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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 September 2006 (21.09.2006)

PCT

(10) International Publication Number
WO 2006/099540 A2

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2006/009525

(22) International Filing Date: 15 March 2006 (15.03.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/661,831 15 March 2005 (15.03.2005) US

(71) Applicant *(for all designated States except US)*: **TRAPEZE NETWORKS, INC.** [US/US]; 5753 W. Las Positas Blvd., Pleasanton, CA 94588 (US).

(72) Inventor: **HARKINS, Dan**; 1886 San Andreas Rd., La Selva Beach, CA 95076 (US).

(74) Agent: **AHMAN, William, F.**; Perkins Coie LLP, 101 Jefferson Drive, Menlo Park, CA 94025 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

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

WO 2006/099540 A2

(54) Title: SYSTEM AND METHOD FOR DISTRIBUTING KEYS IN A WIRELESS NETWORK

(57) Abstract: A technique for improving authentication speed when a client roams from a first authentication domain to a second authentication domain involves coupling authenticators associated with the first and second authentication domains to an authentication server. A system according to the technique may include, for example, a first authenticator using an encryption key to ensure secure network communication, a second authenticator using the same encryption key to ensure secure network communication, and a server coupled to the first authenticator and the second authenticator wherein the server distributes, to the first authenticator and the second authenticator, information to extract the encryption key from messages that a client sends to the first authenticator and the second authenticator.

SYSTEM AND METHOD FOR DISTRIBUTING KEYS IN A WIRELESS NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of US Patent Application No. 60/661,831, filed March 15, 2005, which is incorporated by reference.

BACKGROUND

[0002] Consumer demand for wireless local area network (WLAN) products (e.g. smart phones) grew rapidly in the recent past as the cost of WLAN chipsets and software fell while efficiencies rose. Along with the popularity, however, came inevitable and necessary security concerns.

[0003] The Institute of Electrical and Electronics Engineers (IEEE) initially attempted to address wireless security issues through the Wired Equivalent Privacy (WEP) standard. Unfortunately, the WEP standard quickly proved inadequate at providing the privacy it advertised and the IEEE developed the 802.11i specification in response. 802.11i provides a framework in which only trusted users are allowed to access WLAN network resources. RFC 2284, setting out an in-depth discussion of Point-to-Point Protocol Extensible Authentication Protocol (PPP EAP) by Merit Network, Inc (available at http://rfc.net/rfc2284.html as of March 9, 2006), is one example of the 802.11i network authentication process and is incorporated by reference.

[0004] A typical wireless network based on the 802.11i specification comprises a supplicant common known as a client (e.g. a laptop computer), a number of wireless access points (AP), and an authentication server. In some implementations, the APs also act as authenticators that keep the WLAN closed to all unauthenticated traffic. To access the WLAN securely, an encryption key known as the Pairwise Master Key (PMK) must first be established between the client and an AP. The client and the AP then exchange a sequence of four messages known as the "four-way handshake." The four-way handshake produces encryption keys unique to the client that are subsequently used to perform bulk data protection (e.g. message source authentication, message integrity assurance, message confidentiality, etc.).

[0005] A handoff occurs when the client roams from one AP to another. Prior to 802.11i, it was necessary for the client to re-authenticate itself each time it associates with an AP. This renegotiation results in significant latencies and may prove fatal for real-time exchanges such as voice data transfer.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Embodiments of the present invention are illustrated in the figures. However, the embodiments and figures are illustrative rather than limiting; they provide examples of the present invention.

[0007] FIG. 1 is a block diagram illustrating an example of a WLAN system.

[0008] FIG. 2 is a block diagram illustrating an example of a WLAN system including one or more authenticators.

[0009] FIG. 3 is a block diagram illustrating an example of a WLAN system including one or more authentication domains.

[0010] FIG. 4 depicts a flowchart of an example of a method for secure network communication.

[0011] FIG. 5 depicts a flowchart of another example of a method for secure network communication.

[0012] FIG. 6 depicts a flowchart of a method to obtain an encryption key for secure network communication.

