

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

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
21 December 2006 (21.12.2006)

PCT

(10) International Publication Number
WO 2006/134772 A1

(51) International Patent Classification:
H04L 12/28 (2006.01)

(21) International Application Number:
PCT/JP2006/310833

(22) International Filing Date: 24 May 2006 (24.05.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2005-172968 13 June 2005 (13.06.2005) JP

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

(72) Inventor; and

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

(74) Agent: OHTSUKA, Yasunori; 7th FL., Shuwa 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, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

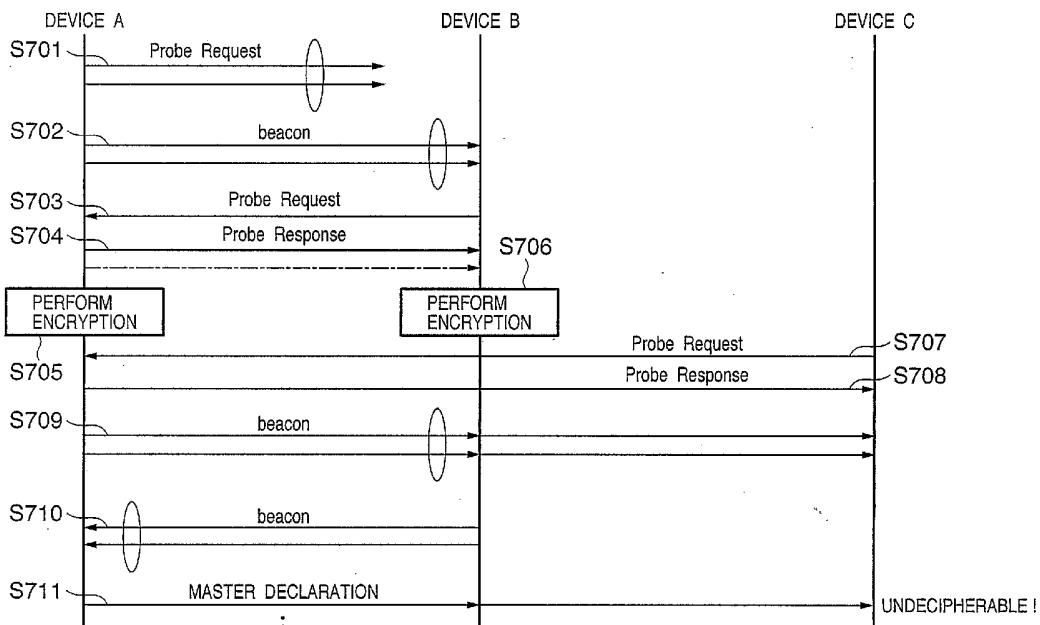
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, 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

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: COMMUNICATION APPARATUS AND COMMUNICATION PARAMETER CONFIGURATION METHOD THEREOF



(57) Abstract: A communication apparatus functioning as a master device denies participation by new communication apparatuses in a network in communication parameter configuration mode based on participation statuses of communication apparatuses functioning as slave devices in the network. The communication apparatus functioning as a master device establishes the network in communication parameter configuration mode between the communication apparatuses participating in the network, and configures communication parameters.

WO 2006/134772 A1

DESCRIPTION

COMMUNICATION APPARATUS AND COMMUNICATION PARAMETER
CONFIGURATION METHOD THEREOF

5 TECHNICAL FIELD

The present invention relates to a communication apparatus and a communication parameter configuration method thereof.

10 BACKGROUND ART

In network devices, cables have been conventionally used as communication media. Recently, however, the use of wireless communication has become popular.

15 For instance, with IEEE 802.11x compliant wireless LANs, there are many configuration items that must be configured prior to use, making such wireless LANs cumbersome and complicated. Consequently, various manufacturers have proposed mechanisms enabling easy
20 configuration of wireless communication parameters such as SSIDs (Service Set Identifiers) or encryption methods.

For example, one such mechanism is disclosed in U.S Patent Application Publication No. 2003-100335
25 (Japanese Patent Laid-Open No. 2003-163668). This document proposes a mechanism for configuring wireless communication parameters using an ad hoc network

- 2 -

wherein wireless communication devices communicate directly with each other in a wireless LAN without accessing an access point (base station).

When configuring wireless communication parameters
5 using wireless communication, such configuration essentially requires strengthening countermeasure against spoofing by third parties who do not need to know such configuration information or third parties with malicious intent.

10

DISCLOSURE OF INVENTION

The present invention has been made in light of the above problems, and an object of the present invention is to strengthen responses against spoofing
15 by third parties by imposing certain restrictions when establishing a communication parameter configuration network. Another object of the present invention is to reduce transmission of communication parameters to unnecessary devices. Other objects and features of the
20 present invention will become apparent through the following description and the accompanying drawings.

The present invention comprises: a denial step of denying participation of new communication apparatuses in a network in communication parameter configuration
25 mode, based on participation statuses of communication apparatuses to participate in the network; and a communication parameter configuration step of

establishing the network in communication parameter configuration mode between communication apparatuses participating in the network to configure communication parameters.

5 In addition, the present invention comprises: a denial step of denying participation of new communication apparatuses in a network in communication parameter configuration mode, based on the capability information of communication apparatuses to participate
10 in the network; and a communication parameter configuration step of establishing the network in communication parameter configuration mode between communication apparatuses participating in the network to configure communication parameters.

15 Other features and advantages of the present invention will be apparent from the following description taken in conjunction with the accompanying drawings, in which like reference characters designate the same or similar parts throughout the figures
20 thereof.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a diagram showing a step of establishing a communication parameter configuration network in an
25 ad hoc network;

- 4 -

FIG. 2 is a diagram showing an example of a configuration of an ad hoc network of two wireless communication devices;

5 FIG. 3 is a schematic block diagram of an example of a configuration of a digital camera 200 (device A);

FIG. 4 is a schematic block diagram of an example of a configuration of a printer 201 (device B);

10 FIG. 5 is a diagram illustrating a sequence when two devices have communication parameter configuration control functions;

FIG. 6 is a diagram showing an example of a configuration of an ad hoc network of three wireless communication devices;

15 FIG. 7 is a diagram illustrating a sequence when three devices have communication parameter configuration control functions;

20 FIG. 8 is a flowchart showing processing performed by a device according to a first embodiment when establishing a communication parameter configuration network;

25 FIG. 9 is a diagram illustrating the sequence from a determination step for determining a master device having a communication parameter configuration control function to a device capability collection step, according to a second embodiment;

FIG. 10 is a flowchart showing processing of a master-side device having a communication parameter

configuration control function, according to the second embodiment;

FIG. 11 is a flowchart showing processing of a slave-side device having a communication parameter configuration control function, according to the second embodiment;

FIG. 12 is a diagram illustrating the sequence from a determination step for determining a master device having a communication parameter configuration control function to a device capability collection step, according to a third embodiment;

FIG. 13 is a diagram illustrating a sequence of three devices having communication parameter control functions from a determination step for determining a master device having a communication parameter configuration control function to a device capability collection step, when two slave devices have respectively transited to the device capability collection step;

FIG. 14 is a flowchart showing processing by a master-side device according to the third embodiment;

FIG. 15 is a diagram illustrating the sequence from a determination step for determining a master device having a communication parameter configuration control function to a device capability collection step, according to a fourth embodiment;

- 6 -

FIG. 16 is a flowchart showing processing of a master-side device having a communication parameter configuration control function, according to the fourth embodiment;

5 FIG. 17 is a diagram illustrating the sequence from a determination step for determining a master device having a communication parameter configuration control function to a device capability collection step, according to a fifth embodiment;

10 FIG. 18 is a flowchart showing processing of a master-side device having a communication parameter configuration control function, according to the fifth embodiment; and

15 FIG. 19 is a flowchart showing processing of a slave-side device having a communication parameter configuration control function, according to the fifth embodiment.

BEST MODE FOR CARRYING OUT THE INVENTION

20 A detailed description of the preferred embodiments for implementing the present invention will now be provided with reference to the drawings.

[First Embodiment]

First, a case where an ad hoc mode communication 25 parameter configuration network in an IEEE802.11 compliant wireless LAN is established between two wireless communication devices will be described.

FIG. 1 shows the steps for configuring communication parameters in ad hoc mode. The steps of FIG. 1 comprise six steps with respectively different purposes. The functions of each step will now be 5 briefly described.

<Communication parameter configuration network formation step 101>

In this step, processing is performed for forming a communication parameter configuration network between 10 devices A and B using ad hoc connection.

<Master device determination step 102>

In this step, processing is performed for determining which of the devices A and B will become a master device of the communication parameter 15 configuration network and which of the devices will become a slave device. In addition, each device will continuously perform processing for monitoring whether the other device exists on the same network. The master device collects capability information of slave 20 devices existing on the same network, and determines which device will transfer and which device will receive a communication parameter. In addition, the master device performs processing such as for transmitting information necessary for communication 25 parameter transfer, to the devices that have been determined. The slave device transmits its own device capability in response to a device capability

transmission request transmitted from the master device. In addition, the slave device performs processing such as for configuring communication parameters, according to instructions from the master device, with devices 5 indicated in the instructions.

<Device capability collection step 103>

In this step, the master device determined in step 102 performs processing for collecting device capability attribute values owned by the slave devices 10 existing on the same network by making inquiries to the slave devices.

<Communication parameter transfer direction determination step 104>

In this step, the master device compares its own 15 device capability attribute values with those of each slave device collected by the master device in step 103. The master device determines which device will be the source of communication parameter transfer and which device will be its destination, and also transfers 20 information necessary for communication parameter transfer, such as destination or source information, to each slave device.

<Communication parameter transfer step 105>

In this step, communication parameters are 25 transferred from a device that is actually capable of providing communication parameters to a device that is actually capable of receiving communication parameters

in the communication parameter transfer direction determined in step 104.

<Communication parameter configuration network termination step 106>

5 In this step, prompted by the termination of the transfer of step 105, processing necessary to terminate the communication parameter configuration network will be performed. After the conclusion of the communication parameter configuration network 10 termination step 106, a new network will be established using communication parameters transferred in the communication parameter transfer step 105.

15 By performing the above six steps, communication parameters can be easily configured in ad hoc wireless communication.

The processing described below is the processing starting at the communication parameter configuration network formation step 101 and ending at the master device determination step 102, as shown in FIG. 1.

20 FIG. 2 is a diagram showing an example of a configuration of an ad hoc network of two wireless communication devices. In FIG. 2, a wireless communication device A is a digital camera 200 having an IEEE 802.11x compliant wireless LAN as its wireless 25 communication function 210, and becomes capable of establishing a network in communication parameter configuration mode when a communication parameter

- 10 -

configuration button 220 is pressed. In addition, a wireless communication device B is a printer 201 having an IEEE 802.11x compliant wireless LAN as its wireless communication function 211, and becomes capable of 5 establishing a network in communication parameter configuration mode when a communication parameter configuration button 221 is pressed.

Ad hoc mode wireless communication parameter configuration is performed between the digital camera 10 200 (device A) and the printer 201 (device B).

The configurations of the digital camera 200 (device A) and the printer 201 (device B) will now be described using FIGS. 3 and 4.

FIG. 3 is a schematic block diagram showing an 15 example of a configuration of the digital camera 200 (device A). In FIG. 3, reference numeral 301 denotes a control section that controls the digital camera 200, 302 denotes an image processing section, 303 denotes a ROM storing control instructions (programs) and control 20 data, and 304 denotes a RAM. Configuration communication parameters for forming a communication parameter configuration network are stored in the RAM 304 in advance. 305 denotes a wireless communication processing section that performs communication control 25 for the wireless LAN. 306 denotes an antenna, and 307 an antenna control section.

Reference numeral 308 denotes an image capturing section that captures pixel signals inputted from a CCD 309. 310 denotes a card interface that controls a storage media card for storing captured images or 5 configuration information, while 311 denotes a display section for displaying error messages and the like. 312 denotes an operating section, and includes buttons for issuing instructions on shooting, playback and configuration. 313 denotes a power source section that 10 includes a secondary battery. 314 denotes a non-wireless communication interface, and comprises a wired interface such as USB or IEEE1394. 315 denotes a communication parameter configuration button, and activates communication parameter configuration.

15 FIG. 4 is a schematic block diagram showing an example of a configuration of the printer 201 (device B). In FIG. 4, reference numeral 401 denotes a control section for controlling the printer 201, 402 denotes an image processing section, 403 denotes a ROM storing 20 control instructions (programs) and control data, 404 denotes a RAM, and 405 denotes a power source section. Configuration communication parameters for forming a communication parameter configuration network are stored in the RAM 404 in advance. 406 denotes a non-wireless communication interface, and comprises a wired 25 interface such as USB or IEEE1394.

Reference numeral 407 denotes a paper feeding/eject section to feed/eject paper for the printer. 408 denotes a printer engine that performs printing control using methods such as the electro-
5 photographic method or the inkjet method. 409 denotes a card interface that controls a storage media card storing images, while 410 denotes a display section. 411 denotes an operating section, and includes menu, configuration and other buttons. 412 denotes a
10 wireless communication processing section that performs communication control for the wireless LAN. 413 denotes an antenna, and 414 an antenna control section. 415 denotes a communication parameter configuration button that activates communication parameter
15 configuration.

The above-described hardware configuration is only one example of a preferred embodiment according to the present embodiment, and it is to be understood that the present invention is not limited to this hardware
20 configuration. Any hardware configuration to which the spirit of the present invention is applicable may be used.

In addition, while a digital camera and a printer have been described as wireless communication devices,
25 it is to be understood that the present invention is not limited to these devices, and may be applied to various devices such as personal computers (PCs),

facsimiles, multiple function machines, and notebook PCs.

The sequence of establishing a communication parameter configuration network when the communication 5 parameter configuration button 220 is first pressed on the digital camera 200 (device A), and the communication parameter configuration button 221 is next pressed on the printer camera 201 (device B) will now be described.

10 FIG. 5 is a diagram illustrating a sequence when two devices have communication parameter configuration control functions. First, when a user presses the communication parameter configuration button 220 of the digital camera 200 (device A) to activate its 15 communication parameter configuration function, the device A initiates formation of a communication parameter configuration network. This prompts the device A to transmit a probe request (S501) to a wireless segment. In the example shown in FIG. 5, 20 since a wireless device does not yet exist in the neighborhood, the device A transmits a beacon (S502) and becomes an IBSS (independent basic service set) creator of an ad hoc network.

Next, as the device B is activated in the same 25 manner as with the device A, the device B transmits a probe request (S503). Since the device A already exists as an IBSS creator, a probe response (S504) is

sent from the device A towards the device B in response to the probe request. A communication parameter configuration network is thereby formed between the devices A and B.

5 Once a communication parameter configuration network is formed, the devices A and B perform encryption (S505 and S506). Encryption algorithms are not specifically prescribed. For instance, the encryption processing may be performed based on a 10 common key stored in advance in the devices. Additionally, the encryption processing may be performed by either wireless communication processing sections 305 and 412, or by control sections 301 and 401.

15 The master device determination step 102 shown in FIG. 1 is now commenced. In this case, the IBSS creator and a joiner both continue to mutually transmit beacons (S507 and S508). Then, when a predetermined algorithm determines one of the devices as the master 20 device, a master declaration (S509) is transmitted from the master device.

