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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 October 2009 (08.10.2009)

PCT

(10) International Publication Number
WO 2009/123074 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04W 12/08* (2009.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/JP2009/056405

(22) International Filing Date:
23 March 2009 (23.03.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2008-095432 1 April 2008 (01.04.2008) JP

(71) Applicant *(for all designated States except US)*: **CANON KABUSHIKI KAISHA** [JP/JP]; 30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo, 1468501 (JP).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HAMACHI, Toshifumi** [JP/JP]; c/o CANON KABUSHIKI KAISHA, 30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo, 1468501 (JP).

(74) Agent: **OHTSUKA, Yasunori**; 7th FL., KIOICHO PARK BLDG., 3-6, KIOICHO, CHIYODA-KU, Tokyo, 1020094 (JP).

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

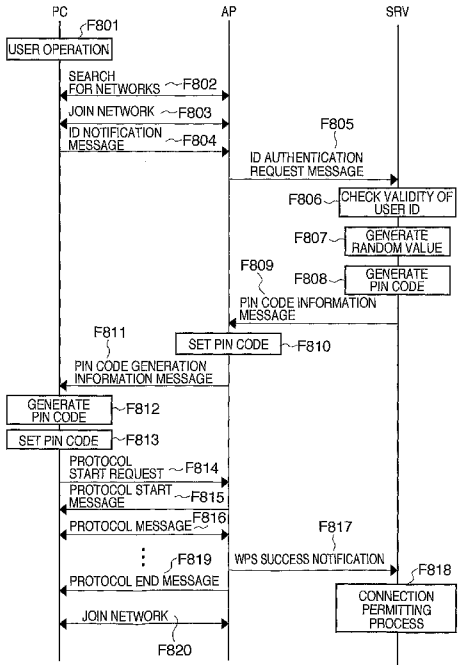
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS,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

Published:

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

(54) **Title**: USER AUTHENTICATION METHOD, WIRELESS COMMUNICATION APPARATUS, BASE STATION, AND ACCOUNT MANAGEMENT APPARATUS

FIG. 8



(57) **Abstract**: A wireless communication apparatus transmits a user identifier to an account management apparatus through a communication apparatus. The account management apparatus generates code generation information, and generates code information using authentication information that corresponds to the user identifier and the code generation information. The account management apparatus transmits the code information and the code generation information to the communication apparatus. The communication apparatus sets code information, and transmits the code generation information to the wireless communication apparatus. The wireless communication apparatus generates code information using the code generation information and the authentication information, and when wireless network parameters are set, notifies the account management apparatus of success of authentication. The account management apparatus performs a process to permit the wireless communication apparatus to connect to a communication network.

WO 2009/123074 A1

DESCRIPTION

USER AUTHENTICATION METHOD, WIRELESS COMMUNICATION APPARATUS, BASE STATION, AND ACCOUNT MANAGEMENT APPARATUS

TECHNICAL FIELD

[0001] The present invention relates to a wireless parameter setting technique and a user authentication technique.

BACKGROUND ART

[0002] When using an IEEE 802.11 wireless LAN, users must set wireless parameters such as a network identifier (ESSID), a frequency channel, an encryption scheme, an encryption key, an authentication scheme, an authentication key, and the like. Because these settings operations are complicated, methods have been proposed for automatically setting wireless parameters between terminals. For example, a method for transferring wireless parameter settings between a relay station (access point) and a terminal station (station) from the access point to the station with a simple operation has been implemented as an actual product.

[0003] In recent years, an organization called the Wi-Fi Alliance has developed a standard for automatic setting of wireless parameters called Wi-Fi Protected

Setup (WPS), which has already been implemented in some products.

[0004] According to WPS, wireless parameters are provided from a Registrar to an Enrollee using a Registration protocol, a special protocol for setting wireless parameters. The Registrar is an apparatus that manages wireless parameters and provides wireless parameters to Enrollees. The Enrollee is an apparatus that receives wireless parameters from a Registrar.

[0005] The communication between the Registrar and the Enrollee according to the Registration protocol is performed using EAP (Extensible Authentication Protocol) packets. The EAP packets are packets that enable communication between the Registrar and the Enrollee without an encryption or authentication.

[0006] An example will be described in which wireless parameters are provided from an access point that acts as a Registrar to a station that acts as an Enrollee. First, the station searches for a network to which the access point belongs, and temporarily joins the network. At this point in time, the ESSIDs and frequency channels of the access point and the station are the same, but the encryption key, authentication key and the like are not the same, and thus, ordinary data communication using an encryption or authentication is not possible.

[0007] The access point and the station perform

transmission/reception of messages using EAP packets according to the Registration protocol, and thereby, wireless parameters are provided from the access point to the station. The provided wireless parameters are newly set in the station, and thereby, data communication using an encryption or authentication is established between the station and the access point.

[0008] Currently, public wireless LANs are available which provide Internet connection services by installing access points in public places such as fast-food restaurants, railway stations, airports, and the like. Such a public wireless LAN authenticates users (performs user authentication) using authentication information, such as user IDs and passwords, in order to check whether or not they have an authorized account, and permits only users who have an authorized account to access the Internet. However, this user authentication has to be executed each time a user uses the public wireless LAN, which is troublesome for the user. To address this, for example, Japanese Patent Laid-Open No. 2004-80138 proposes a method for automating user authentication, wireless connection to a public wireless LAN, and the like.

[0009] According to the WPS, a PIN code is set in the Registrar and the Enrollee, and if it is confirmed that the PIN code set in the Registrar and the Enrollee are the same in the Registration protocol, wireless

parameters are exchanged. So, this system does not permit the exchange of wireless parameters with unintended devices.

[0010] Nevertheless, a case can be conceived in which the WPS is applied to a public wireless LAN. However, since general users cannot operate access points, it is impossible to set a PIN code in the Registrars, so the application of the WPS to a public wireless LAN is not possible.

[0011] Likewise, when a configuration is adopted in which general users can set a PIN code in access points, even users who do not have an authorized account can easily set a PIN code and obtain the wireless LAN parameters, causing problems in terms of security.

[0012] In addition, in public wireless LANs, after the wireless parameters have been set, user authentication has to be performed manually or with dedicated software, requiring users to perform troublesome operations.

DISCLOSURE OF INVENTION

[0013] The present invention provides a user authentication method of improving user operability by ensuring that user authentication is successfully completed by setting code information generated using authentication information in a base station apparatus

and a wireless communication apparatus, and acquiring wireless parameters using the code information.

[0014] According to an embodiment of the present invention, there is provided a user authentication method in a communication system comprising a wireless communication apparatus, a base station that performs wireless communication with the wireless communication apparatus, and an account management apparatus that manages user account information of a user permitted to connect to a communication network, the method comprising: at the wireless communication apparatus, transmitting a user identifier that is used to determine whether or not to permit a connection to the communication network to the account management apparatus through the base station; at the account management apparatus, generating code information that is used to set a wireless parameter for performing wireless communication between the wireless communication apparatus and the base station, based on authentication information that corresponds to the user identifier transmitted from the wireless communication apparatus and code generation information, and transmitting the generated code information and the code generation information to the base station; at the base station, storing the code information transmitted from the account management apparatus and transmitting code generation information to the wireless

communication apparatus; at the wireless communication apparatus, generating code information based on the code generation information transmitted from the base station and the authentication information corresponding to the user identifier transmitted to the account management apparatus; at the base station, checking whether or not the stored code information and the code information generated by the wireless communication apparatus match, and providing the wireless parameter to the wireless communication apparatus and notifying the account management apparatus of success in setting the wireless parameter, when it is confirmed that the stored code information and the code information generated by the wireless communication apparatus match; and at the account management apparatus, permitting the wireless communication apparatus to connect to the communication network, when success in setting the wireless parameters is notified from the base station.

[0015] According to another embodiment of the present invention, there is provided a wireless communication apparatus that connects to a communication network through a wireless network, the apparatus comprising: transmission means for transmitting a user identifier that is used to determine whether or not to permit a connection to the communication network to an account management

apparatus through a base station; reception means for receiving code generation information transmitted from the account management apparatus through the base station; generation means for generating code information using the received code generation information and authentication information that corresponds to the user identifier transmitted to the account management apparatus; and acquisition means for acquiring a parameter of the wireless network from the base station by using the generated code information.

[0016] According to another embodiment of the present invention, there is provided a base station that performs wireless communication with a wireless communication apparatus, the base station comprising: reception means for receiving a user identifier that is used to determine whether or not to permit a connection to a communication network from the wireless communication apparatus; transfer means for transferring the user identifier to an account management apparatus; acquisition means for acquiring, from the account management apparatus, code information that is used to set a wireless parameter for performing wireless communication between the wireless communication apparatus and the base station, and code generation information; transmission means for transmitting the acquired code generation information to the wireless communication apparatus; checking means

for checking whether or not code information generated based on the code generation information by the wireless communication apparatus and the code information acquired from the account management apparatus match; provision means for providing the wireless parameter to the wireless communication apparatus when it is confirmed that the generated code information and the acquired code information match; and notification means for notifying the account management apparatus of success in setting the wireless parameter, when it is confirmed that the generated code information and the acquired code information match.

[0017] According to another embodiment of the present invention, there is provided an account management apparatus that manages user account information of a user permitted to connect to a communication network, the apparatus comprising: reception means for receiving a user identifier that is used to determine whether or not to permit a connection to the communication network from a wireless communication apparatus through a base station; generation means for generating code information that is used to set a wireless parameter for performing wireless communication between the wireless communication apparatus and the base station using authentication information that corresponds to the user identifier and code generation information;

transmission means for transmitting the code information and the code generation information to the base station; reception means for receiving a success notification indicating success in setting the wireless parameters from the base station; and permitting means for permitting the wireless communication apparatus to connect to the communication network when the success notification is received.

[0018] Further features of the present invention will become apparent from the following description of exemplary embodiments with reference to the attached drawings.

BRIEF DESCRIPTION OF DRAWINGS

[0019] FIG. 1 is a diagram illustrating an example of the configuration of a typical communication system according to Embodiment 1.

[0020] FIG. 2 is a block diagram illustrating an example of the configuration of a personal computer according to Embodiment 1.

[0021] FIG. 3 is a block diagram illustrating an example of the configuration of an access point according to Embodiment 1.

[0022] FIG. 4 is a block diagram illustrating an example of the configuration of an account management server according to Embodiment 1.

[0023] FIG. 5 is a flowchart illustrating a

process performed by a wireless communication apparatus according to Embodiment 1.

[0024] FIG. 6 is a flowchart illustrating a process performed by a wireless base station apparatus according to Embodiment 1.

[0025] FIG. 7 is a flowchart illustrating a process performed by an account management server according to Embodiment 1.

[0026] FIG. 8 is a diagram illustrating a user authentication sequence according to Embodiment 1.

[0027] FIG. 9 is a flowchart illustrating a process performed by a wireless communication apparatus according to Embodiment 2.

[0028] FIG. 10 is a flowchart illustrating a process performed by a wireless base station apparatus according to Embodiment 2.

[0029] FIG. 11 is a flowchart illustrating a process performed by an account management server according to Embodiment 2.

[0030] FIG. 12 is a diagram illustrating a user authentication sequence according to Embodiment 2.

