US 20080045181A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2008/0045181 A1

(43) Pub. Date: Feb. 21, 2008

Suzuki

(54) COMMUNICATION SYSTEM, WIRELESS-COMMUNICATION DEVICE, AND CONTROL METHOD THEREFOR

(76) Inventor: **Hideyuki Suzuki**, Tokyo (JP)

Correspondence Address:
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413 (US)

(21) Appl. No.: **11/838,718**

(22) Filed: **Aug. 14, 2007**

(30) **Foreign Application Priority Data**

Aug. 15, 2006 (JP) 2006-221719

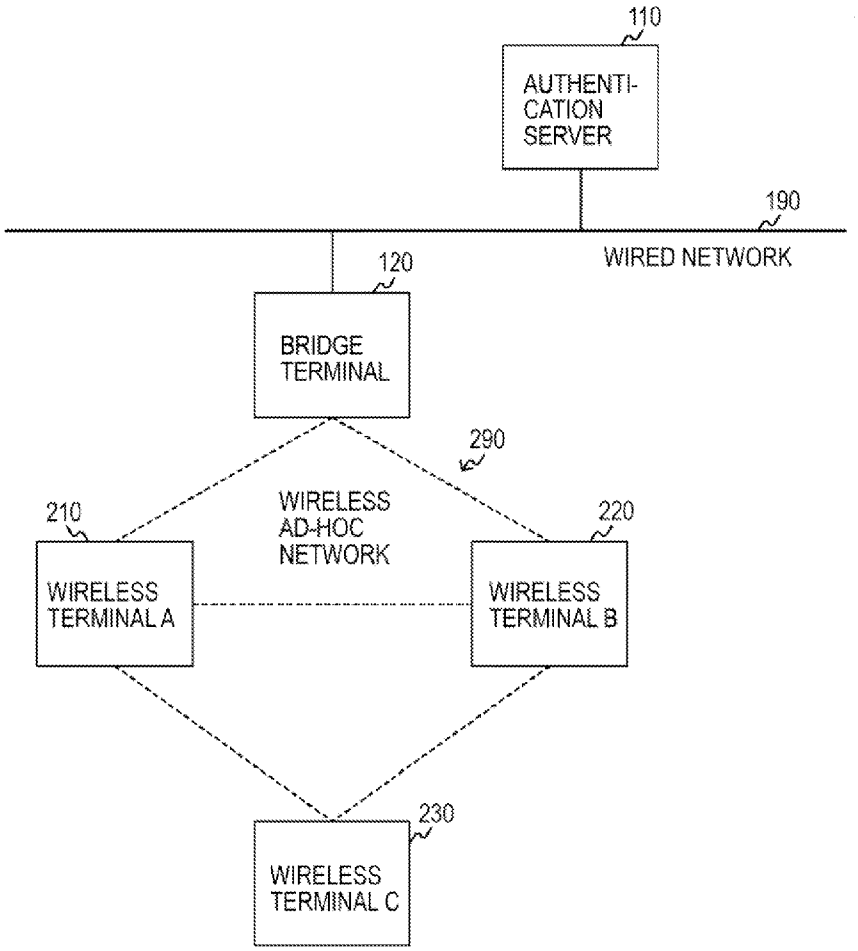
Publication Classification

(51) **Int. Cl.**
H04M 1/66 (2006.01)

(52) **U.S. Cl.** **455/411**

(57) **ABSTRACT**

A wireless-communication device performing mutual authentication between the wireless-communication device and a different wireless-communication device by using an authentication server includes a communication-setting-data-retention unit retaining communication-setting data including a first metric corresponding to the path to the authentication server, as a self-authentication-server metric, a signal-reception unit receiving a predetermined signal transmitted from the different wireless-communication device, the predetermined signal including a second metric corresponding to the path from the different wireless-communication device to the authentication server, as a nonself-authentication-server metric, and a control unit determining the wireless-communication device to be a supplicant when the self-authentication-server metric is better than the non-self-authentication-server metric, and determining the wireless-communication device to be an authenticator when the self-authentication-server metric is worse than the nonself-authentication-server metric.



Apple EX1037
Apple Inc. v. Secure Comm. Techs., LLC
IPR2026-00445

FIG. 1

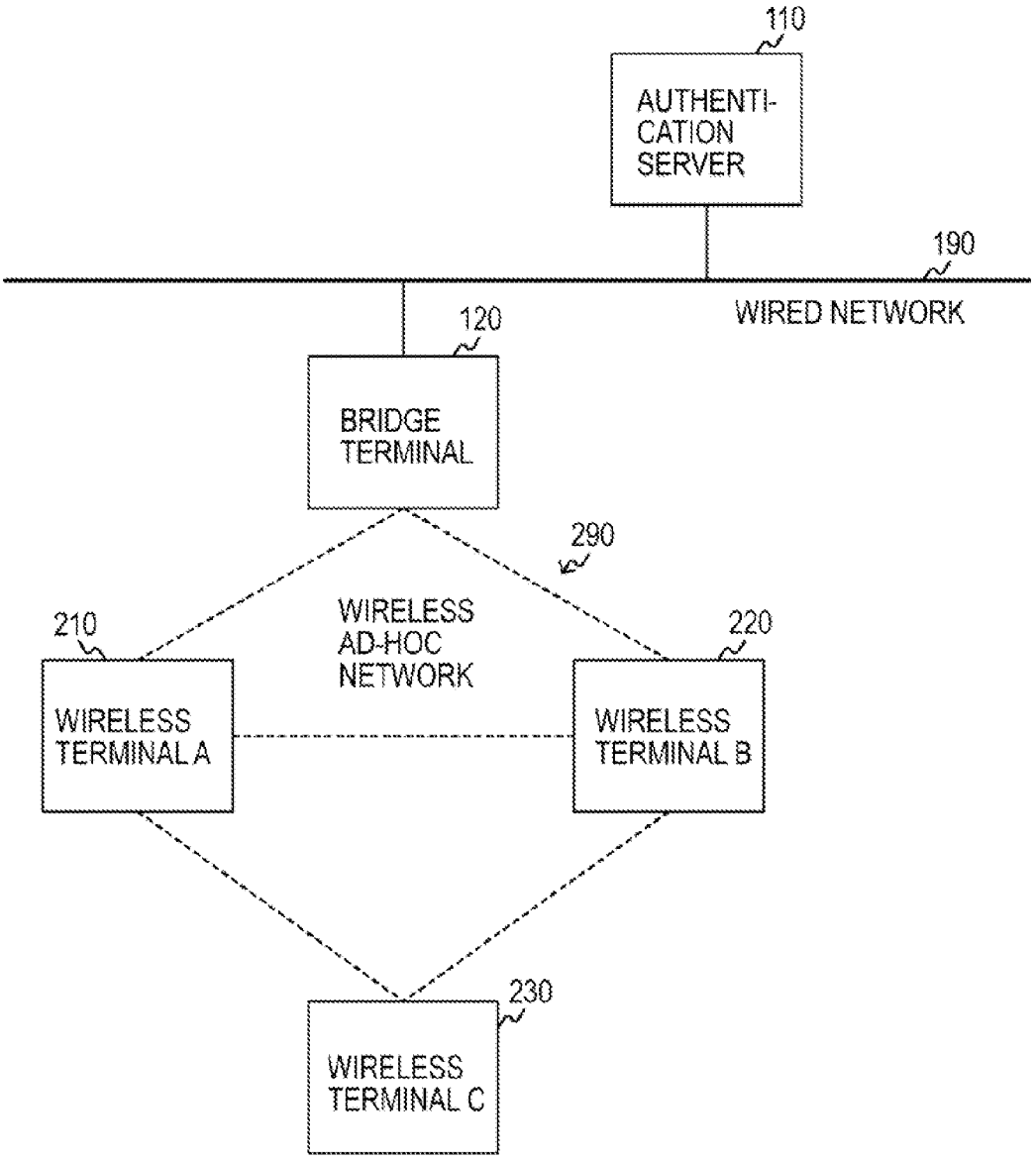

110
AUTHENTI-
CATION
SERVER
190
WIRED NETWORK
120
BRIDGE
TERMINAL
290
WIRELESS
AD-HOC
NETWORK
210
220
WIRELESS
TERMINAL A
WIRELESS
TERMINAL B
230
WIRELESS
TERMINAL C

FIG. 2

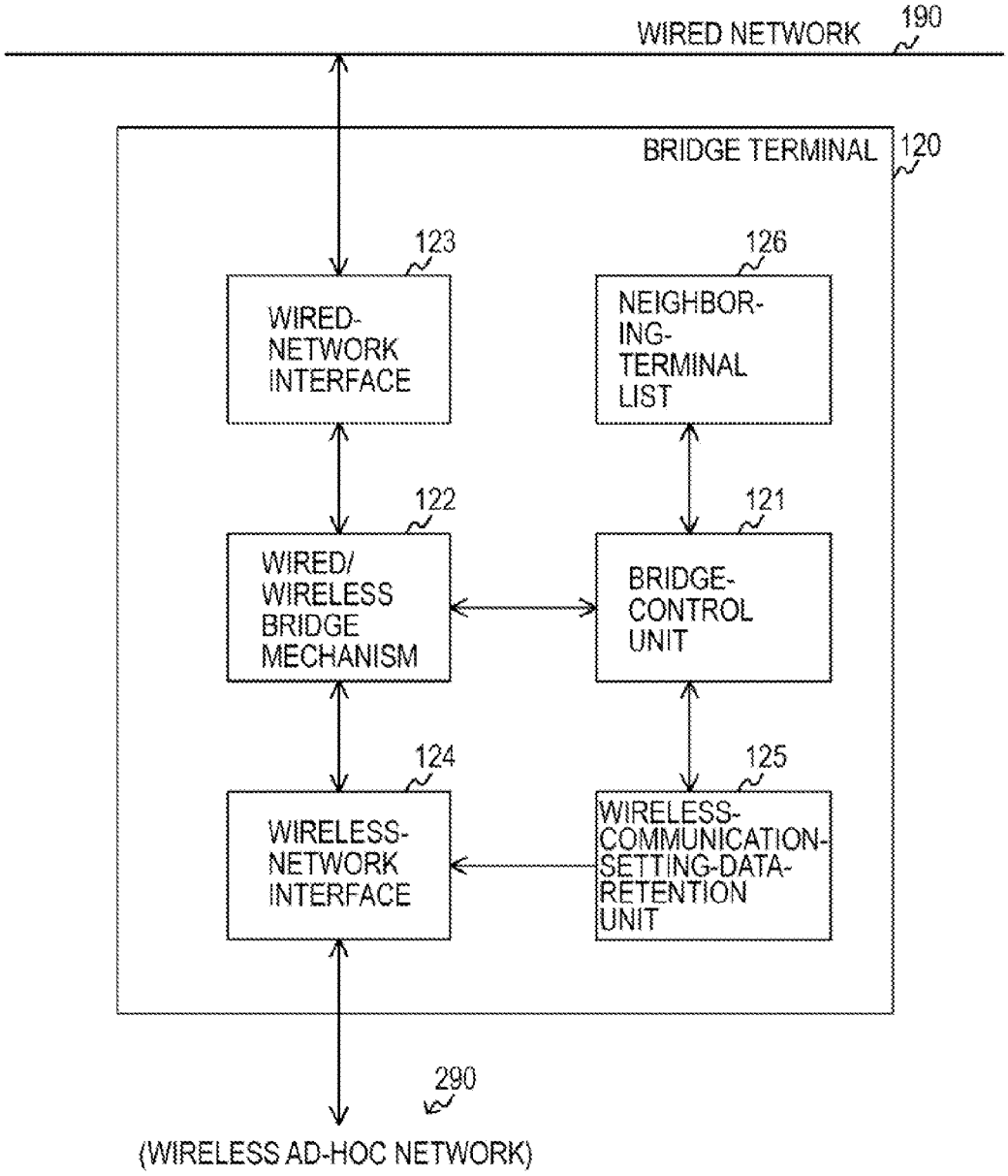

WIRED NETWORK
190
BRIDGE TERMINAL
120
123
WIRED-NETWORK INTERFACE
126
NEIGHBORING-TERMINAL LIST
122
WIRED/WIRELESS BRIDGE MECHANISM
121
BRIDGE-CONTROL UNIT
124
WIRELESS-NETWORK INTERFACE
125
WIRELESS-COMMUNICATION-SETTING-DATA-RETENTION UNIT
290
(WIRELESS AD-HOC NETWORK)

