US 20060179297A1

(19) **United States**

(12) **Patent Application Publication**

**Ikebe et al.**

(10) **Pub. No.: US 2006/0179297 A1**

(43) **Pub. Date: Aug. 10, 2006**

(54) **SERVER APPARATUS**

(76) Inventors: **Hayato Ikebe**, Osaka (JP); **Kazuya Ogawa**, Mizuho-City (JP); **Yoshinori Hatayama**, Komaki-City (JP); **Hiroshi Takemura**, Aisai-City (JP); **Youko Tanaka**, Mizuho-City (JP)

Correspondence Address:
**MCDERMOTT WILL & EMERY LLP**
**600 13TH STREET, N.W.**
**WASHINGTON, DC 20005-3096 (US)**

(21) Appl. No.: **11/331,364**

(22) Filed: **Jan. 13, 2006**

(30) **Foreign Application Priority Data**

Jan. 13, 2005 (JP) .................................. P2005-006796

**Publication Classification**

(51) **Int. Cl.**
*H04L 9/00* (2006.01)

(52) **U.S. Cl.** .......................................................... **713/153**

(57) **ABSTRACT**

A server apparatus is configured to connect client terminal apparatuses through a communication network. The server apparatus receives a signature-attached message having a signature of a different server apparatus connected to the communication network from the different server apparatus, and verifies whether the signature attached to the signature-attached message is valid or invalid. The server apparatus also changes a connection point for the client terminal apparatus to the different server apparatus when the signature verifier verifies that the signature is valid.