BEST MODE FOR CARRYING OUT THE INVENTION

[0031] Hereinafter, best modes for carrying out the invention will be described in detail with reference to the attached drawings of the present invention.

[0032] Embodiment 1

FIG. 1 is a diagram illustrating an example of the configuration of a typical communication system according to Embodiment 1. A personal computer (PC) 101 has a function for performing wireless LAN communication according to the IEEE 802.11 standard series and a WPS Enrollee function. An access point (AP) 102 has a function for performing wireless LAN communication and Ethernet® communication, and a WPS Registrar function. An account management server (SRV) 103 has a function for performing Ethernet® communication, a function for managing user accounts (user IDs and passwords, etc.) of a public wireless LAN, and a function for authenticating users and providing communication permission. The Internet 104 is a communication network capable of connecting computers around the world.

[0033] The AP 102, the SRV 103 and the Internet 104 are connected with a wired LAN, and the PC 101 is connected to an infrastructure mode wireless network to which the AP 102 belongs. Upon activation of an application for automatically setting wireless parameters in the PC 101, it is checked, by a settings information notification protocol, whether or not the PIN code of the PC 101 and the PIN code of the AP 102 match, and if it is confirmed that they match, the PC

101 can acquire wireless parameters. That is, it can be said that the PIN code is code information used for a wireless parameter setting process, or code information used to determine whether or not to provide wireless parameters in a wireless parameter setting process.

[0034] As used herein, the settings information notification protocol refers to a Registration protocol, and EAP packets are used for transmission/reception of various messages. Accordingly, if the ESSIDs and frequency channels of the PC 101 and the AP 102 match, various messages can be transmitted/received by the settings information notification protocol without an encryption or authentication for wireless LAN.

[0035] Also, the wireless parameters set by the settings information notification protocol include an ESSID, a frequency channel, an encryption scheme, an encryption key, an authentication scheme, an authentication key, and so on. The PIN code is the abbreviation of Personal Identification Number, and can be a number string, character string, or the like.

[0036] The PC 101 and the SRV 103 can communicate with each other through the AP 102. The PC 101 executes authentication of a user (executes user authentication) with the SRV 103, and can connect to the Internet 104 only if the user is successfully authenticated. Accordingly, the PC 101 cannot connect

to the Internet 104 even after the PC 101 establishes a connection to the wireless network of the AP 102 until the user is successfully authenticated. The SRV 103 stores a list of valid user accounts (user IDs and passwords, etc.) to execute user authentication. That is, it can be said that a user identifier (user ID) for public wireless LAN, which will be described later, refers to identification information used for user authentication that determines whether or not to permit connection to the Internet as a communication network. Also, it can be said that authentication information (password) for public wireless LAN, which will be described later, refers to authentication information used for user authentication that determines whether or not to permit connection to the Internet as a communication network.

[0037] Next, a configuration of the PC 101 shown in FIG. 1 will be described with reference to FIG. 2. FIG. 2 is a block diagram illustrating an example of the configuration of the personal computer according to Embodiment 1. In FIG. 2, reference numeral 202 denotes a communication unit that performs wireless communication, and reference numeral 203 denotes a communication control unit that controls the communication unit. Reference numeral 204 denotes a timer unit that performs a timer process and manages time; 205 denotes an interface processing unit that

controls various interfaces; 206 denotes a display unit that provides various displays.

[0038] Reference numeral 207 denotes a wireless parameter setting unit that sets wireless parameters by a settings information notification protocol; 208 denotes a code calculation unit that calculates various encryptions, hash values, and the like; 209 denotes a determination unit that makes various determinations in a process described later; 210 denotes a storage unit that stores wireless parameters, user account information and the like. The user account information may be stored in devices in advance, or may be inputted by the user. Reference numeral 211 denotes an apparatus control unit that controls the operation of the whole apparatus.

[0039] A configuration of the AP 102 shown in FIG. 1 will be described next with reference to FIG. 3. FIG. 3 is a block diagram illustrating an example of the configuration of the access point according to Embodiment 1. In FIG. 3, reference numeral 302 denotes a communication unit that performs wireless communication and wired communication; 303 denotes a communication control unit that controls the communication unit; 304 denotes a timer unit that performs a timer process and manages time; 305 denotes an interface processing unit that controls various interfaces.

[0040] Reference numeral 306 denotes a wireless parameter setting unit that sets wireless parameters by a settings information notification protocol; 307 denotes a determination unit that makes various determinations in a process described later; 308 denotes a storage unit that stores wireless parameters, and the like; 309 denotes an apparatus control unit that controls the operation of the whole apparatus.

[0041] A configuration of the SRV 103 shown in FIG. 1 will be described next with reference to FIG. 4. FIG. 4 is a block diagram illustrating an example of the configuration of the account management server according to Embodiment 1. In FIG. 4, reference numeral 402 denotes a communication unit that performs wired communication; 403 denotes a communication control unit that controls the communication unit; 404 denotes a timer unit that performs a timer process and manages time; 405 denotes an interface processing unit that controls various interfaces; 406 denotes a display unit that provides various displays.

[0042] Reference numeral 407 denotes an authentication processing unit that performs user authentication for public wireless LAN; 408 denotes a code calculation unit that calculates various encryptions, hash values, and the like; 409 denotes a determination unit that makes various determinations in a process described later; 410 denotes a storage unit

that stores wireless parameters, user account information and the like; 411 denotes an apparatus control unit that controls the operation of the whole apparatus.

[0043] Now, a processing procedure performed by the PC 101 that operates as a wireless communication apparatus to execute a settings information notification protocol will be described with reference to FIG. 5.

[0044] FIG. 5 is a flowchart illustrating a process performed by the wireless communication apparatus according to Embodiment 1. This process starts when the PC 101 connects to a wireless network to which the AP 102, which operates as a wireless base station apparatus of a public wireless LAN, belongs. At this point in time, the same encryption key, authentication key and the like are not set in the PC 101 and the AP 102. Accordingly, the PC 101 is in a state in which the PC 101 can communicate with the AP 102 using only particular signals (alert signals, EAP packets, etc.) in the wireless network of the AP 102, and cannot perform ordinary data communication using an encryption or authentication. Here, it is assumed that various messages are transmitted/received between the PC 101 and the AP 102 using EAP packets.

[0045] The PC 101 transmits, to the AP 102, an ID notification message to which a user identifier (user

ID) for public wireless LAN is assigned (F501). After transmitting the ID notification message, the PC 101 waits for reception of a PIN code generation information message or a protocol failure notification from the AP 102 (F502, F503). If the PC 101 receives a protocol failure notification, the PC 101 ends this process.

[0046] If, on the other hand, the PC 101 receives a PIN code generation information message, it generates a PIN code based on a random value and authentication information (password) for public wireless LAN that are assigned to the message (F504). The method for generating a PIN code using a random value and a password can be any method such as a method of using a cryptographic algorithm such as RC4 or AES, or a method of using a hash algorithm such as MD5 or SHA1.

[0047] After generating the PIN code, the PC 101 sets the PIN code in the application for automatically setting wireless parameters (F505), and then executes a settings information notification protocol using the set PIN code (F506). The settings information notification protocol authenticates mutual validity between the Enrollee and the Registrar by determining whether or not their PIN codes match. Accordingly, the Enrollee can acquire wireless parameters from a Registrar with the same PIN code. Subsequently, after the settings information notification protocol ends, it

is determined whether or not the settings information notification protocol has been executed successfully (F507). As used herein, the phrase "the settings information notification protocol has been executed successfully" refers to a state in which the Enrollee has acquired wireless parameters from the Registrar with a PIN code that matches the PIN code of the Enrollee. If it is determined that the settings information notification protocol has failed, the PC 101 ends this process. If, on the other hand, the settings information notification protocol has been executed successfully, the PC 101 connects to the wireless network to which the AP 102 belongs using the acquired wireless parameters (F508). By doing so, the same encryption key, authentication key and the like as those of the AP 102 is set in the PC 101, and therefore, the PC 101 can perform ordinary data communication using an encryption or authentication.

[0048] A processing procedure performed by the AP 102 that operates as a wireless base station apparatus to execute a settings information notification protocol will be described next with reference to FIG. 6.

[0049] FIG. 6 is a flowchart illustrating a process performed by the wireless base station apparatus according to Embodiment 1. This process starts when the PC 101 requesting the execution of automatic setting of wireless parameters joins the

wireless network to which the AP 102 belongs. At this point in time, the same encryption key, authentication key and the like are not set in the PC 101 and the AP 102. Accordingly, the PC 101 is in a state in which the PC 101 can communicate with the AP 102 using only particular signals (alert signals, EAP packets, etc.) in the wireless network of the AP 102, and cannot perform ordinary data communication using an encryption or authentication. Here, it is assumed that various messages are transmitted/received between the PC 101 and the AP 102 using EAP packets.

[0050] The AP 102 waits for reception of an ID notification message from the PC 101 (F601). If the AP 102 receives an ID notification message from the PC 101, the AP 102 assigns the user ID assigned to the message to an ID authentication request message, and transmits the ID authentication request message to the SRV 103 (F602). After transmitting the ID authentication request message, the AP 102 waits for reception of a PIN code information message or a rejection notification message from the SRV 103 (F603, F604). If the AP 102 receives a rejection notification message, it transmits a protocol failure notification to the wireless communication apparatus (F609), and then ends this process.

[0051] If, on the other hand, the AP 102 receives a PIN code information message, it sets the PIN code

assigned to the message in the application for automatically setting wireless parameters (F605), and then assigns the random value assigned to the PIN code information message to a PIN code generation information message and transmits the PIN code generation information message to the PC 101 (F606). Next, after transmitting the PIN code generation information message, the AP 102 executes the settings information notification protocol with the PC 101 using the set PIN code (F607).

[0052] Next, the AP 102 determines whether or not the settings information notification protocol has been executed successfully (F608). As used herein, the phrase "the settings information notification protocol has been executed successfully" refers to a state in which the PIN code of the Registrar and the PIN code of the Enrollee match, and wireless parameters have been provided from the Registrar to the Enrollee. If it is determined that settings information notification protocol has been executed successfully, the AP 102 transmits a WPS success notification to the SRV 103 (F610), and then ends this process. If, on the other hand, the settings information notification protocol fails, the AP 102 ends this process.

[0053] A processing procedure performed by the account management server (SRV) 103 that performs user authentication when the PC 101 connects to the Internet

104 will be described next with reference to FIG. 7.

[0054] FIG. 7 is a flowchart illustrating a process performed by the account management server according to Embodiment 1. The SRV 103 waits for reception of an ID authentication request message from the AP 102 (F701). If the SRV 103 receives an ID authentication request message from the AP 102, the SRV 103 checks whether or not the user ID assigned to the message is valid (F702). The method for checking the validity of user IDs can be, for example, a method in which user account information that is stored in the storage unit 410 is referred to, and if a user ID that is the same as the received user ID is found, the received user ID is validated.

[0055] If the received user ID is invalid, the SRV 103 transmits a rejection notification message to the AP 102 (F710), and then ends this process. If, on the other hand, the received user ID is valid, the SRV 103 generates a random value (F703). Then, the SRV 103 generates a PIN code using the password corresponding to the received user ID and the generated random value (F704).