FIG. 3

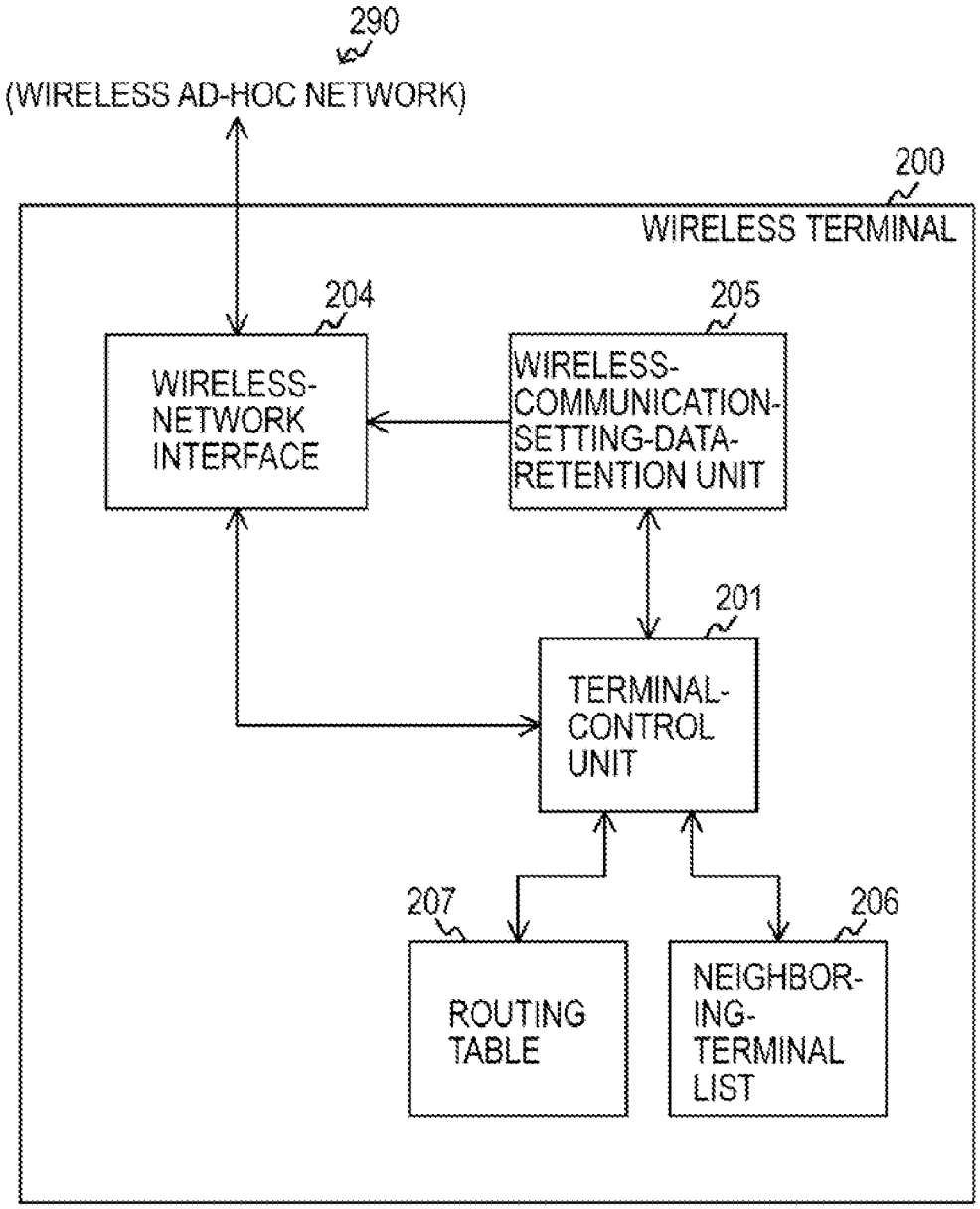

290
(WIRELESS AD-HOC NETWORK)
200
WIRELESS TERMINAL
204
WIRELESS-NETWORK INTERFACE
205
WIRELESS-COMMUNICATION-SETTING-DATA-RETENTION UNIT
201
TERMINAL-CONTROL UNIT
207
ROUTING TABLE
206
NEIGHBOR-ING-TERMINAL LIST

FIG. 4

610

611 612

TERMINAL IDENTIFIER	AUTHENTICATION STATE
WIRELESS TERMINAL A	AUTHENTICATED
WIRELESS TERMINAL B	UNAUTHENTICATED

FIG. 5

620

621 TRANSMISSION-DESTINATION-TERMINAL IDENTIFIER	622 RELAY TERMINAL IDENTIFIER	623 AUTHENTICATION-SERVER METRIC
BRIDGE TERMINAL	WIRELESS TERMINAL A	0
WIRELESS TERMINAL A	WIRELESS TERMINAL A	1
WIRELESS TERMINAL B	WIRELESS TERMINAL B	2

FIG. 6

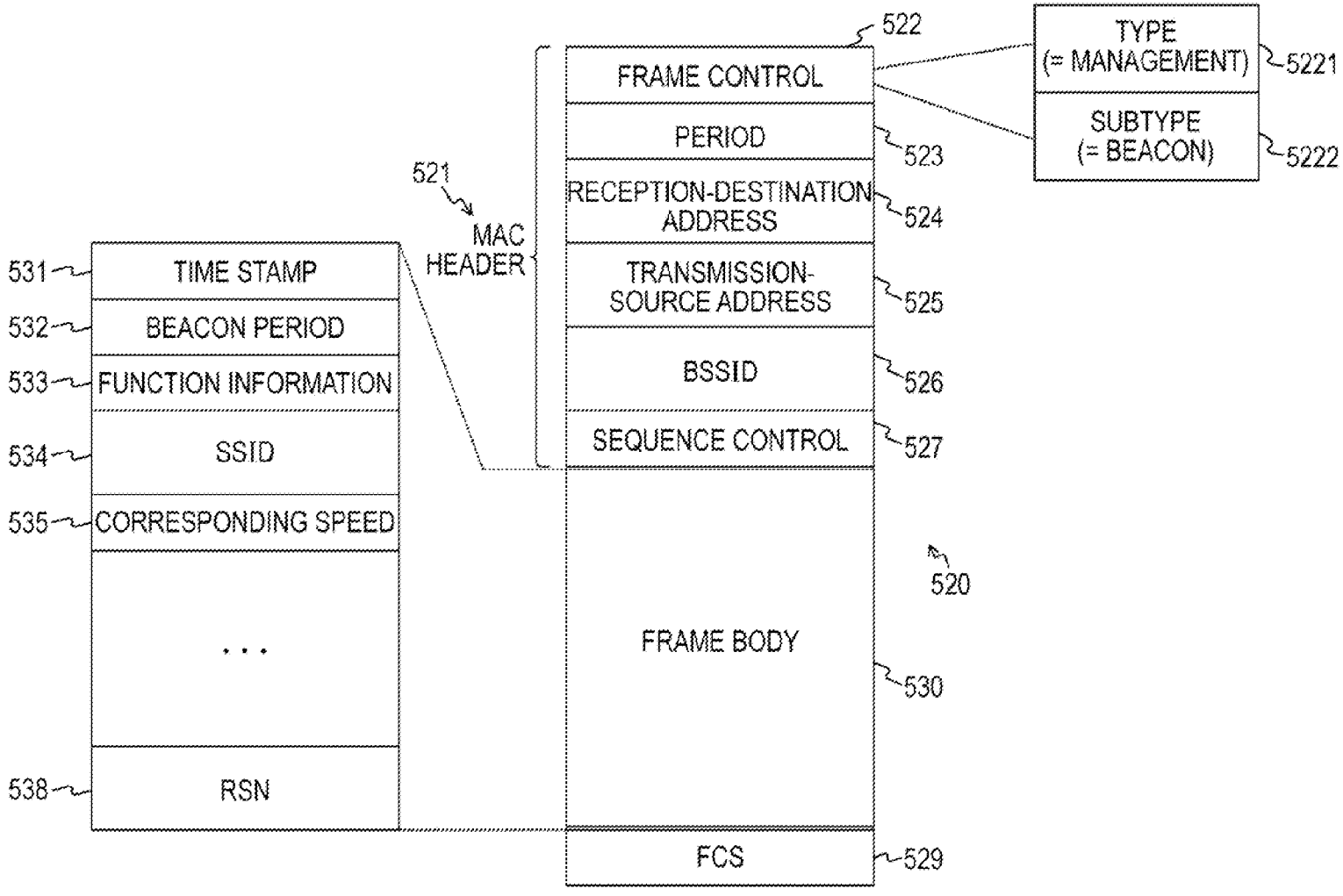

522
FRAME CONTROL
TYPE
(= MANAGEMENT)
5221
SUBTYPE
(= BEACON)
5222
PERIOD
523
521
MAC
HEADER
RECEPTION-DESTINATION
ADDRESS
524
531
TIME STAMP
TRANSMISSION-
SOURCE ADDRESS
525
532
BEACON PERIOD
533
FUNCTION INFORMATION
BSSID
526
534
SSID
SEQUENCE CONTROL
527
535
CORRESPONDING SPEED
520
. . .
FRAME BODY
530
538
RSN
FCS
529

FIG. 7

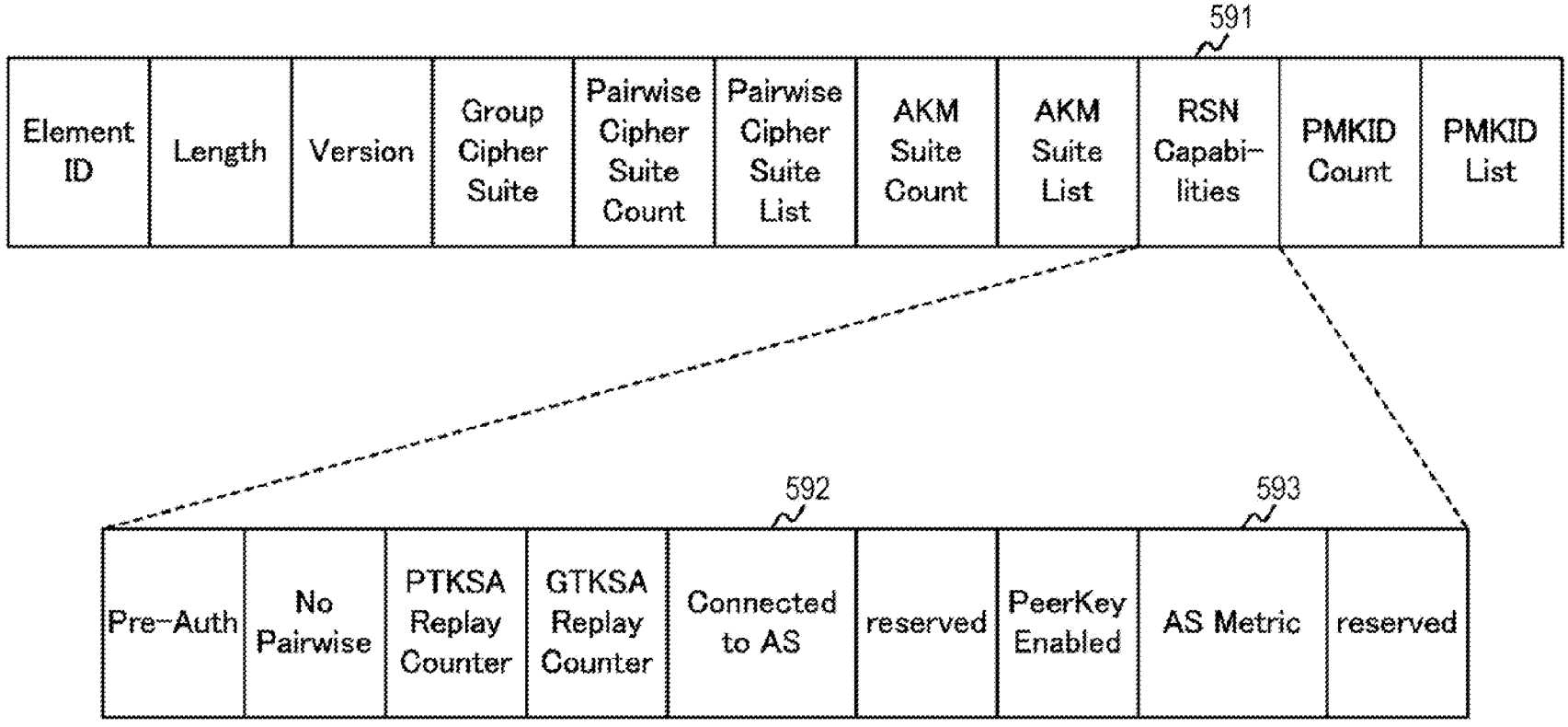

591
Element ID
Length
Version
Group Cipher Suite
Pairwise Cipher Suite Count
Pairwise Cipher Suite List
AKM Suite Count
AKM Suite List
RSN Capabi-lities
PMKID Count
PMKID List
592
593
Pre-Auth
No Pairwise
PTKSA Replay Counter
GTKSA Replay Counter
Connected to AS
reserved
PeerKey Enabled
AS Metric
reserved