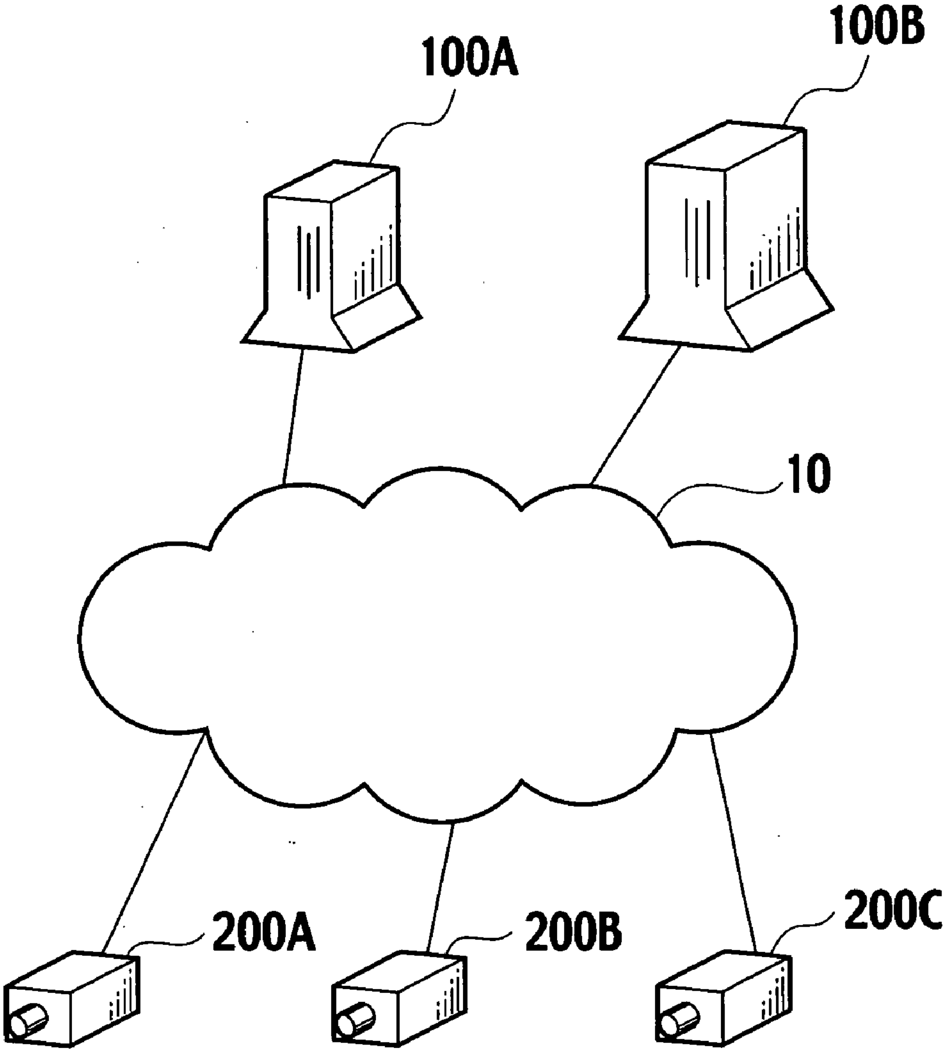

FIG. 1

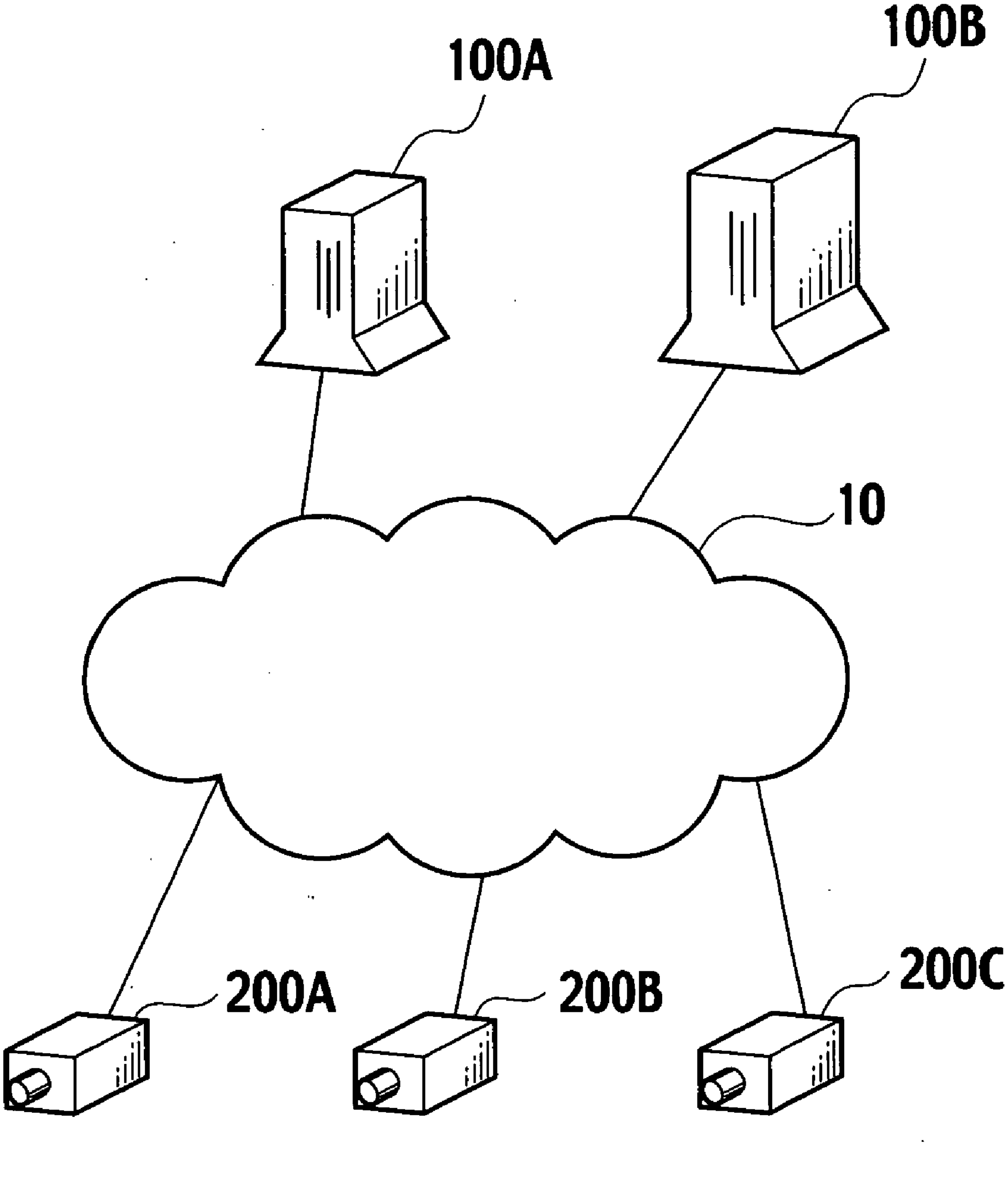

FIG. 2

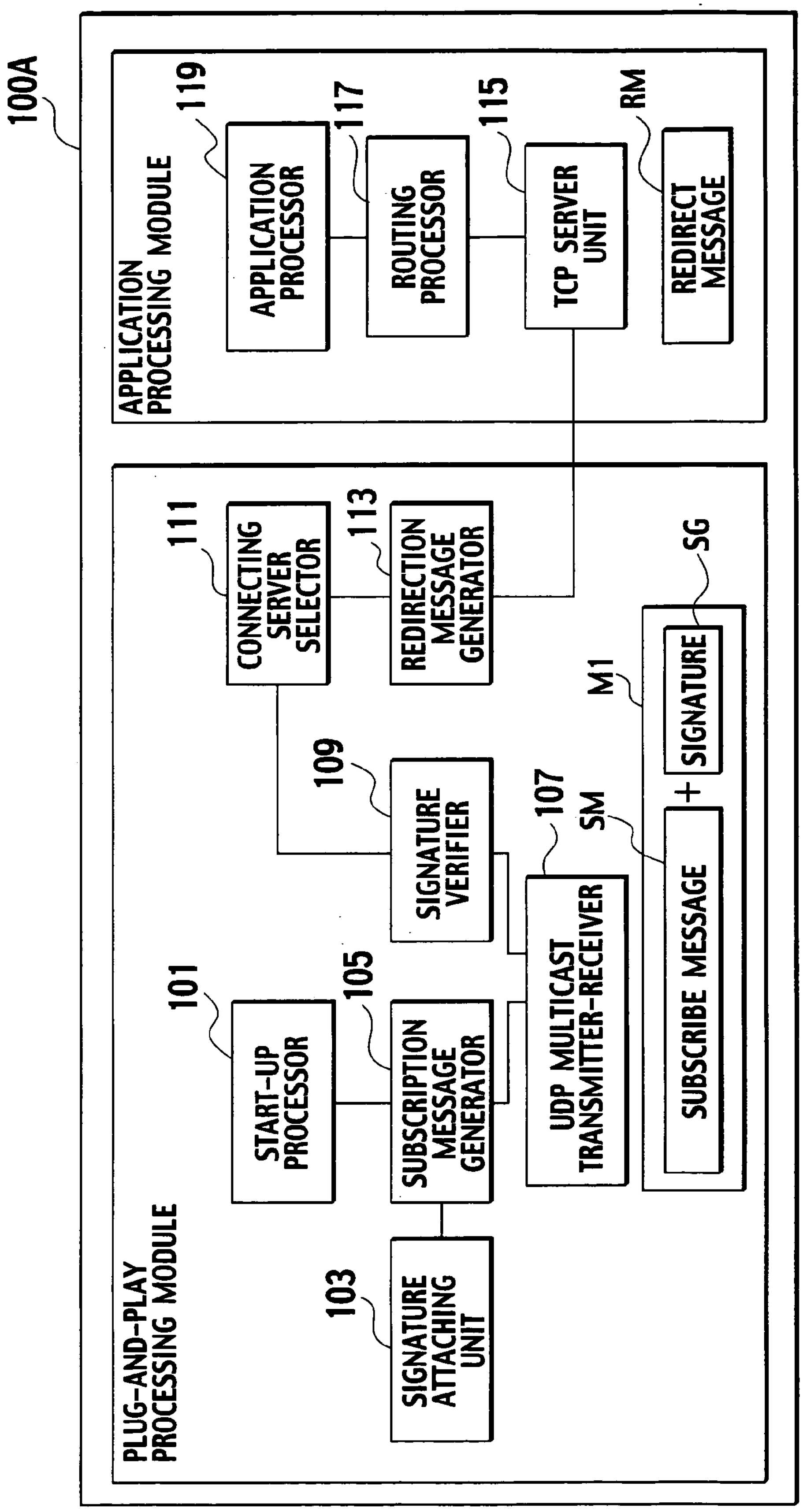
100A
APPLICATION PROCESSING MODULE
119
APPLICATION PROCESSOR
117
ROUTING PROCESSOR
115
TCP SERVER UNIT
RM
REDIRECT MESSAGE
PLUG-AND-PLAY PROCESSING MODULE
111
CONNECTING SERVER SELECTOR
113
REDIRECTION MESSAGE GENERATOR
SG
M1
SIGNATURE
+
109
SIGNATURE VERIFIER
107
SM
UDP MULTICAST TRANSMITTER-RECEIVER
SUBSCRIBE MESSAGE
101
START-UP PROCESSOR
105
SUBSCRIPTION MESSAGE GENERATOR
103
SIGNATURE ATTACHING UNIT