[0056] After generating the PIN code, the SRV 103 assigns the generated PIN code and the random value used to generate the PIN code to a PIN code information message, and transmits the message to the AP 102 (F705). After transmitting the PIN code information message,

the SRV 103 activates a user authentication period timer (F706), and waits for reception of a WPS success notification from the AP 102, or for timeout of the user authentication period timer (F707, F708).

[0057] If the user authentication period timer times out, the SRV 103 ends this process. If, on the other hand, the SRV 103 receives a WPS success notification, the SRV 103 performs a process for permitting the PC 101, which transmitted the user ID received in F701, to connect to the Internet 104 (F709), and then ends this process.

[0058] A user authentication sequence performed by the PC 101, the AP 102 and the SRV 103 will be described next with reference to FIG. 8.

[0059] FIG. 8 is a diagram illustrating a user authentication sequence according to Embodiment 1. In the PC 101, when an application for automatically setting wireless parameters is activated by a user operation or the like (F801), the PC 101 searches for wireless networks in the surrounding area (F802). Next, a wireless network is automatically or manually selected from among the found wireless networks. In this example, the wireless network of the AP 102 is selected, and the PC 101 joins the wireless network of the AP 102 (F803). However, at this point in time, the same encryption key, authentication key and the like are not set in the PC 101 and the AP 102. Accordingly,

the PC 101 is in a state in which the PC 101 can communicate with the AP 102 using only particular signals (alert signals, EAP packets, etc.) in the wireless network of the AP 102, and cannot perform ordinary data communication using an encryption or authentication. Here, it is assumed that various messages are transmitted/received between the PC 101 and the AP 102 using EAP packets.

[0060] Next, the PC 101 assigns a user ID to an ID notification message, and transmits the message to the AP 102 (F804). Here, in the case where the PC 101 stores multiple user IDs for public wireless LAN, it is possible to adopt a configuration that permits the user to manually select a user ID, or a configuration in which a user ID is selected automatically based on network information such as an ESSID. If the AP 102 receives the ID notification message, it assigns the user ID assigned to the message to an ID authentication request message, and transmits the ID authentication request message to the SRV 103 (F805). Here, an example is described in which the ID notification message and the ID authentication request message are separate messages, but they may be configured as a single message.

[0061] If the SRV 103 receives the ID authentication request message, it checks the validity of the received user ID (F806). After confirming the

validity of the received user ID, the SRV 103 generates a random value (F807). After generating the random value, the SRV 103 generates a PIN code using the password corresponding to the received user ID and the generated random value (F808).

[0062] Next, after generating the PIN code, the SRV 103 assigns the generated PIN code and the random value to a PIN code information message, and transmits the message to the AP 102 (F809). If the AP 102 receives the PIN code information message, it starts an application for automatically setting wireless parameters, and sets the assigned PIN code in the application for automatically setting wireless parameters (F810). After setting the PIN code, the AP 102 assigns the random value to a PIN code generation information message, and transmits the message to the PC 101 (F811).

[0063] If the PC 101 receives the PIN code generation information message, it generates a PIN code using the assigned random value and the password stored in the PC 101 (F812). After generating the PIN code, the PC 101 sets the PIN code in an application for automatically setting wireless parameters (F813). After setting the PIN code, the PC 101 transmits a protocol start request to the AP 102 so as to start the settings information notification protocol (F814).

[0064] If the AP 102 receives the protocol start

request from the PC 101, it transmits a protocol start message to the PC 101 (F815). Then, the PC 101 and the AP 102 exchange protocol messages in accordance with the WPS Registration protocol (F816). Here, the wireless parameters of the AP 102 are transmitted to and set in the PC 101 only if it is confirmed by both the PC 101 and the AP 102 that the PIN code set in the PC 101 and the PIN code set in the AP 102 match.

[0065] Next, if the AP 102 confirms that its PIN code and the PIN code set in the PC 101 match, it transmits a WPS success notification to the SRV 103 (F817). If the SRV 103 receives the WPS success notification, it performs a process for permitting the PC 101 to connect to the Internet 104 (F818). After completion of the settings information notification protocol, the AP 102 transmits a protocol end message to the PC 101 (F819).

[0066] If the PC 101 receives the protocol end message, it temporarily disconnects from the network, and reconnects to the wireless network of the AP 102 using the wireless parameters acquired from the AP 102 (F820). Here, because the same encryption key, authentication key and the like as the AP 102 are set in the PC 101, ordinary data communication using an encryption or authentication is possible. The SRV 103 permits the PC 101 to connect to the Internet 104, and the PC 101 can connect to the Internet 104 through the

AP 102.

[0067] According to Embodiment 1, it becomes possible to safely and automatically set the same PIN code in a wireless communication apparatus and a wireless base station apparatus that execute a wireless parameter setting scheme in a public wireless LAN.

[0068] In addition, because a PIN code to be set is generated based on a random value and a password, a different PIN code is generated each time, and therefore, a high level of security is achieved.

[0069] Furthermore, because the password is used only within the wireless communication terminal and the account management server, the password will not be leaked to the outside of the wireless base station apparatus and the like, and therefore, a high level of security is achieved.

[0070] In addition, in a wireless parameter setting scheme, by regarding the matching of PIN codes as the matching of passwords instead of performing user authentication, it is possible to permit the wireless communication apparatus to connect to the Internet.

[0071] Accordingly, the user's task of setting a PIN code in the wireless communication apparatus and an access point of a public wireless LAN as well as the user's task of undergoing user authentication can be eliminated, and as a result, user operability is improved.

[0072] Embodiment 2

Next, Embodiment 2 of the present invention will be described in detail with reference to the drawings.

[0073] The configurations of a communication system, a PC, an AP and a SRV according to Embodiment 2 are the same as those of Embodiment 1 described above with reference to FIGS. 1 to 4, and thus, descriptions thereof are omitted here.

[0074] A processing procedure performed by the PC 101 that operates as a wireless communication apparatus to execute a settings information notification protocol will be described with reference to FIG. 9.

[0075] FIG. 9 is a flowchart illustrating a process performed by the wireless communication apparatus according to Embodiment 2. The processes spanning from F901 to F905 are the same as those of F501 to F505 shown in FIG. 5, and thus, descriptions thereof are omitted here.

[0076] Similar to Embodiment 1, the PC 101 sets a PIN code in the application for automatically setting wireless parameters (F905), and activates a PIN invalidation timer (F906). Specifically, the PIN invalidation timer is activated based on time information assigned to a PIN code generation information message sent from the AP 102. The time information can be a time period after which the PIN is invalidated. When the PIN invalidation timer times out,

the processing of the application for automatically setting wireless parameters is suspended, and then this process ends.

[0077] The subsequent processes (F907 to F909) are the same as F506 to F508 of Embodiment 1, and thus, descriptions thereof are omitted here.

[0078] A processing procedure performed by the AP 102 that operates as a wireless base station apparatus to execute a settings information notification protocol will be described next with reference to FIG. 10.

[0079] FIG. 10 is a flowchart illustrating a process performed by the wireless base station apparatus according to Embodiment 2. Because the processes spanning from F1001 to F1005 are the same as those of F601 to F605 shown in FIG. 6, descriptions thereof are omitted here.

[0080] Similar to Embodiment 1, the AP 102 sets a PIN code in the application for automatically setting wireless parameters (F1005), and activates a PIN invalidation timer (F1006). Specifically, the PIN invalidation timer is activated based on time information assigned to a PIN code information message sent from the SRV 103. When the PIN invalidation timer times out, the processing of the application for automatically setting wireless parameters is forcibly suspended, and then this process ends. Next, the AP 102 assigns the received time information to a PIN code

generation information message, and transmits the message to the PC 101 (F1007).

[0081] The subsequent processes (F1008 to F1011) are the same as F607 to F610 of Embodiment 1, and thus, descriptions thereof are omitted here.

[0082] A processing procedure performed by the account management server (SRV) 103 that performs user authentication when the PC 101 connects to the Internet 104 will be described next with reference to FIG. 11.

[0083] FIG. 11 is a flowchart illustrating a process performed by the account management server according to Embodiment 2. Because the processes spanning from F1101 to F1102 and the process of F1111 are the same as those of F701 to F702 and F710 shown in FIG. 7, descriptions thereof are omitted here.

[0084] Similar to Embodiment 1, the SRV 103 generates time information to be transmitted to the AP 102 if the received user ID is valid (F1103). After generating the time information, the SRV 103 generates a PIN code using the password corresponding to the user ID received from the AP 102 and the generated time information (F1104). After generating the PIN code, the SRV 103 activates a PIN invalidation timer using the generated time information (F1105). When the PIN invalidation timer times out, the authentication process is forcibly suspended, and then this process ends.

[0085] Next, the SRV 103 assigns the generated PIN code and the time used to generate the PIN code to a PIN code information message, and transmits the message to the AP 102 (F1106).

[0086] The subsequent processes (F1107 to F1110) are the same as F706 to F709 of Embodiment 1, and thus, descriptions thereof are omitted here.

[0087] A user authentication sequence performed by the PC 101, the AP 102 and the SRV 103 will be described next with reference to FIG. 12.

[0088] FIG. 12 is a diagram illustrating a user authentication sequence according to Embodiment 2. The processes spanning from F1201 to F1206 are the same as those of F801 to F806 shown in FIG. 8, and thus, descriptions thereof are omitted here.

[0089] Similar to Embodiment 1, the SRV 103 checks the validity of the received user ID, and generates time information that is a feature of Embodiment 2 (F1207). After generating the time information, the SRV 103 generates a PIN code using the password corresponding to the received user ID and the generated time information (F1208). Next, after generating the PIN code, the SRV 103 activates a PIN code invalidation timer using the time information (F1209). After activating the PIN code invalidation timer, the SRV 103 assigns the generated PIN code and the time information to a PIN code information message, and transmits the

message to the AP 102 (F1210).

[0090] If the AP 102 receives the PIN code information message, it starts the application for automatically setting wireless parameters, and sets the assigned PIN code in the application for automatically setting wireless parameters (F1211). Next, after setting the PIN code, the AP 102 activates the PIN code invalidation timer using the assigned time information (F1212). Then, after activating the PIN code invalidation timer, the AP 102 assigns the time information to a PIN code generation information message, and transmits the message to the PC 101 (F1213).

[0091] If the PC 101 receives the PIN code generation information message, it generates a PIN code using the assigned time information and the password stored in the PC 101 (F1214). After generating the PIN code, the PC 101 sets the PIN code in the application for automatically setting wireless parameters (F1215). After setting the PIN code, the PC 101 activates the PIN code invalidation timer using the assigned time information (F1216). After setting the PIN code invalidation timer, the PC 101 transmits a protocol start request to start the settings information notification protocol to the AP 102 (F1217).

[0092] The subsequent processes (F1217 to F1223) in this sequence are the same as F814 to F820 of

Embodiment 1, and thus, descriptions thereof are omitted here.

[0093] According to Embodiment 2, by providing a validity period to the PIN code, in addition to the effects of Embodiment 1, it is possible to prevent a single PIN code from being continuously set for a long time between a wireless communication terminal and a wireless base station apparatus. In addition, because the validity period can be set to expire substantially at the same time in the apparatuses, it is possible to prevent mismatching of valid PIN codes stored in the apparatuses. Accordingly, the possibility of success in automatically setting wireless parameters with unintended devices can be reduced.