FIG. 8

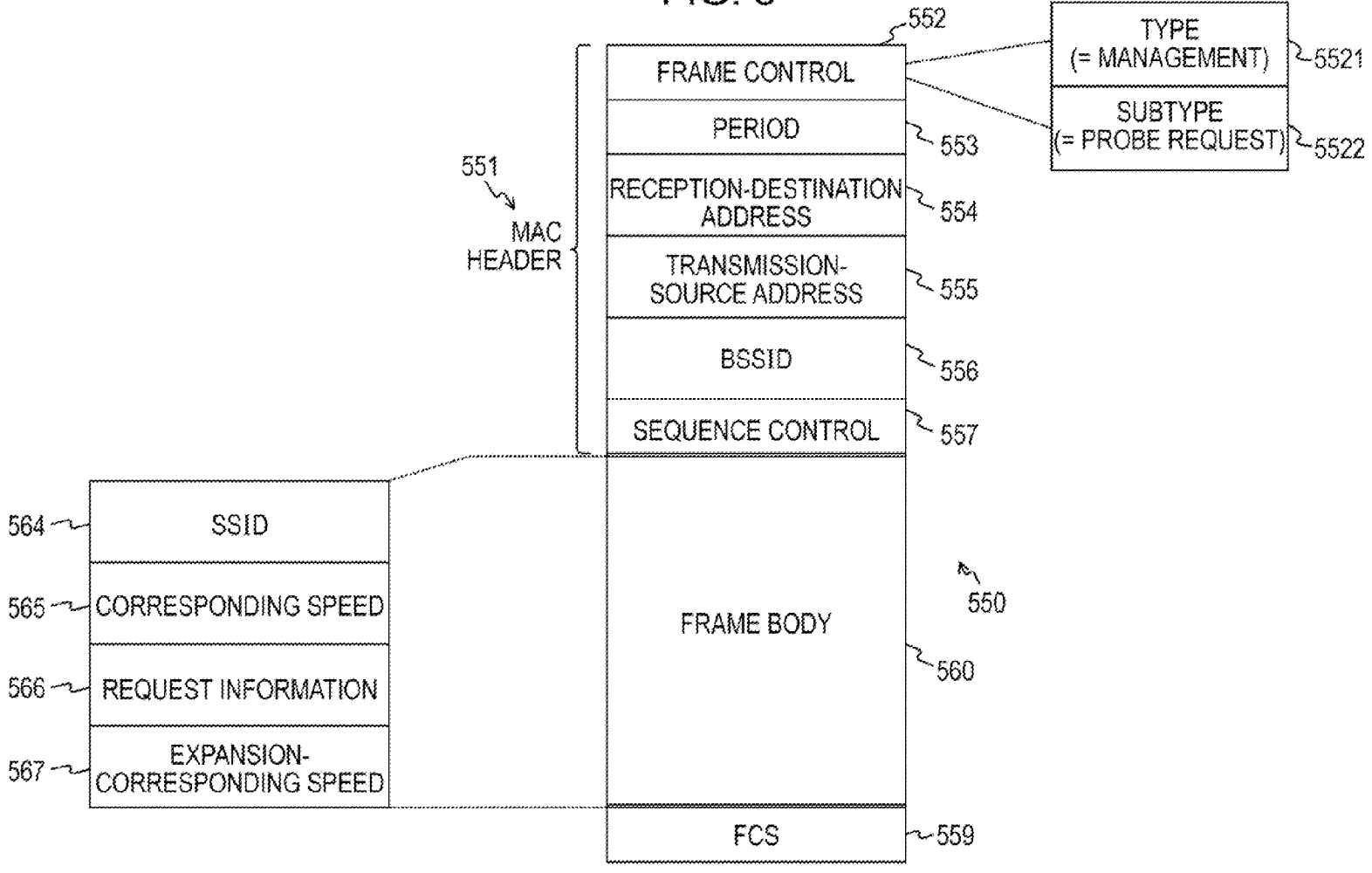

552
FRAME CONTROL
TYPE
(= MANAGEMENT)
5521
SUBTYPE
(= PROBE REQUEST)
5522
PERIOD
553
551
MAC
HEADER
RECEPTION-DESTINATION
ADDRESS
554
TRANSMISSION-
SOURCE ADDRESS
555
BSSID
556
SEQUENCE CONTROL
557
564
SSID
565
CORRESPONDING SPEED
566
REQUEST INFORMATION
567
EXPANSION-
CORRESPONDING SPEED
FRAME BODY
550
560
FCS
559

FIG. 9

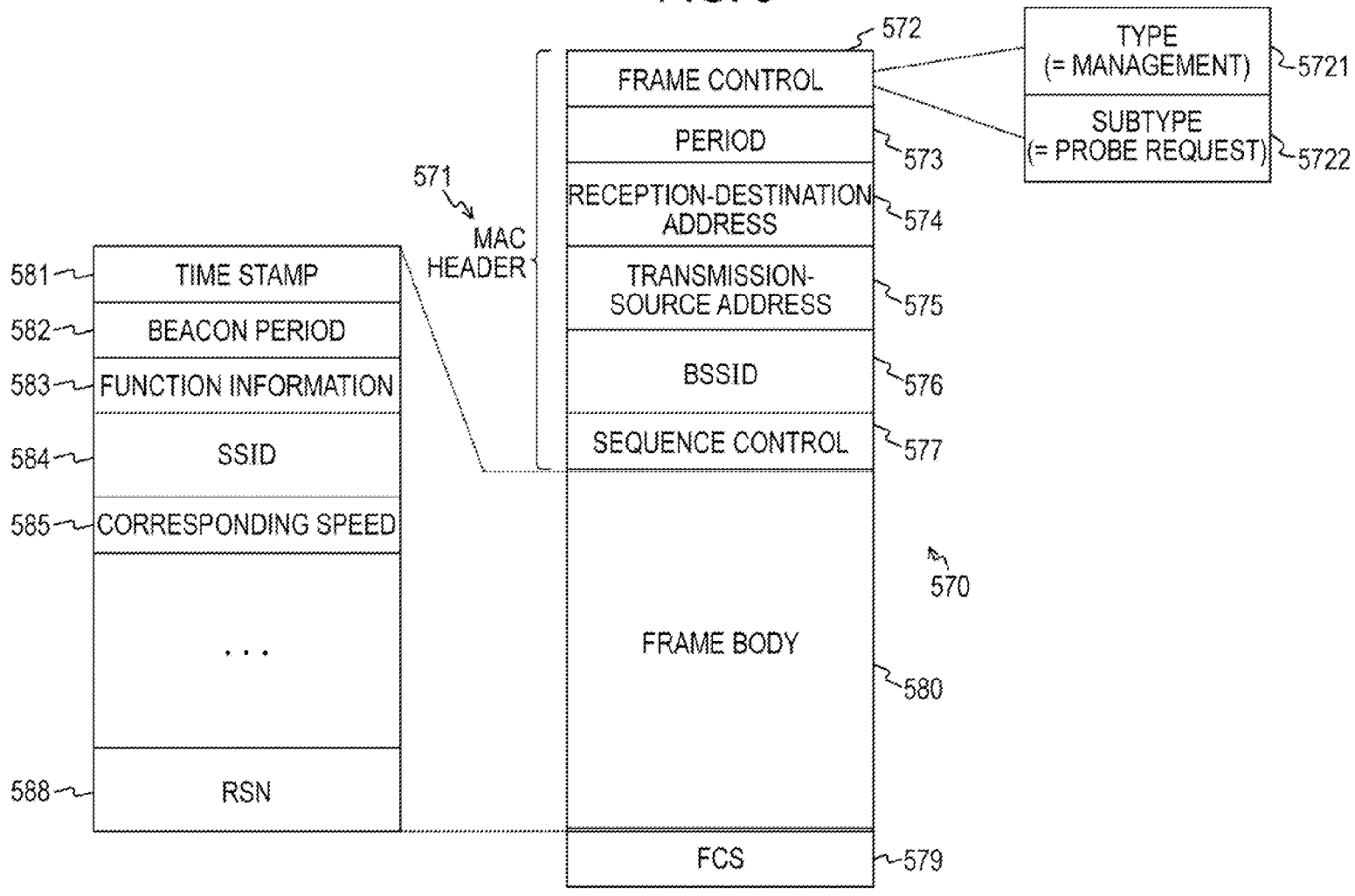

572
FRAME CONTROL
TYPE
(= MANAGEMENT)
5721
SUBTYPE
(= PROBE REQUEST)
5722
PERIOD
573
571
MAC
HEADER
RECEPTION-DESTINATION
ADDRESS
574
581
TIME STAMP
TRANSMISSION-
SOURCE ADDRESS
575
582
BEACON PERIOD
583
FUNCTION INFORMATION
BSSID
576
584
SSID
SEQUENCE CONTROL
577
585
CORRESPONDING SPEED
570
. . .
FRAME BODY
580
588
RSN
FCS
579

FIG. 10

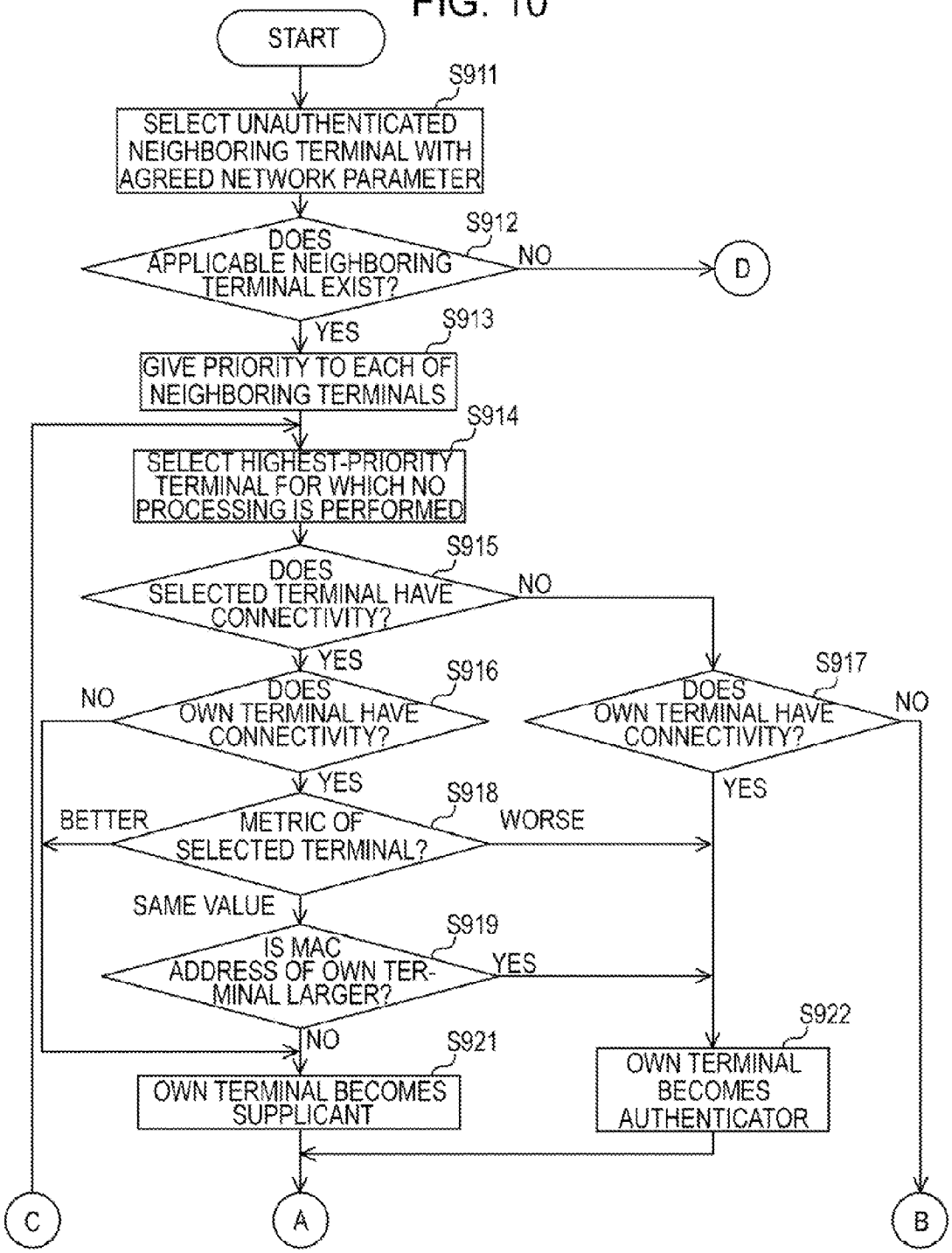

START
S911
SELECT UNAUTHENTICATED NEIGHBORING TERMINAL WITH AGREED NETWORK PARAMETER
S912
DOES APPLICABLE NEIGHBORING TERMINAL EXIST?
NO
D
YES
S913
GIVE PRIORITY TO EACH OF NEIGHBORING TERMINALS
S914
SELECT HIGHEST-PRIORITY TERMINAL FOR WHICH NO PROCESSING IS PERFORMED
S915
DOES SELECTED TERMINAL HAVE CONNECTIVITY?
NO
YES
S916
DOES OWN TERMINAL HAVE CONNECTIVITY?
NO
YES
S917
DOES OWN TERMINAL HAVE CONNECTIVITY?
NO
YES
S918
METRIC OF SELECTED TERMINAL?
BETTER
WORSE
SAME VALUE
S919
IS MAC ADDRESS OF OWN TERMINAL LARGER?
YES
NO
S921
OWN TERMINAL BECOMES SUPPLICANT
S922
OWN TERMINAL BECOMES AUTHENTICATOR
C
A
B