[0013] The foregoing examples of the related art and limitations related therewith are intended to be illustrative and not exclusive. Other limitations of the related art will become apparent to those of skill in the art upon a reading of the specification and a study of the drawings.

DETAILED DESCRIPTION

[0014] In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without one or more of these specific details or in combination with other components or process steps. In other instances, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the present invention.

[0015] FIG. 1 is a block diagram illustrating an example of a Wireless Local Area Network (WLAN) system 100. In the example of FIG. 1, the WLAN system 100 includes an authentication server 102, switches 104-1 to 104-N (referred to collectively hereinafter as switches 104), Access Points (APs) 106-1 to 106-N (referred to collectively hereinafter as APs 106), and clients 108-1 to 108-N (referred to collectively hereinafter as clients 108).

[0016] In the example of FIG. 1, the authentication server 102 may be any computer system that facilitates authentication of a client in a manner described later with reference to FIGS. 4-6. The authentication server 102 may be coupled to one or more of the switches 104 through, for example, a wired network, a wireless network, or a network such as the Internet. The term "Internet" as used herein refers to a network of networks which uses certain protocols, such as the TCP/IP protocol, and possibly other protocols such as the hypertext transfer protocol (HTTP) for hypertext markup language (HTML) documents that make up the World Wide Web (the web). The physical connections of the Internet and the protocols and communication procedures of the Internet are well known to those of skill in the art. In

an alternative embodiment, the authentication server 102 may reside on one of the switches 104 (or, equivalently, one of the switches 104 may reside on the authentication server).

[0017] In the example of FIG. 1, the switches 104 may be any computer system that serves as an intermediary between a subset of the APs 106 and the server 102. In an alternative, the APs may include the functionality of the switches 104, obviating the need for the switches 104.

[0018] In the example of FIG. 1, the APs 106 typically include a communication port for communicating with one or more of the clients 108. The communication port for communicating with the clients 108 typically includes a radio. In an embodiment, at least some of the clients 108 are wireless clients. Accordingly, APs 108 may be referred to in the alternative as "wireless access points" since the APs 106 provide wireless access for the clients 108 to a network, such as a Local Area Network (LAN) or Virtual LAN (VLAN). The APs 106 may be coupled to the network through network interfaces, which can be Ethernet network or other network interfaces. The network may also be coupled to a gateway computer system (not shown) that can provide firewall and other Internet-related services for the network. This gateway computer system may be coupled to an Internet Service Provider (ISP) to provide Internet connectivity to the clients 108. The gateway computer system can be a conventional server computer system.

[0019] In the example of FIG. 1, the clients 108 may include any wireless device. It should be noted that clients may or not be wireless, but for illustrative purposes only, the clients 108 are assumed to include wireless devices, such as by way of example but not limitation, cell phones, PDAs, laptops, notebook computers, or any other device that makes use of 802.11 or

other wireless standards. When the clients 108 are authenticated, they can communicate with the network. For illustrative purposes, clients 108 are coupled to the APs 106 by lines 110, which represent a secure connection.

[0020] In the example of FIG. 1, in operation, to communicate through data traffic in the WLAN system 100, the clients 108 typically initiate a request to access the network. An authenticator (not shown) logically stands between the clients 108 and the network to authenticate the client's identity and ensure secure communication. The authenticator may reside in any convenient location on the network, such as on one, some, or all of the APs 106, on one, some, or all of the switches 104, or at some other location. Within the 802.11i context, the authenticator ensures secure communication by encryption schemes including the distribution of encryption keys. For example, the authenticator may distribute the encryption keys using existing encryption protocols such as, by way of example but not limitation, the Otway-Rees and the Wide-Mouth Frog protocols. The authenticator may distribute the encryption keys in a known or convenient manner, as described later with reference to FIGS. 4-6.

[0021] In the example of FIG. 1, a client may transition from one authenticator to another and establish secure communication via a second authenticator. The change from one authenticator to another is illustrated in FIG. 1 as a dotted line 112 connecting the client 108-N to the AP 106-N. In a non-limiting embodiment, the secure communication via the second authenticator may be accomplished with one encryption key as long as both the first and second authenticators are coupled to the same authentication server 102. In alternative embodiments, this may or may not be the case.