[0094] Embodiments 1 and 2 have been described in the context of using an IEEE 802.11 wireless LAN as an example, but these embodiments are applicable to other wireless communication schemes such as wireless USB, Bluetooth®, UWB (Ultra Wide Band), etc.

[0095] It goes without saying that the object of the present invention can also be achieved by supplying, to a system or apparatus, a recording medium in which the program code for software that realizes the functions of the above-described embodiments has been recorded, and causing a computer (CPU or MPU) of the system or apparatus to read out and execute the program code stored in the recording medium.

[0096] In such a case, the program code itself read out from the computer-readable recording medium realizes the functions of the above-described embodiments, and the present invention is configured of the recording medium in which the program code is stored.

[0097] Examples of a recording medium for supplying the program code include a flexible disk, a hard disk, an optical disk, a magneto-optical disk, a CD-ROM, a CD-R, magnetic tape, a non-volatile memory card, a ROM, and so on.

[0098] Moreover, it goes without saying that the following case also falls under the scope of the present invention, which is not limited to implementing the functions of the above-described embodiments by a computer executing the read-out program code. That is, the case where an operating system (OS) or the like running on a computer performs part or all of the actual processing based on instructions of the program code, and the functions of the above-described embodiments are realized by that processing.

[0099] Furthermore, needless to say, the case in which the program code read out from the recording medium is written into a memory included in a function expansion board inserted into the computer, a function expansion unit connected to the computer, or the like, a CPU or the like included in the function expansion

board or function expansion unit then performs all or part of the actual processing based on instructions of the program code, and the functions of the above-described embodiments are implemented through that processing, is also included within the scope of the present invention.

[0100] While the present invention has been described with reference to exemplary embodiments, it is to be understood that the invention is not limited to the disclosed exemplary embodiments. The scope of the following claims is to be accorded the broadest interpretation so as to encompass all such modifications and equivalent structures and functions.

[0101] This application claims the benefit of Japanese Patent Application No. 2008-095432, filed on April 1, 2008, which is hereby incorporated by reference herein in its entirety.

CLAIMS

1. A user authentication method in a communication system comprising a wireless communication apparatus, a base station that performs wireless communication with the wireless communication apparatus, and an account management apparatus that manages user account information of a user permitted to connect to a communication network, the method comprising:

at the wireless communication apparatus,

transmitting a user identifier that is used to determine whether or not to permit a connection to the communication network to the account management apparatus through the base station;

at the account management apparatus,

generating code information that is used to set a wireless parameter for performing wireless communication between the wireless communication apparatus and the base station, based on authentication information that corresponds to the user identifier transmitted from the wireless communication apparatus and code generation information, and

transmitting the generated code information and the code generation information to the base station;

at the base station,

storing the code information transmitted from the account management apparatus and transmitting code generation information to the wireless communication

apparatus;

at the wireless communication apparatus,

generating code information based on the code generation information transmitted from the base station and the authentication information corresponding to the user identifier transmitted to the account management apparatus;

at the base station,

checking whether or not the stored code information and the code information generated by the wireless communication apparatus match, and

providing the wireless parameter to the wireless communication apparatus and notifying the account management apparatus of success in setting the wireless parameter, when it is confirmed that the stored code information and the code information generated by the wireless communication apparatus match; and

at the account management apparatus,

permitting the wireless communication apparatus to connect to the communication network, when success in setting the wireless parameters is notified from the base station.

2. A wireless communication apparatus that connects to a communication network through a wireless network, the apparatus comprising:

transmission means for transmitting a user

identifier that is used to determine whether or not to permit a connection to the communication network to an account management apparatus through a base station;

reception means for receiving code generation information transmitted from the account management apparatus through the base station;

generation means for generating code information using the received code generation information and authentication information that corresponds to the user identifier transmitted to the account management apparatus; and

acquisition means for acquiring a parameter of the wireless network from the base station by using the generated code information.

3. The apparatus according to claim 2, wherein the code generation information is a numerical value generated at random or character string information.

4. The apparatus according to claim 2, wherein the code generation information is information indicative of time.

5. The apparatus according to claim 4, further comprising setting means for setting a validity period for the code information based on the code generation information.

6. A base station that performs wireless communication with a wireless communication apparatus, the base station comprising:

reception means for receiving a user identifier that is used to determine whether or not to permit a connection to a communication network from the wireless communication apparatus;

transfer means for transferring the user identifier to an account management apparatus;

acquisition means for acquiring, from the account management apparatus, code information that is used to set a wireless parameter for performing wireless communication between the wireless communication apparatus and the base station, and code generation information;

transmission means for transmitting the acquired code generation information to the wireless communication apparatus;

checking means for checking whether or not code information generated based on the code generation information by the wireless communication apparatus and the code information acquired from the account management apparatus match;

provision means for providing the wireless parameter to the wireless communication apparatus when it is confirmed that the generated code information and

the acquired code information match; and

notification means for notifying the account management apparatus of success in setting the wireless parameter, when it is confirmed that the generated code information and the acquired code information match.

7. The base station according to claim 6, wherein the code generation information is a numerical value generated at random or character string information.

8. The base station according to claim 6, wherein the code generation information is information indicative of time.

9. The base station according to claim 8, further comprising setting means for setting a validity period for the code information based on the code generation information.

10. An account management apparatus that manages user account information of a user permitted to connect to a communication network, the apparatus comprising:

reception means for receiving a user identifier that is used to determine whether or not to permit a connection to the communication network from a wireless communication apparatus through a base station;

generation means for generating code information

that is used to set a wireless parameter for performing wireless communication between the wireless communication apparatus and the base station using authentication information that corresponds to the user identifier and code generation information;

transmission means for transmitting the code information and the code generation information to the base station;

reception means for receiving a success notification indicating success in setting the wireless parameters from the base station; and

permitting means for permitting the wireless communication apparatus to connect to the communication network when the success notification is received.

11. The apparatus according to claim 10, wherein the code generation information is a numerical value generated at random or character string information.

12. The apparatus according to claim 10, wherein the code generation information is information indicative of time.

13. The apparatus according to claim 12, further comprising setting means for setting a validity period for the code information based on the code generation information.

14. A program for causing a computer to function as the wireless communication apparatus according to claim 2.

15. A program for causing a computer to function as the base station according to claim 6.

16. A program for causing a computer to function as the account management apparatus according to claim 10.

17. A computer-readable recording medium in which any one of the programs according to claims 14 to 16 is recorded.

FIG. 1

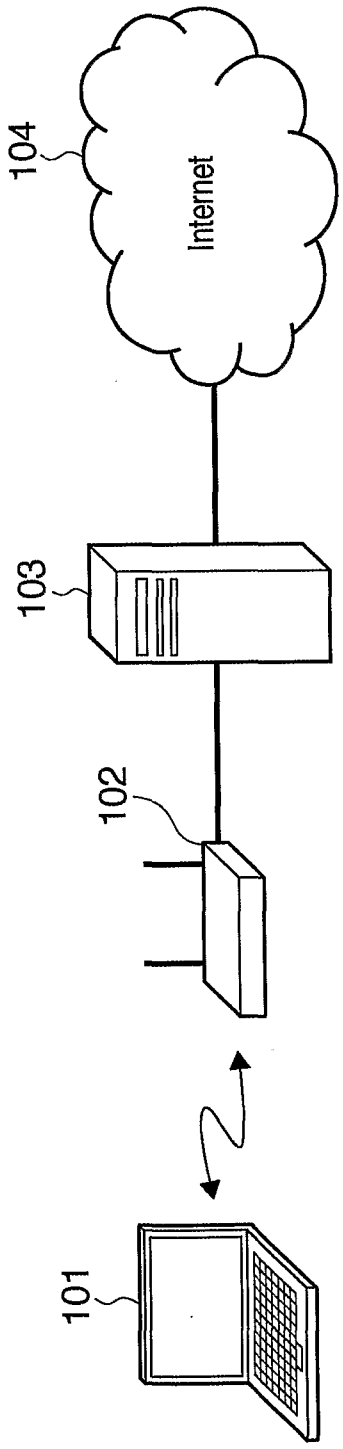


FIG. 2

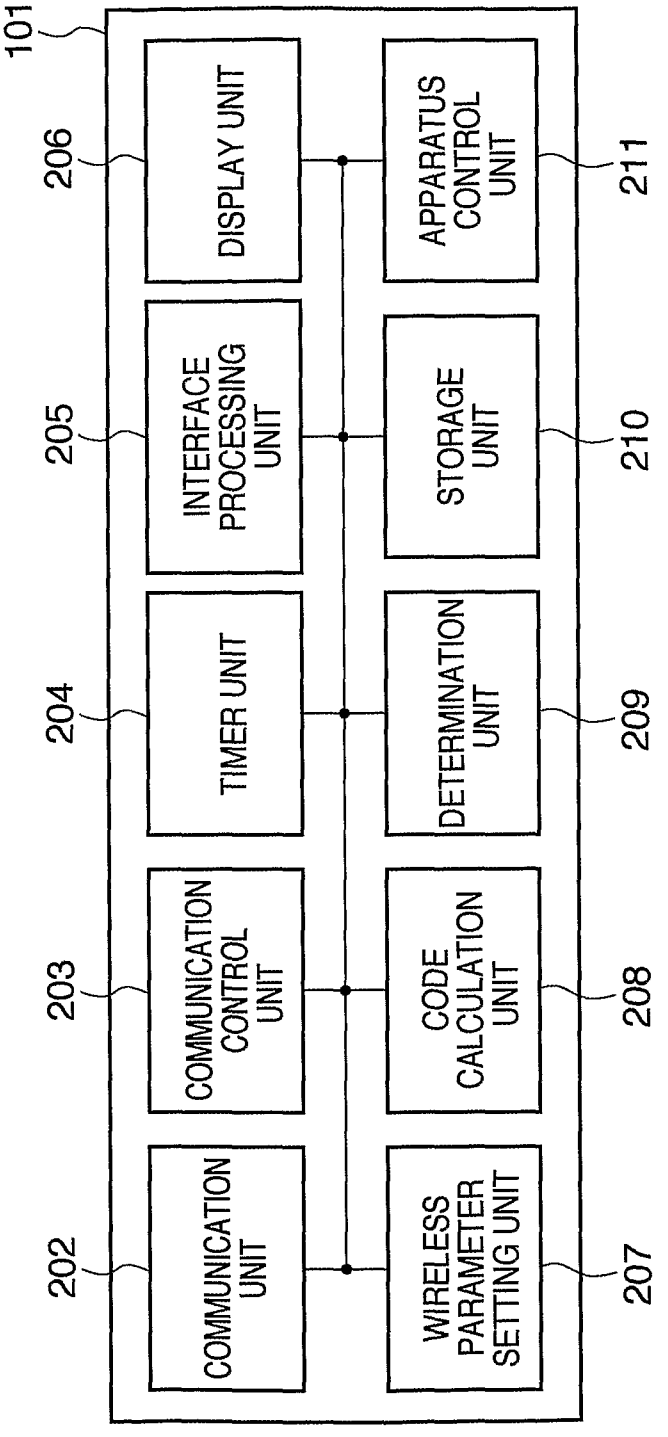

101
206
DISPLAY UNIT
APPARATUS CONTROL UNIT
211
205
INTERFACE PROCESSING UNIT
STORAGE UNIT
210
204
TIMER UNIT
DETERMINATION UNIT
209
203
COMMUNICATION CONTROL UNIT
CODE CALCULATION UNIT
208
202
COMMUNICATION UNIT
WIRELESS PARAMETER SETTING UNIT
207