FIG. 11

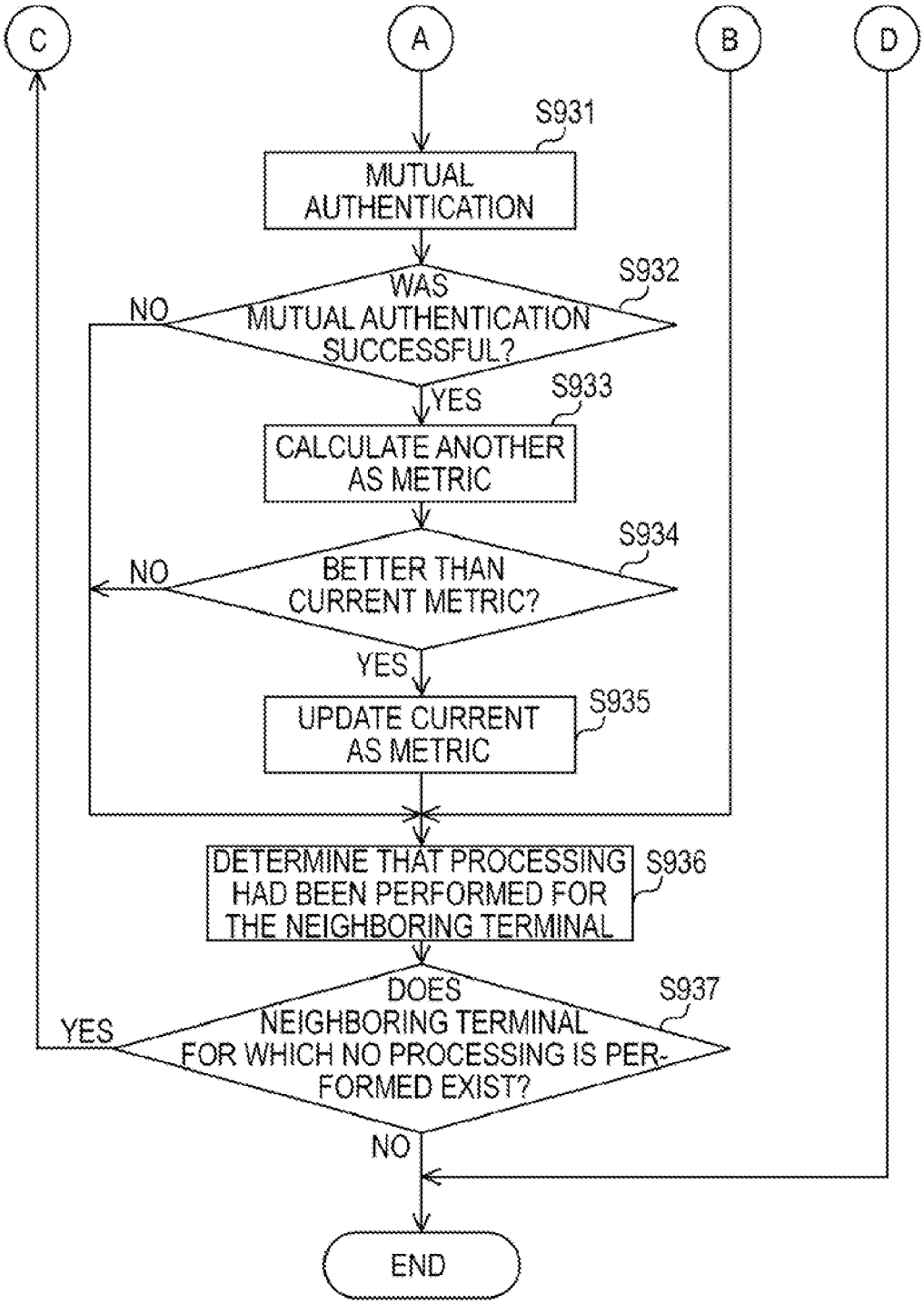

C
A
B
D
S931
MUTUAL AUTHENTICATION
S932
WAS MUTUAL AUTHENTICATION SUCCESSFUL?
NO
YES
S933
CALCULATE ANOTHER AS METRIC
S934
BETTER THAN CURRENT METRIC?
NO
YES
S935
UPDATE CURRENT AS METRIC
S936
DETERMINE THAT PROCESSING HAD BEEN PERFORMED FOR THE NEIGHBORING TERMINAL
S937
DOES NEIGHBORING TERMINAL FOR WHICH NO PROCESSING IS PERFORMED EXIST?
YES
NO
END

FIG. 12

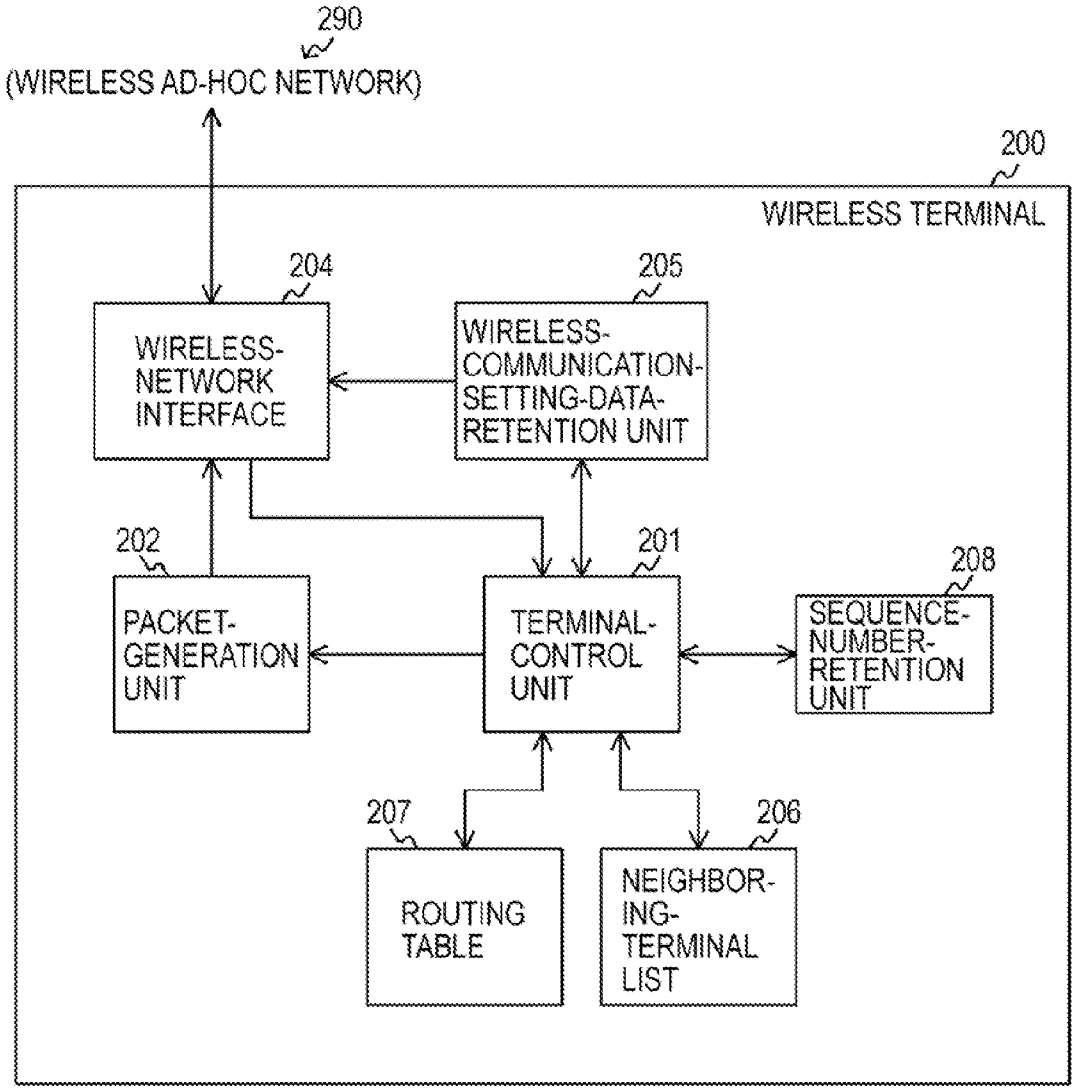

290
(WIRELESS AD-HOC NETWORK)
200
WIRELESS TERMINAL
204
WIRELESS-NETWORK INTERFACE
205
WIRELESS-COMMUNICATION-SETTING-DATA-RETENTION UNIT
202
PACKET-GENERATION UNIT
201
TERMINAL-CONTROL UNIT
208
SEQUENCE-NUMBER-RETENTION UNIT
207
ROUTING TABLE
206
NEIGHBORING-TERMINAL LIST

FIG. 13

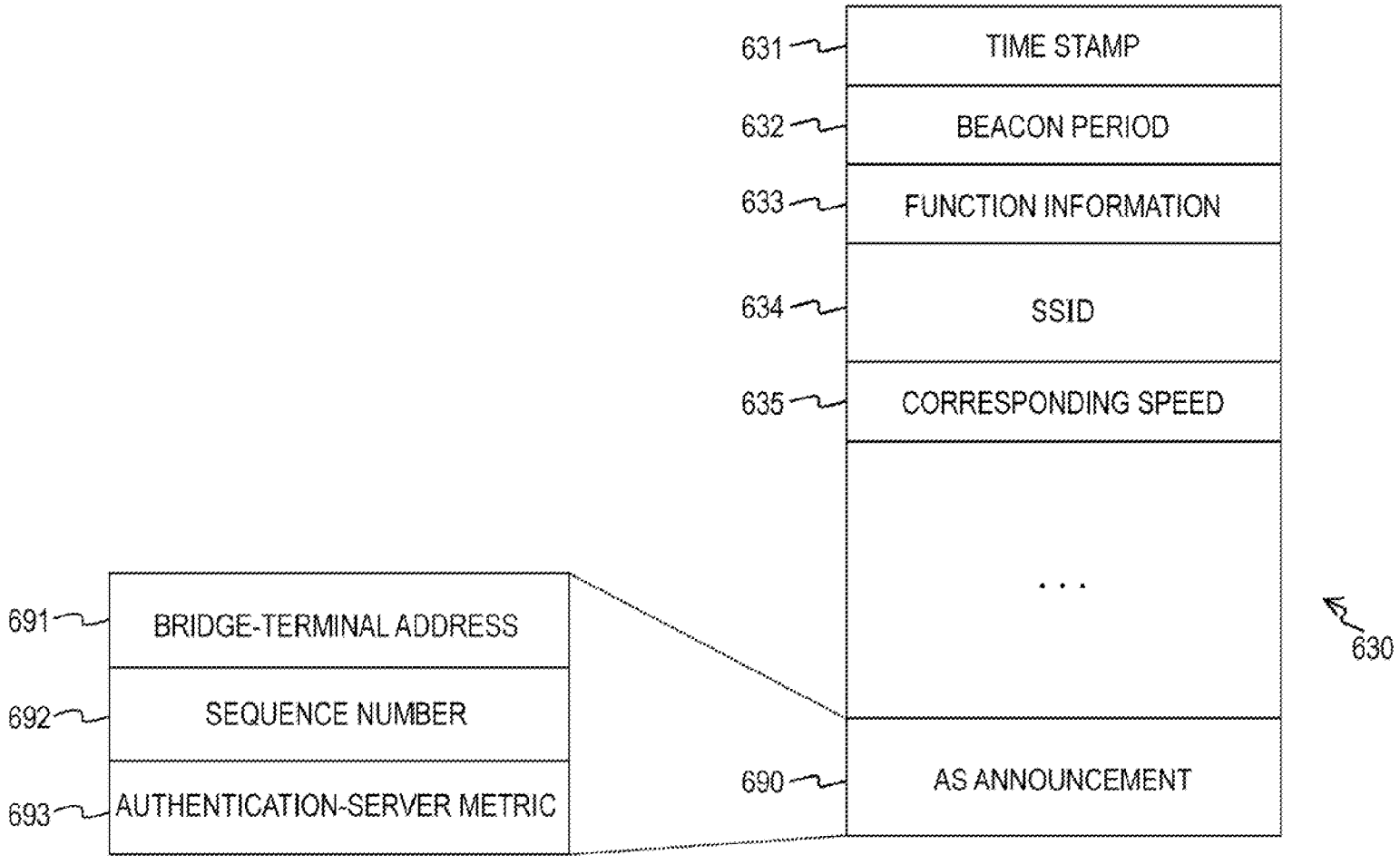
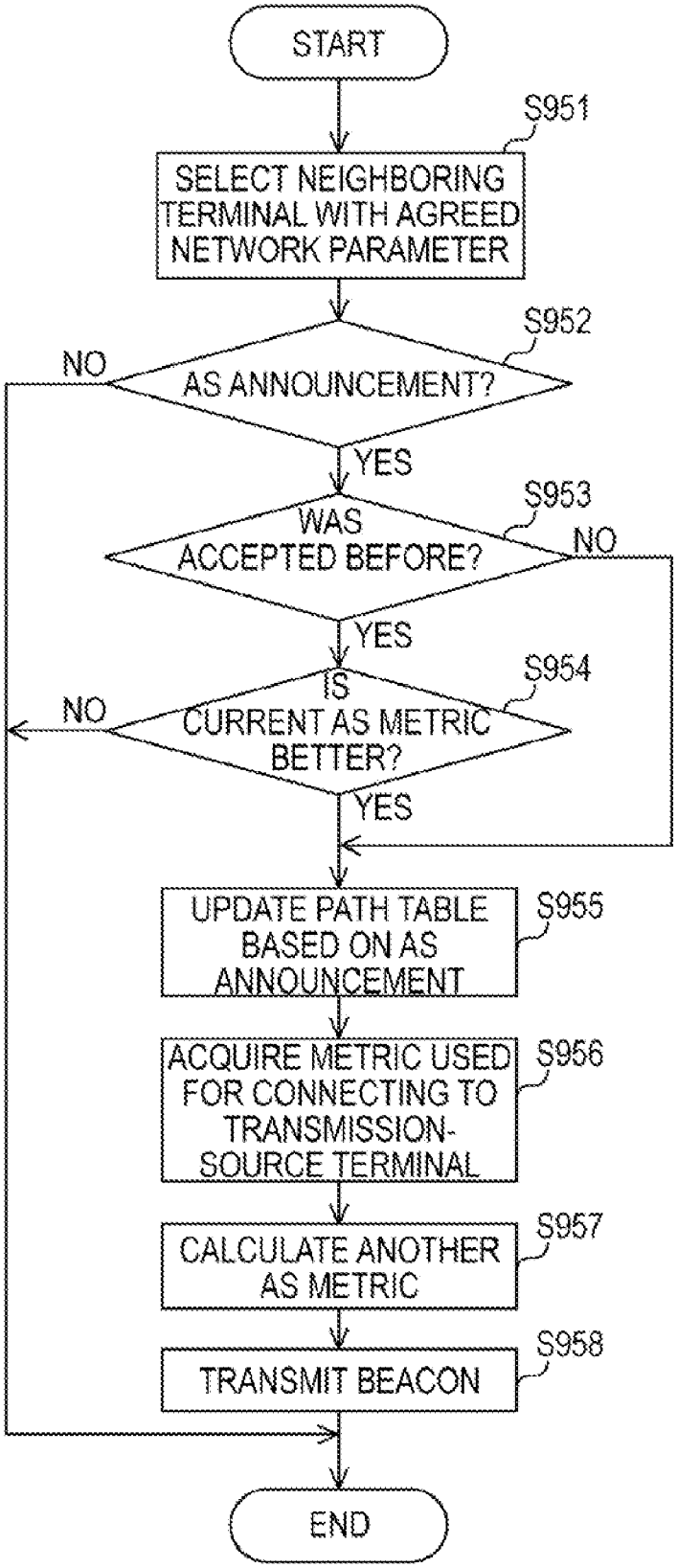

631
TIME STAMP
632
BEACON PERIOD
633
FUNCTION INFORMATION
634
SSID
635
CORRESPONDING SPEED
. . .
630
690
AS ANNOUNCEMENT
691
BRIDGE-TERMINAL ADDRESS
692
SEQUENCE NUMBER
693
AUTHENTICATION-SERVER METRIC

FIG. 14


START
S951
SELECT NEIGHBORING TERMINAL WITH AGREED NETWORK PARAMETER
S952
AS ANNOUNCEMENT?
NO
YES
S953
WAS ACCEPTED BEFORE?
NO
YES
S954
IS CURRENT AS METRIC BETTER?
NO
YES
UPDATE PATH TABLE BASED ON AS ANNOUNCEMENT
S955
ACQUIRE METRIC USED FOR CONNECTING TO TRANSMISSION-SOURCE TERMINAL
S956
CALCULATE ANOTHER AS METRIC
S957
TRANSMIT BEACON
S958
END

COMMUNICATION SYSTEM, WIRELESS-COMMUNICATION DEVICE, AND CONTROL METHOD THEREFOR

CROSS REFERENCES TO RELATED APPLICATIONS

[0001] The present invention contains subject matter related to Japanese Patent Application JP 2006-221719 filed in the Japanese Patent Office on Aug. 15, 2006, the entire contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates to a communication system and particularly relates to a communication system and a wireless-communication device, a communication-control method used therefor, and a program making a computer perform the communication-control method that are provided to authenticate the authority to access a wireless network.