FIG. 3

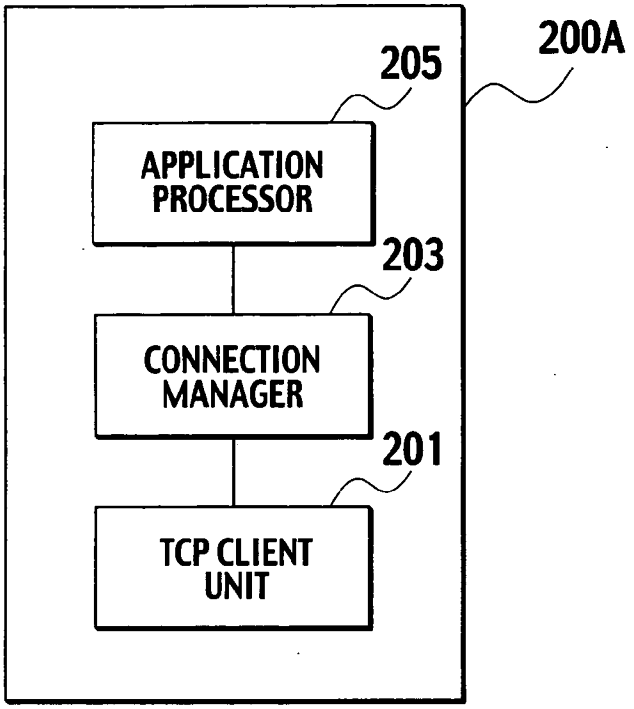
200A
205
APPLICATION PROCESSOR
203
CONNECTION MANAGER
201
TCP CLIENT UNIT

FIG. 4

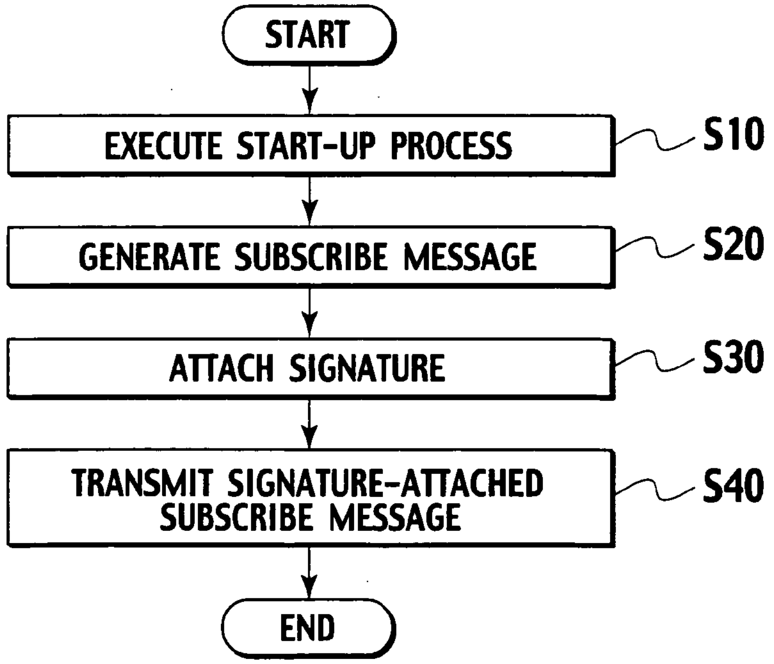
START
EXECUTE START-UP PROCESS
S10
GENERATE SUBSCRIBE MESSAGE
S20
ATTACH SIGNATURE
S30
TRANSMIT SIGNATURE-ATTACHED SUBSCRIBE MESSAGE
S40
END