Since communication between the devices A and B have been encrypted by the above steps S505 and S506, all communication from this master device determination 25 step 102 and onwards will be securely performed.

Processing for performing encryption while establishing an ad hoc mode communication parameter

configuration network with an IEEE 802.11x compliant wireless LAN between three wireless communication devices, and preventing network participation by unexpected devices will now be described.

5 FIG. 6 is a diagram showing an example of a configuration of an ad hoc network of three wireless communication devices. As shown in FIG. 6, wireless communication devices A and B are respectively the digital camera 200 and the printer 201 shown in FIG. 2.

10 A device C is a digital camera 600 similar to the device A having an IEEE 802.11x compliant wireless LAN as its wireless communication function 610, and becomes capable of establishing a network in communication parameter configuration mode by pressing a

15 communication parameter configuration button 620.

The configuration of the digital camera 600 (device C) is the same as the configuration of the digital camera 200 (device A) shown in FIG. 3, and therefore will not be described here.

20 First, the communication parameter configuration button 220 is pressed on the digital camera 200 (device A). The communication parameter configuration button 221 is next pressed on the printer 201 (device B), thereby establishing an ad hoc mode communication

25 parameter configuration network. A sequence initiated when the communication parameter configuration button

- 16 -

620 on the digital camera 600 (device C) is pressed will now be described.

FIG. 7 is a diagram illustrating a sequence when three devices have communication parameter 5 configuration control functions. First, a communication parameter configuration network is established (Steps S701 to S706) in the same way as the formation of a communication parameter configuration network between the devices A and B (Steps S501 to 10 S506) as shown in FIG. 5.

At this point, power of the device C, which is an unexpected third device, is activated. The device C initiates its communication parameter configuration function in the same way as the devices A and B. The 15 device C transmits a probe request (S707), and since the device A already exists as an IBSS creator, a probe response (S708) is transmitted from the device A towards the device C as a response to the probe request. The device C thereby participates in the communication 20 parameter configuration network.

However, because the device C is an unexpected third party, encryption has not yet been performed as between the devices A and B. Therefore, after establishment of the communication parameter 25 configuration network, the device C is unable to recognize a master declaration (S711) from the master

device determined by the master device determination step 102.

As seen, by performing encryption on communication, participation by unexpected third party devices to the 5 communication parameter configuration network can be prevented.

Next, using FIG. 8, a sequence (FIG. 7) of establishing a communication parameter configuration network between the devices A, B and C will be 10 described from the viewpoint of the processing performed by the devices.

FIG. 8 is a flowchart showing processing performed by a device according to a first embodiment when establishing a communication parameter configuration 15 network. First, when either power or a wireless communication function is activated at the device, a random timer is activated, and the device waits for time-out of the timer (S801). This processing is performed to avoid conflicts among probe requests 20 generated when a plurality of devices are simultaneously turned on. When the random timer times out, the device transmits a probe request (S802). The device next waits for a response to the probe request (S803).

25 Next, when a probe response is transmitted in response to the probe request (response transmitted in S803), the device is configured as a joiner (S804). In

the case the device is a joiner, if the number of devices participating in the communication parameter configuration network is within a prescribed number, the device receives an encryption instruction from the 5 IBSS creator. At this point, when an encryption instruction is received (YES in S805), the device, namely device B, enables encryption (S806).

Meanwhile, when an encryption instruction is not received (NO in S805), this means that the device was 10 unable to participate in the communication parameter configuration network, and the processing terminates as is.

On the other hand, when a probe response is not transmitted in response to the probe request (no in 15 S803), it is determined that a communication parameter configuration network does not exist in the vicinity of this device. Thus, this device, namely device A, performs configuration as an IBSS creator (S807). Then, as a function of an IBSS creator, the device stands by 20 for probe requests from other devices (S808).

When the device configured as the IBSS creator acknowledges probe requests from other devices (YES in S808), the device transmits probe responses to the other devices (S809). At this point, the IBSS creator 25 memorizes the number of devices to which probe responses were transmitted, and determines whether the number of devices has reached a predetermined

prescribed number (S810). If the prescribed number has been reached (YES in S810), processing is terminated as is.

On the other hand, when the prescribed number has 5 not been reached (NO in S810), the IBSS creator issues encryption instructions to the joiners under the IBSS creator (S811). Next, when the encryption instructions have reached all intended destinations, the IBSS creator enables its own encryption (S812).

10 According to the first embodiment, the IBSS creator counts the number of devices participating in the communication parameter configuration network, and when the number of devices exceeds a prescribed number, ensures that encryption instructions are not 15 transmitted to any other device subsequently desiring to participate in the communication parameter configuration network. Thus, participation of third parties or third parties with malicious intent in the communication parameter configuration network can be 20 denied.

[Second Embodiment]

Next, a detailed description of a second embodiment according to the present invention will be provided with reference to the drawings. The first 25 embodiment prevented participation by third parties to a communication parameter configuration network by imposing restrictions on the number of participating

devices when establishing the communication parameter configuration network. The second embodiment prevents participation by third parties during the device capability collection step 103.

5 As shown in FIG. 6, processing for preventing participation to a network by an unexpected third party while two wireless communication devices perform communication parameter configuration will be described for the second embodiment.

10 FIG. 9 is a diagram illustrating the sequence from a determination step for determining a master device having a communication parameter configuration control function to a device capability collection step, according to the second embodiment. In FIG. 9, it is 15 assumed that the communication parameter configuration network formation step 101 of FIG. 1 has already been completed between the devices A and B, and that the device A is the IBSS creator, while devices B and C are joiners.

20 The device A transmits a master inquiry message (S901) as a broadcast message. At this point, the master device determination step 102 has just commenced and a master device does not yet exist. Thus, a response to the master inquiry message (S901) is not 25 transmitted.

Therefore, the device A configures itself as the master device, terminates transmission of the master

inquiry message (S901), and instead commences transmission of a master declaration message (S902). Upon transmitting the first master declaration message, an internally retained participation acceptance 5 condition is configured to "permit" (S903).

Next, after a lapse of a random interval, the device B transmits a master inquiry message (S904). At this time, the device A transmits a master declaration message (S905) once it acknowledges transmission of the 10 master inquiry message (S904) by the device B. On the other hand, upon receiving the master declaration message (S905) transmitted by the device A, the device B transmits a slave declaration message (S906).

Incidentally, in this example, it is assumed that 15 the prescribed number of devices to compose the communication parameter configuration network preconfigured in the device A is two.

When the device A receives the slave declaration message (S906) from the device B, the device A changes 20 its internally retained participation acceptance condition to "deny" (S907). Since the participation acceptance condition of the master device is now "deny", the processing of the device capability collection step 103 and onwards will be performed solely between the 25 devices A and B.

For instance, suppose a third device, device C, attempts to participate at this point. The device C

first transmits a master inquiry message (S908) in the same manner as the devices A and B. The device A, which has already assumed the role of the master device in this communication parameter configuration network, 5 receives the master inquiry message (S908) from the device C.

At this point, the device A references its internally retained participation acceptance condition. In this example, since the participation acceptance 10 condition has already been changed to "deny", the device A transmits a participation denial notification message (S909) to the device C. This participation denial notification message (S909) is transmitted only to the device C, while communication with the device B 15 continues. The device B periodically transmits a slave declaration message (S910) to the device A.

Following the above description on the sequence between the devices, processing performed by the master-side device and the slave-side device will now 20 be described. Description on the determination method of the master and slave devices of the master device determination step 102 will be omitted. First, the processing performed by the master-side device will be described using FIG. 10.

25 FIG. 10 is a flowchart showing processing of a master-side device having a communication parameter configuration control function, according to the second

embodiment. It is assumed that a device having a communication parameter configuration control function determines apparatus types already determined in the master device determination step 102, and acknowledges 5 that the device itself is the master-side device.

The master-side device receives master inquiry messages from the other network participating devices (S1001). Once the master inquiry messages are received, the master-side device references its internally 10 retained participation acceptance condition (S1002).

When the participation acceptance condition is "deny" (NO in S1002), participation denial notification messages are sent to the transmission source devices of the master inquiry messages (S1007), and communication 15 with the transmission source devices of the master inquiry messages is terminated.

On the other hand, when the participation acceptance condition is "permit" (YES in S1002), a number of slaves retained in a RAM 304 is added (S1003). 20 The added number of slaves is next determined whether it has reached an upper limit (S1004). When the number of slaves has reached the upper limit (YES in S1004), the master device changes the participation acceptance condition retained in the RAM 304 from "permit" to 25 "deny" (S1005). Due to this processing, all subsequent participation in the network by new slave devices can be denied.

Meanwhile, if the number of slaves has not reached the upper limit (NO in S1004), the participation acceptance condition remains unchanged. The master device performs exchange of the sequence of the next 5 device capability collection step 103 with the group of slave devices (S1006).

Following the above description on the processing by the master-side device, processing performed by the slave-side devices will now be described.

10 FIG. 11 is a flowchart showing processing of a slave-side device having a communication parameter configuration control function, according to the second embodiment. It is assumed that a device having a communication parameter configuration control function 15 determines apparatus types already determined in the master device determination step 102, and acknowledges that the device itself is a slave-side device.

The slave-side device transmits a master inquiry messages towards the master-side device (S1101). The 20 device next monitors whether a master declaration message will be transmitted from the master-side device (S1102). The slave-side device thereby acknowledges the existence of the master-side device.

The slave-side device next verifies whether a 25 participation denial notification message is transmitted from the master-side device (S1103). If a participation denial notification message is not

transmitted from the master-side device (NO in S1103), the slave-side device proceeds to determine whether a device capability transmission request will be transmitted (S1104). This determination processing is 5 performed because reception failure or the like of participation denial notifications due to factors such as propagation status of communication pathways can be anticipated.

When a device capability transmission request is 10 received, the slave-side device transmits (S1105) a device capability response towards the master-side device, which is the transmission source of the device capability transmission request.

On the other hand, when the slave-side device 15 either receives a participation denial notification message from the master-side device (YES in S1103), or does not receive a device capability transmission request (NO in S1104), the slave-side device determines that its participation in the communication parameter 20 configuration network has been denied. The slave-side device next terminates communication with the communication parameter configuration network, and terminates its wireless communication function.

Incidentally, when participation in the 25 communication parameter configuration network has been denied, the slave-side device can be arranged so as to display the participation denial via a user interface.

As seen, by performing the above-described series of processing, it is possible to limit the number of devices that can participate in the wireless parameter configuration network.

5 [Third Embodiment]

Next, a detailed description of a third embodiment according to the present invention will be provided with reference to the drawings. In the first and second embodiments, a state of participation of a 10 prescribed number of devices was described as the participation state of wireless devices participating in a communication parameter configuration network. In the third embodiment, a description will be provided on a case where participation to a communication parameter 15 configuration network is limited by time.

As shown in FIG. 6, processing for preventing participation to a network by an unexpected third party while two wireless communication devices perform communication parameter configuration will also be 20 described for the third embodiment.

FIG. 12 is a diagram illustrating the sequence from a determination step for determining a master device having a communication parameter configuration control function to a device capability collection step, 25 according to a third embodiment. In FIG. 12, it is assumed that the communication parameter configuration network formation step 101 of FIG. 1 has already been

completed between the devices A and B, and that the device A is the IBSS creator, while devices B and C are joiners.

5 The device A transmits a master inquiry message (S1201) as a broadcast message. At this point, the master device determination step 102 has just commenced and a master device does not yet exist. Thus, a response to the master inquiry message (S1201) will not be transmitted.

10 Therefore, the device A configures itself as the master device, terminates transmission of the master inquiry message (S1201), and instead commences transmission of a master declaration message (S1202).

15 Next, after a lapse of a random interval, the device B transmits a master inquiry message (S1203) as a broadcast message. At this time, the device A transmits a master declaration message (S1204) once it acknowledges transmission of the master inquiry message (S1203) by the device B. On the other hand, upon 20 receiving the master declaration message (S1204) transmitted by the device A, the device B transmits a slave declaration message (S1205).

25 When the device A receives the slave declaration message (S1205) from the device B, the device A commences the device capability collection step 103 shown in FIG. 1. In other words, the device A transmits a device capability collection request

(S1206), while master-side device simultaneously starting a participation acceptance timer. Transition of the status to the next communication parameter configuration direction determination step 104 is 5 achieved by receiving a device capability response (S1207) from the device B during the activation of the participation acceptance timer.

Afterwards, upon occurrence of a timeout of the participation acceptance timer (S1208), the device A 10 changes the participation acceptance status to "deny". This makes all subsequent, new participations in the communication parameter configuration network impossible.

At this point, for instance, if the device C 15 transmits a master inquiry message (S1209), the device A transmits a participation denial notification message (S1210) to the device C to deny its participation in this communication parameter configuration network.

Although FIG. 12 describes a case where a slave 20 device (device C) attempts participation when the devices A and B have already transited to the device capability collection step 103, the present invention is not limited to this example. For instance, the present invention can also be applied to a state where 25 two slave devices (devices B and C) already exist and have both transited to the device capability collection step 103.

FIG. 13 is a diagram illustrating a sequence where two slave devices have respectively transited to the device capability collection step. In FIG. 13, it is assumed that the communication parameter configuration 5 network formation step 101 of FIG. 1 has already been completed among the devices A, B and C, and that the device A is the IBSS creator, while devices B and C are joiners.

The device A transmits a master inquiry message 10 (S1301) as a broadcast message. At this point, the master device determination step 102 has just commenced and a master device does not yet exist. Thus, a response to the master inquiry message (S1301) will not be transmitted.

15 Therefore, the device A configures itself as the master device, terminates transmission of the master inquiry message (S1301), and instead commences transmission of a master declaration message (S1302).

Next, after a lapse of a random interval, the 20 device B transmits a master inquiry message (S1303) as a broadcast message. The device C also transmits a master inquiry message (S1304) in the same way as the device B. At this time, the device A transmits a master declaration message (S1305) once it acknowledges 25 transmission of the master inquiry messages (S1303 and S1304) from the devices B and C.

On the other hand, upon receiving the master declaration message (S1305) transmitted by the device A, the device B transmits a slave declaration message (S1306). The device C also transmits a slave declaration message (S1307), in the same way as the device B, upon receiving the master declaration message (S1305) transmitted by the device A.

Next, when the device A receives the slave declaration messages (S1306 and S1307) from the devices B and C, the device A commences the device capability collection step 103 shown in FIG. 1. In other words, the device A transmits a device capability collection request (S1308) as a broadcast transmission, while simultaneously starting a participation acceptance timer. Transition of the status to the next communication parameter configuration direction determination step 104 is achieved by receiving a device capability response (S1309) from the device B during the activation of the participation acceptance timer.

Afterwards, upon occurrence of a timeout of the participation acceptance timer (S1310), the device A changes the participation acceptance status to "deny". This makes all subsequent, new participations in the communication parameter configuration network impossible.

At this point, for instance, if the device C transmits a device capability response (S1311) after the participation acceptance timer has timed out, the device A transmits a participation denial notification 5 message (S1312) to the device C to deny its participation in this communication parameter configuration network.

In the third embodiment, while a case where only the device C times out has been described, 10 participation by the device B will also be denied in the case where the device B is only able to transmit a device capability response after the timeout.