[0004] 2. Description of the Related Art

[0005] The infrastructure mode and the ad-hoc mode are known, as modes of forming a network by using a wireless technology. In the infrastructure mode, a network is formed under the centralized control of a wireless-communication device referred to as an access point (AP) or the like. On the other hand, in the ad-hoc mode, the centralized control is not performed by a specified access point, and asynchronous wireless communications are directly performed between arbitrary wireless-communication devices operating, as wireless terminals, so that a network is formed.

[0006] Methods of improving the security function of the above-described wireless networks have been proposed. For example, Japanese Unexamined Patent Application Publication No. 2004-180324 proposes a technology of applying an authentication system using an authentication server (AS) typified by Institute of Electrical and Electronics Engineers (IEEE) 802.1X to the infrastructure mode of IEEE802.11.

SUMMARY OF THE INVENTION

[0007] According to the known technologies, the AP used in the infrastructure mode functions, as authentication proxy provided to access the authentication server, and mediates an authentication-protocol sequence between the wireless terminal and the authentication server. An entity operating, as the authentication proxy provided to access the authentication server for a different wireless terminal in the above-described manner is referred to as an authenticator and an entity subjected to authentication processing via the authenticator is referred to as a supplicant.

[0008] On the other hand, since the role of each of wireless terminals is not determined explicitly in the ad-hoc mode, the roles of the wireless terminals should be determined by a standard of some kind. In that case, a wireless terminal that can access the authentication server may be selected, as the authenticator. However, there may be a plurality of the wireless terminals that can access the authentication server. If two wireless terminals performing authentication can access the authentication server, the roles of the two wireless terminals may be determined according to the value of each of media-access-control (MAC) addresses.

[0009] In the ad-hoc mode, however, each of wireless-communication devices may move and the wireless-communication quality of a path between the wireless-communication devices is not consistent. If the roles of the authenticator and the supplicant are determined and fixed in the above-described state, it is apprehended that an authentication message may be transferred through an inefficient authentication path eventually.

[0010] Therefore, it is desirable to determine the roles of the authenticator and the supplicant in consideration of a path leading to the authentication server.

[0011] Therefore, according to an embodiment of the present invention, there is provided a wireless-communication device performing mutual authentication between the wireless-communication device and a different wireless-communication device by using an authentication server. The wireless-communication device includes a communication-setting-data-retention unit configured to retain communication-setting data including a first metric corresponding to the path from the wireless-communication device to the authentication server, as a self-authentication-server metric, a signal-reception unit configured to receive a predetermined signal transmitted from the different wireless-communication device, the predetermined signal including a second metric corresponding to the path from the different wireless-communication device to the authentication server, as a nonself-authentication-server metric, and a control unit configured to make a first setting so that the wireless-communication device operates, as a supplicant, during the mutual authentication when the self-authentication-server metric is better than the nonself-authentication-server metric, and make a second setting so that the wireless-communication device operates, as an authenticator, during the mutual authentication when the self-authentication-server metric is worse than the nonself-authentication-server metric. Subsequently, the roles of the supplicant and the authenticator, the roles being played during the mutual authentication, are determined with reference to the metric corresponding to the path to the authentication server. Namely, a wireless-communication device having a path which makes it easier to access the authentication server becomes the authenticator, whereby the mutual authentication is performed with efficiency.

[0012] Further, in the above-described embodiment, the communication-setting data retained in the communication-setting-data-retention unit may include data on a first address of the wireless-communication device, the predetermined signal may include data on a second address of the different wireless-communication device, and when the self-authentication-server metric is equivalent to the nonself-authentication-server metric, the control unit may make a third setting so that the wireless-communication device operates, as either the authenticator or the supplicant, during the mutual authentication according to a relationship between the first address and the second address. More specifically, when the first address is larger than the second address, the control unit may make a fourth setting so that the wireless-communication device operates, as the authenticator, during the mutual authentication, and when the first address is not larger than the second address, the control unit

may make a fifth setting so that the wireless-communication device operates, as the supplicant, during the mutual authentication. Subsequently, when the metrics corresponding to the paths to the authentication server are equivalent to each other, the roles of the supplicant and the authenticator, the roles being played during the mutual authentication, are determined according to the relationship between the addresses of the wireless-communication devices. Namely, even though it is difficult to determine the roles of the wireless-communication devices based on the metrics corresponding to the paths to the authentication server, the role determination can be made between the wireless-communication devices without contradiction.

[0013] Further, in the above-described embodiment, the predetermined signal may include first accessibility information indicating whether or not the different wireless communication device can make access to the authentication server, and the communication-setting data retained in the communication-setting-data-retention unit may include second accessibility information indicating whether or not the wireless-communication device can make access to the authentication server. Still further, in the above-described embodiment, when the first accessibility information shows that the different wireless-communication device can make access to the authentication server and the second accessibility information shows that the wireless-communication device makes access to the authentication server with difficulty, the control unit may make a sixth setting so that the wireless-communication device operates, as the supplicant, during the mutual authentication irrespective of a relationship between the self-authentication-server metric and the nonself-authentication-server metric, and when the first accessibility information shows that the different wireless-communication device makes access to the authentication server with difficulty and the second accessibility information shows that the wireless-communication device can make access to the authentication server, the control unit may make a seventh setting so that the wireless-communication device operates, as the authenticator, during the mutual authentication irrespective of the relationship between the self-authentication-server metric and the nonself-authentication-server metric. Subsequently, the roles of the supplicant and the authenticator, the roles being played during the mutual authentication, are determined according to whether or not access to the authentication server can be made.

[0014] Further, in the above-described embodiment, the first metric and/or the second metric may show the number of at least one hop of a wireless-communication path leading to the authentication server, and/or the wireless-communication quality of the wireless-communication path may be considered.

[0015] Further, in the above-described embodiment, when the control unit calculates a third metric corresponding to the path to the authentication server after the mutual authentication is achieved and the third metric is better than the self-authentication-server metric retained in the communication-setting-data-retention unit, the control unit may make the communication-setting-data-retention unit retain the third metric. Subsequently, the self-authentication-server metric can be updated.

[0016] Further, in the above-described embodiment, the wireless-communication device may further include a nonself-authentication-server-metric-retention unit provided for the different wireless-communication device, the nonself-authentication-server-metric-retention unit being configured to retain the nonself-authentication-server metric, and a neighboring-metric-acquisition unit configured to acquire a fourth metric provided between the wireless-communication device and the different wireless-communication device, as a neighboring metric, wherein the control unit may calculate the self-authentication-server metric by adding the nonself-authentication-server metric to the neighboring metric. Subsequently, the nonself-authentication-server-metric-retention unit is made to retain the nonself-authentication-server metric in advance through an AS announcement or the like, whereby the self-authentication-server metric is calculated. Further, when there is a plurality of the different wireless-communication devices, upon receiving the predetermined signal transmitted from each of the different wireless-communication devices, the signal-reception unit may make the nonself-authentication-server-metric-retention unit retain the nonself-authentication-server metric based on the predetermined signal including the nonself-authentication-server metric which is the best of the nonself-authentication-server metrics of all of the predetermined signals. Subsequently, upon receiving an AS announcement transmitted from each of different wireless-communication devices, the AS announcement being transmitted from a single bridge terminal operating, as a transmission source, the signal-reception unit makes the nonself-authentication-server-metric-retention unit retain the most appropriate nonself-authentication-server metric.

[0017] Further, according to another embodiment of the present invention, there is provided a communication system performing mutual authentication between at least two wireless-communication devices by using an authentication server, wherein each of the wireless-communication devices includes a communication-setting-data-retention unit configured to retain communication-setting data including a first metric corresponding to the path from the wireless-communication device to the authentication server, as a self-authentication-server metric, a signal-transmission unit configured to transmit a first signal including the self-authentication-server metric, a signal-reception unit configured to receive a second signal transmitted from the different wireless-communication device, the second signal including a second metric corresponding to the path from the different wireless-communication device to the authentication server, as a nonself-authentication-server metric, and a control unit configured to make a first setting so that the wireless-communication device operates, as a supplicant, during the mutual authentication when the self-authentication-server metric is better than the nonself-authentication-server metric, and make a second setting so that the wireless-communication device operates, as an authenticator, during the mutual authentication when the self-authentication-server metric is worse than the nonself-authentication-server metric. Subsequently, the roles of the supplicant and the authenticator, the roles being played during the mutual authentication, are determined with reference to the metric corresponding to the path to the authentication server.

[0018] According to an embodiment of the present invention, the state of a path leading to an authentication server will be reflected when the roles of an authenticator and a supplicant that are provided to perform authentication are determined.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] FIG. **1** shows an example configuration of a communication system according to an embodiment of the present invention;

[0020] FIG. **2** shows an example configuration of a bridge terminal according to an embodiment of the present invention;

[0021] FIG. **3** shows an example configuration of a wireless terminal according to an embodiment of the present invention;

[0022] FIG. **4** shows an example configuration of a neighboring-terminal list according to an embodiment of the present invention;

[0023] FIG. **5** shows an example configuration of a routing table according to an embodiment of the present invention;

[0024] FIG. **6** shows the format of a beacon frame generated by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard;

[0025] FIG. **7** shows example data items included in an RSN field according to an embodiment of the present invention;

[0026] FIG. **8** shows the format of a probe-request frame generated by the IEEE 802.11 standard;

[0027] FIG. **9** shows the format of a probe-response frame generated by the IEEE 802.11 standard;

[0028] FIG. **10** shows the first half of example processing procedures performed by a wireless terminal according to an embodiment of the present invention;

[0029] FIG. **11** shows the latter half of the example processing procedures performed by the wireless terminal;

[0030] FIG. **12** shows an example modification of a wireless terminal according to an embodiment of the present invention;

[0031] FIG. **13** shows a frame body of a beacon frame of the example modification of the wireless terminal shown in FIG. **12**; and

[0032] FIG. **14** shows example processing procedures performed by the example modification of the wireless terminal shown in FIG. **12**.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0033] Next, embodiments of the present invention will be described in detail with reference to the attached drawings.

[0034] FIG. **1** shows an example configuration of a communication system according to an embodiment of the present invention. The communication system includes a wired network **190** connecting an authentication server **110** and a bridge terminal **120** to each other, and a wireless ad-hoc network **290** connecting the bridge terminal **120**, a wireless terminal A**210**, a wireless terminal B**220**, and a wireless terminal C**230** to one another.

[0035] The authentication server **110** is configured to authenticate the access authority of a wireless terminal which is going to access the communication system. The authentication server **110** authenticates a wireless terminal operating, as a supplicant, via a wireless terminal operating, as an authenticator.

[0036] The bridge terminal **120** functions, as a bridge connecting the wired network **190** and the wireless ad-hoc network **290** to each other. The bridge terminal **120** functions, as a wired-communication device connected to the wired network **190**, and functions, as a wireless-communication device included in the wireless ad-hoc network **290**.

[0037] Each of the wireless terminals A**210**, B**220**, and C**230** (hereinafter collectively referred to as a wireless terminal **200**, as required), and the bridge terminal **120** function, as wireless-communication devices included in the wireless ad-hoc network **290**.

[0038] When another wireless terminal is to be connected to the wireless ad-hoc network **290**, mutual authentication is performed between the wireless terminal and different wireless terminals that had already been included in the wireless ad-hoc network **290**. For example, when the wireless terminal C**230** is to be connected to the wireless ad-hoc network **290**, and the bridge terminal **120** and the wireless terminals A**210** and B**220** had already been included in the wireless ad-hoc network **290**, mutual authentication is performed between the wireless terminal C**230** and the wireless terminal A**210**, and the wireless terminal C**230** and the wireless terminal B**220**.