FIG. 3

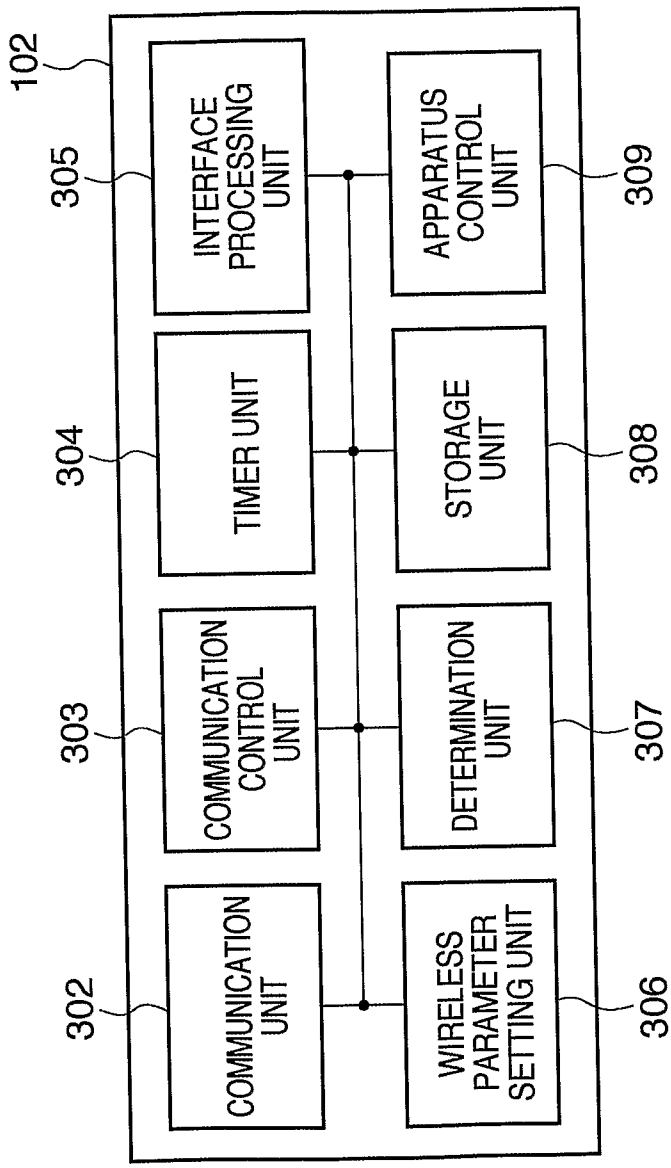

102
305
INTERFACE PROCESSING UNIT
309
APPARATUS CONTROL UNIT
304
TIMER UNIT
308
STORAGE UNIT
303
COMMUNICATION CONTROL UNIT
307
DETERMINATION UNIT
302
COMMUNICATION UNIT
306
WIRELESS PARAMETER SETTING UNIT

FIG. 4

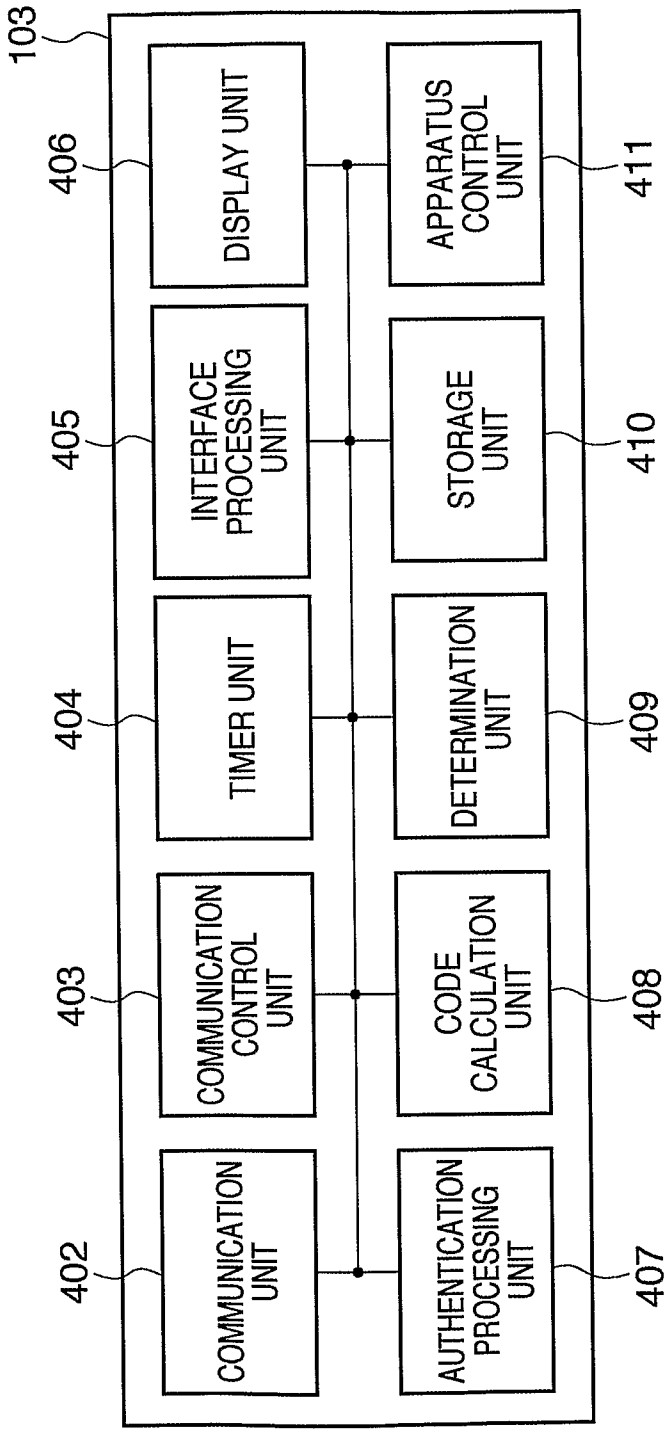

103
406
DISPLAY UNIT
411
APPARATUS CONTROL UNIT
405
INTERFACE PROCESSING UNIT
410
STORAGE UNIT
404
TIMER UNIT
409
DETERMINATION UNIT
403
COMMUNICATION CONTROL UNIT
408
CODE CALCULATION UNIT
402
COMMUNICATION UNIT
407
AUTHENTICATION PROCESSING UNIT

FIG. 5

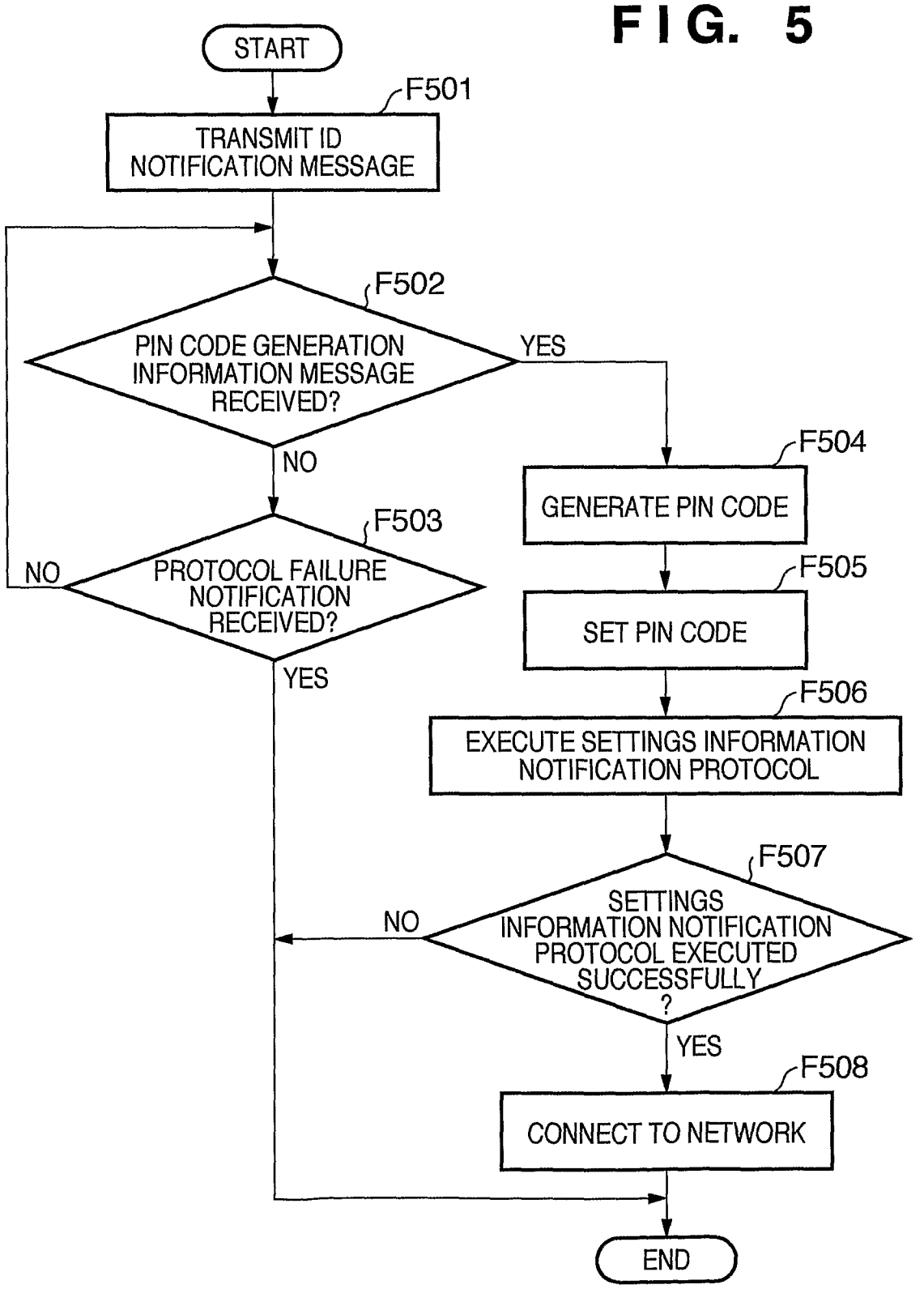

START
F501
TRANSMIT ID NOTIFICATION MESSAGE
F502
PIN CODE GENERATION INFORMATION MESSAGE RECEIVED?
YES
NO
F503
PROTOCOL FAILURE NOTIFICATION RECEIVED?
NO
YES
F504
GENERATE PIN CODE
F505
SET PIN CODE
F506
EXECUTE SETTINGS INFORMATION NOTIFICATION PROTOCOL
F507
SETTINGS INFORMATION NOTIFICATION PROTOCOL EXECUTED SUCCESSFULLY ?
NO
YES
F508
CONNECT TO NETWORK
END

