSID
305
310 Send SSID
Selection
320 Hide All SSIDs
Except Selected SSID
Activate Pairing
325
330 Send Logical Button
Activation
Detect Logical
Button Pressed
335
340 Pairing Exchanges
Finish Pairing
with STA
345
350 Restore All SSIDs
355 Data Exchanges
300

Fig. 3

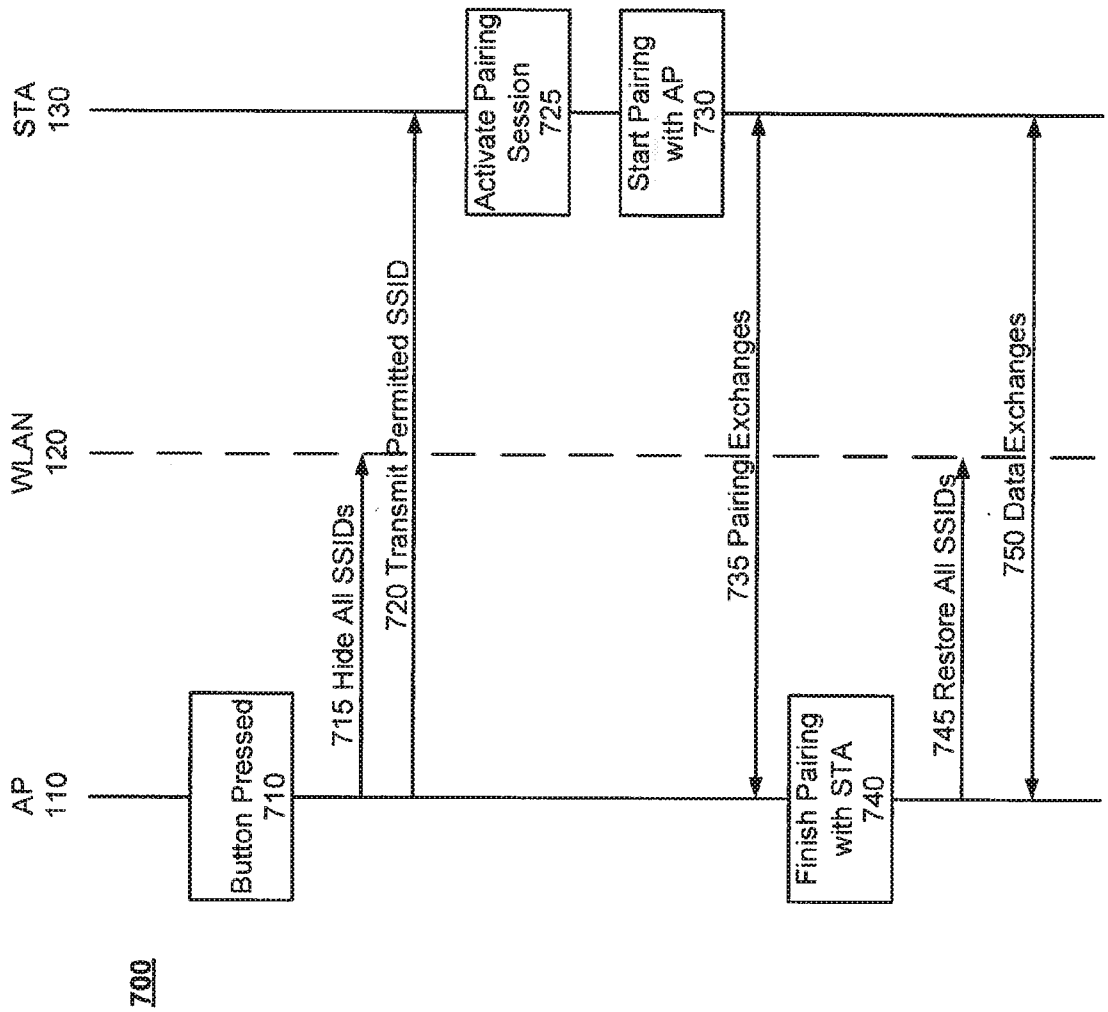
700
AP 110
WLAN 120
STA 130
Button Pressed 710
715 Hide All SSIDs
720 Transmit Permitted SSID
Activate Pairing Session 725
Start Pairing with AP 730
735 Pairing Exchanges
Finish Pairing with STA 740
745 Restore All SSIDs
750 Data Exchanges