Next, processing by the devices to achieve the above-described sequence will be describing using FIG. 15 14.

FIG. 14 is a flowchart showing processing by a master-side device according to the third embodiment. Since the processing by a slave-side device is identical to that in the second embodiment, a 20 description thereof will be omitted.

First, when a device having a communication parameter configuration control function determines itself to be the master-side device, the device performs initial configuration by configuring the 25 participation acceptance status to "permit" (S1401). The device next waits to receive master inquiries from other devices having communication parameter

configuration control functions that will become slave-side devices, and receives the master inquiries from the other devices (S1402). Next, upon receiving the master inquiries, the master-side device transmits a 5 master declaration to the transmission sources of the master inquiries (S1403).

On the other hand, the transmission source devices of the master inquiries determines themselves to be slave-side devices by receiving the master declaration, 10 and transmit slave declarations to the transmission source device of the master declaration. The master-side device that receives the slave declarations determines whether slave declarations have been received from one or more communication devices (S1404). 15 When slave declarations have not been received from one or more communication devices (NO in S1404), this means that there are no slave-side devices owned by the master-side device, and the master device returns processing to a master inquiry standby state (S1402) 20 until a slave-side device appears.

On the other hand, when slave declarations have been received from one or more devices (YES in S1404), the master-side device transmits a device capability transmission request (S1405). After transmission of 25 the device capability transmission request, a participation acceptance timer is initiated (S1406). Subsequently, after transmitting device capability

transmission request, when the master-side device receives device capability responses from the slave-side devices (S1407), the master-side device transits to the communication parameter transfer direction 5 determination step 104.

Afterwards, a timer value of the participation acceptance timer is determined. If the timer value has expired (YES in S1408), the participation acceptance status is changed to "deny" (S1409).

10 On the other hand, if the timer value has not expired (NO in S1408), processing once again transits to a master inquiry message reception standby state (S1402).

In the third embodiment, while the participation 15 acceptance timer has been configured so that it is activated after transmission of the device capability transmission request. However, the participation acceptance timer can also be configured so that it is activated upon participation by the first slave-side 20 device after establishing the communication parameter configuration network. In this case, it is sufficient to merely switch around S1405 and S1406 shown in FIG. 14.

In addition, the above-described participation 25 acceptance timer can also be configured to be activated immediately following the start of master declaration transmission and after S1403 shown in FIG. 14, instead

of during transmission of the device capability transmission request.

Moreover, it is also possible to expand function so that the participation acceptance period can be 5 extended at the discretion of the user upon expiration of the timer via a predetermined user interface.

As seen, in the third embodiment, acceptance of participation to a communication parameter configuration network is controlled by determining 10 whether device capability responses have been received within a certain period of time as the participation state of wireless devices participating in the network.

[Fourth Embodiment]

Next, a detailed description of a fourth 15 embodiment according to the present invention will be provided with reference to the drawings. In devices having communication parameter configuration controlling functions, in addition to the methods of the first to third embodiments described above, modes 20 for preventing participation by unnecessary devices in a communication parameter configuration network include, as a different perspective, a method according to device capabilities. The fourth embodiment determines device capabilities of devices attempting to 25 participate in a communication parameter configuration network as the participation statuses of communication devices participating in the network.

For the fourth embodiment, as shown in FIG. 6, processing for preventing participation to a network by an unexpected third party while two wireless communication devices perform communication parameter configuration will also be described.

FIG. 15 is a diagram illustrating the sequence from a determination step for determining a master device having a communication parameter configuration control function to a device capability collection step, according to a fourth embodiment. In FIG. 15, it is assumed that the communication parameter configuration network formation step 101 of FIG. 1 has already been completed between the devices A and B, and that the device A is the IBSS creator, while devices B and C are joiners.

The device A transmits a master inquiry message (S1501) as a broadcast message. At this point, the master device determination step 102 has just commenced and a master device does not yet exist. Thus, a response to the master inquiry message (S1501) will not be transmitted.

Therefore, the device A configures itself as the master device, terminates transmission of the master inquiry message (S1501), and instead commences transmission of a master declaration message (S1502).

Next, after a lapse of a random interval, the device B transmits a master inquiry message (S1503) as

a broadcast message. At this time, the device A transmits a master declaration message (S1504) once it acknowledges transmission of the master inquiry message (S1503) by the device B. On the other hand, upon 5 receiving the master declaration message (S1504) transmitted by the device A, the device B transmits a slave declaration message (S1505).

When the device A receives the slave declaration message (S1505) from the device B, the device A 10 commences the device capability collection step 103. In other words, the device A transmits a device capability transmission request (S1506). Meanwhile, upon receiving the device capability transmission request (S1506), the device B configures its own device 15 capability, and transmits a device capability response (S1507) to the device A.

The device A next receives the device capability response (S1507) from the device B, and matches it with device capability information retained in a RAM 304 to 20 determine whether the device B meets the device capability required by the device A. When it is determined that the device capability requirement is met, a communication parameter recipient request (S1508) is transmitted towards the device B. Upon 25 receiving the communication parameter recipient request, the device B stands by for communication parameters to be transferred from the communication parameter

provider in the communication parameter transfer step 105.

Next, after a lapse of a random interval, the device C transmits a master inquiry message (S1509).

5 Upon acknowledging the transmission of the master inquiry message by the device C, the device A transmits a master declaration message (S1510).

On the other hand, upon receiving the master declaration message (S1510) transmitted by the device A, 10 the device C transmits a slave declaration message (S1511).

When the device A receives the slave declaration message (S1511) from the device C, the device capability collection step 103 is initiated. In other 15 words, the device A transmits a device capability transmission request (S1512). Meanwhile, by receiving the device capability collection request (S1512), the device C configures its own device capability, and transmits a device capability response (S1513) to the 20 device A.

The device A next receives the device capability response (S1513) from the device C, and matches it with the device capability information retained in the RAM 304 to determine whether the device C meets the device 25 capability required by the device A. Unlike in the case of the device B, when it is determined that the device C does not meet the device capability

requirement, a participation denial notification message (S1514) is transmitted. Upon receiving the participation denial notification, the device C terminates its communication parameter configuration 5 controlling function.

Although FIG. 15 describes a case where a new slave device (device C) attempts participation when the devices A and B have already transited to the device capability collection step 103, the present invention 10 is not limited to this example. For instance, the present invention can also be applied to a state where two slave devices (devices B and C) already exist and have both transited to the device capability collection step 103.

15 Next, processing performed by the devices to achieve the above-described sequence shown in FIG. 15 will be described using FIG. 16. The description will involve only the processing performed by the master-side device. Processing by the slave-side devices is 20 identical to that in the second embodiment, and a description thereof will be omitted.

FIG. 16 is a flowchart showing processing at a master-side device having a communication parameter configuration control function, according to the fourth 25 embodiment. The master-side device receives a slave declaration message from a slave-side device (S1601). After receiving the slave declaration message, the

master-side device transmits a device capability transmission request to the slave-side device, and performs a device capability exchange by receiving a device capability response from the slave-side device 5 (S1602).

Next, the master-side device determines whether the device capability exchange has been successful. If not (NO in S1602), the master-side device transmits at this point a participation denial notification message 10 to the slave-side device (S1605).

On the one hand, if the device capability exchange has been successful (YES in S1602), the master-side device compares the device capability obtained from the slave-side device with the device capability retained 15 by itself (S1603). At this point, if the device capabilities are inconsistent (NO in S1603), the master-side device transmits a participation denial notification message to the slave-side device (S1605) in the same way as with a device capability exchange 20 failure.

On the other hand, if it is determined that the device capabilities are either consistent or sufficient (YES in S1603), the communication parameter transfer direction determination step 104 of the communication 25 parameter configuration control function is performed (S1604).

Incidentally, while encryption methods or authentication methods were assumed to be the device capabilities according to the fourth embodiment, determination can also be performed based on other 5 capabilities.

As seen, in the fourth embodiment, acceptance of participation to a communication parameter configuration network is controlled by determination based on device capabilities of slave devices as the 10 participation state of communication devices participating in the network.

[Fifth Embodiment]

Next, a detailed description of a fifth embodiment according to the present invention will be provided 15 with reference to the drawings. The fifth embodiment uses random numbers for the request signals and the response signals in the master device determination step 102, and encrypts the sequence from the device capability collection step and onwards using the random 20 number values as elements thereof.

For the fifth embodiment, as shown in FIG. 6, processing for preventing participation to a network by an unexpected third party while two wireless communication devices perform communication parameter 25 configuration will also be described.

FIG. 17 is a diagram illustrating the sequence from a determination step for determining a master

device having a communication parameter configuration control function to a device capability collection step, according to a fifth embodiment. In FIG. 17, it is assumed that the communication parameter configuration 5 network formation step 101 has already been completed between the devices A and B, and that the device A is the IBSS creator, while devices B and C are joiners.

The device A transmits a master inquiry message (S1701) as a broadcast message. At this point, the 10 master device determination step 102 has just commenced and a master device does not yet exist. Thus, a response to the master inquiry message (S1701) will not be transmitted.

Therefore, the device A configures itself as the 15 master device, terminates transmission of the master inquiry message (S1701), and instead commences transmission of a master declaration message (S1702). A random number (M Nonce) generated by the master-side device is attached to the master declaration message 20 (S1702).

When receiving a master declaration message (S1702) from the device A, the device B generates (S1703) a session key using the abovementioned random number (M Nonce), a random number (S Nonce) generated 25 within the device B, and Seed that is stored in the device B. For Seed, it is assumed that a common value is stored in advance in devices having communication

parameter configuration controlling functions. Next, after a lapse of a random interval, the device B transmits a master inquiry message (S1704) as a broadcast message. The random number (S Nonce) is 5 attached to the master inquiry message (S1704).

After receiving the master inquiry message (S1704) from the device B, the device A generates a session key using the random number (M Nonce), the random number (S Nonce) attached to the master inquiry message, and Seed 10 that is stored in the device A (S1705).

After generating the above-described session key, the device A transmits a master declaration message (S1706) to the device B in plaintext. The device A next performs encryption of transmitted data and 15 decryption of received data using the generated session key (S1707).

On the other hand, when receiving the master declaration message (S1706) transmitted by the device A, the device B applies the generated session key for all 20 subsequent communication (S1708). The device B encrypts a slave declaration message (S1709) with the session key, and transmits the message to the device A. All subsequent communication between the devices A and B will be encrypted.

25 Suppose a third terminal device C has appeared afterwards. In addition, assume that the device C has already intercepted the master declaration message

(S1706) transmitted by the device A, and has generated a session key (1710) in the same manner as the device B.

The device C first transmits a master inquiry message (S1711) towards the device A. Meanwhile, since 5 the device A has already established encryption with the device B, the device A is unable to decrypt the received master inquiry message (S1711) that was transmitted by the device C, and thus will not return a response.

10 Therefore, since the device C cannot receive a response to its master inquiry message (S1711), a timeout occurs (S1712). The device C terminates processing related to the communication parameter configuration network the moment the timeout occurs.

15 Following the above description on the sequence between the devices, processing performed by the master-side device and the slave-side device will now be described. First, the processing performed by the master-side device will be described using FIG. 18.

20 FIG. 18 is a flowchart showing processing of a master-side device having a communication parameter configuration control according to the fifth embodiment. The master device attaches a random number generated internally to a master declaration message and 25 transmits the message (S1801). After transmission, the master device stands by for master inquiry messages from slave candidate devices (S1802). During standby

for master inquiry messages, when a master inquiry message is not received, the master device repeats this standby processing.

Afterwards, when a master inquiry message is received from a slave device (YES in S1802), the master device generates a session key that is effective within the communication parameter configuration network (S1803). To be more specific, the device A generates the session key using the random number generated internally (M Nonce), the random number (S Nonce) generated within the slave-side device and attached to the master inquiry message, and Seed that is retained within the master device.

Next, the master device transmits a master declaration message to the slave device without performing encryption (S1804). After transmission of the master declaration message, the master device applies the generated session key (S1805), and stands by for a slave declaration message from the slave device. Upon receiving the slave declaration message (S1806), the master device performs decryption of the slave declaration message using the session key (S1807). When the decryption is failed (NO in S1807), the master device returns to slave declaration message standby processing again (S1806).

On the other hand, when the decryption of the slave declaration message is successful (YES in S1807),

processing transits to the device capability collection step 103 (S1808), which is the next step of the communication parameter configuration control function.

Following the above description on the processing 5 performed by the master-side device, the processing performed by the slave-side device will be described using FIG. 19.

FIG. 19 is a flowchart showing processing of a slave-side device having a communication parameter 10 configuration control function, according to the fifth embodiment. First, when a master-side device already exists in the vicinity, a device having a communication parameter configuration control function receives a master declaration message (S1901). The master 15 declaration message contains a master-side device random number (M Nonce). A session key to be used in the communication parameter configuration network is generated from the random number (M Nonce), a slave-side device random number (S Nonce) generated within 20 the slave-side device and Seed (S1902).

After generating the session key, the slave-side device transmits a master inquiry as a broadcast transmission (S1903). Once the master inquiry message is transmitted, the slave-side device stands by for a 25 master declaration message to be transmitted from the master-side device. Upon receiving the master declaration message from the master-side device (YES in

S1904), the slave-side device compares the above-described random number (M Nonce) upon generation of the session key with the random number (M Nonce) contained within the master declaration message 5 received at this point. When the random number (M Nonce) is identical, the generated session key is applied (S1905).

The slave-side device next transmits a slave declaration encrypted using the session key to the 10 master-side device (S1906). If the slave declaration is successfully transmitted to the master-side device, the slave-side device stands by for a device capability transmission request to be transmitted from the master-side device (S1907). When a decipherable device 15 capability transmission request is not received from the master-side (NO in S1907), the slave-side device terminates processing related to the communication parameter configuration network (S1909).

On the other hand, when a device capability 20 transmission request is received from the master-side device (YES in S1907), the slave-side device performs the device capability collection step 103 (S1908), which is the next step in the communication parameter configuration controlling function.

25 According to the fifth embodiment, communication parameter configuration can be performed between the master device and the slave devices with an encryption

processing that is stronger than is used in the first embodiment. As seen, in the fifth embodiment, acceptance of participation to a communication parameter configuration network is controlled by 5 determining whether a communication device has already commenced encrypted communication with another communication device as the participation state of communication devices participating in the network.

The present invention may be applied to both 10 systems comprising a plurality of devices (for example, a host computer, an interface device, a reader or a printer), or apparatuses composed of a single device (for example, a copying machine or facsimile machine).

It is obvious that the object of the present 15 invention may also be achieved by supplying a storage media that stores a program code of a software capable of achieving the functions of the described embodiments to a system or an apparatus, and having a computer (CPU or MPU) of the system or apparatus read out and execute 20 the program stored in the storage media.

In this case, the program codes themselves that 25 are read out from the storage media achieve the functions of the above mentioned embodiments, while the storage media containing the program codes compose the present invention.

Storage devices to which the program codes are supplied may include, for instance, a floppy disk

(registered trademark), a hard disk, an optical disk, a magneto-optical disk, a CD-ROM, a CD-R, a magnetic tape, a nonvolatile memory card, a ROM or the like.