FIG. 5

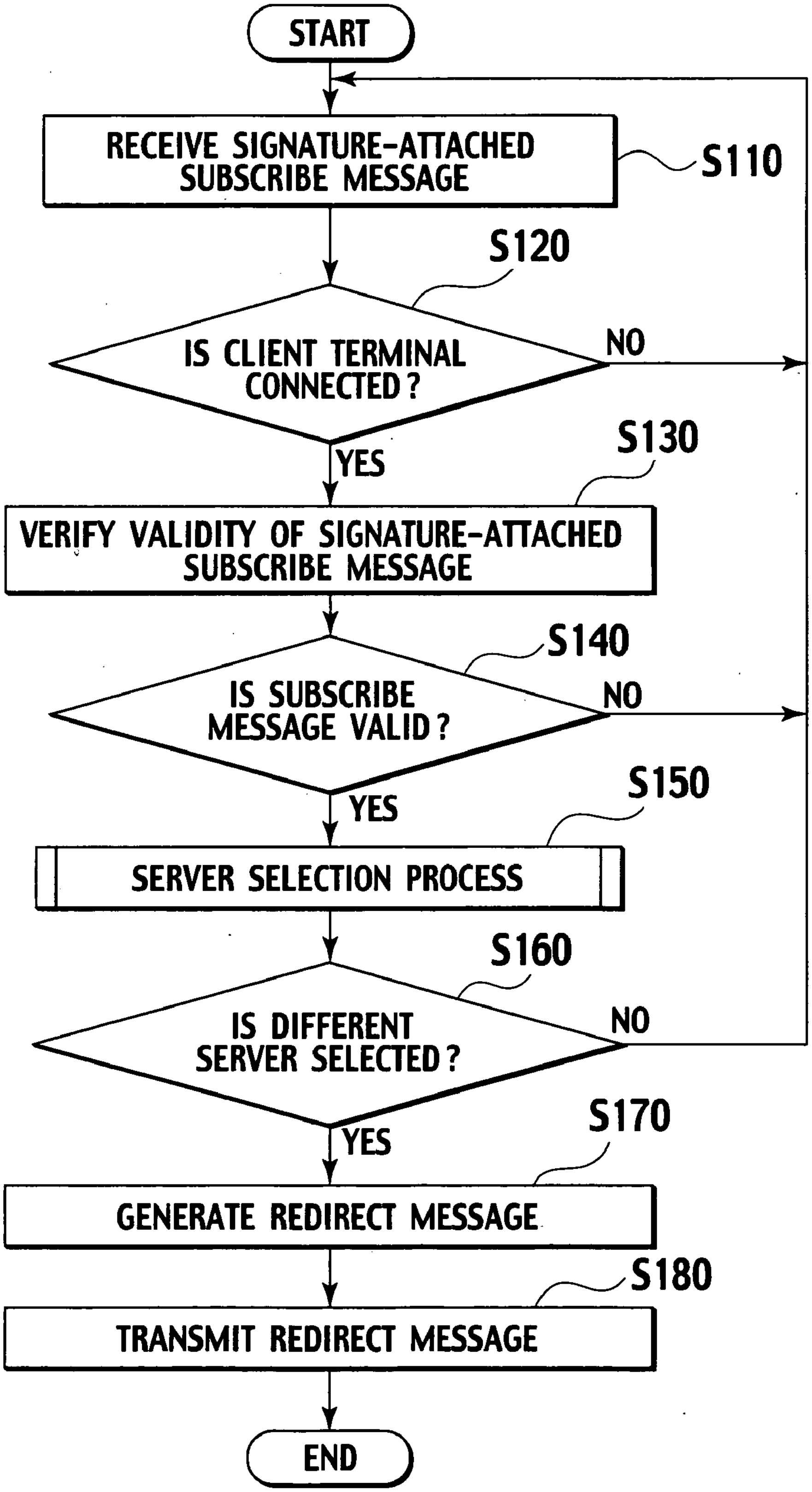
START
RECEIVE SIGNATURE-ATTACHED SUBSCRIBE MESSAGE
S110
S120
IS CLIENT TERMINAL CONNECTED?
NO
YES
S130
VERIFY VALIDITY OF SIGNATURE-ATTACHED SUBSCRIBE MESSAGE
S140
IS SUBSCRIBE MESSAGE VALID?
NO
YES
S150
SERVER SELECTION PROCESS
S160
IS DIFFERENT SERVER SELECTED?
NO
YES
S170
GENERATE REDIRECT MESSAGE
S180
TRANSMIT REDIRECT MESSAGE
END

FIG. 6

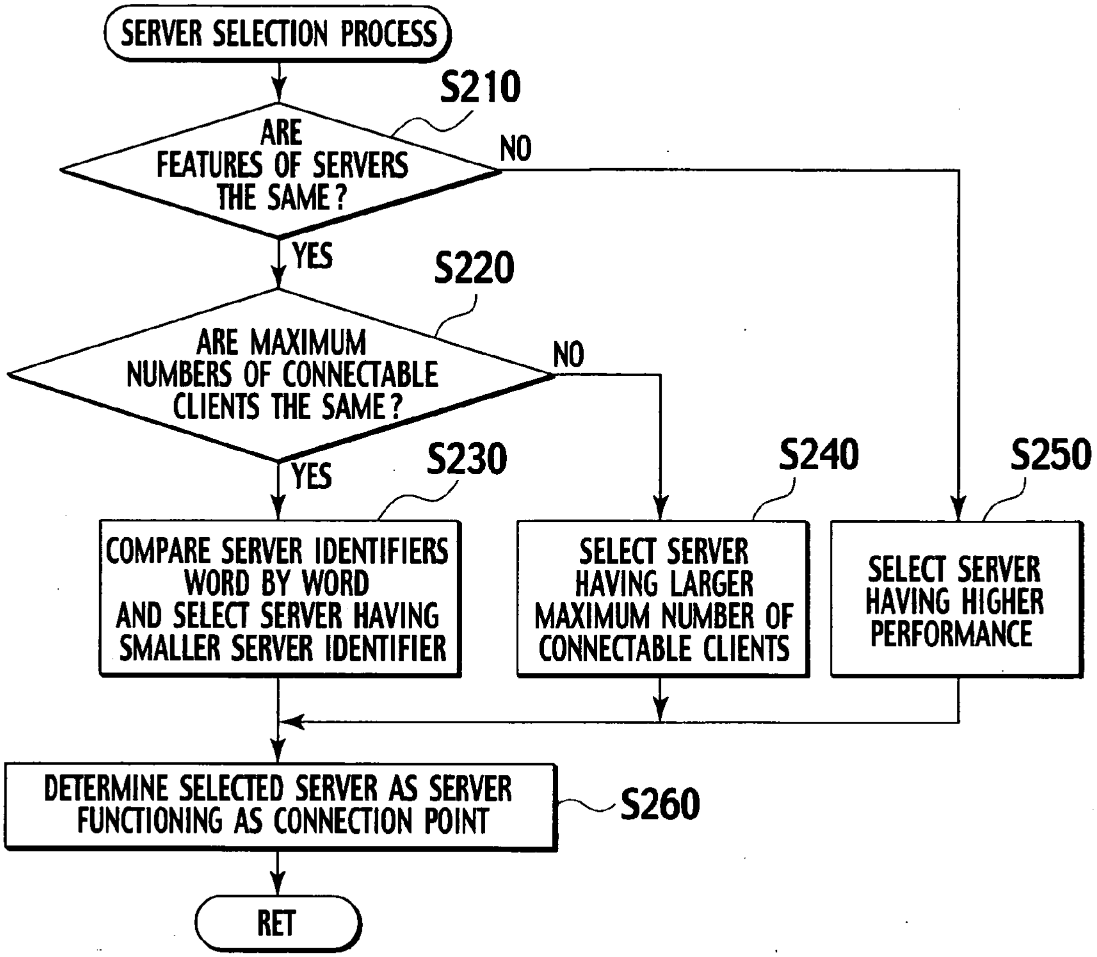
SERVER SELECTION PROCESS
S210
ARE FEATURES OF SERVERS THE SAME?
NO
YES
S220
ARE MAXIMUM NUMBERS OF CONNECTABLE CLIENTS THE SAME?
NO
YES
S230
COMPARE SERVER IDENTIFIERS WORD BY WORD AND SELECT SERVER HAVING SMALLER SERVER IDENTIFIER
S240
SELECT SERVER HAVING LARGER MAXIMUM NUMBER OF CONNECTABLE CLIENTS
S250
SELECT SERVER HAVING HIGHER PERFORMANCE
DETERMINE SELECTED SERVER AS SERVER FUNCTIONING AS CONNECTION POINT
S260
RET