FIG. 6

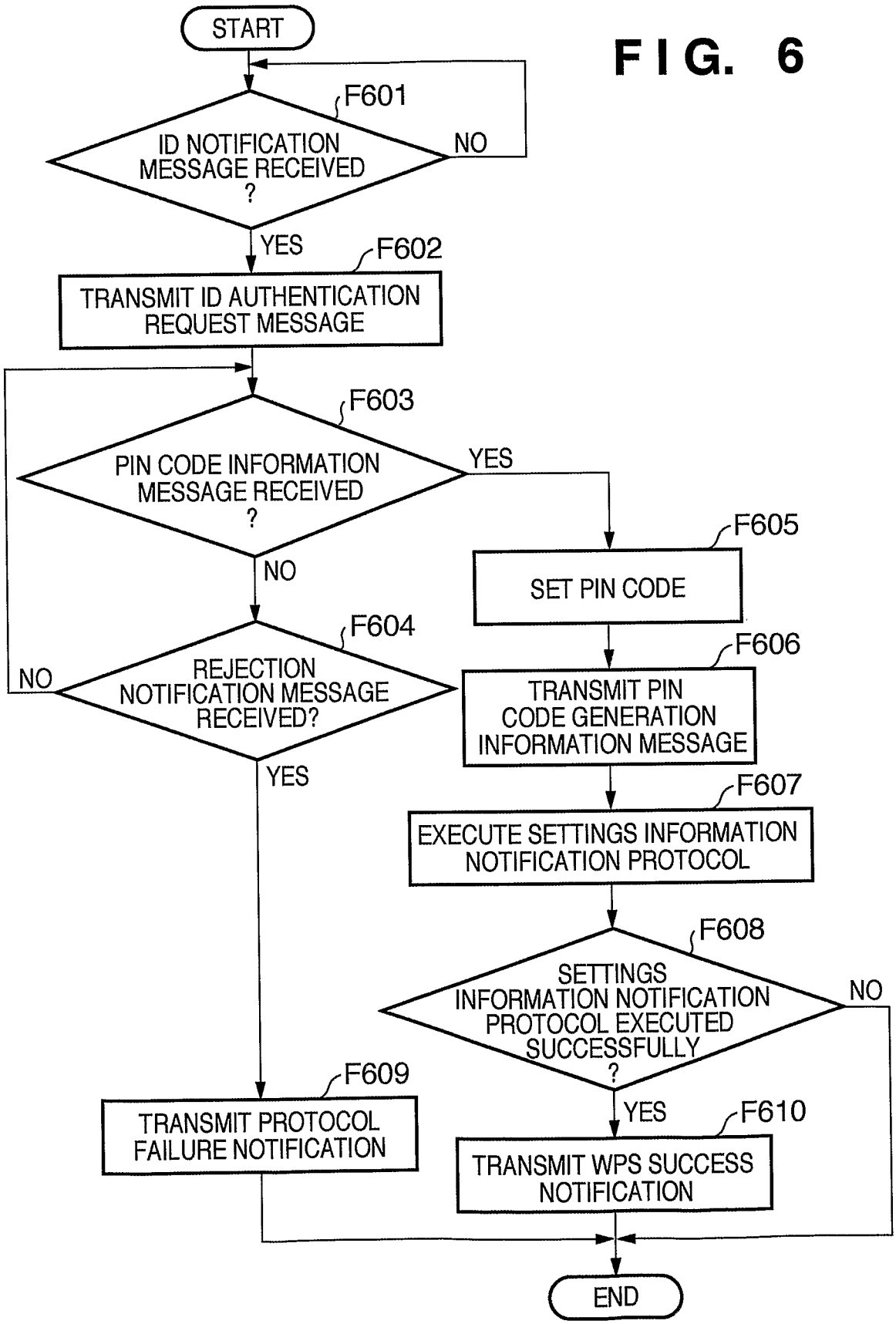

START
F601
ID NOTIFICATION MESSAGE RECEIVED ?
NO
YES
F602
TRANSMIT ID AUTHENTICATION REQUEST MESSAGE
F603
PIN CODE INFORMATION MESSAGE RECEIVED ?
YES
NO
F604
REJECTION NOTIFICATION MESSAGE RECEIVED?
NO
YES
F605
SET PIN CODE
F606
TRANSMIT PIN CODE GENERATION INFORMATION MESSAGE
F607
EXECUTE SETTINGS INFORMATION NOTIFICATION PROTOCOL
F608
SETTINGS INFORMATION NOTIFICATION PROTOCOL EXECUTED SUCCESSFULLY ?
NO
YES
F609
TRANSMIT PROTOCOL FAILURE NOTIFICATION
F610
TRANSMIT WPS SUCCESS NOTIFICATION
END

FIG. 7

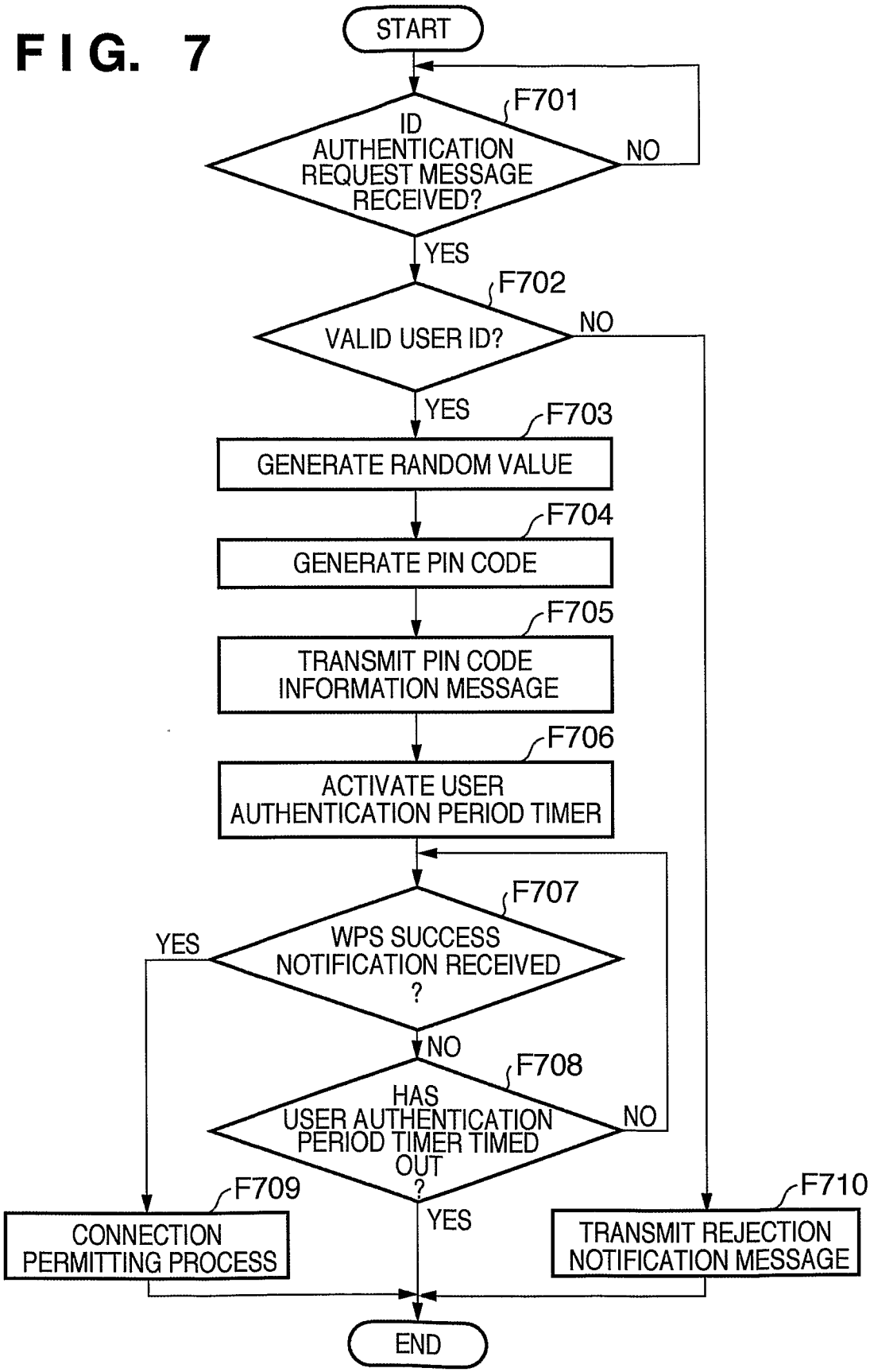

START
F701
ID AUTHENTICATION REQUEST MESSAGE RECEIVED?
NO
YES
F702
VALID USER ID?
NO
YES
F703
GENERATE RANDOM VALUE
F704
GENERATE PIN CODE
F705
TRANSMIT PIN CODE INFORMATION MESSAGE
F706
ACTIVATE USER AUTHENTICATION PERIOD TIMER
F707
WPS SUCCESS NOTIFICATION RECEIVED ?
YES
NO
F708
HAS USER AUTHENTICATION PERIOD TIMER TIMED OUT ?
NO
YES
F709
CONNECTION PERMITTING PROCESS
F710
TRANSMIT REJECTION NOTIFICATION MESSAGE
END