In addition, it is obvious that the functions of
5 the aforementioned embodiments can be achieved not only by executing program codes read out by a computer, but also through the processing performed by an OS (operating system) or the like, which is running on a computer, that performs a portion or all of the actual
10 processing based on instructions from the program code.

Furthermore, it is obvious that the functions of the aforementioned embodiments can also be achieved by writing program codes read out by a computer into either a function enhancement board inserted into a
15 computer or a memory built into a function enhancement unit connected to a computer, and having a CPU or the like built into the function enhancement board or the function enhancement unit perform a portion or all of the actual processing based on instructions from the
20 program code.

According to the above description, the present invention is capable of strengthening countermeasure against spoofing by third parties by applying certain restrictions when establishing a communication
25 parameter configuration network. In addition, the present invention is capable of reducing transmission

of communication parameters to unnecessary devices, thereby reducing unnecessary information leakage.

In addition, a certain level of security may be ensured by encrypting communication performed in a 5 communication parameter configuration network.

Furthermore, participation to the network by a third party can be denied while continuing already established wireless communication parameter configuration control functions performed between 10 devices, thereby improving the operating efficiency of a user.

As shown, according to the present embodiments, responses against spoofing by third parties can be strengthened by applying certain restrictions when 15 establishing a communication parameter configuration network. In addition, the present invention is capable of reducing transmittance of communication parameters to unnecessary devices, thereby reducing unnecessary information leakage.

20 As many apparently widely different embodiments of the present invention can be made without departing from the spirit and scope thereof, it is to be understood that the invention is not limited to the specific embodiments thereof except as defined in the 25 appended claims.

This application claims the benefit of Japanese Patent Application No. 2005-172968 filed on June 13,

- 50 -

2005, which is hereby incorporated by reference herein in its entirety.

CLAIMS

1. A communication parameter configuration method for a communication apparatus, comprising:
 - a control step of controlling a network in communication parameter configuration mode, based on participation statuses of communication apparatuses to participate in the network, so that participation of new communication apparatuses to the network is not accepted; and
- 10 a communication parameter configuration step of establishing the network in communication parameter configuration mode between communication apparatuses participating in the network to configure communication parameters.
- 15 2. The method according to claim 1, wherein the communication apparatus that establishes the network is a communication apparatus that functions as a master device, and the communication apparatus that participates in the network is a communication apparatus that functions as a slave device.
- 20 3. The method according to claim 2, wherein the control step issues instructions for encryption processing to the participating communication apparatuses till a prescribed number of communication apparatuses is participated in the network, and does not accept participation of new communication apparatuses to the network.

4. The method according to claim 2, wherein, in the control step, the communication apparatus that functions as the master device does not accept participation of new communication apparatuses to the 5 network in accordance with the number of participations of the communication apparatuses, which function as slave devices, that participation to the network has been accepted.

5. The method according to claim 2, wherein, in the 10 control step, the communication apparatus that functions as the master device does not accept participation of new communication apparatuses to the network when a predetermined period of time has lapsed after transmitting a device capability transmission 15 request to at least one communication apparatus that functions as the slave device.

6. The method according to claim 1, wherein the control step controls the network so as not to accept participation of new communication apparatuses to the 20 network by performing encrypted communication.

7. The method according to claim 1, wherein, in the control step, messages denying participation are transmitted to communication apparatuses to be denied participation in the network when participation of new 25 communication apparatuses to the network is not accepted.

8. A communication parameter configuration method for a communication apparatus, comprising:

a control step of controlling a network in communication parameter configuration mode, based on

5 capability information of communication apparatuses to participate in the network, so that participation of new communication apparatuses to the network is not accepted; and

10 a communication parameter configuration step of establishing the network in communication parameter configuration mode between communication apparatuses participating in the network to configure communication parameters.

9. The method according to claim 8, wherein the 15 communication apparatus that establishes the network is a communication apparatus that functions as a master device, and the communication apparatus that participates in the network is a communication apparatus that functions as a slave device.

20 10. The method according to claim 9, wherein the control step controls the network so as not to accept participation of new communication apparatuses to the network in accordance with capability information collected by the communication apparatus that functions 25 as the master device from the communication apparatuses that function as slave devices.

11. The method according to claim 8, wherein the capability information is information related to authentication methods.

12. The method according to claim 8, wherein the 5 capability information is information related to encryption methods.

13. A communication parameter configuration method for a communication apparatus, comprising:

10 a transmission step of transmitting a first random number value when declaring that a master device on a network in communication parameter configuration mode is the master device;

15 a reception step of receive a second random number value transmitted from another communication apparatus when inquiring the master device on the network in communication parameter configuration mode;

20 a generation step of generating an encryption key based on the first random number value, the second random number value and a particular constant; and a step of initiating encrypted communication using the encryption key generated in the generation step in response to a transmission of a response to the master device inquiry.

14. A communication apparatus, comprising:

25 a control unit adapted to control a network in communication parameter configuration mode, based on participation statuses of communication apparatuses to

participate in the network, so that participation of new communication apparatuses to the network is not accepted; and

5 a communication parameter configuration unit adapted to establish the network in communication parameter configuration mode between communication apparatuses participating in the network to configure communication parameters.

15. A communication apparatus, comprising:

10 a control unit adapted to control a network in communication parameter configuration mode, based on capability information of communication apparatuses to participate in the network, so that participation of new communication apparatuses to the network is not accepted; and

15 a communication parameter configuration unit adapted to establish the network in communication parameter configuration mode between communication apparatuses to participate in the network to configure communication parameters.

20 16. A communication apparatus, comprising:

a transmission unit adapted to transmit a first random number value in order to declare that the apparatus is the master device on a network in communication parameter configuration mode;

25 a reception unit adapted to receive a second random number value transmitted from another

communication apparatus when inquiring the master device on the network in communication parameter configuration mode;

5 a generation unit adapted to generate an encryption key based on the first random number value, the second random number value and a particular constant; and

10 a unit adapted to initiate encrypted communication using the encryption key generated by said generation unit in response to a transmission of a response to the master device inquiry.

17. A program for causing a computer to execute a communication parameter configuration method for a communication apparatus, the program stored in a computer-readable storage medium, the method comprising:

20 a control step of controlling a network in communication parameter configuration mode, based on participation statuses of communication apparatuses to participate in the network, so that participation of new communication apparatuses to the network is not accepted; and

25 a communication parameter configuration step of establishing the network in communication parameter configuration mode between communication apparatuses participating in the network to configure communication parameters.

18. A program for causing a computer to execute a communication parameter configuration method for a communication apparatus, the program stored in a computer-readable storage medium, the method

5 comprising:

10 a control step of controlling a network in communication parameter configuration mode, based on capability information of communication apparatuses to participate in the network, so that participation of new communication apparatuses to the network is not accepted; and

15 a communication parameter configuration step of establishing the network in communication parameter configuration mode between communication apparatuses participating in the network to configure communication parameters.

19. A program for causing a computer to execute a communication parameter configuration method for a communication apparatus, the program stored in a computer-readable storage medium, the method

20 comprising:

25 a transmission step of transmitting a first random number value when declaring that a master device on a network in communication parameter configuration mode is the master device;

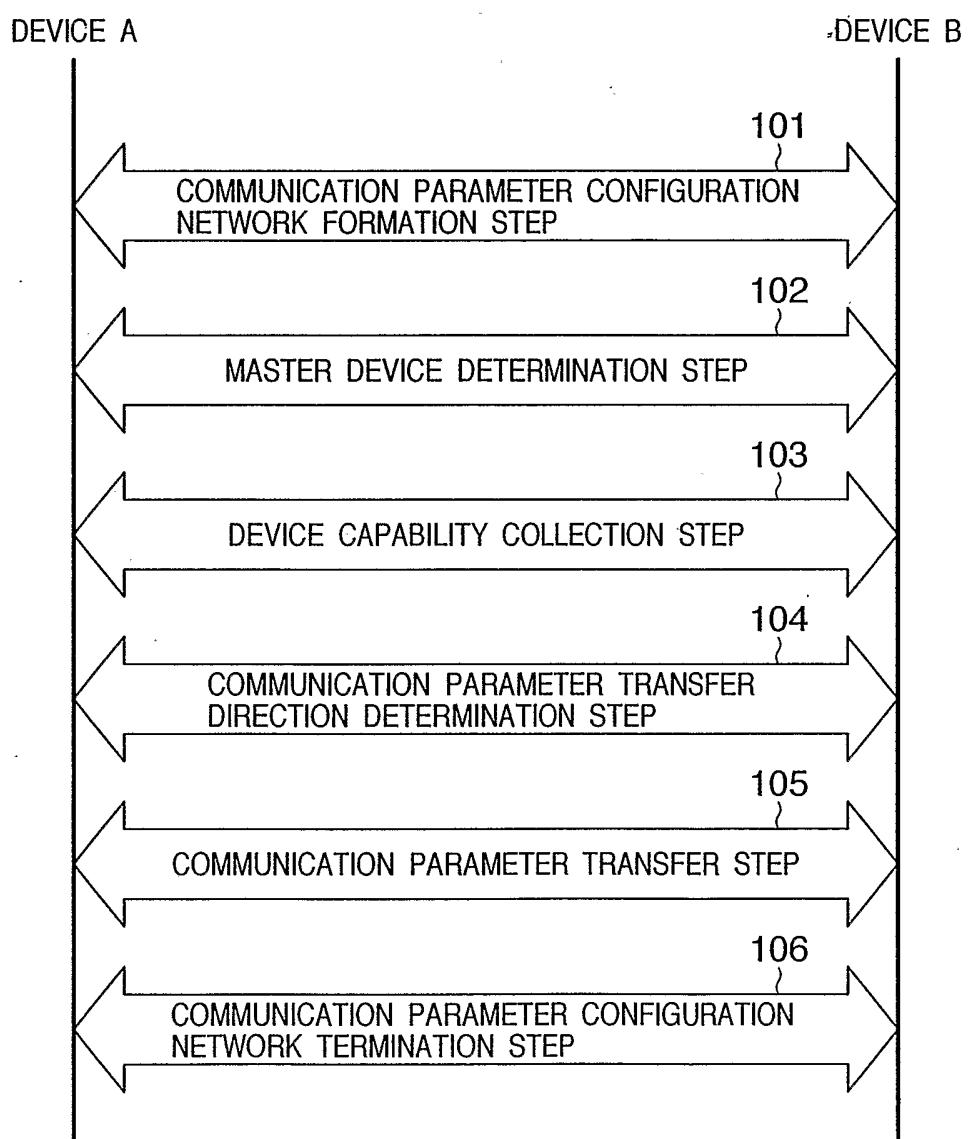
30 a reception step of receive a second random number value transmitted from another communication apparatus

when inquiring the master device on the network in communication parameter configuration mode;

5 a generation step of generating an encryption key based on the first random number value, the second random number value and a particular constant; and

a step of initiating encrypted communication using the encryption key generated in the generation step in response to a transmission of a response to the master device inquiry.