Fig. 4

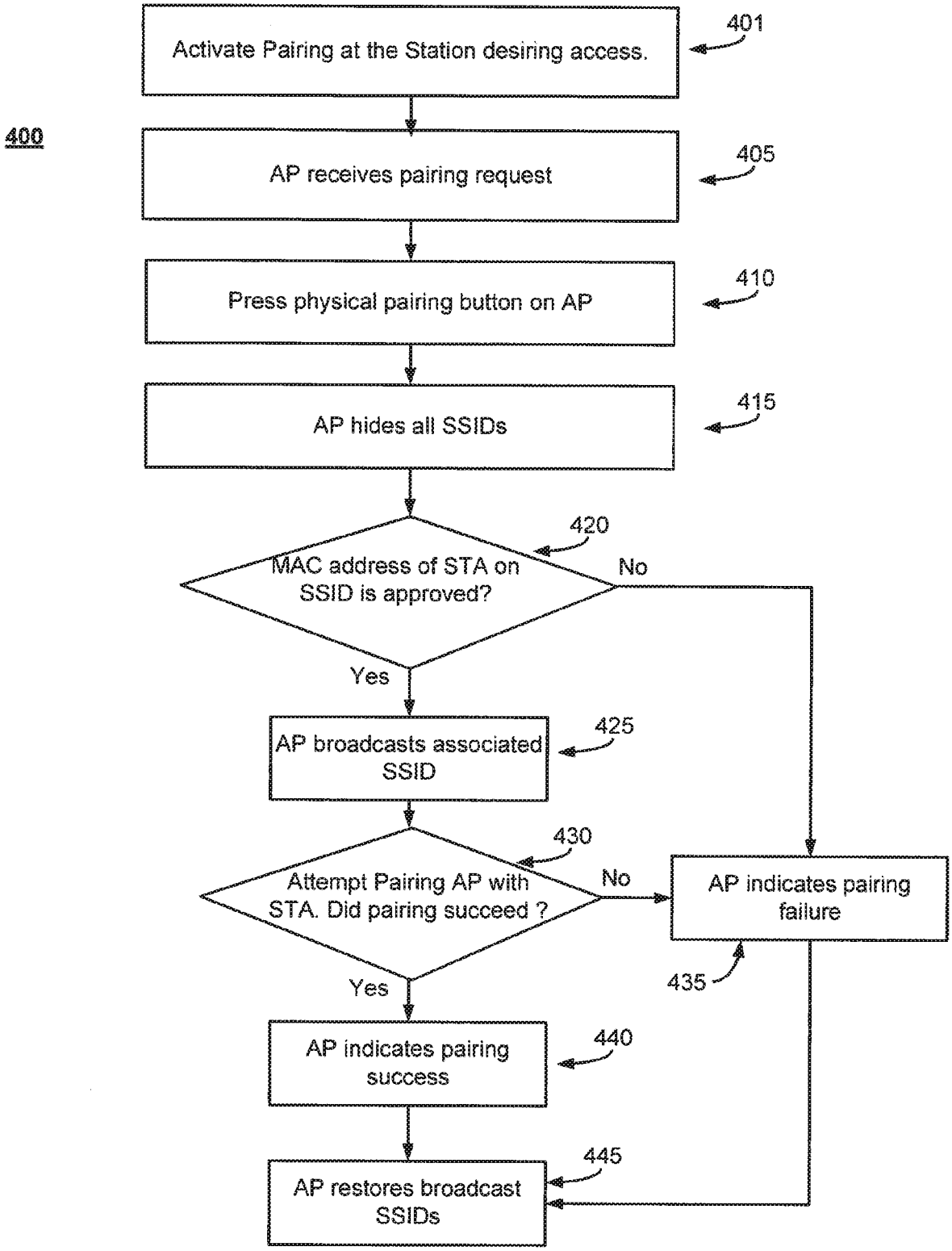
400
Activate Pairing at the Station desiring access.
401
AP receives pairing request
405
Press physical pairing button on AP
410
AP hides all SSIDs
415
MAC address of STA on SSID is approved?
420
No
Yes
AP broadcasts associated SSID
425
Attempt Pairing AP with STA. Did pairing succeed ?
430
No
AP indicates pairing failure
435
Yes
AP indicates pairing success
440
AP restores broadcast SSIDs
445