FIG. 8

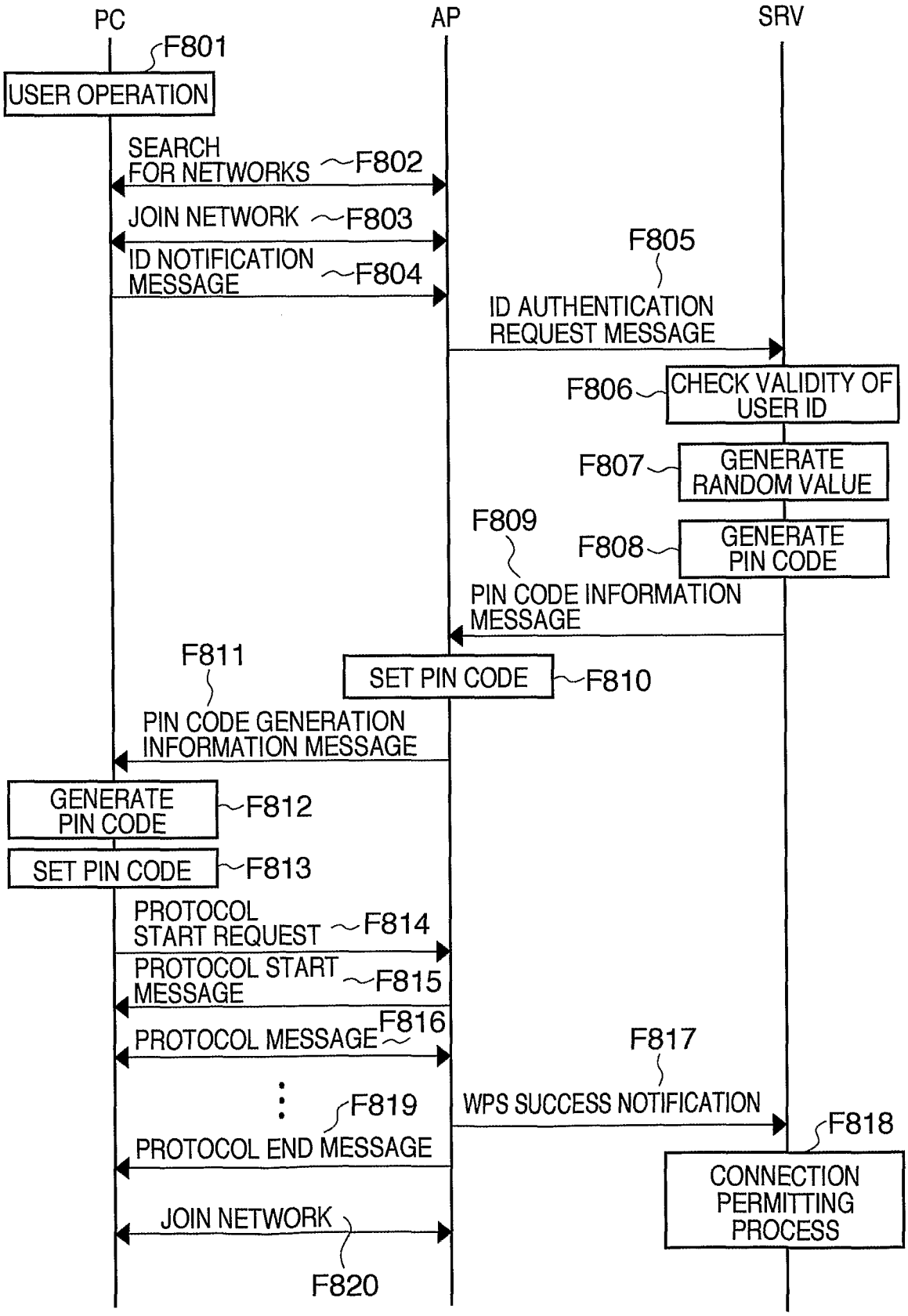

PC
AP
SRV
F801
USER OPERATION
SEARCH FOR NETWORKS
F802
JOIN NETWORK
F803
ID NOTIFICATION MESSAGE
F804
F805
ID AUTHENTICATION REQUEST MESSAGE
F806
CHECK VALIDITY OF USER ID
F807
GENERATE RANDOM VALUE
F809
F808
GENERATE PIN CODE
PIN CODE INFORMATION MESSAGE
F811
SET PIN CODE
F810
PIN CODE GENERATION INFORMATION MESSAGE
GENERATE PIN CODE
F812
SET PIN CODE
F813
PROTOCOL START REQUEST
F814
PROTOCOL START MESSAGE
F815
PROTOCOL MESSAGE
F816
F817
F819
WPS SUCCESS NOTIFICATION
F818
PROTOCOL END MESSAGE
CONNECTION PERMITTING PROCESS
JOIN NETWORK
F820

FIG. 9

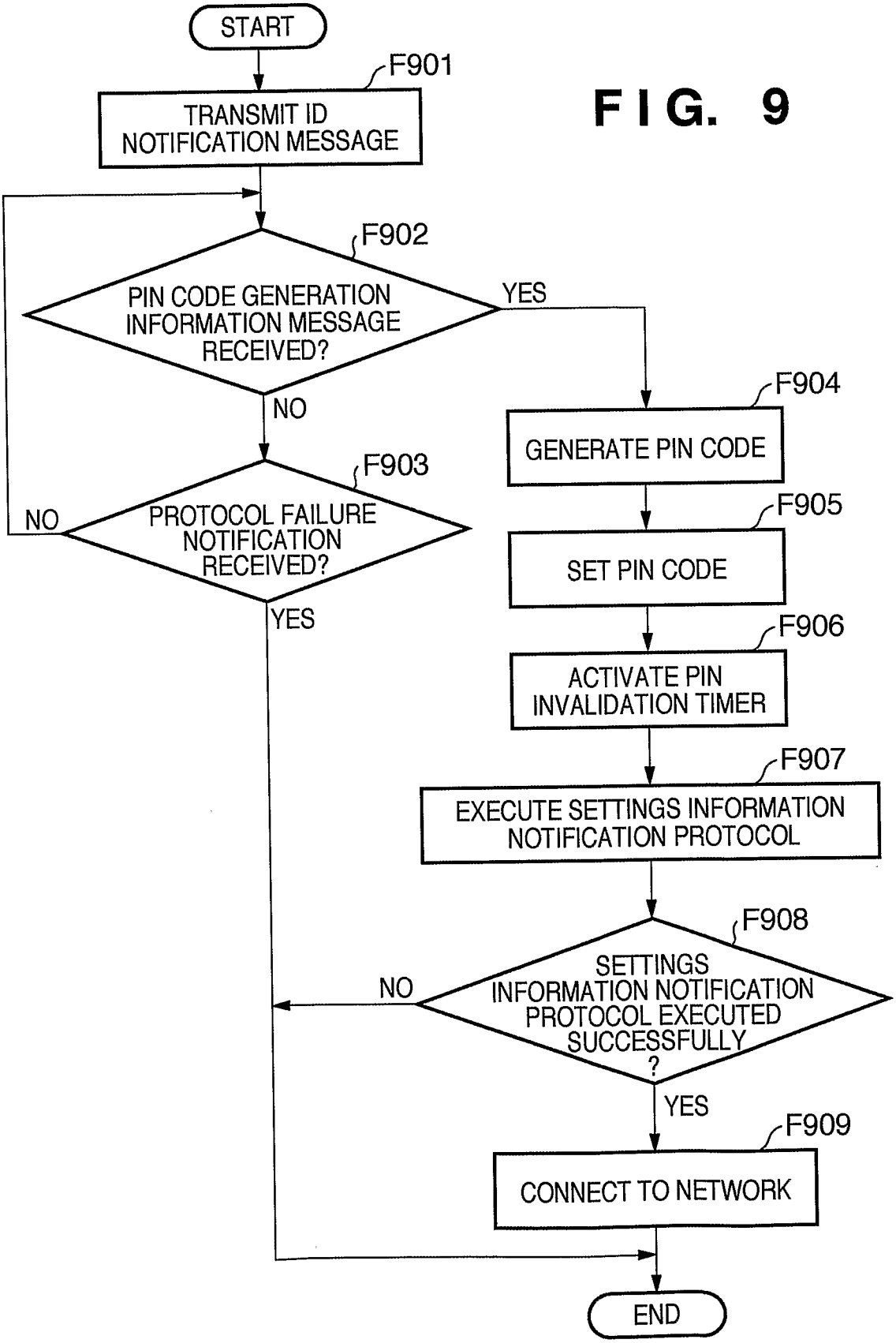

START
F901
TRANSMIT ID NOTIFICATION MESSAGE
F902
PIN CODE GENERATION INFORMATION MESSAGE RECEIVED?
YES
NO
F903
PROTOCOL FAILURE NOTIFICATION RECEIVED?
NO
YES
F904
GENERATE PIN CODE
F905
SET PIN CODE
F906
ACTIVATE PIN INVALIDATION TIMER
F907
EXECUTE SETTINGS INFORMATION NOTIFICATION PROTOCOL
F908
SETTINGS INFORMATION NOTIFICATION PROTOCOL EXECUTED SUCCESSFULLY ?
NO
YES
F909
CONNECT TO NETWORK
END

FIG. 10

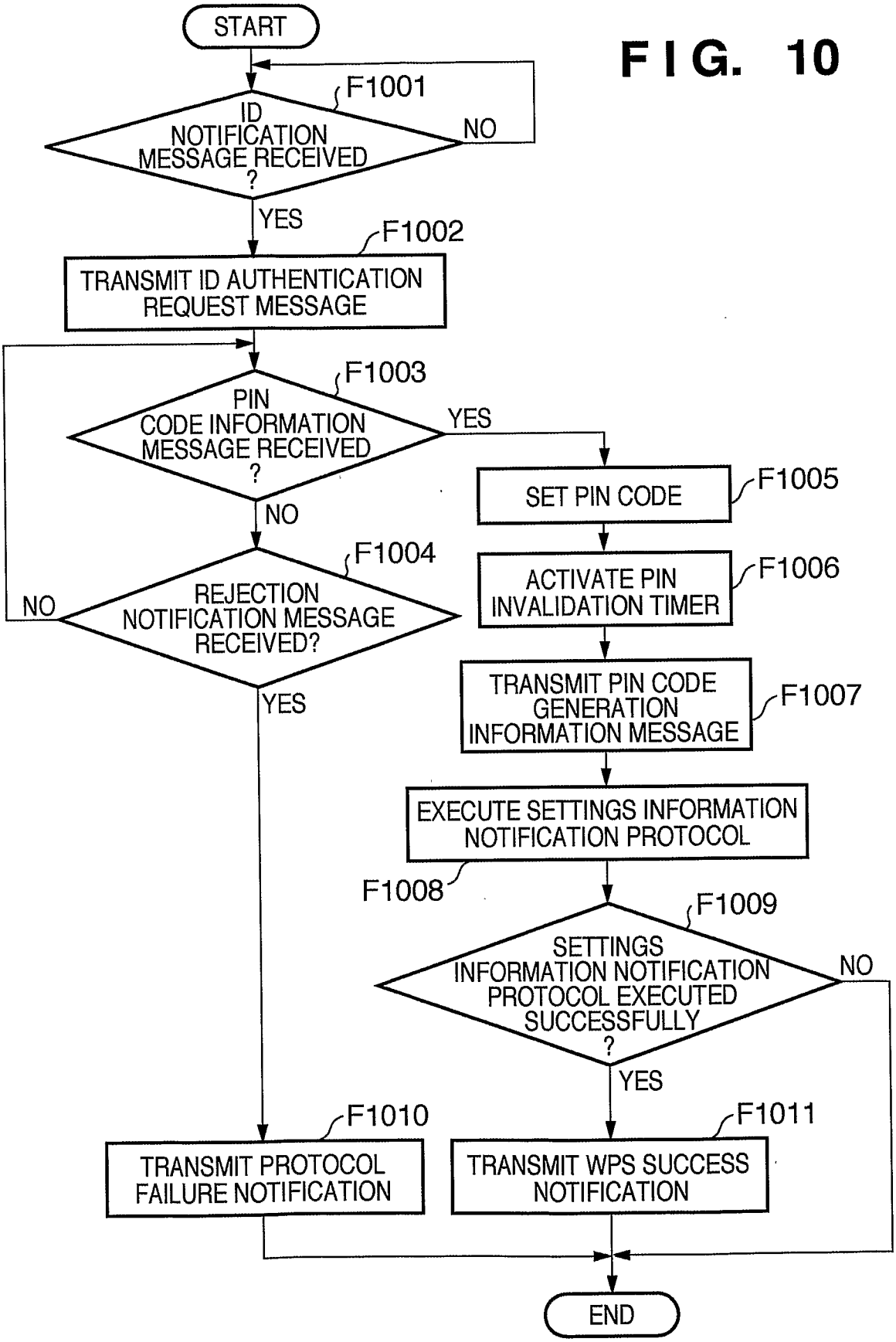

START
F1001
ID NOTIFICATION MESSAGE RECEIVED ?
NO
YES
F1002
TRANSMIT ID AUTHENTICATION REQUEST MESSAGE
F1003
PIN CODE INFORMATION MESSAGE RECEIVED ?
YES
NO
F1004
REJECTION NOTIFICATION MESSAGE RECEIVED?
NO
YES
F1005
SET PIN CODE
F1006
ACTIVATE PIN INVALIDATION TIMER
F1007
TRANSMIT PIN CODE GENERATION INFORMATION MESSAGE
EXECUTE SETTINGS INFORMATION NOTIFICATION PROTOCOL
F1008
F1009
SETTINGS INFORMATION NOTIFICATION PROTOCOL EXECUTED SUCCESSFULLY ?
NO
YES
F1010
TRANSMIT PROTOCOL FAILURE NOTIFICATION
F1011
TRANSMIT WPS SUCCESS NOTIFICATION
END