FIG. 1



2/19

FIG. 2

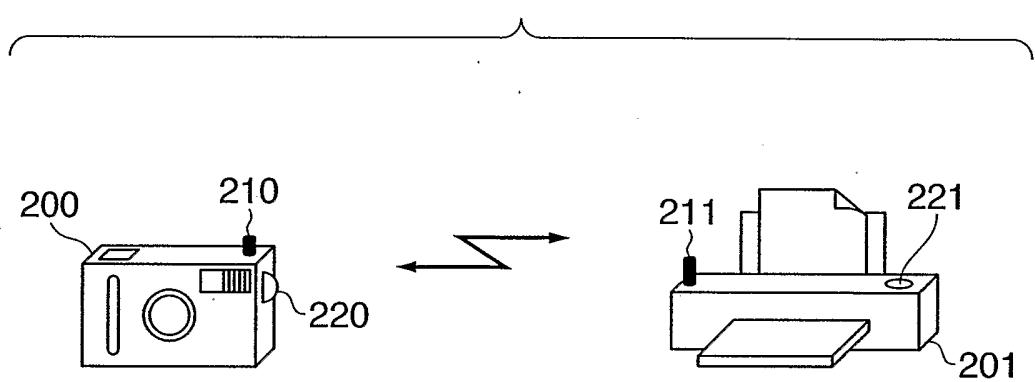


FIG. 3

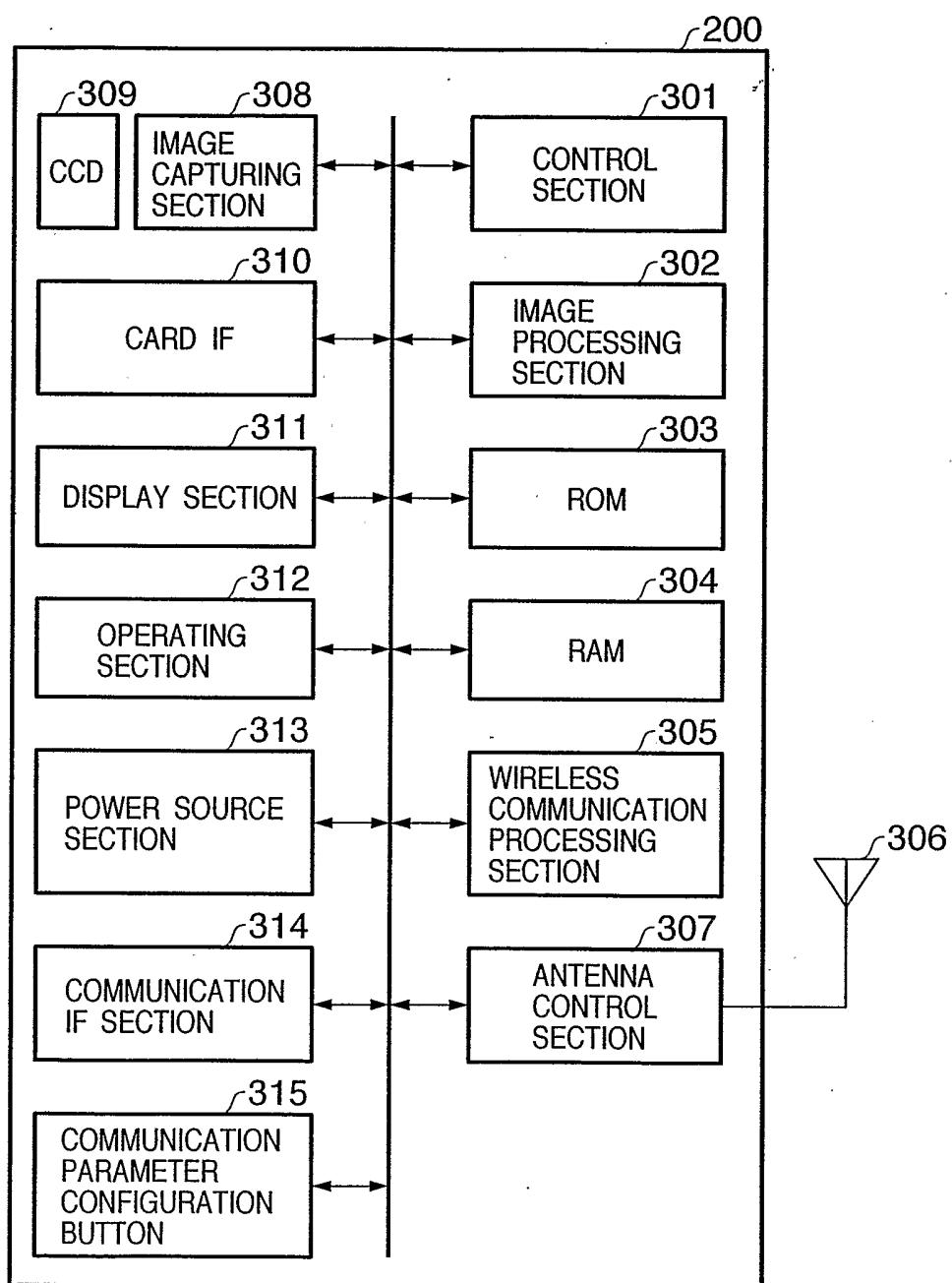
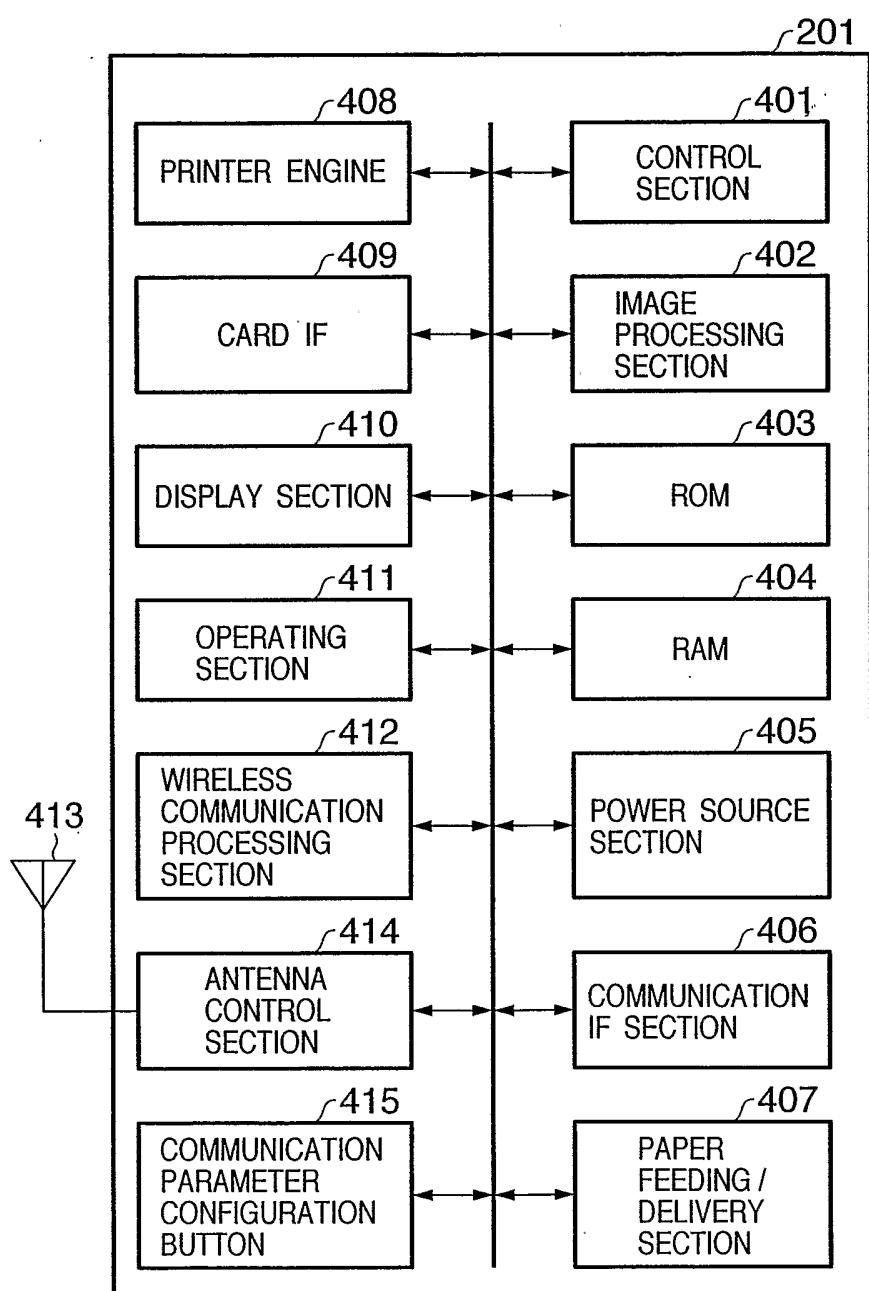
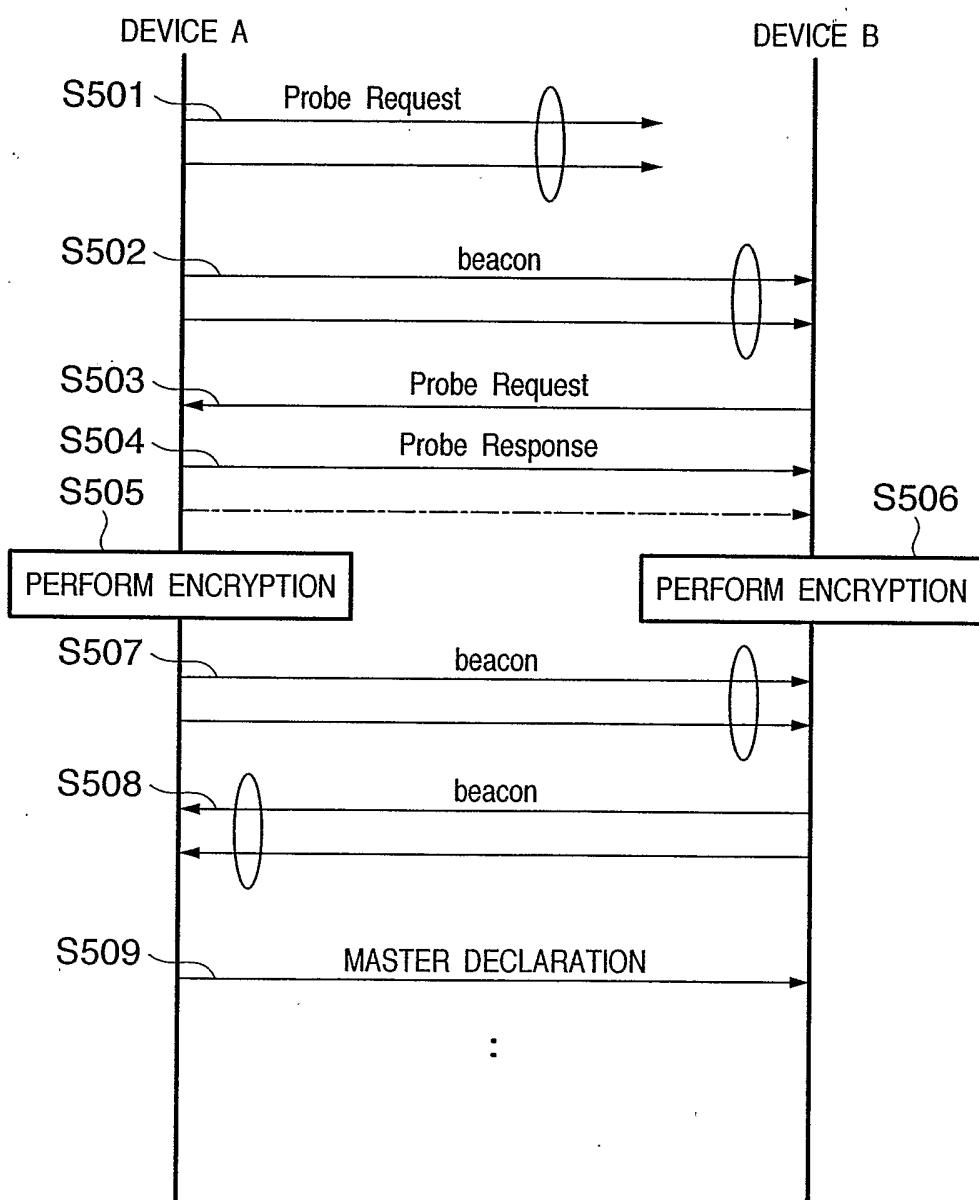