Fig. 5

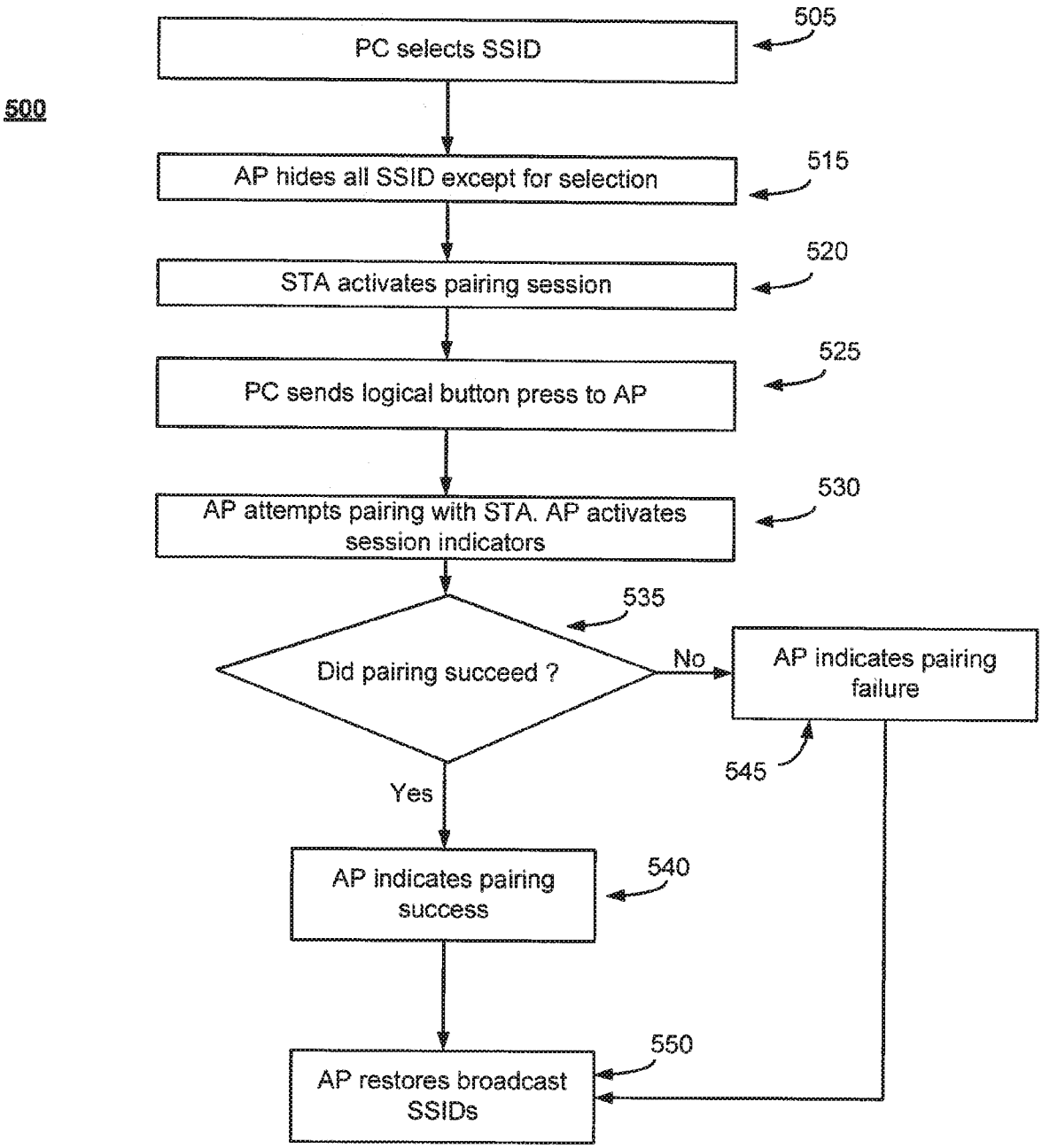
500
PC selects SSID
505
AP hides all SSID except for selection
515
STA activates pairing session
520
PC sends logical button press to AP
525
AP attempts pairing with STA. AP activates session indicators
530
Did pairing succeed ?
535
No
AP indicates pairing failure
545
Yes
AP indicates pairing success
540
AP restores broadcast SSIDs
550