FIG. 11

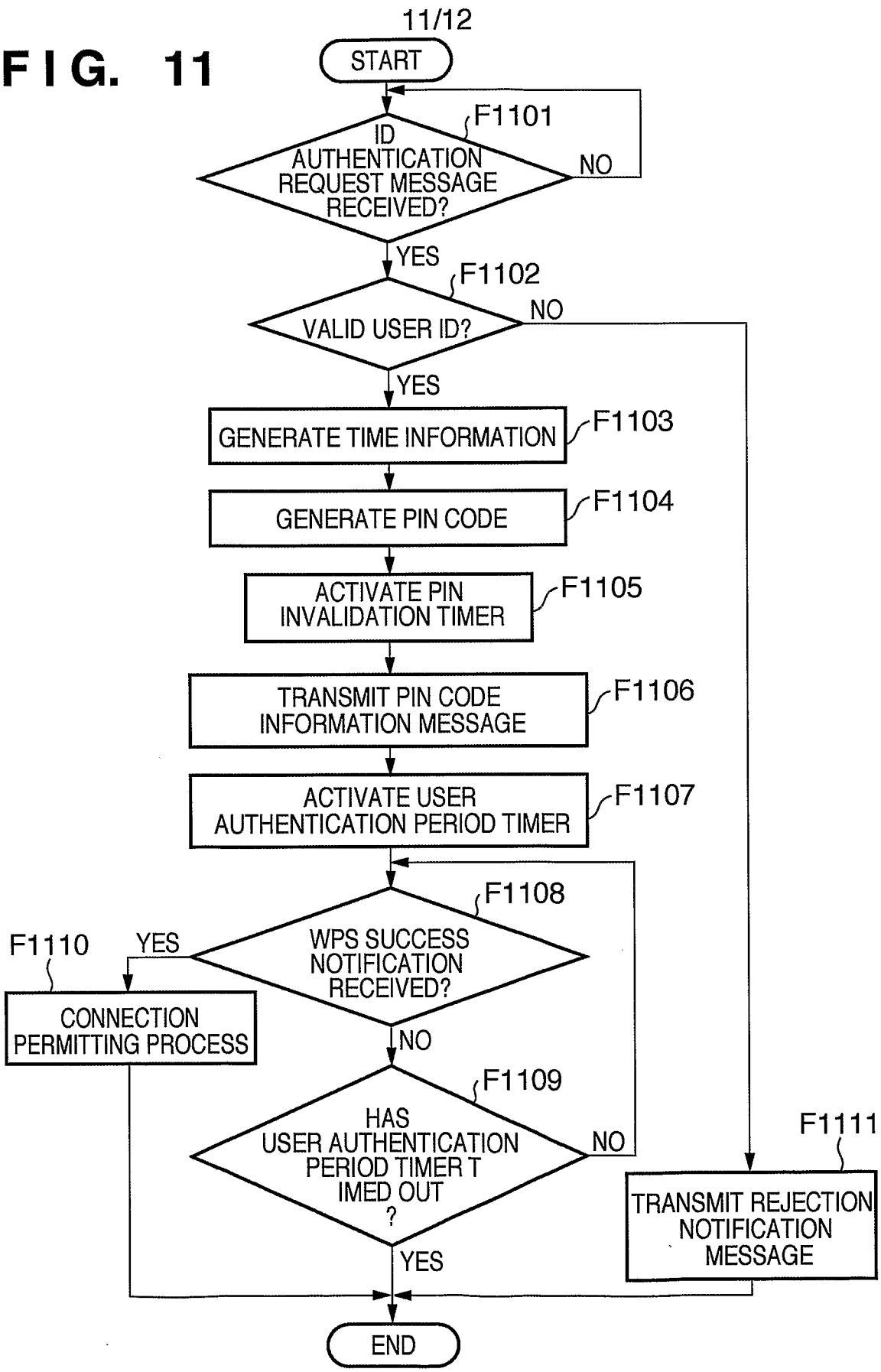
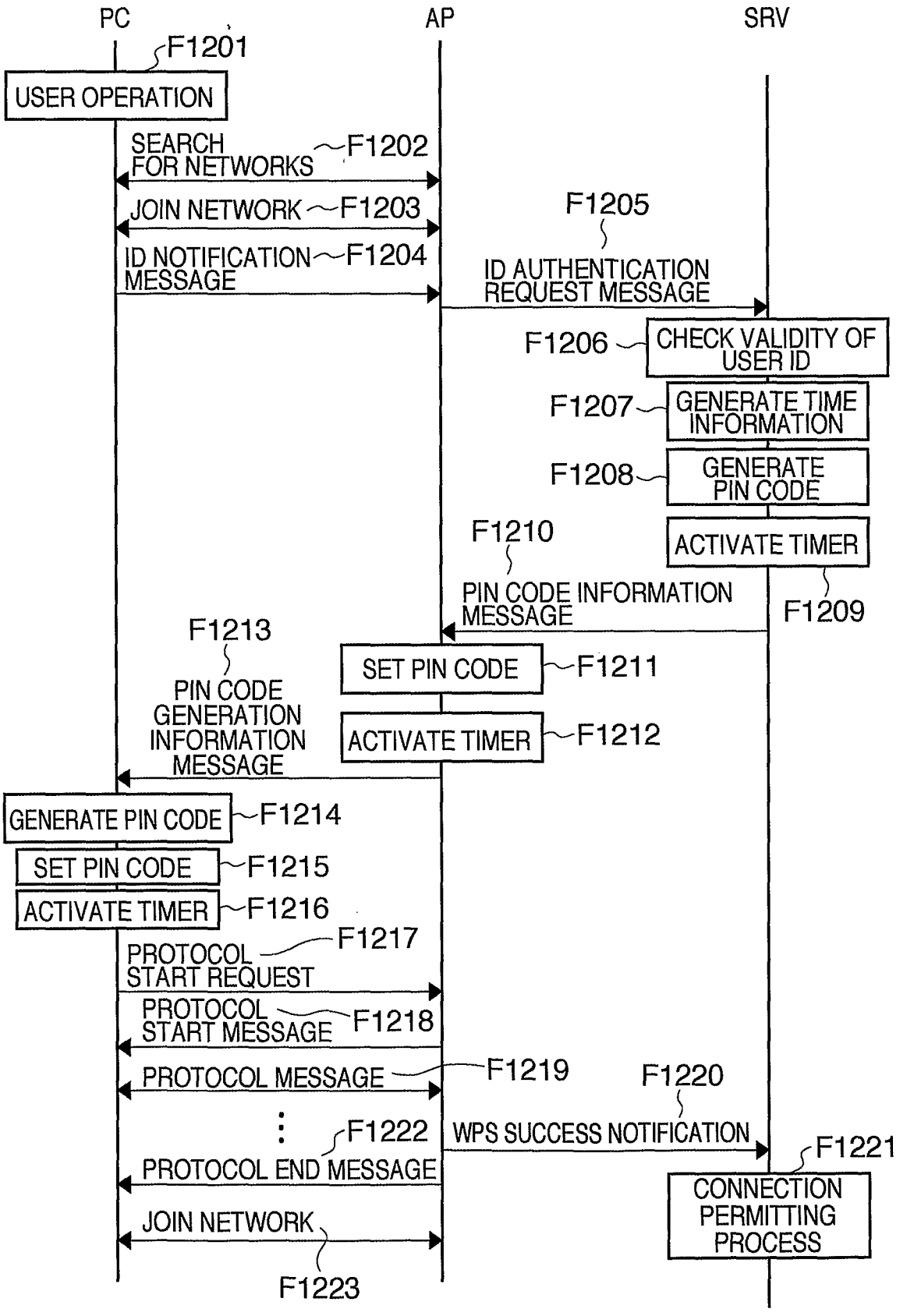

START
F1101
ID AUTHENTICATION REQUEST MESSAGE RECEIVED?
NO
YES
F1102
VALID USER ID?
NO
YES
GENERATE TIME INFORMATION
F1103
GENERATE PIN CODE
F1104
ACTIVATE PIN INVALIDATION TIMER
F1105
TRANSMIT PIN CODE INFORMATION MESSAGE
F1106
ACTIVATE USER AUTHENTICATION PERIOD TIMER
F1107
F1108
WPS SUCCESS NOTIFICATION RECEIVED?
F1110
YES
CONNECTION PERMITTING PROCESS
NO
F1109
HAS USER AUTHENTICATION PERIOD TIMER T IMED OUT ?
NO
YES
F1111
TRANSMIT REJECTION NOTIFICATION MESSAGE
END

FIG. 12


PC
AP
SRV
F1201
USER OPERATION
SEARCH FOR NETWORKS
F1202
JOIN NETWORK
F1203
ID NOTIFICATION MESSAGE
F1204
F1205
ID AUTHENTICATION REQUEST MESSAGE
F1206
CHECK VALIDITY OF USER ID
F1207
GENERATE TIME INFORMATION
F1208
GENERATE PIN CODE
ACTIVATE TIMER
F1209
F1210
PIN CODE INFORMATION MESSAGE
F1213
PIN CODE GENERATION INFORMATION MESSAGE
SET PIN CODE
F1211
ACTIVATE TIMER
F1212
GENERATE PIN CODE
F1214
SET PIN CODE
F1215
ACTIVATE TIMER
F1216
PROTOCOL START REQUEST
F1217
PROTOCOL START MESSAGE
F1218
PROTOCOL MESSAGE
F1219
F1220
WPS SUCCESS NOTIFICATION
F1221
CONNECTION PERMITTING PROCESS
F1222
PROTOCOL END MESSAGE
JOIN NETWORK
F1223

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/056405

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04W12/06(2009.01)i, H04L9/32(2006.01)i, H04W12/08(2009.01)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)

Int.Cl. H04W12/06, H04L9/32, H04W12/08

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2009
Registered utility model specifications of Japan 1996-2009
Published registered utility model applications of Japan 1994-2009

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2005-269571 A (NIHON DENKI Corp.) 2005.09.29, Abstract, Claims 1-2, Fig.2 (Family: none)	1-17
A	JP 2002-55955 A (DoCoMo SYSTEMS Inc.) 2002.02.20, Whole document (Family: none)	1-17

☐ 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
07.05.2009	19.05.2009

Name and mailing address of the ISA/JP	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Takahiko TOYAMA Telephone No. +81-3-3581-1101 Ext. 3534

5J 9855