FIG. 4



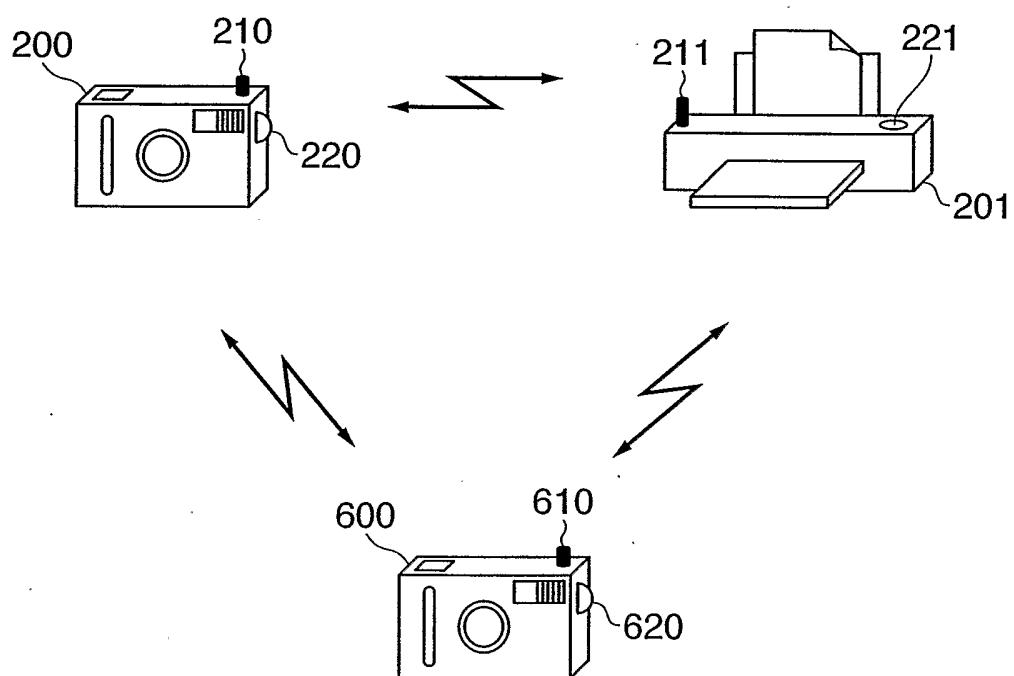
5/19

FIG. 5



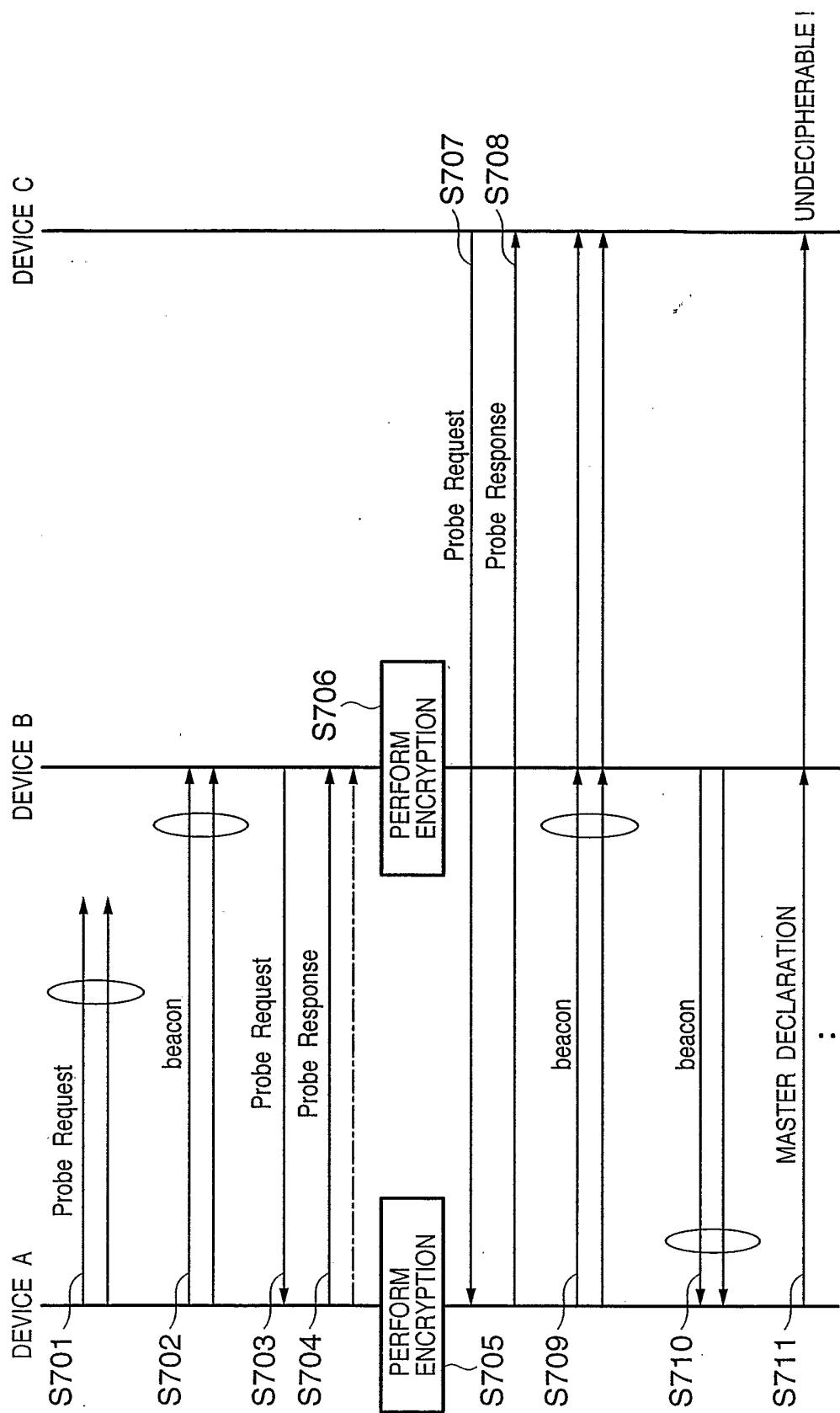
6/19

FIG. 6



7/19

FIG. 7



8/19

FIG. 8

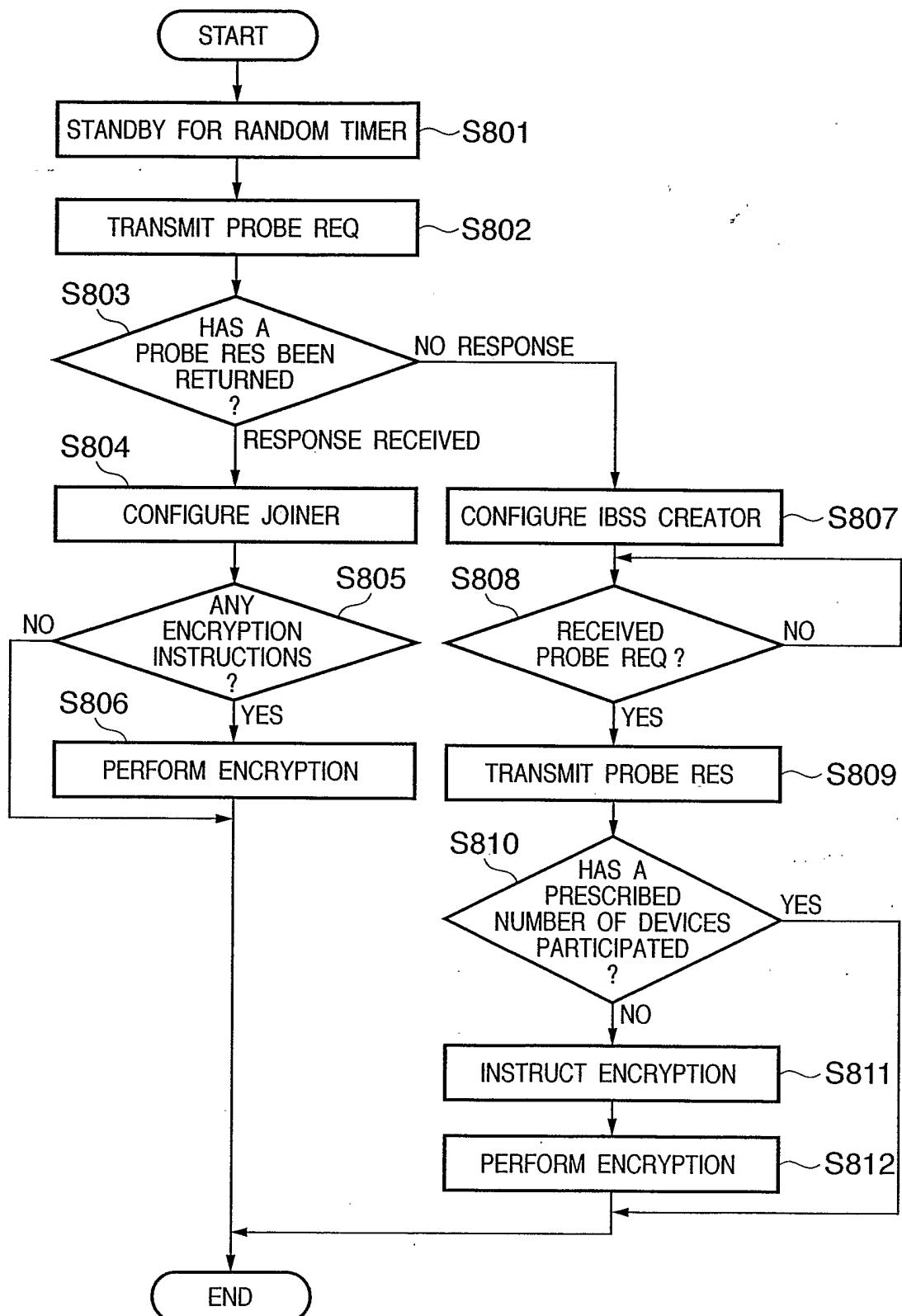
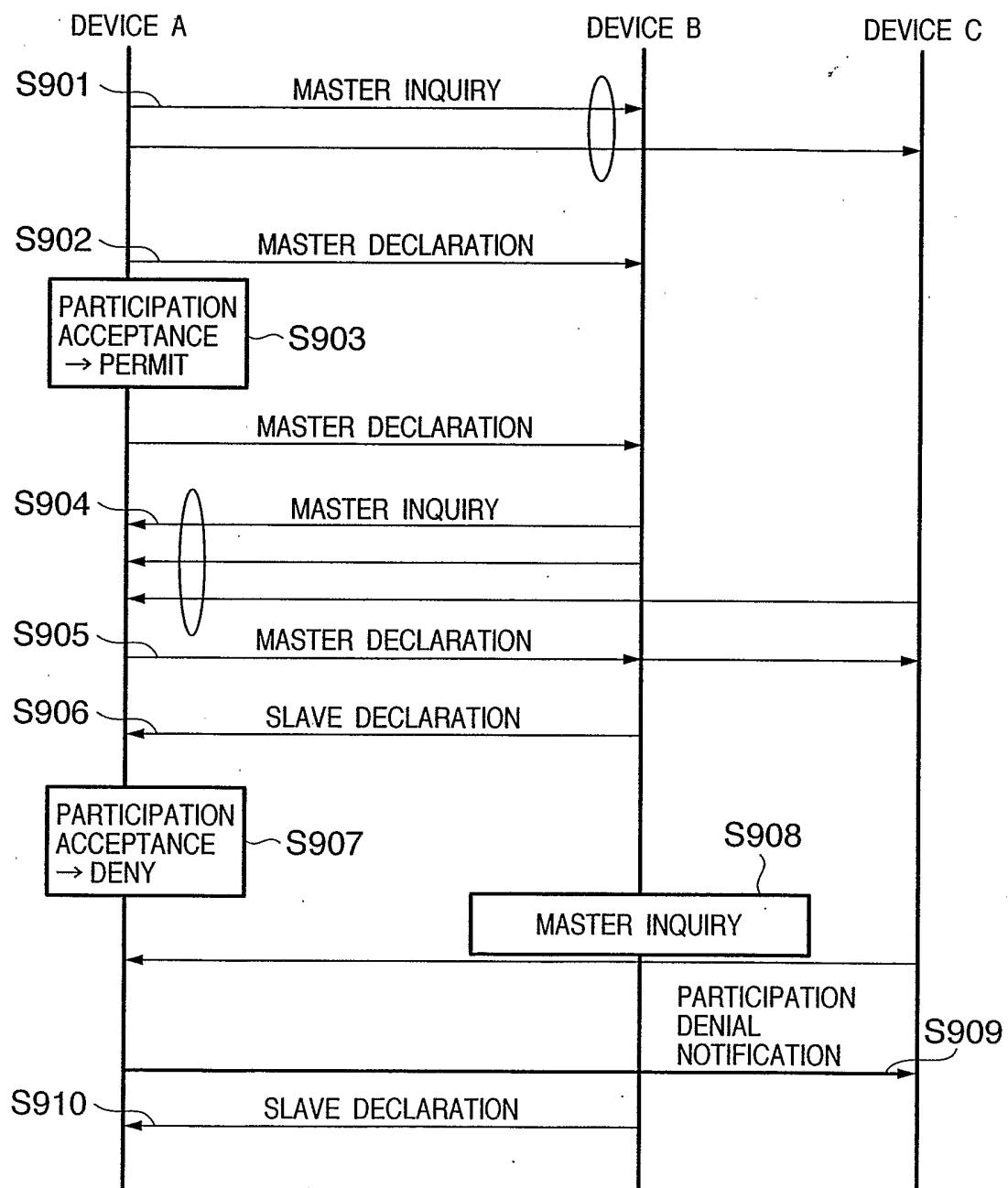
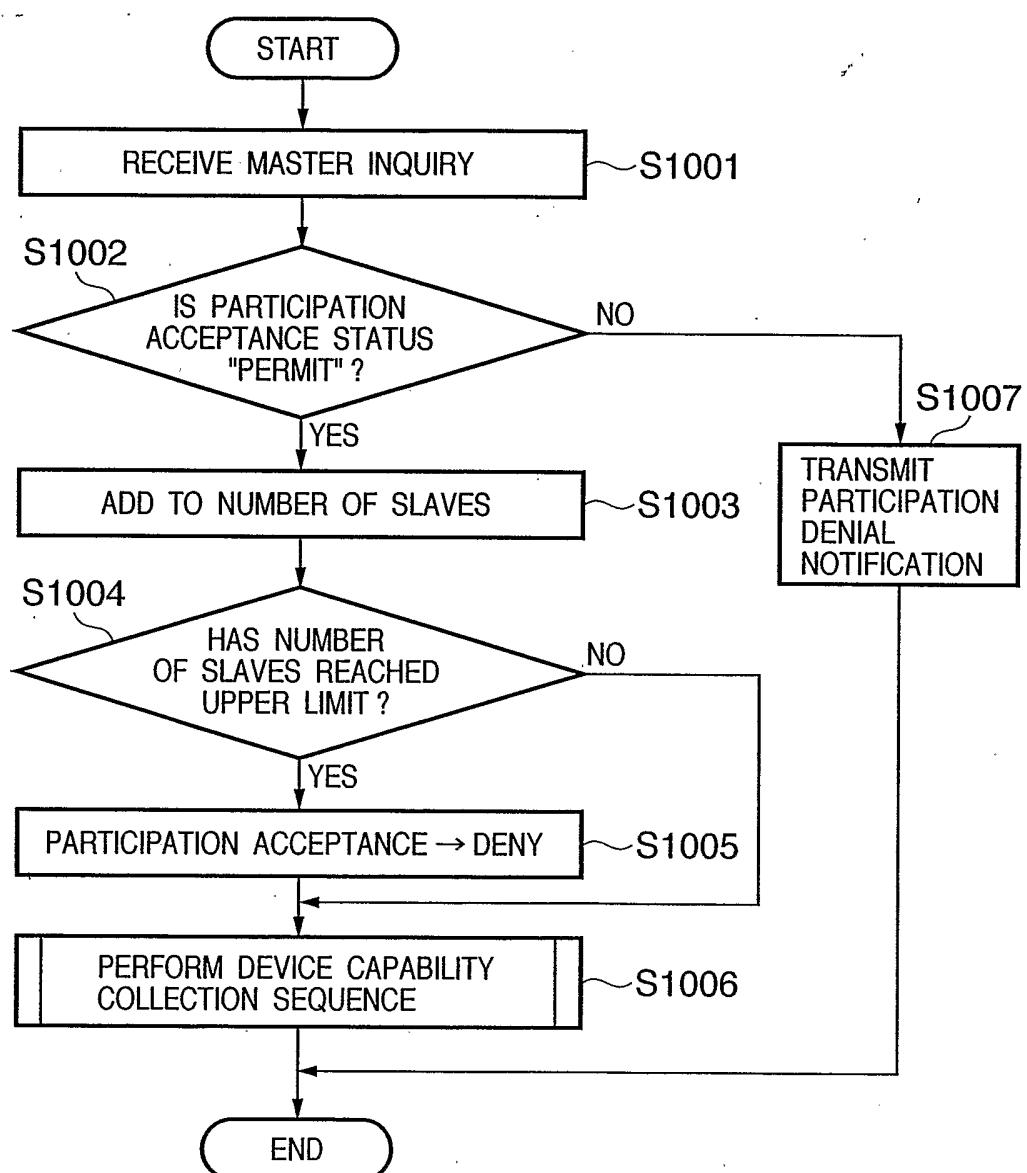