Fig. 6

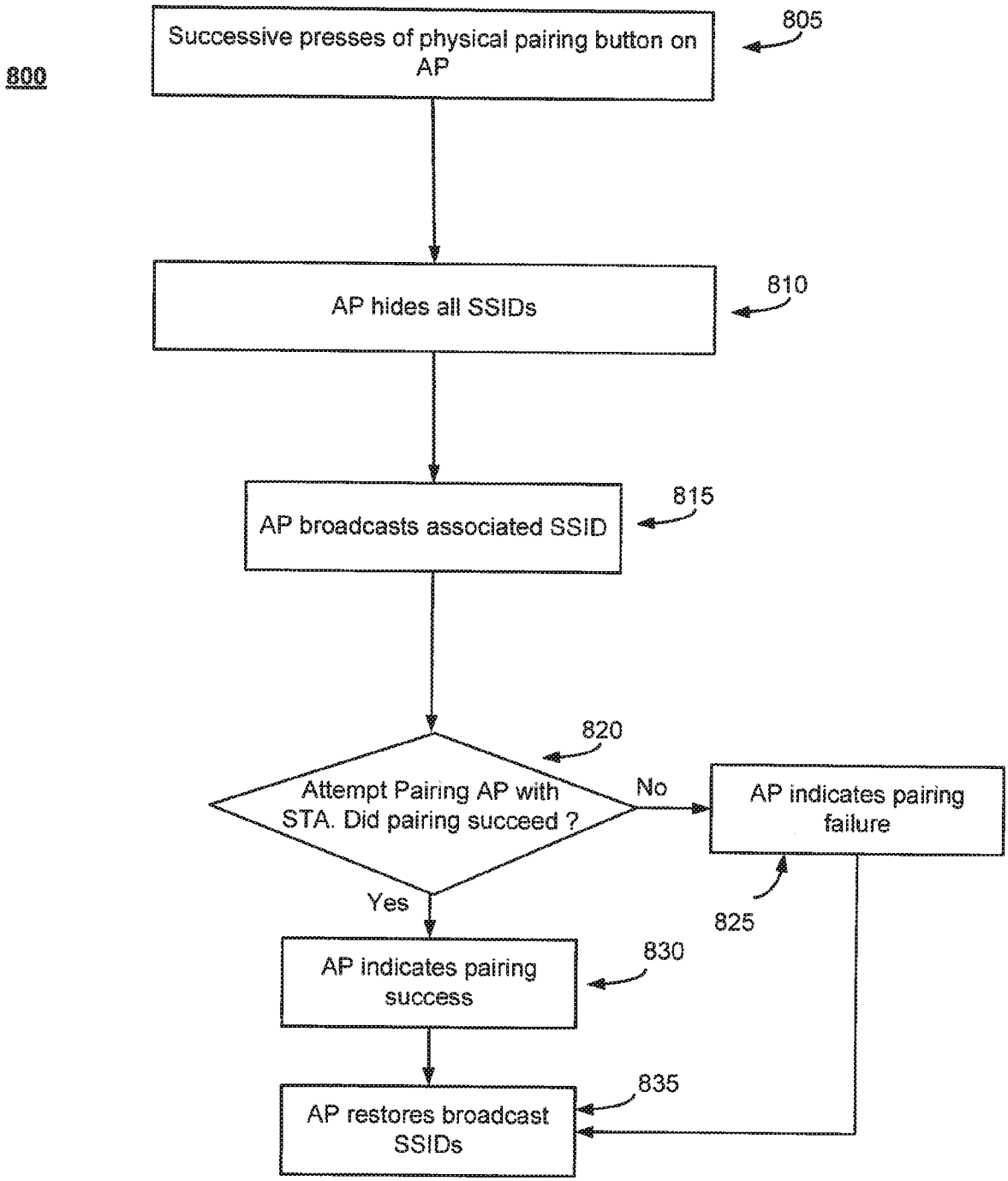
800
Successive presses of physical pairing button on AP
805
AP hides all SSIDs
810
AP broadcasts associated SSID
815
820
Attempt Pairing AP with STA. Did pairing succeed ?
No
AP indicates pairing failure
825
Yes
AP indicates pairing success
830
AP restores broadcast SSIDs
835