FIG. 7

| SERVER IDENTIFIER | IP ADDRESS | FEATURE LIST | MAXIMUM NUMBER OF CONNECTABLE CLIENTS |
|---|---|---|---|
| hcsps:/PtPvXYJSQSqwTJpPGjwog | 192.168.1.1:17320 | hcsps,webs,db | 3 |

## FIG. 8A

```
SUBSCRIBE
DOCUMENT: <hcsp xmlns= “http://www.darwin-hcs.org/arch/hcsp/1.0”
          to= “ [ADDRESS OF DESTINATION CLIENT] ”
          from= “ [IDENTIFIER OF ORIGINATING SERVER];ip=[IP ADDRESS] ” >
           <subscribe features= “ [FEATURE LIST]”connected= “ [NUMBERS OF CONNECTED CLIENTS]”max=“[MAXIMUM CONNECTABLE NUMBER]”/>
           </hcsp>

    [EXAMPLE] <hcsp xmlns= “http://www.darwin-hcs.org/arch/hcsp/1.0”
              to= “ab:*”
              from= “hcsps;/PtPvXYJSQSqwTJpPGjw0g;ip=192.168.1.9.17320” >
              <subscribe features= “hcsps” connected= “0” max= “5” />
              </hcsp>
```

## FIG. 8B

```
REDIRECTION
 DOCUMENT: <hcsp xmlns= “http://www.darwin-hcs.org/arch/hcsp/1.0”
           to= “ [ADDRESS OF DESTINATION CLIENT] ” from= “ [IDENTIFIER OF ORIGINATING SERVER] ” >
           <redirect id= “ [IDENTIFIER OF CHANGED SERVER] ;ip= [IP ADDRESS OF CHANGED SERVER] ”
                   features= “ [FEATURE LIST OF CHANGED SERVER] ” />
           </hcsp>

    [EXAMPLE] <hcsp xmlns= “http://www.darwin-hcs.org/arch/hcsp/1.0”
              to= “ab:EIW6Qe0ARnWrsJZTsHWadA” from= “hcsps;/PtPvXYJSQSqwTJpPGjw0g” >
              <redirect id= “hpsps:gC3YWhxMRQGZVBboYIEgxw;ip=192.168.1.9.17320”
                     features= “hcsps,webs,db” />
              </hcsp>
```

# SERVER APPARATUS

## CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is based upon and claims the benefit of priority from the prior Japanese Patent Applications No. P2005-006796 filed on Jan. 13, 2005; 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 server apparatus configured to connect a client terminal apparatus through a communication network. More specifically, the present invention relates to a server apparatus configured to verify validity of a server apparatus newly connected to a communication network.

[0004] 2. Description of the Related Art

[0005] In recent years, a home network which is a communication network configured to connect a client terminal apparatus such as a security camera or a sensor to be installed in a house has been put into practical use.

[0006] In such a home network, an information processing system (a client-server system) often includes a minimal server apparatus and a small number of client terminal apparatuses to be connected to the home network at the time of introduction of a home network.

[0007] Subsequently, a high-performance server apparatus (another server apparatus) may be further added to the information processing system in response to an increase in the number of client terminal apparatuses to be connected to the home network, and a connection point for the client terminal apparatuses may be changed to the new server apparatus.

[0008] Accordingly, to facilitate a changeover operation associated with addition of the new server apparatus, there has been disclosed a method of automatically executing operations including registration of addresses of client terminal apparatuses and server apparatuses, which become necessary upon addition of a new server apparatus. Specifically, the registration is performed by use of an apparatus (an address resolution apparatus) for managing addresses for identifying the client terminal apparatuses and the server apparatuses (see Japanese Unexamined Patent Publication No. 2000-354062, p. 8-9, FIGS. 1 and 2, for example).

## BRIEF SUMMARY OF THE INVENTION

[0009] However, the above-described conventional method has the following problem. Specifically, even when an invalid server apparatus is newly connected to the home network, an address or other information of the invalid server apparatus is registered to the respective client terminal apparatuses connected to the home network. Consequently, each client terminal apparatus executes logical connection to the invalid server apparatus.

[0010] The present invention has been made in view of the above-described circumstance. An object of the present invention is to provide a server apparatus which is capable of allowing a client terminal apparatus to change a connection point to a different server apparatus only when the different server apparatus newly connected to a home network is a valid server apparatus.

[0011] To attain the object, the present invention provides the following aspects. A first aspect of the present invention provides a server apparatus configured to connect a client terminal apparatus through a communication network, which includes a signature-attached message receiver configured to receive a signature-attached message having a signature of a different server apparatus connected to the communication network from the different server apparatus, a signature verifier configured to verify whether the signature attached to the signature-attached message is valid or invalid, and a connection point changer configured to change a connection point for the client terminal apparatus to the different server apparatus when the signature verifier verifies that the signature is valid.

[0012] According to this aspect, it is possible to change the connection point for the client terminal apparatus to the server apparatus only when the server apparatus is newly connected to a communication network and is verified to be a valid server apparatus.

[0013] A second aspect of the present invention provides the server apparatus according to the first aspect, which further includes a signature attaching unit configured to attach the signature of the server apparatus to a message to be transmitted to the network, and a signature-attached message transmitter configured to transmit the signature-attached message having the signature attached by the signature attaching unit to the network.

[0014] A third aspect of the present invention provides the server apparatus according to any one of the first and second aspects, in which the connection point changer compares a feature list indicating a feature of the different server apparatus, which is included in the signature-attached message received by the signature-attached message receiver, with a feature list of the server apparatus, and the connection point changer changes the connection point for the client terminal apparatus to the different server apparatus when the feature of the different server apparatus is higher than that of the server apparatus.

[0015] A fourth aspect of the present invention provides the server apparatus according to any one of the first to third aspects, in which the signature-attached message receiver receives the signature-attached message transmitted by the different server apparatus using the user datagram protocol (UDP).

[0016] A fifth aspect of the present invention provides the server apparatus according to any one of the second to fourth aspects, in which signature-attached message transmitter transmits the signature-attached message by use of the UDP.