FIG. 9



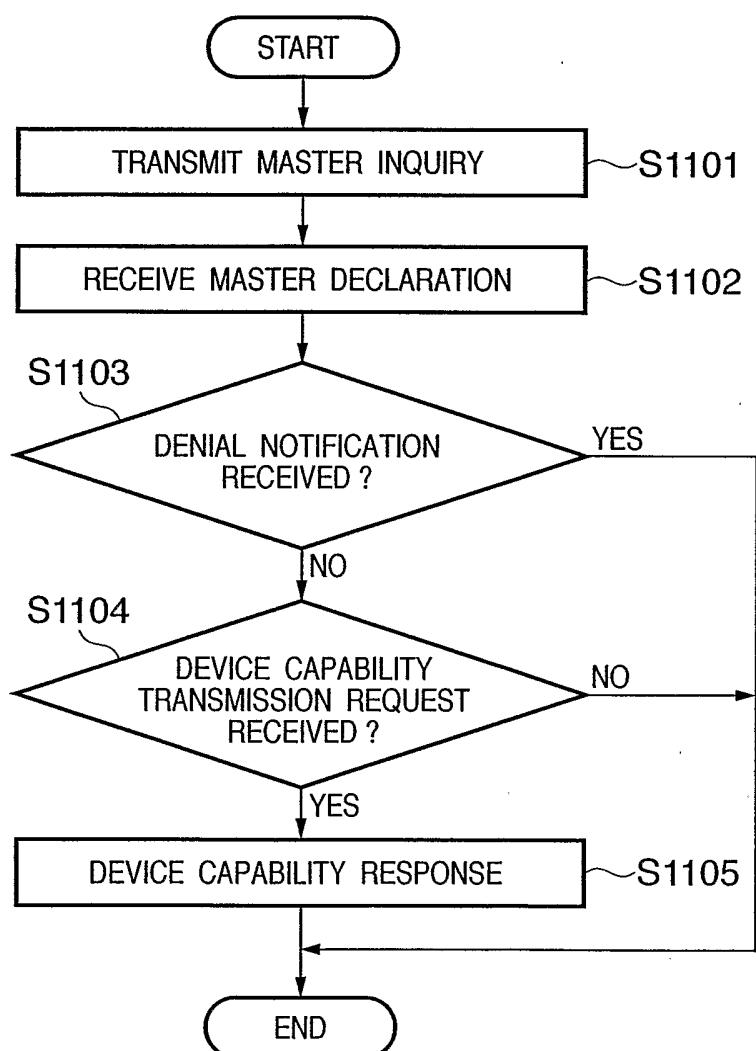
10/19

FIG. 10



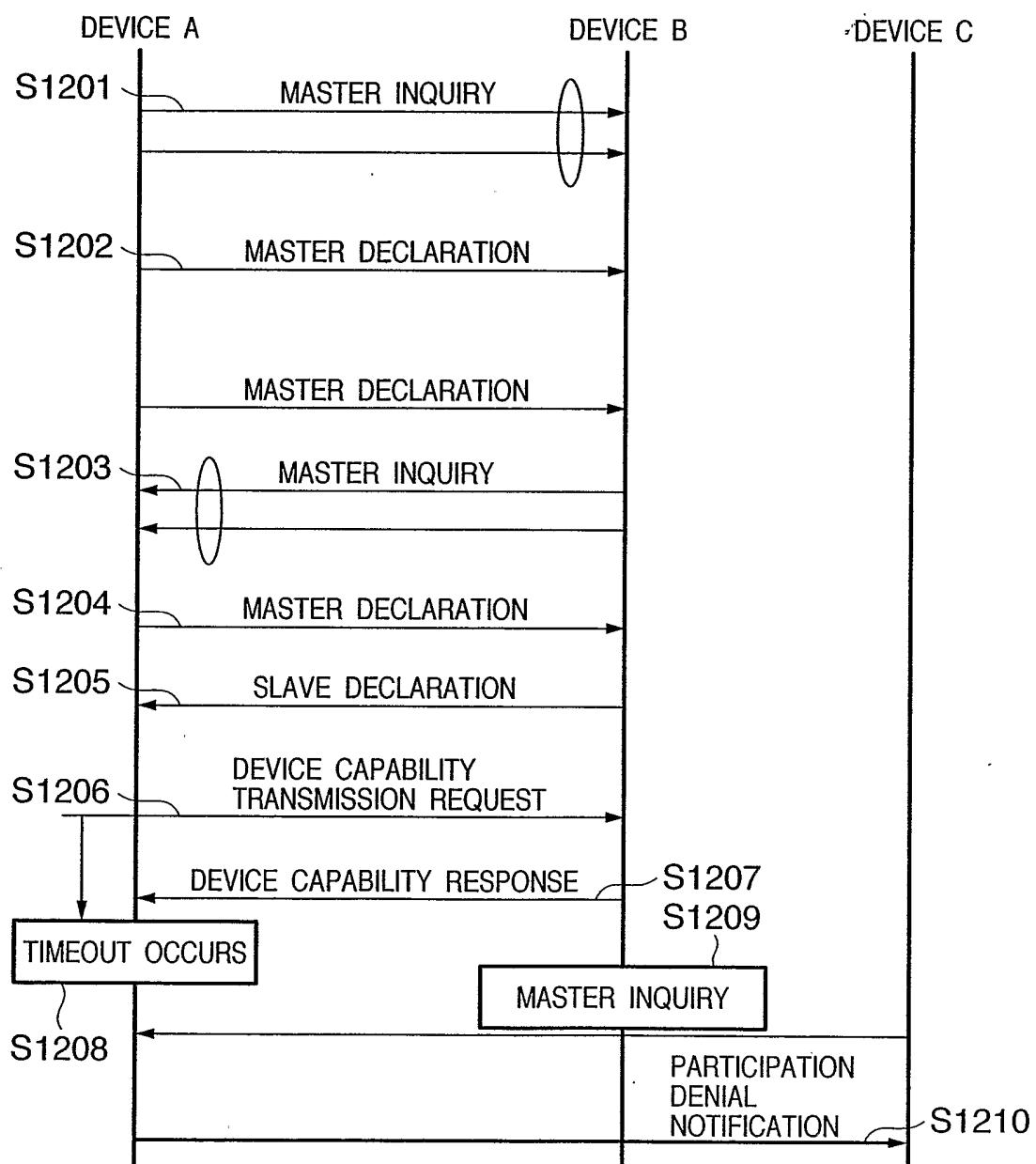
11/19

FIG. 11



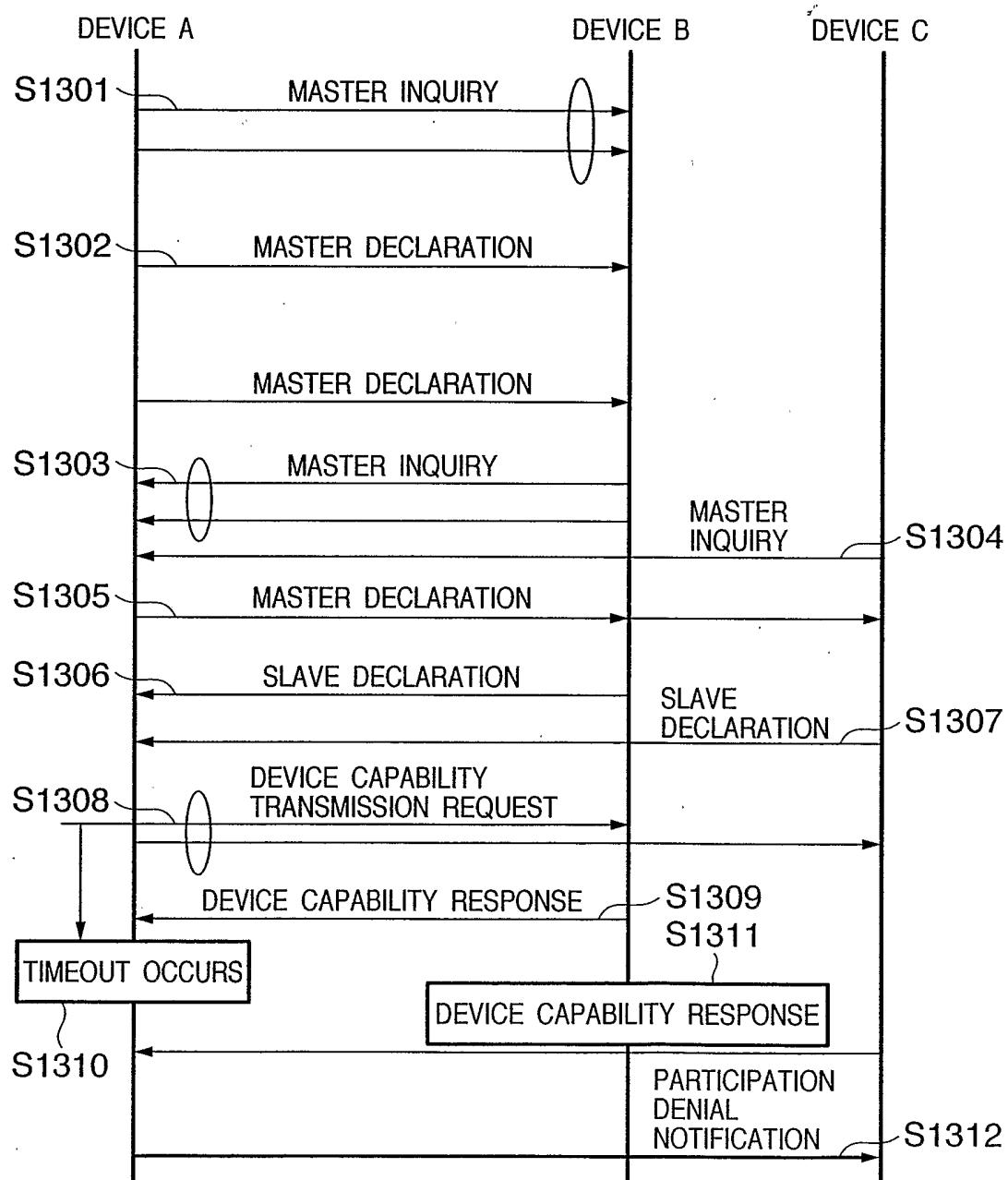
12/19

FIG. 12



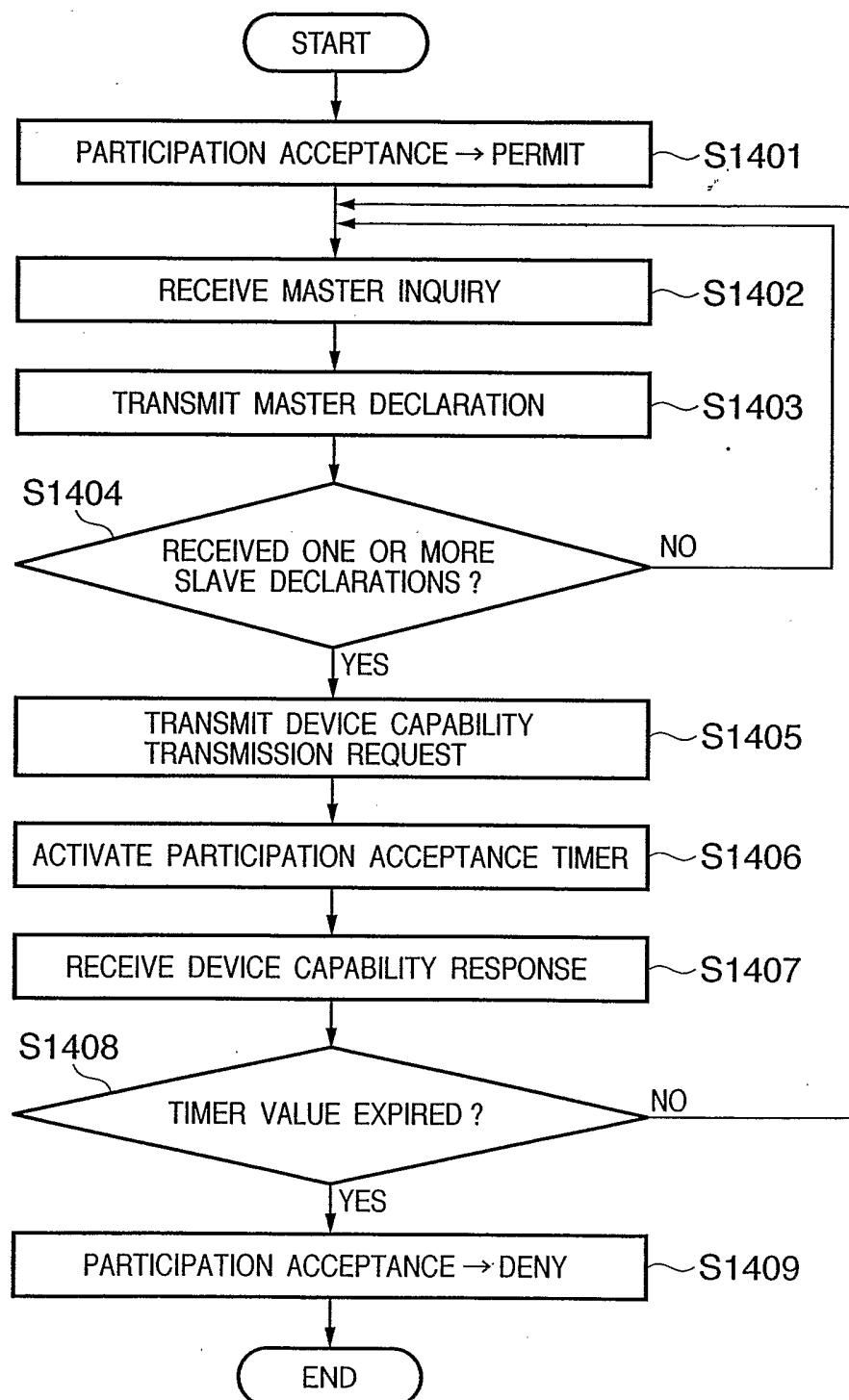
13/19

FIG. 13



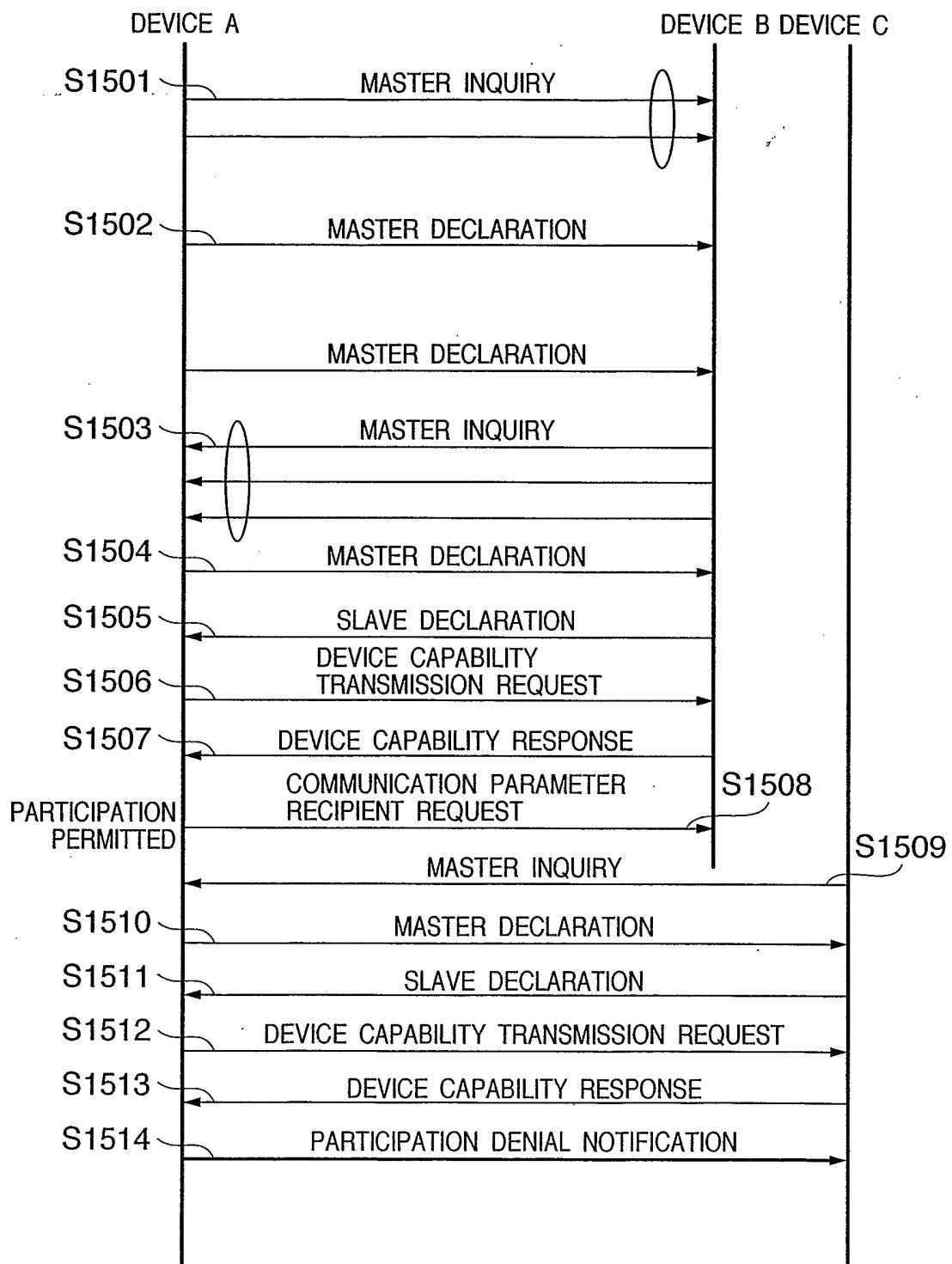
14/19

FIG. 14



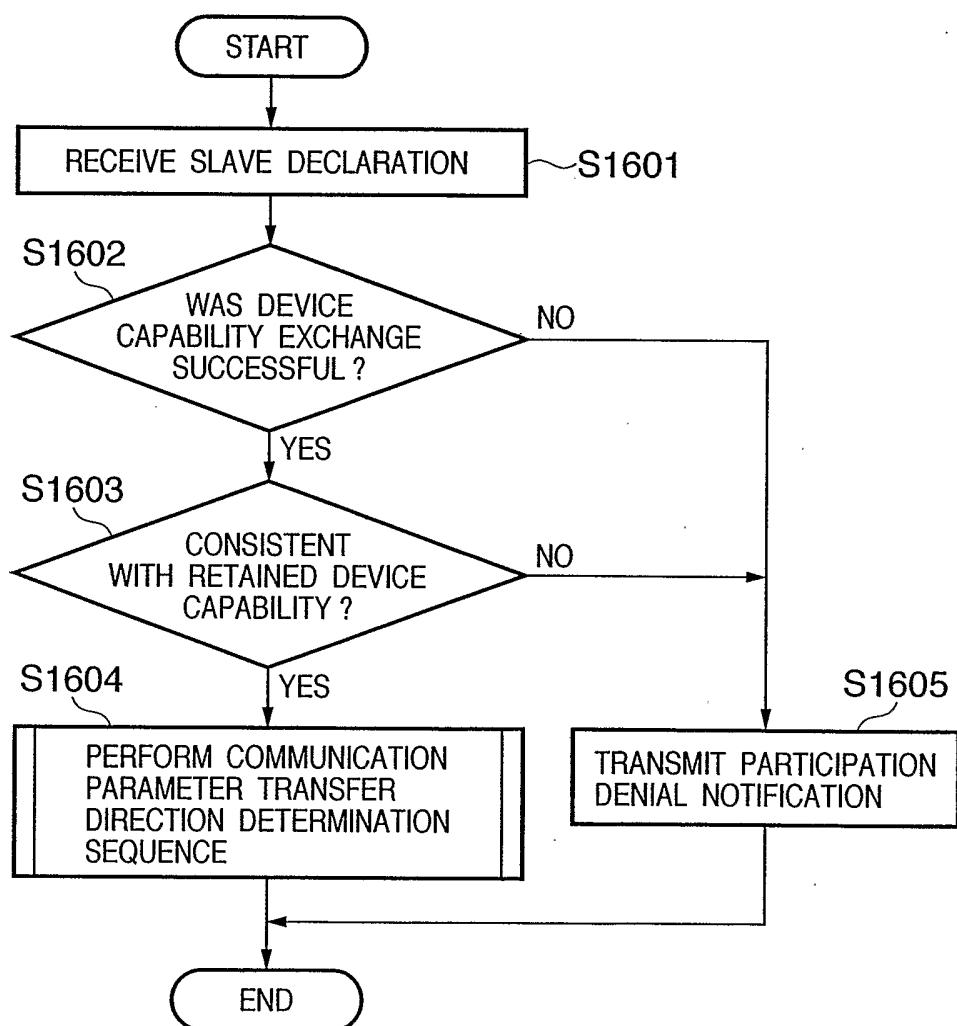
15/19

FIG. 15



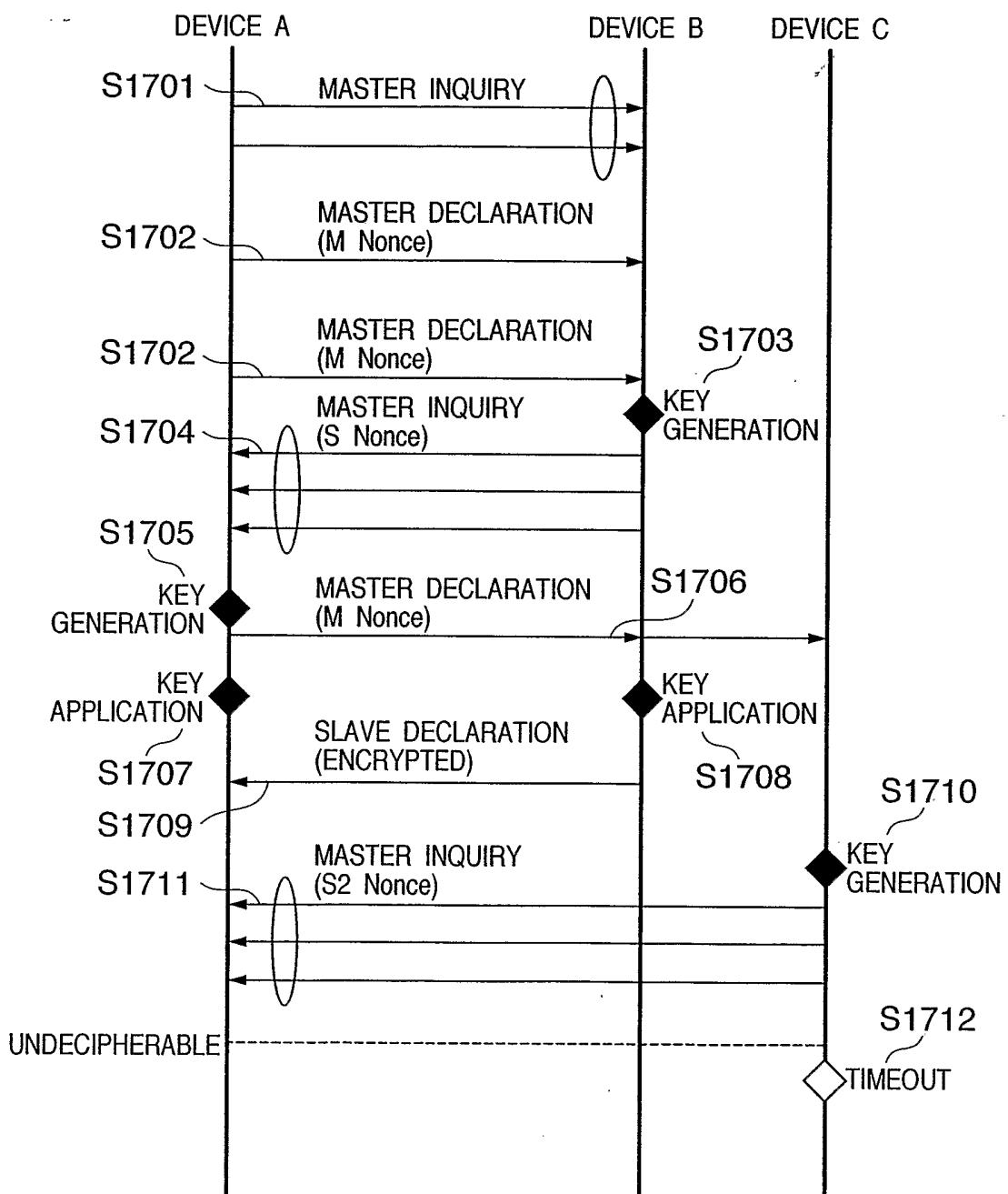
16/19

FIG. 16



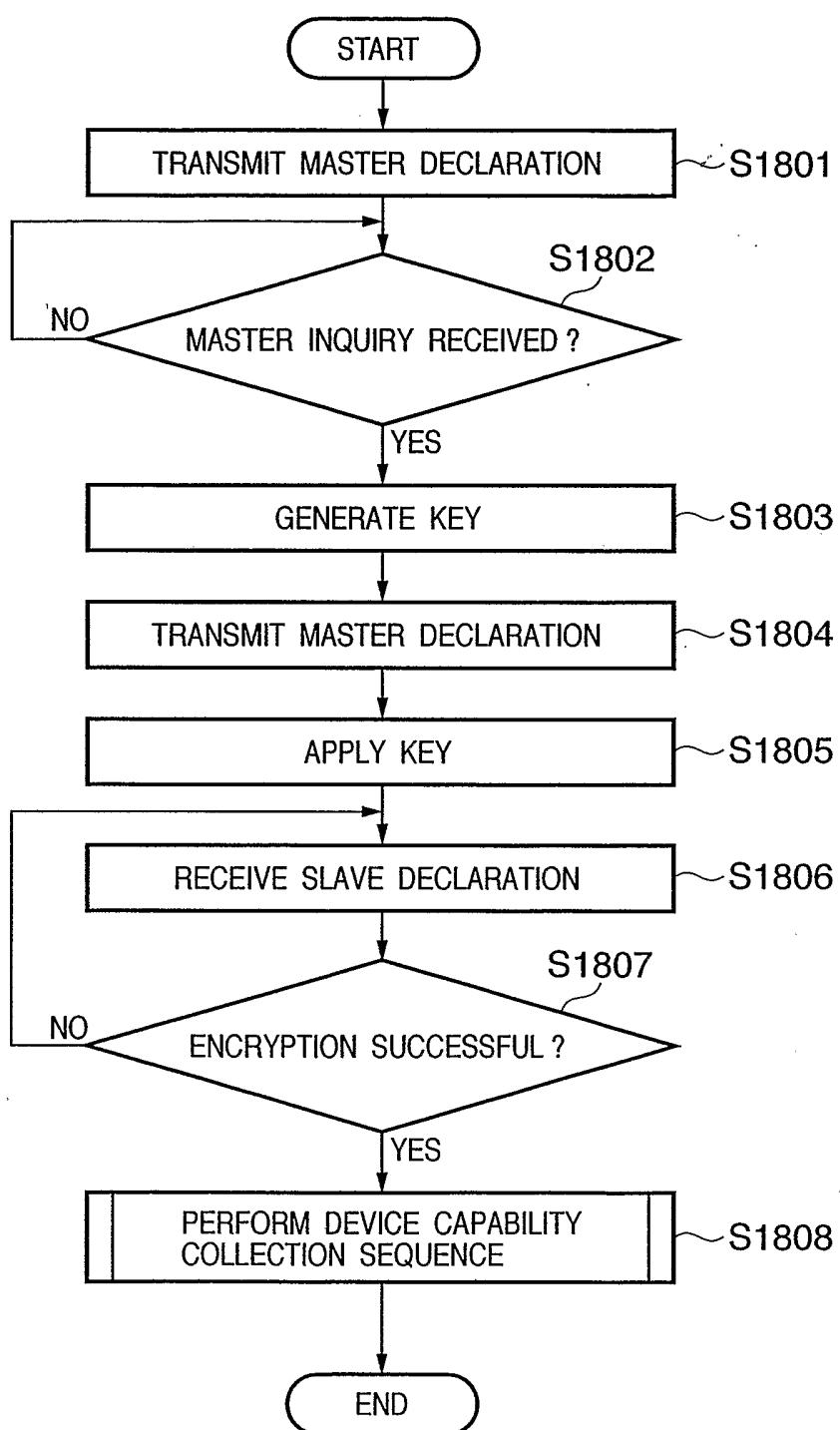
17/19

FIG. 17



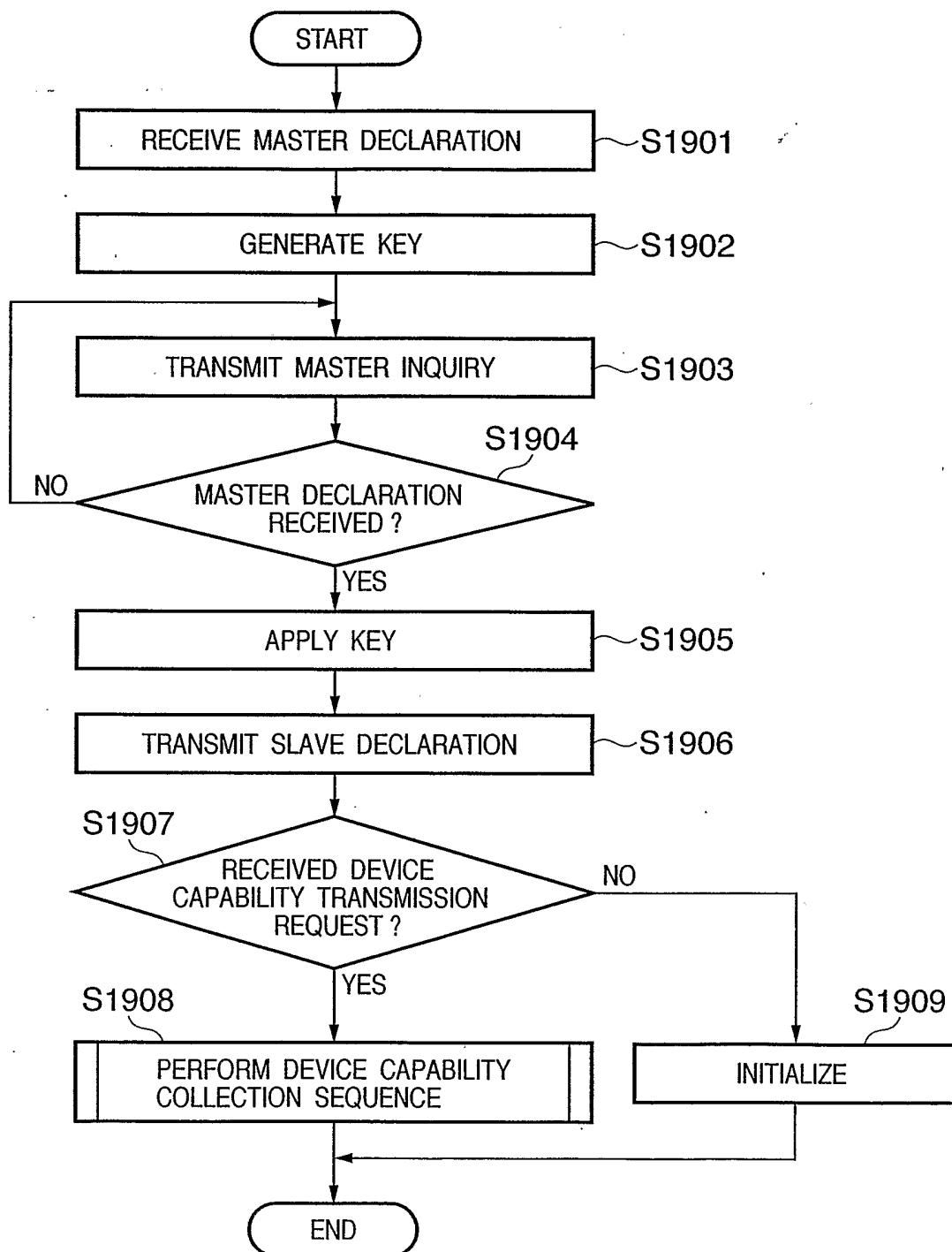
18/19

FIG. 18



19/19

FIG. 19



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/310833

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04L12/28 (2006.01)

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. H04L12/28, H04B7/24-7/26

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 1971-2006
 Registered utility model specifications of Japan 1996-2006
 Published registered utility model applications of Japan 1994-2006

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. |
|-----------|---|-----------------------|
| Y | JP 2003-338821 A (NEC Viewtechnology KABUSHIKIKAISYA) 2003.11.28, [0027], [0028], [0042]-[0049], Fig.6 (Family none) | 1-12, 14, 15, 17, 18 |
| Y | JP 2001-326658 A (FUJITSU KABUSHIKIKAISYA) 2001.11.22, [0006], [0007], [0033], [0034], Fig.2 (Family none) | 1-7, 14, 17 |
| Y | JP 2004-32664 A (KABUSHIKIKAISYA TOSHIBA) 2004.01.29, [0158]-[0165], Fig.23, Fig.24 & US 2003/0119484 A1 & EP 1324541 A2 & CN 1430342 A | 3, 6, 8-12, 15, 18 |
| Y | JP 2001-313723 A (FUJITSU KABUSHIKIKAISYA) 2001.11.09, [0040], [0045], [0046], Fig.8 (Family none) | 5 |