Fig. 7

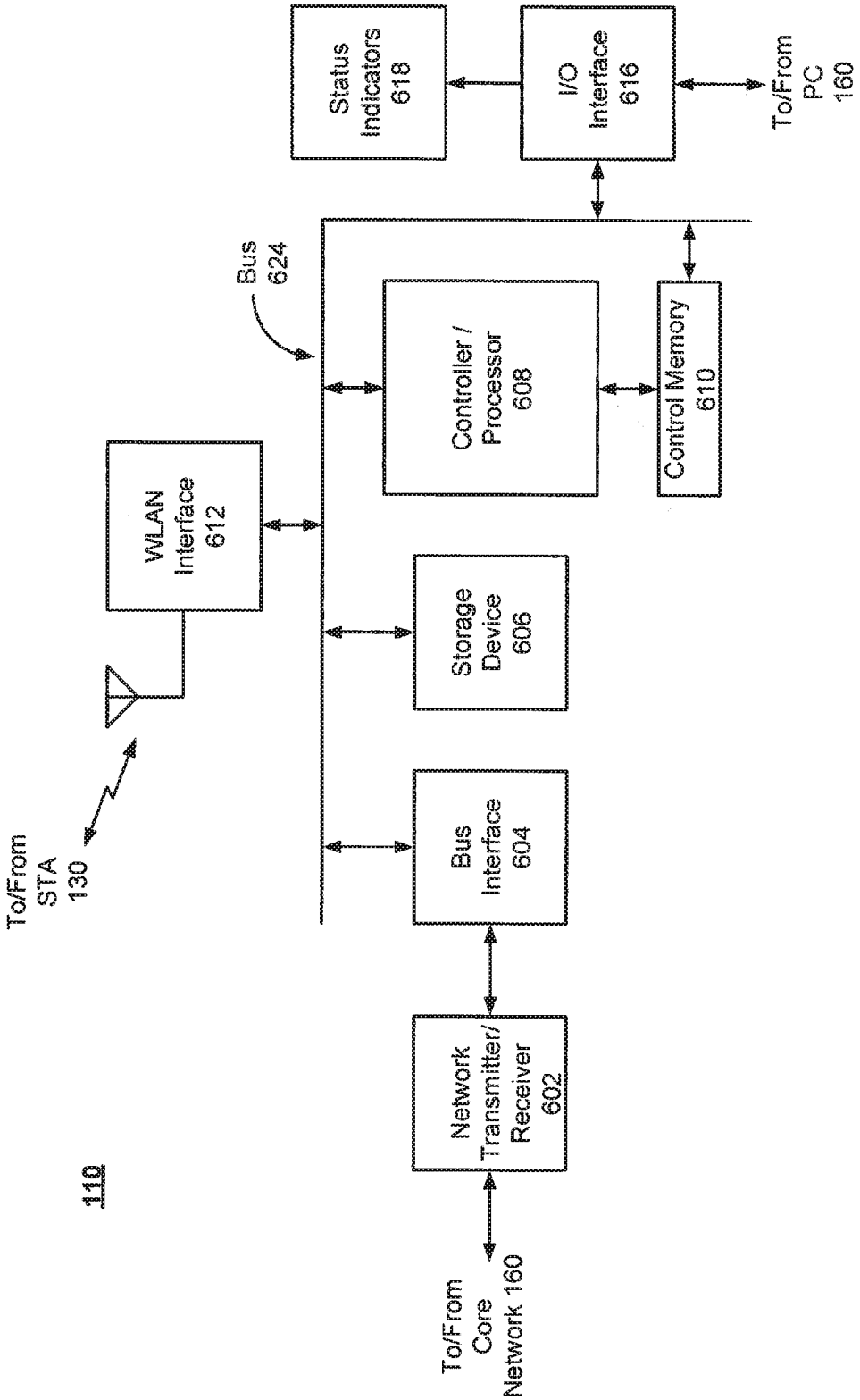
110
To/From STA 130
WLAN Interface 612
Network Transmitter/ Receiver 602
Bus Interface 604
Storage Device 606
Controller / Processor 608
Control Memory 610
Bus 624
Status Indicators 618
I/O Interface 616
To/From PC 160
To/From Core Network 160