[0017] According to the aspects of the present invention, it is possible to provide a server apparatus which is capable of allowing a client terminal apparatus to change a connection point to a different server apparatus only when the different server apparatus newly connected to a network is a valid server apparatus.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0018] **FIG. 1** is an overall schematic block diagram of an information processing system according to an embodiment of the present invention.

[0019] **FIG. 2** is a view showing a logic block configuration of a server apparatus according to the embodiment of the present invention.

[0020] **FIG. 3** is a view showing a logic block configuration of a client terminal apparatus according to the embodiment of the present invention.

[0021] **FIG. 4** is a view showing a process flow executed by a server apparatus which is newly added to the information processing system according to the embodiment of the present invention.

[0022] **FIG. 5** is a view showing a process flow executed by the existing server apparatus according to the embodiment of the present invention.

[0023] **FIG. 6** is another view showing the process flow executed by the existing server apparatus according to the embodiment of the present invention.

[0024] **FIG. 7** is a view showing an example of a feature list stored in the server apparatus according to the present invention.

[0025] **FIGS. 8A and 8B** are views showing examples of a subscribe message and a redirect message to be transmitted and received in the information processing system according to the embodiment of the present invention.

## DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0026] Next, embodiments of the present invention will be described below. Note that, in the following description of the drawings, the same or similar parts will be denoted by the same or similar reference numerals. However, the drawings are schematic and actual proportions of dimensions and the like are different from reality.

[0027] It is therefore recommended to determine the concrete dimensions and other features in consideration of the following description. Moreover, it is needless to say that dimensional relations or proportion may vary between the drawings.

(Overall Schematic Configuration of Information Processing System)

[0028] **FIG. 1** shows an overall schematic configuration of an information processing system according to an embodiment of the present invention. As shown in the drawing, the information processing system of this embodiment includes servers **100**A and **100**B, and client terminals **200**A to **200**C.

[0029] The servers **100**A and **100**B connect the client terminals **200**A to **200**C through a home network **10**.

[0030] The server **100**A (a server apparatus) and the server **100**B (a different server apparatus) offer features and processing capabilities which are different from each other. In this embodiment, the server **100**B offers a higher performance than the server **100**A.

[0031] The client terminals **200**A to **200**C are connected either to the server **100**A or to the server **100**B through the home network **10**. In this embodiment, each of the client terminals **200**A to **200**C includes a security camera. Moving image data captured by the camera is transmitted to the server connected client terminals (the server **100**A or the server **100**B).

[0032] The home network **10** is a communication network configured to connect the servers **100**A and **100**B, and the client terminals **200**A to **200**C. The home network **10** may be formed by use of a LAN (such as 100BASE-TX) installed in a building (such as a house). Note that the home network **10** may include a wireless LAN, and the home network **10** may be connected to a wide area network (WAN) or to the Internet.

(Logic Block Configurations of Information Processing System)

[0033] Next, logic block configuration of the servers **100**A and **100**B, and the clients terminals **200**A to **200**C, which constitute the information processing system will be described.

[0034] **FIG. 2** shows a logic block configuration of the server **100**A. The server **100**B also has a similar logic block configuration to the server **100**A.

[0035] **FIG. 3** shows a logic block configuration of the client terminal **200**A. The client terminals **200**B and **200**C have a similar logic block configuration to the client terminal **200**A.

[0036] Now, portions related to the present invention will be mainly explained below. Accordingly, it should be noted that the server **100**A shown in **FIG. 2** and the client terminal **200**A shown in **FIG. 3** may further include unillustrated or unexplained logic blocks (such are a power unit and the like) which are essential for realizing the features of the apparatuses.

(1) Server

[0037] As shown in **FIG. 2**, the server **100**A includes a plug-and-play processing module and an application processing module.

[0038] The plug-and-play processing module includes a start-up processor **101**, a signature attaching unit **103**, a subscribe message generator **105**, a UDP multicast transmitter-receiver **107**, a signature verifier **109**, a connecting server selector **111**, and a redirect message generator **113**.

[0039] The application processing module includes a TCP server unit **115**, a routing processor **117**, and an application processor **119**.

(1.1) Plug-and-Play Processing Module

[0040] The start-up processor **101** executes a start-up process such as resetting respective logic blocks constituting the server **100**A when the server **100**A is turned on.

[0041] Further, the start-up processor **101** makes a request to the subscribe message generator **105** for generating a subscribe message (see **FIG. 8A**) to notify the start-up of the server **100**A.

[0042] The signature attaching unit **103** attaches a signature SG (a digital signature) to the subscribe message SM which is transmitted to the server **100**B (the different server apparatus).

[0043] Specifically, the signature attaching unit **103** attaches the signature SG to the subscribe message SM, which is generated by the subscribe message generator **105**, by use of a secret key corresponding to a public key of the server **100**B certified by a certificate authority (CA), and a given one-way hash function.

[**0044**] The subscribe message generator **105** generates the subscribe message SM to be transmitted to the server **100**B.

[**0045**] Further, the subscribe message generator **105** makes a request to the signature attaching unit **103** for attachment of the signature to the generated subscribe message SM. The subscribe message generator **105** outputs a signature-attached subscribe message **M1** (a signature-attached message), which is generated by attaching the signature SG to the subscribe message SM, to the UDP multicast transmitter-receiver **107**.

[**0046**] The UDP multicast transmitter-receiver **107** transmits the signature-attached subscribe message **M1** outputted by the subscribe message generator **105** to the server **100**B.

[**0047**] Further, the UDP multicast transmitter-receiver **107** receives a signature signature-attached subscribe message **M1** transmitted by the server **100**B.

[**0048**] In particular, the UDP multicast transmitter-receiver **107** is configured to transmit the signature-attached subscribe message **M1** (the signature-attached message) to the server **100**B, and constitutes a signature-attached message transmitter in this embodiment.

[**0049**] Further, the UDP multicast transmitter-receiver **107** is configured to receive the signature-attached subscribe message **M1** from the server **100**B connected to the home network **10**, and constitutes a signature-attached message receiver in this embodiment.

[**0050**] Note that the UDP multicast transmitter-receiver **107** transmits and receives the signature-attached subscribe message **M1** using the UDP.

[**0051**] The signature verifier **109** verifies whether or not the signature SG attached to the signature-attached subscribe message **M1** transmitted from the server **100**B is valid.