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 12.07.2006 | Date of mailing of the international search report 18.07.2006 |
| Name and mailing address of the ISA/JP Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan | Authorized officer Moro Sayaka Telephone No. +81-3-3581-1101 Ext. 3596 |

INTERNATIONALSEARCHREPORT

International application No.
PCT/JP2006/310833

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|--|-----------------------|
| Y | JP 2004-158954 A (NEC Viewtechnology KABUSHIKIKAISYA) 2004.06.03, [0027], [0028], [0031], [0032], Fig.2 (Family none) | 13, 16, 19 |
| Y | JP 9-238132 A (Oki Electric Industry Co., Ltd. et al) 1997.09.09, [0007]-[0011], Fig.1 & US 6018581 A & EP 0793367 A2 & CN 1211776 A & KR 97063006 A & TW 335581 A | 13, 16, 19 |

INTERNATIONALSEARCHREPORT

International application No.
PCT/JP2006/310833

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The "special technical features" of claim 1-7, 14, 17 relates to denying participation of the new communication apparatus to a network based on participation statuses of communication apparatuses.

The "special technical features" of claim 8-12, 15, 18 relates to denying participation of the new communication apparatus to a network based on capability information of communication apparatuses.

The "special technical features" of claim 13, 16, 19 relates to generating an encryption key based on the first random number value, the second random number value and a particular constant.

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- No protest accompanied the payment of additional search fees.