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/055740

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W48/12 H04W84/12
ADD.

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

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)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2012/147777 A1 (ARASHIN NOBUHIKO [JP] ET AL) 14 June 2012 (2012-06-14) paragraph [0063] - paragraph [0095] -----	1-11, 19-23 12-18
Y	David D. Coleman: "6.2 Wi-Fi Protected Setup (WPS)" In: "CWSP Certified Wireless Security Professional Official: Study Guide", 17 February 2010 (2010-02-17), Sybex, XP55216095, ISBN: 978-0-47-043891-6 paragraph [6.2.1.4] -----	12-18
A	US 2011/276672 A1 (KWON HYUK-CHOON [KR] ET AL) 10 November 2011 (2011-11-10) paragraph [0065] - paragraph [0084] -----	1-23

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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
23 December 2015	11/01/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Roberti, Vincenzo

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/055740

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WI-FI ALLIANCE: "Wi-Fi CERTIFIED for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi Networks", WI-FI ALLIANCE, , 1 January 2007 (2007-01-01), pages 1-14, XP002568003, Retrieved from the Internet: URL:http://www.wi-fi.org/files/kc/20090123_Wi-Fi__Protected_Setup.pdf [retrieved on 2010-02-11] the whole document	1-23
A	EP 1 928 125 A1 (RESEARCH IN MOTION LTD [CA]) 4 June 2008 (2008-06-04) paragraph [0003] - paragraph [0004]	1-23
A	US 2010/034120 A1 (NAKAJIMA TAKAFUMI [JP]) 11 February 2010 (2010-02-11) paragraph [0057] - paragraph [0080]	1-23
A	EP 2 112 844 A2 (SAMSUNG ELECTRONICS CO LTD [KR]) 28 October 2009 (2009-10-28) paragraph [0031] - paragraph [0050]	1-23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/055740

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012147777 A1	14-06-2012	CN 102948240 A	27-02-2013
		CN 102948241 A	27-02-2013
		EP 2584856 A1	24-04-2013
		JP 5362853 B2	11-12-2013
		JP 5796201 B2	21-10-2015
		US 2012147777 A1	14-06-2012
		US 2012163324 A1	28-06-2012
		WO 2011161950 A1	29-12-2011
		WO 2011161951 A1	29-12-2011
US 2011276672 A1	10-11-2011	NONE	
EP 1928125 A1	04-06-2008	CA 2610112 A1	30-05-2008
		CN 101202686 A	18-06-2008
		EP 1928125 A1	04-06-2008
		JP 4642832 B2	02-03-2011
		JP 2008141755 A	19-06-2008
		KR 20080049678 A	04-06-2008
US 2010034120 A1	11-02-2010	JP 5538692 B2	02-07-2014
		JP 2010041666 A	18-02-2010
		US 2010034120 A1	11-02-2010
EP 2112844 A2	28-10-2009	CN 101568189 A	28-10-2009
		EP 2112844 A2	28-10-2009
		KR 20090113033 A	29-10-2009
		US 2009271709 A1	29-10-2009