[**0052**] Specifically, the signature verifier **109** verifies the signature SG by use of the public key of the server **100**B. Moreover, when the signature verifier **109** verifies that the signature SG attached to the signature-attached subscribe message **M1** is valid, the signature verifier **109** outputs the subscribe message SM included in the signature-attached subscribe message **M1** to the connecting server selector **111**.

[**0053**] The connecting server selector **111** compares a feature list indicating features of the server **100**B, which is included in the signature-attached subscribe message **M1** received from the server **100**B, with a feature list indicating features of the server **100**A.

[**0054**] The connecting server selector **111** compares a feature list (see **FIG. 8A**) indicating features of the server **100**B, which is included the subscribe message SM inputted from the signature verifier **109**, with a feature list (see **FIG. 8B**) indicating features of the server **100**A. As the comparison result, when the server **100**B has a higher performance than the server **110**A, the connecting server selector **111** makes a request to the redirect message generator **113** for generating a redirect message RM.

[**0055**] The redirect message generator **113** generates the redirect message RM in response to the request from the connecting server selector **111**.

[**0056**] The redirect message RM is for directing change of a connection point for the client terminals previously connected to the server **100**A to the server **100**B. In this embodiment, the connecting server selector **111** and the redirect message generator **113** constitute a connection point changer.

(1.2) Application Processing Module

[**0057**] The TCP server unit **115** executes processing such as establishment of logical connection to the client terminal (such as the client terminal **200**A) by use of the TCP (transmission control protocol)/IP (Internet protocol).

[**0058**] Further, the TCP server unit **115** transmits the redirect message RM generated by the redirect message generator **113** to the client terminals **200**A to **200**C.

[**0059**] The routing processor **117** executes processing related to routing of the redirect message RM and so on which are to be transmitted to the home network **10**.

[**0060**] Specifically, the routing processor **117** determines destination addresses of these messages and updates contents of a routing table stored therein based on received routing information.

[**0061**] Further, the routing processor **117** executes relaying of any messages between the TCP server unit **115** and the application processing unit **119**.

[**0062**] The application processing unit **119** executes various applications to be offered by the server **100**A (such as an application that offers a service to the client terminals **200**A to **200**C through the home network **10**).

(2) Client Terminal

[**0063**] As shown in **FIG. 3**, the client terminal **200**A includes a TCP client unit **201**, a connection manager **203**, and an application processor **205**.

[**0064**] The TCP client unit **201** executes processing such as establishment of logical connection to the server (such as the server **100**A) by use of the TCP (transmission control protocol)/IP (Internet protocol).

[**0065**] Further, the TCP client unit **201** receives the redirect message RM transmitted from the server **100**A and relays the message to the connection manager **203**.

[**0066**] The connection manager **203** manages the logical connection to the server. Specifically, the connection manager **203** makes a request to the TCP client unit **201** for release of the logical connection to the server **100**A based on the redirect message RM relayed by the TCP client unit **201**.

[**0067**] Further, the connection manager **203** executes establishment of logical connection to the server **100**B after the logical connection to the server **100**A is released.

[**0068**] The application processor **205** executes the various applications offered to the client terminal **200**A. In this embodiment, the client terminal **200**A includes the function of the security camera, and thereby executes processing of moving image data captured by use of a charge-coupled device (CCD; not shown) and the like.

(Operations of Information Processing System)

[**0069**] Next, operations of the information processing system of this embodiment will be described with reference to **FIG. 4** to **FIG. 8B**. Specifically, operations to be executed when the server **100**B (the different server apparatus) is connected to the home network as a new server apparatus will be described.

**[0070]** **FIG. 4** shows a process flow to be executed by the server **100**B. Meanwhile, **FIGS. 5 and 6** show a process flow to be executed by the server **100**A.

(1) Process Flow by Server **100**B

**[0071]** First, the process flow by the server **100**B will be described. As shown in **FIG. 4**, in Step S**10**, the server **100**B newly connected to the home network **10** executes the start-up process. Specifically, the server **100**B executes initialization of respective logic blocks that constitute the server **100**B, or the like.

**[0072]** In Step S**20**, the server **100**B generates the subscribe message SM upon completion of the start-up process.

**[0073]** In Step S**30**, the server **100**B attaches the signature SG to the generated subscribe message SM. Specifically, the server **100**B attaches the signature SG to the generated subscribe message SM by use of the secret key of the server **100**B corresponding to the public key certified by the certificate authority (CA), and the given one-way hash function.

**[0074]** In Step S**40**, the server **100**B transmits the signature-attached subscribe message M**1** attaching the signature SG to the home network **10** by use of the UDP.

(2) Process Flow by Server **100**A.

**[0075]** Next, the process flow by the server **100**A receiving the signature-attached subscribe message M**1** will be described. As shown in **FIG. 5**, in Step S**110**, the server **100**A receives the signature-attached subscribe message M**1** which is transmitted from the server **100**B.

**[0076]** In Step S**120**, the server **100**A checks whether or not there are any client terminals currently connected to the server **100**A.

**[0077]** When there is at least one a client terminal currently connected to the server **100**A (Yes in Step S**120**), in Step S**130**, the server **100**A verifies validity of the received signature-attached subscribe message M**1**.

**[0078]** Specifically, the server **100**A verifies the signature SG by use of the public key of the server **100**B.

**[0079]** In Step S**140**, the server **100**A judges whether the subscribe message SM is valid or invalid. When the signature SG is authorized, the server **100**A judges that the subscribe message SM included in the signature-attached subscribe message M**1** is valid.

**[0080]** When the subscribe message SM is judged to be invalid (No in Step S**140**), the server **100**A repeats the processing from Step S**110**. In other words, the server **100**A terminates the processing with the received subscribe message SM, and stands by for receiving a new signature-attached subscribe message SM.

**[0081]** When the subscribe message SM is judged to be valid (Yes in Step S**140**), in Step S**150**, the server **100**A executes a "server selection process" as a subroutine. **FIG. 6** shows the content of the server selection process.

**[0082]** As shown in **FIG. 6**, in Step S**210**, the server **100**A compares the feature list included in the subscribe message SM transmitted from the server **100**B with the feature list of the server **100**A, and determines whether or not the features of those serves are at the same level.