[0039] Before the above-described mutual authentication is performed, the wireless terminals transmit and/or receive beacons (broadcast signals) to and/or from one another. When the wireless terminal C**230** receives the beacon transmitted from the wireless terminal A**210** before receiving the beacon transmitted from the wireless terminal B**220**, the mutual authentication is performed between the wireless terminals A**210** and C**230**. During the mutual authentication, one of the wireless terminals A**210** and C**230** operates, as an authenticator, and the other operates, as a supplicant. At that time, it is difficult for the wireless terminal C**230** to connect to the authentication server **110**. Therefore, the wireless terminal A**210** operates, as the authenticator and the wireless terminal C**230** operates, as the supplicant. Namely, the wireless terminal A**210** functions, as authentication proxy of the authentication server **110** so that the wireless terminal C**230** is authenticated. As a result, an authenticated link is formed between the wireless terminals A**210** and C**230**.

[0040] After that, when the wireless terminal C**230** receives the beacon transmitted from the wireless terminal B**220**, mutual authentication is performed between the wireless terminals B**220** and C**230**. At that time, a link had already been made between the wireless terminal C**230** and the authentication server **110**. Therefore, either of the wireless terminals B**220** and C**230** can operate, as the authenticator. According to the above-described embodiment of the present invention, a path extending the wireless terminal B**220** to the authentication server **110** and a path from the wireless terminal C**230** to the authentication server **110** are compared to each other. Subsequently, the wireless terminal having a path which allows easier access to the authentication server **110** is determined to be the authenticator.

[0041] A metric functions, as the standard of the "path which allows easier access to the authentication server 110" is referred to as an "authentication-server metric". As the

authentication-server metric, for example, the number of hops of a wireless-communication path extending to the authentication server **110**, namely, the number of hops used to reach the bridge terminal **120** can be used, as the authentication-server metric. In that case, the less the number of hops of the path (the better the authentication-server metric), the easier it becomes to access the authentication server. According to the above-described embodiment, the wireless terminal B**220** has an authentication-server metric better than that of the wireless terminal C**230**.

[**0042**] Further, the authentication-server metric may be not only the number of hops of a wireless-communication path extending to the authentication server, but also a value including the value of the wireless-communication quality of each of links of the path. For example, an expected transmission count (ETX) suggested for a path-control protocol may be used, as the authentication-server metric. The ETX is a value obtained based on interactive delivery ratios obtained through wireless terminals transmitting and/or receiving a probe request and a probe response to and/or from one another (D. Couto, et al.: "A High-Throughput Path Metric for Multi-Hop Wireless Routing", Proc. of the 9th ACM International Conference on Mobile Computing and Networking (MobiCom '03), September 2003).

[**0043**] Further, the wireless-communication quality that can be used for the authentication-server metric may be the number of frame retransmission, the transmission-queue length, the radio-wave intensity, and so forth.

[**0044**] FIG. **2** shows an example configuration of the bridge terminal **120** according to the above-described embodiment. The bridge terminal **120** includes a bridge-control unit **121**, wired/wireless-bridge mechanism **122**, a wired-network interface **123**, a wireless-network interface **124**, a wireless-communication-setting-data-retention unit **125**, and a neighboring-terminal list **126**.

[**0045**] The bridge-control unit **121** controls the entire bridge terminal **120**. The wired/wireless-bridge mechanism **122** performs protocol conversion for the wired network **190** and the wireless ad-hoc network **290**. The wired-network interface **123** is an interface used for transmitting and/or receiving data between the wired network **190** and the bridge terminal **120**. The wireless-network interface **124** is an interface used for transmitting and/or receiving data between the wireless ad-hoc network **290** and the bridge terminal **120**.

[**0046**] The wireless-communication-setting-data-retention unit **125** is configured to retain setting data used for performing wireless communications. For example, a service-set identifier (SSID), security-setting data, the MAC address of the bridge terminal **120**, and so forth are retained, as the setting data. Here, the SSID is an identifier used for identifying the wireless ad-hoc network **290**. For example, an arbitrary character string input by a user is used, as the SSID. Further, a code, an identifier, and so forth used for a robust security network (RSN) can be retained, as the security-setting data.

[**0047**] The neighboring-terminal list **126** is a list of wireless terminals operating on the wireless ad-hoc network **290**, the wireless terminals existing in the vicinity of the bridge terminal **120**. Upon receiving beacons transmitted from the wireless terminals at regular intervals, the bridge-control unit **121** performs control so that the neighboring-terminal list **126** shows the latest state.

[**0048**] FIG. **3** shows an example configuration of the wireless terminal **200** according to the above-described embodiment. The wireless terminal **200** includes a terminal-control unit **201**, a wireless-network interface **204**, a wireless-communication-setting-data-retention unit **205**, a neighboring-terminal list **206**, and a routing table **207**.

[**0049**] The terminal-control unit **201** controls the entire wireless terminal **200**. The wireless-network interface **204** is an interface used for transmitting and/or receiving data between the wireless ad-hoc network **290** and the wireless terminal **200**.

[**0050**] The wireless-communication-setting-data-retention unit **205** is configured to retain setting data used for performing wireless communications. For example, an SSID used to identify the wireless ad-hoc network **290**, security-setting data including a code, an identifier, and so forth that are used for the RSN, the MAC address of the wireless terminal **200**, the current identification-server metric of the wireless terminal **200**, and so forth are retained, as the setting data.

[**0051**] The neighboring-terminal list **206** is a list of wireless terminals operating on the wireless ad-hoc network **290**, the wireless terminals existing in the vicinity of the wireless terminal **200**. Upon receiving beacons transmitted from different wireless terminals at regular intervals, the bridge-control unit **201** performs control so that the neighboring-terminal list **206** shows the latest state.

[**0052**] The routing table **207** is a table including the list of paths of the wireless ad-hoc network **290**, the paths extending to the bridge terminal **120** and/or the different wireless terminals.

[**0053**] FIG. **4** shows an example configuration of a neighboring-terminal list **610** according to an embodiment of the present invention. The neighboring-terminal list **610** corresponds to the neighboring-terminal list **126** of the bridge terminal **120** and/or the neighboring-terminal list **206** of the wireless terminal **200**.

[**0054**] The neighboring-terminal list **610** retains data on a terminal identifier **611** of each of wireless terminals in the neighborhood of the bridge terminal **200** and/or the wireless terminal **200** (hereinafter referred to as neighboring terminals) and data on an authentication state **612** between the bridge terminal **200** and/or the wireless terminal **200**, and each of the neighboring terminals.

[**0055**] The terminal identifier **611** of each of the neighboring terminals may be the MAC address of the wireless terminal corresponding to the neighboring terminal. Further, a flag indicating whether or not mutual authentication is finished between the bridge terminal **200** and/or the wireless terminal **200**, and the wireless terminal is shown, as the authentication state **612**. More specifically, the flag is shown, as "authenticated", or "unauthenticated".

[**0056**] FIG. **5** shows an example configuration of a routing table **620** according to an embodiment of the present invention. The routing table **620** corresponds to the routing table **207** of the wireless terminal **200**. The routing table **620** retains data on a terminal identifier **621** of a wireless terminal which becomes the final transmission destination

during the frame transmission (hereinafter referred to as a transmission-destination terminal), a terminal identifier **622** of a wireless terminal relaying a frame which is to be transmitted to the transmission-destination terminal (hereinafter referred to as a relay terminal), and an authentication-server metric **623** used to transmit data from the transmission-destination terminal to the authentication server **110**. The routing table **620** retains the data on the terminal identifier **621**, the terminal identifier **622**, and the authentication-server metric **623** for each of the transmission-destination terminals.

[**0057**] The transmission-destination-terminal identifier **621** and the relay terminal **622** may be the MAC address of the corresponding wireless terminal, for example. Further, the authentication-server metric **623** may be the number of hops of a path leading to the bridge terminal **120** and/or a value including the wireless-communication quality of each of links of the path.

[**0058**] At the data-transmission time, routing is performed on the basis of the routing table **620**. For example, when data is transmitted to the bridge terminal, a search is made for the terminal identifier of the bridge terminal in the field of the transmission-destination-terminal identifier **621**, and the terminal identifier of the wireless terminal A corresponding to the bridge terminal is acquired, where data on the wireless terminal A is retained in the relay-terminal identifier **622**. Subsequently, user can learn that the wireless terminal A should be used, as the relay terminal, so as to transmit data to the bridge terminal.

[**0059**] FIG. **6** shows the format of a beacon frame generated by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard. A beacon frame **520** is used to transmit beacon information of a MAC sub layer. The beacon frame **520** includes a MAC header **521**, a frame body **530**, and a frame check sequence (FCS) **529**. The MAC header **521** includes data on a frame control **522**, a period **523**, a reception-destination address **524**, a transmission-source address **525**, a basic-service-set identifier (BSSID) **526**, and a sequence control **527**.

[**0060**] The frame control **522** is a field showing control information about a frame and includes information about the kind of the frame and/or the communication mode. A type **5221** included in the frame control **522** shows the type of the frame. Further, a sub type **5222** shown in the frame control **522** shows the sub type of the frame. According to the above-described beacon frame, the frame type is a management frame, and the sub type is a beacon frame.

[**0061**] The period **523** is a field showing a reserved time required to finish the frame transmission.

[**0062**] The transmission-source address **525** indicates the address of a wireless terminal existing on the transmission side. For example, a terminal identifier can be used, as the transmission-source address **525**. Further, the reception-destination address **524** indicates the address of a wireless terminal existing on the reception side. In the case where the beacon frame **520** is used, a broadcast address is used, as the reception-destination address **524**.

[**0063**] The BSSID **526** is provided to retain data on a basic-service-set identifier (BSSID) defined by the IEEE 802.11 standard. In the ad-hoc mode, the MAC address of the first wireless terminal started on a network to which the wireless terminal belongs is used.

[**0064**] The sequence control **527** is a field showing the fragment number used when data is divided into fragments and the sequence number.

[**0065**] The frame body **530** corresponds to the payload of the beacon frame **520** and is used to transfer data existing in the MAC-sub layer. The FCS **529** is a field used to detect an error occurring in the beacon frame **520**. In the FSC **529**, 1's complement of the remainder of a remainder calculation of a generator polynomial is set.

[**0066**] The beacon frame **520** includes data on a time stamp **531**, a beacon period **532**, function information **533**, an SSID **534**, corresponding speed **535**, an RSN **538**, and so forth, as the frame body **530**.

[**0067**] The time stamp **531** shows the value of a timer used for a time-synchronization function in microseconds. The beacon period **532** shows the period in which a beacon frame is transmitted in microseconds.

[**0068**] The function information **533** shows various types of information relating to a point-coordination function (PCF), data encryption, and so forth. The function information **533** includes information about network-operation mode indicating whether a wireless terminal which transmits data is a basic-service set (BSS) under the control of an access point used in infrastructure mode, or an independent-basic-service set (IBSS) used in the ad-hoc mode.

[**0069**] The SSID **534** shows a service-set identifier used to identify the wireless ad-hoc network **290**. The corresponding speed **535** shows the list of supported wireless-transfer rates. The RSN **538** is a field provided to retain information including a code, an identifier, and so forth that are used for the RSN.

[**0070**] FIG. **7** shows example data items included in an RSN field according to an embodiment of the present invention. The RSN **538** of the beacon frame **520** retains security-setting data including a code, an identifier, and so forth that are used to make a network robust. According to an embodiment of the present invention, the field of Connected-to-AS **592** and that of authentication-server metric (AS metric) **593** are provided in a reserve area of RSN Capabilities **591** of the RSN **538**. Subsequently, each of wireless terminals is informed of the connectivity of a different wireless terminal to the authentication server **110** and/or the metric of a path leading to the authentication server **110** through the beacon frame **520**.

[**0071**] The Connected-to-AS **592** is a field provided to show whether or not the wireless terminal which transmits the beacon frame **520** can be connected to the authentication server **110** via the wired network **190** and the wireless ad-hoc network **290**. If no mutual authentication is performed between the above-described wireless terminal and any of the wireless terminals operating on the wireless ad-hoc network **290**, the wireless terminal is not connected to the authentication server **110**.

[**0072**] The authentication-server metric **593** is a field showing the authentication-server metric of a path extending from the wireless terminal which transmits the beacon frame **520** to the authentication server **110**. Upon receiving the beacon frame **520**, the wireless terminal **200** compares the

current authentication-server metric retained in the wireless-communication-setting-data-retention unit **205** to the transmitted authentication-server metric **593**, whereby it is determined whether the wireless terminal **200** should be an authenticator or a supplicant.

[**0073**] In the above-described embodiment, a passive-scan system is used so that the wireless terminals transmit beacon frames at regular intervals and/or receive the transmitted beacon frames to and/or from one another. However, another system can be used. For example, according to an embodiment of the present invention, in response to a probe request (shown in FIG. **8**) transmitted from a predetermined wireless terminal, each of wireless terminals surrounding the predetermined wireless terminal transmits necessary information, as a probe response (shown in FIG. **9**). The above-described system is referred to as the active-scan system.

[**0074**] FIG. **8** shows the format of a probe-request frame **550** generated by the IEEE 802.11 standard. A wireless-communication system may include a wireless terminal which transmits no beacon frame. The above-described wireless terminal can make a search request by transmitting the above-described probe-request frame **550**.

[**0075**] The probe-request frame **550** is provided to transmit a probe request generated in the MAC sub layer and includes a MAC header **551**, a frame body **560**, and an FCS **559**. The MAC header **551** and the FCS **559** have the same configurations as those of the MAC header **521** and the FCS **529** of the beacon frame **520** shown in FIG. **6**. However, a subtype **5522** shows the probe request.

[**0076**] Further, the frame body **560** corresponds to the payload of the probe-request frame **550** and is used to transfer data generated in the MAC sub layer. The frame body **560** includes data on an SSID **564**, corresponding speed **565**, request information **566**, expansion-corresponding speed **567**, and so forth. The frame body **560** has a configuration similar to that of the beacon frame **520** shown in FIG. **6**.

[**0077**] FIG. **9** shows the format of a probe-response frame **570** generated by the IEEE 802.11 standard. The probe-response frame **570** is used by a wireless terminal to which the probe-request frame **550** had been transmitted, so as to respond to the probe-request frame **550**.

[**0078**] The probe-response frame **570** is used to transmit a probe response generated in the MAC sub layer and includes data on a MAC header **571**, a frame body **580**, and an FCS **579**. Here, the MAC header **571** and the FCS **579** have the same configurations as those of the MAC header **521** and the FCS **529** of the beacon frame **520** shown in FIG. **6**. However, a subtype **5722** shows the probe response.

[**0079**] Further, the frame body **580** corresponds to the payload of the probe-request frame **570** and is used to transfer data existing in the MAC sub layer. The frame body **580** includes data on a time stamp **581**, a beacon period **582**, function information **583**, an SSID **584**, corresponding speed **585**, RSN **588**, and so forth, and has the same configuration as that of the beacon frame **520** shown in FIG. **6**.

[**0080**] Next, operations of the wireless terminal **200** according to an embodiment of the present invention will be described with reference to the attached drawings.

[**0081**] Processing procedures are performed when the bridge terminal **120** is connected to the authentication server **110** via the wired network **190**. Upon being started, the bridge terminal **120** enables the wireless-network interface **124** and starts transmitting the beacon frame **520**. Further, upon receiving the probe-request frame **550** transmitted from a wireless terminal, the bridge terminal **120** transmits the probe-response frame **570**. At that time, in the field of the RSN-function information **591** of the beacon frame **520** and/or the probe-response frame **570**, data reading as "with connectivity" is set in the field of the Connected-to-AS **592**, and data reading as "0" is set in the field of the authentication-server metric **593**.

[**0082**] On the other hand, the wireless terminal **200** enables the wireless-network interface **204** after a host computer is started, whereby transmission of the beacon frame **520** is started and/or the probe-request frame **550** is transmitted. At that time, in the field of the RSN-function information **591** of the beacon frame **520**, data reading as "without connectivity" is set in the field of the Connected-to-AS **592**, and the most inferior value is set in the field of the authentication-server metric **593**.

[**0083**] Each of FIGS. **10** and **11** shows example processing procedures performed by the wireless terminal **200** according to an embodiment of the present invention. Upon receiving the beacon frames **520** and/or the probe-response frames **570** transmitted from different wireless-communication devices, the wireless terminal **200** selects an unauthenticated neighboring terminal having network parameters agreeing with those of the wireless terminal **200**, at step S**911**. The term "network parameters" denotes an SSID, network-operation mode, security-setting data, and so forth. Namely, the wireless terminal **200** compares network parameters included in the SSID **534**, the function information **533**, and the RSN **538** of the beacon frame **520** and/or the SSID **584**, the function information **583**, and the RSN **588** of the probe-response frame **570** to the wireless-communication-setting data retained in the wireless-communication-setting-data-retention unit **205**. Further, the wireless terminal **200** can determine whether or not the neighboring terminal is authenticated by referring to the authentication state **612** corresponding to the terminal identifier **611** shown on the neighboring-terminal list **610** based on the transmission-source address **525** of the beacon frame **520** and/or the transmission-source address **575** of the probe-response frame **570**.

[**0084**] As a result, if the wireless terminals corresponding to "unauthenticated neighboring terminals with agreed network parameters" exist, the following processing procedures are performed. First, priority is given to each of the neighboring terminals, at step S**913**, and the wireless terminals are selected in decreasing order of priority so that processing is performed for the selected wireless terminals, at step S**914**. Here, the priority of each of the wireless terminals is determined so that the highest priority is given to a neighboring terminal of which Connected-to-AS **592** of the RSN-function information **591** of the beacon frame **520** and/or the probe-response frame **570** shows the data reading as "with connectivity". If there is a plurality of the wireless terminals whose Connected-to-AS **592** show the data reading as "with connectivity", the highest priority is given to a neighboring terminal having the most appropriate authentication-server

metric **593** included in the RSN-function information **591** of the beacon frame **520** and/or the probe-response frame **570**.

[**0085**] Then, at step S**915**, if the Connected-to-AS **592** included in the RSN-function information **591** of the beacon frame **520** and/or the probe-response frame **570** transmitted from the selected neighboring terminal shows the data reading as "with connectivity", the processing advances to step S**916**. On the other hand, if the Connected-to AS **592** shows the data reading as "without connectivity", the processing advances to step S**917**.

[**0086**] When the Connected-to-AS **592** of the selected neighboring terminal shows the data reading as "without connectivity" and the wireless terminal **200** can be connected to the authentication server **110**, at step S**917**, it is determined that the wireless terminal **200** should operate, as an authenticator during mutual authentication, at step S**922**. Here, the connectivity between the wireless terminal **200** and the authentication server **100** will be described, as below. If there is a neighboring terminal whose authentication state **612** shown on the neighboring-terminal list **206** shows data reading as "authenticated", the wireless terminal **200** can be connected to the authentication server **110**. If there is no neighboring terminal whose authentication state **612** shows the data reading as "authenticated", it is difficult to connect the wireless terminal **200** to the authentication server **110** with difficulty. On the other hand, if the Connected-to-AS **592** of the selected neighboring terminal shows the data reading as "with connectivity" and it is difficult to connect the wireless terminal **200** to the authentication server **110**, at step S**916**, it is determined that the wireless terminal **200** should operate, as a supplicant, during the mutual authentication, at step S**921**. Namely, when the Connected-to-AS **592** of the selected neighboring terminal shows the data reading as "without connectivity", or when it is difficult to connect the wireless terminal **200** to the authentication server **110**, the wireless terminal provided with the connectivity is determined to be the authenticator and the wireless terminal provided with no connectivity is determined to be the supplicant.

[**0087**] Further, when the Connected-to-AS **592** of the selected neighboring terminal show the data reading as "without connectivity" and it is difficult to connect the wireless terminal **200** to the authentication server **110**, at step S**917**, the mutual authentication is not performed between the wireless terminals.

[**0088**] When the Connected-to-AS **592** of the selected neighboring terminal shows the data reading as "with connectivity" and when the wireless terminal **200** can be connected to the authentication server **110**, at step S**916**, the roles played by the terminals during the mutual authentication are determined according to the relationship between the authentication-server metric **593** Of the RSN-function information **591** of the beacon frame **520** and/or the probe-response frame **570** transmitted from the selected neighboring terminal and the current authentication-server metric of the wireless terminal **200**, the authentication-server metric being retained in the wireless-communication-setting-data-retention unit **205**, at step S**918**.

[**0089**] Namely, when the authentication-server metric **593** of the selected neighboring terminal is better than the current authentication-server metric of the wireless terminal **200**, it is determined that the wireless terminal **200** should operate, as the supplicant, during the mutual authentication, at step S**921**. On the other hand, when the authentication-server metric **593** of the selected neighboring terminal is worse than the current authentication-server metric of the wireless terminal **200**, it is determined that the wireless terminal **200** should operate, as the authenticator, during the mutual authentication, at step S**922**.

[**0090**] Further, when the value of the authentication-server metric **593** of the selected neighboring terminal is the same as that of the current authentication-server metric of the wireless terminal **200**, the roles played by the terminals during the mutual authentication are determined based on the sizes of the MAC addresses, at step S**919**. Namely, when the MAC address of the wireless terminal **200** is larger than that of the selected neighboring terminal, it is determined that the wireless terminal **200** should operate, as the authenticator, during the mutual authentication, at step S**922**. If the MAC address of the wireless terminal **200** is not larger than that of the selected neighboring terminal, it is determined that the wireless terminal **200** should operate, as the supplicant, during the mutual authentication, at step S**921**. Further, the MAC address of the selected neighboring terminal can be acquired from the transmission-source address **525** and/or the transmission-source address **575** of the transmitted beacon frame **520** and/or the transmitted probe-response frame **570**, and/or the terminal identifier **611** shown on the neighboring-terminal list **206**. The MAC address of the wireless terminal **200** can be acquired from the wireless-communication-setting-data-retention unit **205**.

[**0091**] Further, when the wireless terminal **200**, which is one of wireless terminals performing the mutual authentication, is determined to be the authenticator, the other wireless terminal is determined to be the supplicant. When the wireless terminal **200** is determined to be the supplicant, the other wireless terminal becomes the authenticator.

[**0092**] After the roles played by the wireless terminals during the mutual authentication are determined, the mutual authentication is performed between the selected neighboring terminal and the wireless terminal **200**, at step S**931**. When the mutual authentication is achieved, at step S**932**, the wireless terminal that had shown no connectivity to the authentication server **110** by then can be connected to the authentication server **110** via the wireless terminal operating, as the authenticator. Then, a different authentication-server metric used to connect to the authentication server **110** is calculated by both the wireless terminals, at step S**933**. More specifically, the metric from the neighboring terminal to the wireless terminal **200** is added to the authentication-server metric **593** of the beacon frame **520** and/or the probe-response frame **570** transmitted from the neighboring terminal, whereby the different authentication-server metric is calculated.

[**0093**] When the different authentication-server metric calculated in the above-described manner is better than the current authentication-server metric of the wireless terminal **200**, the current authentication-server metric being retained in the wireless-communication-setting-data-retention unit **205**, at step S**934**, the contents of the wireless-communication-setting-data-retention unit **205** are updated through the different authentication-server metric, at step S**935**. Namely, the wireless-communication-setting-data-retention unit **205** retains the calculated different authentication-server metric,

as the current authentication-server metric of the wireless terminal **200**. Subsequently, the calculated different authentication-server metric is shown in the field of the authentication-server metric **593** of the beacon frame **520** and/or the probe-response frame **570** transmitted from the wireless terminal **200**.

[**0094**] After the above-described processing procedures are performed for a specified neighboring terminal, the neighboring terminal is determined to be a terminal that had been subjected to the processing procedures, at step S**936**. If a neighboring terminal that is not subjected to the processing procedures exists, at step S**937**, a neighboring terminal with the second highest priority is selected, at step S**914**, and the above-described processing procedures are performed again.

[**0095**] In the wireless ad-hoc network, the topology may change dynamically due to the entry and/or withdraw of a wireless terminal. Therefore, it is preferable that the authentication-server metric retained by the wireless-communication-setting-data-retention unit **205** be updated every time another authentication-server metric is acquired through a routing protocol operating in the terminal-control unit **201**.

[**0096**] Thus, according to the above-described embodiment, a metric used for connecting to the authentication server **110** (an authentication-server metric) is used, as the standard, so as to determine the roles played by wireless terminals during the mutual authentication. Subsequently, it becomes possible to determine one of the wireless-communication devices, the one having a path that provides a user with an easier access to the authentication server **110**, to be the authenticator and the other wireless-communication device to be the supplicant.

[**0097**] Further, according to the above-described embodiment of the present invention, the authentication-server metric **593** is transmitted by using the field of the RSN **538** of the beacon frame **520** and/or the probe-response frame **570**. However, the above-described method can be modified in various ways. For example, another field may be provided in the beacon frame **520**, as described below.

[**0098**] FIG. **12** shows an example modification of the wireless terminal **200** according to an embodiment of the present invention. The example modification of the wireless terminal **200** is formed by adding a sequence-number-retention unit **208** to the wireless terminal **200** illustrated in FIG. **3**. The sequence-number-retention unit **208** is provided to retain data on the sequence number used for performing an AS announcement that will be described later. Subsequently, upon receiving an AS announcement transmitted from each of different wireless-communication devices, the AS announcement that had been transmitted from a single bridge terminal, it becomes possible to identify each of the AS announcements.

[**0099**] FIG. **13** shows a frame body **630** of a beacon frame of the example modification of the wireless terminal **200**. Being different from the frame body **530** shown in FIG. **6**, the frame body **630** is provided with the field of an AS announcement **690**. The beacon frame including the AS announcement **690** is specifically referred to as an AS-announcement beacon. The AS-announcement beacon is expected to be transmitted once in about a few minutes, for example.

[**0100**] The AS-announcement **690** includes data on a bridge-terminal address **691**, a sequence number **692**, and an authentication-server metric **693**.

[**0101**] The bridge-terminal address **691** is a field provided to show the address of the bridge terminal **120** functioning, as the transmission source of the AS-announcement beacon. The address of the bridge terminal **120** may be the MAC address of the bridge terminal **120**, for example.

[**0102**] The sequence number **692** is a field showing a sequence number provided to each of AS-announcement beacons transmitted from the bridge terminal **120**. Since different AS-announcement beacons are provided with different sequence numbers, the user can learn the reception of the same AS-announcement beacons transmitted via different paths. Every time the AS-announcement beacon is transmitted to the sequence-number-retention unit **208**, the sequence-number-retention unit **208** makes the sequence-number-retention unit **208** retain the sequence number **692**.

[**0103**] The authentication-server metric **693** is provided to retain the authentication-server metric of a path extending from a wireless-communication device which is the transmission source of the AS-announcement beacon to the authentication server **110**. When the AS-announcement beacon is directly transmitted from the bridge terminal **120**, the bridge terminal **120** becomes the transmission source of the AS-announcement beacon. If the AS-announcement beacon is not directly transmitted from the bridge terminal **120**, the next previous wireless terminal which relayed the AS-announcement beacon becomes the transmission source of the AS-announcement beacon. Here, the address of the wireless terminal operating, as the transmission source, is shown in the field of the transmission-source address **525** of the MAC header of the beacon frame.