**[0083]** For example, the server **100**A compares the feature list (feature="hcsps" shown in **FIG. 8A**), which is included in the subscribe message SM transmitted from the server **100**B, with the feature list (feature="hcsps, webs, and db" shown in **FIG. 7**) stored in the server **100**A.

**[0084]** When the features are not at the same level between the servers (No in Step S**210**), in Step S**250**, the server **100**A selects the server having a higher performance.

**[0085]** When the features are at the same level between the servers (Yes in Step S**210**), in Step S**220**, the server **100**A checks whether the maximum number of connectable client terminals (max="5" shown in **FIG. 8A**) are the same between the servers.

**[0086]** When the maximum numbers of connectable client terminals are not the same (No in Step S**220**), in Step S**240**, the server **100**A selects the server having a larger value of the maximum number of connectable client terminals.

**[0087]** When the maximum numbers of connectable client terminals are the same (Yes in Step S**220**), the server compares server identifiers (see **FIG. 7**) word by word and selects the server having a smaller server identifier, i.e. in accordance with the alphabetical order.

**[0088]** In Step S**260**, the server **100**A determines the selected server as the server functioning as the connection point for the client terminals, and terminates the server selection process.

**[0089]** Subsequently, as shown in **FIG. 5**, the server **100**A checks whether or not the selected server is the server that newly connected to the home network (server **100**B) in Step S**160**. Here, an assumption will be made that the server **100**B is selected.

**[0090]** When the selected server is the server **100**B (Yes in Step S**160**), in Step S**170**, the server **100**A generates the redirect message RM (see **FIG. 8B**) for changing the connection point for the client terminals currently connected to the server **100**A to the server **100**B. Specifically, the server **100**A generates the redirect message RM having an IP address of the server **100**B in the IP address section (ip=192.168.1.9:17320 shown in **FIG. 8B**) for a destination of redirection (the server **100**B).

**[0091]** In Step S**180**, the server **100**A transmits the generated redirect message RM to the client terminals **200**A to **200**C.

**[0092]** Here, the client terminals **200**A to **200**C which receive the redirect message RM change the connection point from the server **100**A to the server **100**B.

(Operation and Effect)

**[0093]** According to the above-described information processing system of this embodiment, when the signature of the server **100**B is verified as valid by the signature verifier **109** of the server **100**A, the connection point for the client terminal connected to the server **100**A is changed to the server **100**B.

**[0094]** Therefore, it is possible to change the connection point for the client terminal to the server **100**B only when the server **100**B is newly connected to the home network **10** and is verified to be a valid server apparatus.

**[0095]** In other words, according to the information processing system, it is possible to prevent confusion in the information processing system due to an attempt by a client terminal to establish connection to an invalid server when the invalid server is connected to the home network **10**.

**[0096]** Further, according to the information processing system, the connection point for the client terminals **200**A to **200**C is changed to the server **100**B which is newly connected to the home network **10** when the feature of the server **100**B is higher than that of the server **100**A.

**[0097]** Therefore, it is possible to connect the client terminals **200**A to **200**C to the highest performance server connected to the home network **10**.

**[0098]** In addition, according to the information processing system, the UDP is used for transmission and reception of the signature-attached subscribe message **M1**. Therefore, it is possible to suppress processing loads on the servers **100**A and **100**B, and the home network **10** as compared to the case of using the TCP.

## Other Embodiments

**[0099]** The present invention has been described above with reference to a certain embodiment. It should be noted, however, that the description and drawings constituting part of this disclosure shall not be deemed to limit the scope of the present invention. It is obvious to those skilled in the art that various substitutions and modifications are possible by the teaching of this specification.

**[0100]** For example, in the above-described embodiment of the present invention, the client terminals **200**A to **200**C have the functions of the security cameras. However, these functions are not always essential to the client terminals **200**A to **200**C. Meanwhile, it is also possible to apply a personal computer or the like as the client terminal.

**[0101]** In addition, it is also possible to combine the features of the server **100**A shown in **FIG. 2** and the features of the client terminal **200**A shown in **FIG. 3** into one apparatus.

**[0102]** Meanwhile, in the above-described embodiment of the present invention, the feature list of the server **100**B is compared with the feature list of the server **100**A, and the connection point for the client terminals **200**A to **200**C is changed to the server **100**B when the server **100**B newly connected to the home network **10** has the higher performance than the server **100**A. Nevertheless, it is not always necessary that the server **100**A compare the feature list of the server **100**B with the feature list of the server **100**A.

**[0103]** Moreover, in the above-described embodiment of the present invention, the UDP is used for transmission and reception of the signature-attached subscribe message **M1**. However, upon transmission and reception of the signature-attached subscribe message **M1**, it is possible to use the TCP instead of the UDP.

**[0104]** In this manner, it is needless to say that the present invention encompasses various other embodiments which are not expressly stated herein. In this context, the technical scope of the present invention shall be solely determined by the matter to define the present invention relevant to the appended claims that deem to be appropriate in conjunction with the above descriptions.

What is claimed is:

**1**. A server apparatus configured to connect a client terminal apparatus through a communication network, the server apparatus comprising:

a signature-attached message receiver configured to receive a signature-attached message having a signature of a different server apparatus connected to the communication network from the different server apparatus;

a signature verifier configured to verify whether the signature attached to the signature-attached message is valid or invalid; and

a connection point changer configured to change a connection point for the client terminal apparatus to the different server apparatus when the signature verifier verifies that the signature is valid.

**2**. The server apparatus of claim 1, further comprising:

a signature attaching unit configured to attach the signature of the server apparatus to a message to be transmitted to the communication network; and

a signature-attached message transmitter configured to transmit the signature-attached message having the signature attached by the signature attaching unit to the communication network.

**3**. The server apparatus of claim 1, wherein

the connection point changer compares a feature list indicating a feature of the different server apparatus, which is included in the signature-attached message received by the signature-attached message receiver, with a feature list of the server apparatus, and

the connection point changer changes the connection point for the client terminal apparatus to the different server apparatus when the feature of the different server apparatus is higher than the server apparatus.

**4**. The server apparatus of claim 1, wherein the signature-attached message receiver receives the signature-attached message transmitted by the different server apparatus using the user datagram protocol.

**5**. The server apparatus of claim 2, wherein the signature-attached message transmitter transmits the signature-attached message by use of the user datagram protocol.

* * * * *