[**0104**] FIG. **14** shows example processing procedures performed by the example modification of the wireless terminal **200** according to the embodiment of the present invention. The wireless terminal **200** selects an adjacent terminal whose network parameters agree with those of the wireless terminal **200**, at step S**951**, and receives an AS-announcement beacon transmitted from the neighboring terminal, at step S**952**. Then, the wireless terminal **200** compares the sequence-number data retained in the field of the sequence number **692** and sequence-number data retained in the field of the sequence-number-retention unit **208**. If the comparison result shows that the above-described sequence numbers are different from each other, it is determined that the AS-announcement beacon had never been transmitted by then, at step S**953**, and the routing table **207** is updated based on the AS-announcement beacon, at step S**955**.

[**0105**] Namely, due to the above-described update, the transmission-source address **525** of the AS-announcement beacon is set to the relay-terminal identifier **622** of the routing table **207** and the authentication-server metric **693** of the AS-announcement beacon is set to the authentication-server metric **623** of the routing table **207** when making entries onto the routing table **207** (FIG. **5**) showing that the transmission-destination-terminal identifier **621** of the routing table **207** agrees with the bridge-terminal address **691** of the AS-announcement beacon.

[**0106**] Then, the wireless terminal **200** acquires a metric used for connecting to a wireless terminal which is the

transmission source of the AS-announcement beacon, at step S**956**, and calculates a different authentication-server metric of the wireless terminal **200** by adding the acquired metric to the authentication-server metric **623** shown on the routing table **207** shown in FIG. **5**, at step S**957**. The wireless terminal **200** determines the calculated different authentication-server metric to be the authentication-server metric **693** shown in FIG. **13**, the authentication-server metric **693** being included in the AS-announcement beacon. Further, the wireless terminal **200** determines the address of the wireless terminal **200** to be the transmission-source address **525** and transfers the AS-announcement beacon. At that time, the bridge-terminal address **691** and the sequence number **692** are used without being changed.

[**0107**] After that, upon receiving the AS-announcement beacon, at step S**952**, the wireless terminal **200** makes the sequence-number comparison in the above-described manner. If the sequence numbers are the same as each other, it is determined that the AS-announcement beacon had been received before, at step S**953**. In that case, the authentication-server metric **693** of the AS-announcement beacon received at that time is compared to the authentication-server metric **623** shown on the routing table **207** (namely, the authentication-server metric of an AS-announcement beacon that had been received previously). If the comparison result shows that the authentication-server metric **693** of the AS-announcement beacon received at that time is better than that of the authentication-server metric of the AS-announcement beacon that had been received previously, at step S**954**, the routing table **207** is updated based on the AS-announcement beacon received at that time, at step S**955**.

[**0108**] Thus, according to the above-described example modifications, each of the wireless terminals transfers the AS-announcement beacon through flooding. Subsequently, the wireless terminals generate a tree topology showing paths leading to the authentication server **110**. The authentication-server metric can be calculated based on the tree topology.

[**0109**] An embodiment of the present invention shows an example of how the present invention is embodied. There are correspondences between the features of the claims and the specific elements disclosed in an embodiment of the present invention. However, without being limited to the above-described correspondences, it should be understood by those skilled in the art that various modifications, combinations, sub-combinations and alterations may occur depending on design requirements and other factors insofar as they are within the scope of the appended claims or the equivalents thereof.

[**0110**] Namely, according to an embodiment of the present invention, an authentication server corresponds to the authentication server **110**, for example. Further, a communication-setting-data-retention section corresponds to the communication-setting-data-retention unit **205**, for example. Further, a signal-reception section corresponds to the wireless-network interface **204**. Further, a control section corresponds to the terminal-control unit **201**, for example. Further, a self-authentication-server metric corresponds to the "current authentication-server metric of the wireless terminal 200" retained in the communication-setting-data-retention unit **205**, and a nonself-authentication-server metric corresponds to the authentication-server metric **593** of the RSN and/or the authentication-server metric **693** included in the AS announcement **690**.

[**0111**] Further, according to an embodiment of the present invention, the address of a pertinent wireless-communication device corresponds to the MAC address of the wireless terminal **200**, for example, the MAC address being retained in the communication-setting-data-retention unit **205**. Further, the address of a different wireless-communication device corresponds to the transmission-source address **525** of the beacon frame **520** and/or the transmission-source address **575** of the probe-response frame **570**, and/or the terminal identifier **611** shown on the neighboring-terminal list **206**.

[**0112**] Further, according to an embodiment of the present invention, first connectivity information corresponds to the Connected-to-AS **592**, and second connectivity information corresponds to the authentication state **612** shown on the neighboring-terminal list **206**, for example.

[**0113**] Further, according to an embodiment of the present invention, a nonself-authentication-server-metric-retention section corresponds to the routing table **207**, for example. Further, a neighboring-metric-acquisition section corresponds to the wireless-network interface **204**, for example.

[**0114**] Further, according to an embodiment of the present invention, an authentication server corresponds to the authentication server **110**, for example. Further, a communication-setting-data-retention section corresponds to the communication-setting-data-retention unit **205**, for example. Further, a signal-transmission section and a signal-reception section correspond to the wireless-network interface **204**, for example. Further, a control section corresponds to the terminal-control unit **201**, for example.

[**0115**] Further, according to embodiments of the present invention, a signal-reception-processing procedure corresponds to step S**911**, for example. Further, a supplicant-setting-processing procedure corresponds to step S**921**, for example. Further, an authenticator-setting-processing procedure corresponds to step S**922**, for example.

[**0116**] Here, the series of processing procedures described in the above-described embodiments may be understood, as a method including the above-described series of processing procedures. Further, the series of processing procedures may be provided, as a program making a computer perform the series of processing procedures and/or a recording medium recording the program.

What is claimed is:

1. A wireless-communication device performing mutual authentication between the wireless-communication device and a different wireless-communication device by using an authentication server, the wireless-communication device comprising:

communication-setting-data-retention means configured to retain communication-setting data including a first metric corresponding to the path from the wireless-communication device to the authentication server, as a self-authentication-server metric;

signal-reception means configured to receive a predetermined signal transmitted from the different wireless-communication device, the predetermined signal including a second metric corresponding to the path

from the different wireless-communication device to the authentication server, as a nonself-authentication-server metric; and

control means configured to make a first setting so that the wireless-communication device operates, as a supplicant, during the mutual authentication when the self-authentication-server metric is better than the nonself-authentication-server metric, and make a second setting so that the wireless-communication device operates, as an authenticator, during the mutual authentication when the self-authentication-server metric is worse than the nonself-authentication-server metric.

2. The wireless-communication device according to claim 1, wherein the communication-setting data retained in the communication-setting-data-retention means includes data on a first address of the wireless-communication device,

wherein the predetermined signal includes data on a second address of the different wireless-communication device, and

wherein when the self-authentication-server metric is equivalent to the nonself-authentication-server metric, the control means makes a third setting so that the wireless-communication device operates, as either the authenticator or the supplicant, during the mutual authentication according to a relationship between the first address and the second address.

3. The wireless-communication device according to claim 2, wherein when the first address is larger than the second address, the control means makes a fourth setting so that the wireless-communication device operates, as the authenticator, during the mutual authentication, and

wherein when the first address is not larger than the second address, the control means makes a fifth setting so that the wireless-communication device operates, as the supplicant, during the mutual authentication.

4. The wireless-communication device according to claim 1, wherein the predetermined signal includes first accessibility information indicating whether or not the different wireless communication device can make access to the authentication server,

wherein the communication-setting data retained in the communication-setting-data-retention means includes second accessibility information indicating whether or not the wireless-communication device can make access to the authentication server,

wherein when the first accessibility information shows that the different wireless-communication device can make access to the authentication server and the second accessibility information shows that the wireless-communication device makes access to the authentication server with difficulty, the control means makes a sixth setting so that the wireless-communication device operates, as the supplicant, during the mutual authentication irrespective of a relationship between the self-authentication-server metric and the nonself-authentication-server metric, and

wherein when the first accessibility information shows that the different wireless-communication device makes access to the authentication server with difficulty and the second accessibility information shows that the wireless-communication device can make access to the authentication server, the control means makes a seventh setting so that the wireless-communication device operates, as the authenticator, during the mutual authentication irrespective of the relationship between the self-authentication-server metric and the nonself-authentication-server metric.

5. The wireless-communication device according to claim 1, wherein the first metric and/or the second metric shows wireless-communication quality of a wireless-communication path leading to the authentication server.

6. The wireless-communication device according to claim 1, wherein the first metric and/or the second metric shows the number of at least one hop of a wireless-communication path leading to the authentication server.

7. The wireless-communication device according to claim 1, wherein the predetermined signal is a broadcast signal transmitted from the different wireless-communication device.

8. The wireless-communication device according to claim 1, wherein the predetermined signal is an acknowledgment signal transmitted from the different wireless-communication device in response to a request issued from the wireless-communication device.

9. The wireless-communication device according to claim 1, wherein when the control means calculates a third metric corresponding to the path to the authentication server after the mutual authentication is achieved and the third metric is better than the self-authentication-server metric retained in the communication-setting-data-retention means, the control means makes the communication-setting-data-retention means retain the third metric.

10. The wireless-communication device according to claim 1, further comprising:

nonself-authentication-server-metric-retention means provided for the different wireless-communication device, the nonself-authentication-server-metric-retention means being configured to retain the nonself-authentication-server metric; and

neighboring-metric-acquisition means configured to acquire a fourth metric provided between the wireless-communication device and the different wireless-communication device, as a neighboring metric,

wherein the control means calculates the self-authentication-server metric by adding the nonself-authentication-server metric to the neighboring metric.

11. The wireless-communication device according to claim 10, wherein when there is a plurality of the different wireless-communication devices, upon receiving the predetermined signal transmitted from each of the different wireless-communication devices, the signal-reception means makes the nonself-authentication-server-metric-retention means retain the nonself-authentication-server metric based on the predetermined signal including the nonself-authentication-server metric which is the best of the nonself-authentication-server metrics of all of the predetermined signals.

12. A communication system performing mutual authentication between at least two wireless-communication devices by using an authentication server, wherein each of the wireless-communication devices comprises:

communication-setting-data-retention means configured to retain communication-setting data including a first metric corresponding to the path from the wireless-

communication device to the authentication server, as a self-authentication-server metric;

signal-transmission means configured to transmit a first signal including the self-authentication-server metric;

signal-reception means configured to receive a second signal transmitted from the different wireless-communication device, the second signal including a second metric corresponding to the path from the different wireless-communication device to the authentication server, as a nonself-authentication-server metric; and

control means configured to make a first setting so that the wireless-communication device operates, as a supplicant, during the mutual authentication when the self-authentication-server metric is better than the nonself-authentication-server metric, and make a second setting so that the wireless-communication device operates, as an authenticator, during the mutual authentication when the self-authentication-server metric is worse than the nonself-authentication-server metric.

13. A communication-control method used for a wireless-communication device performing mutual authentication between the wireless-communication device and a different wireless-communication device by using an authentication server, the communication-control method comprising the steps of:

receiving a predetermined signal transmitted from the different wireless-communication device, the predetermined signal including a first metric corresponding to the path from the different wireless-communication device to the authentication server, as a nonself-authentication-server metric;

making a first setting so that the wireless-communication device operates, as a supplicant, during the mutual authentication when a second metric corresponding to the path from the wireless-communication device to the authentication server is better than the nonself-authentication-server metric; and

making a second setting so that the wireless-communication device operates, as an authenticator, during the mutual authentication when the second metric is worse than the nonself-authentication-server metric.

14. A program installed onto a wireless-communication device performing mutual authentication between the wireless-communication device and a different wireless-communication device by using an authentication server, the program making a computer perform the steps of:

receiving a predetermined signal transmitted from the different wireless-communication device, the predetermined signal including a first metric corresponding to the path from the different wireless-communication device to the authentication server, as a nonself-authentication-server metric;

making a first setting so that the wireless-communication device operates, as a supplicant, during the mutual authentication when a second metric corresponding to the path from the wireless-communication device to the authentication server is better than the nonself-authentication-server metric; and

making a second setting so that the wireless-communication device operates, as an authenticator, during the mutual authentication when the second metric is worse than the nonself-authentication-server metric.

15. A wireless-communication device performing mutual authentication between the wireless-communication device and a different wireless-communication device by using an authentication server, the wireless-communication device comprising:

a communication-setting-data-retention unit configured to retain communication-setting data including a first metric corresponding to the path from the wireless-communication device to the authentication server, as a self-authentication-server metric;

a signal-reception unit configured to receive a predetermined signal transmitted from the different wireless-communication device, the predetermined signal including a second metric corresponding to the path from the different wireless-communication device to the authentication server, as a nonself-authentication-server metric; and

a control unit configured to make a first setting so that the wireless-communication device operates, as a supplicant, during the mutual authentication when the self-authentication-server metric is better than the nonself-authentication-server metric, and make a second setting so that the wireless-communication device operates, as an authenticator, during the mutual authentication when the self-authentication-server metric is worse than the nonself-authentication-server metric.

16. A communication system performing mutual authentication between at least two wireless-communication devices by using an authentication server, wherein each of the wireless-communication devices comprises:

a communication-setting-data-retention unit configured to retain communication-setting data including a first metric corresponding to the path from the wireless-communication device to the authentication server, as a self-authentication-server metric;

a signal-transmission unit configured to transmit a first signal including the self-authentication-server metric;

a signal-reception unit configured to receive a second signal transmitted from the different wireless-communication device, the second signal including a second metric corresponding to the path from the different wireless-communication device to the authentication server, as a nonself-authentication-server metric; and

a control unit configured to make a first setting so that the wireless-communication device operates, as a supplicant, during the mutual authentication when the self-authentication-server metric is better than the nonself-authentication-server metric, and make a second setting so that the wireless-communication device operates, as an authenticator, during the mutual authentication when the self-authentication-server metric is worse than the nonself-authentication-server metric.

* * * * *