[0022] FIG. 2 is a block diagram illustrating an example of a WLAN system 200 including one or more authenticators. In the example of FIG. 2, the WLAN system 200 includes authenticators 204-1 to 204-N (referred to hereinafter as the authenticators 204), and a client 208. As was previously indicated with reference to FIG. 1, the authenticators 204 may reside on APs (see, e.g., FIG. 1), switches (see, e.g., FIG. 1) or at some other location in a network.

[0023] In the example of FIG. 2, in a non-limiting embodiment, the client 208 scans different channels for an access point with which to associate in order to access the network. In an alternative embodiment, scanning may or may not be necessary to detect an access point. For example, the client 208 may know of an appropriate access point, obviating the need to scan for one. The access point may or may not have a minimum set of requirements, such as level of security or Quality of Service (QoS). In the example of FIG. 2, the client 208 determines that access point meets the required level of service and thereafter sends an association request. In an embodiment, the access request includes information such as client ID and cryptographic data. The request may be made in the form of a data packet. In another embodiment, the client 208 may generate and later send information including cryptographic data when that data is requested.

[0024] In the example of FIG. 2, the authenticator 204-1 authenticates the client 208. By way of example but not limitation, the authenticator 204-1 may first obtain a session encryption key (SEK) in order to authenticate the client 208. In one implementation, the authenticator requests the SEK and relies on an existing protocol (e.g. 802.1X) to generate a PMK as the SEK. In an alternative implementation, the SEK is pre-configured by mapping a preset value (e.g. user password) into a SEK. In the event that a preset value is used,

convenient or well-known methods such as periodically resetting the value, or remapping the value with randomly generated numbers, may be employed to ensure security. In this example, once the authenticator 204-1 obtains the SEK, it proceeds to a four-way handshake whereby a new set of session keys are established for data transactions originating from client 208. Typically, the client 208 need not be authenticated again while it communicates via the authenticator 204-1. In the example of FIG. 2, the connection between the client 208 and the server 204-1 is represented by the line 210.

[0025] In the example of FIG. 2, the client 208 roams from the authenticator 204-1 to the authenticator 204-N. The connection process is represented by the arrows 212 to 216. In an embodiment, when the client 208 roams, the server 202 verifies the identity of the (new) authenticator 204-N and the client 208. When roaming, the client 208 sends a cryptographic message to authenticator 204-N including the identity of the client 208 (IDc); the identity of the server 202 (IDs); a first payload including the identity of the authenticator 204-N (IDa) and a randomly generated key (k) encrypted by a key that client 208 and the server 202 share (eskey); and a second payload including the SEK encrypted by the random key k. This cryptographic message is represented in FIG. 2 as arrow 212. In an alternative embodiment, the client 208 sends the cryptographic message along with its initial association request.

[0026] In the example of FIG. 2, in an embodiment, once authenticator 204-N receives the cryptographic message, it keeps a copy of the encrypted SEK, identifies the server 202 by the IDs, and sends a message to the server 202 including the identity of the client IDc and the first payload from the original cryptographic message having the identity of the authenticator IDa and the random key k encrypted by the share key eskey.

[0027] In the example of FIG. 2, when the server 202 receives the message from authenticator 204-N, it looks up the shared key eskey based on the identity of the client IDc and decrypts the message using the eskey. The server 202 then verifies that a trusted entity known by IDa exists and, if so, constructs another message consisting of the random key k encrypted with a key the server 202 shares with authenticator 204-N (askey) and sends that message to the authenticator 204-N. However, if the server 202 can not verify the authenticator 204-N according to IDa, the process ends and client 201 cannot access the network through the authenticator 204-N. In the event that the authenticator 204-N cannot be verified the client may attempt to access the network via another authenticator after a preset waiting period elapses.

[0028] Upon receipt of the message from the server 202, the authenticator 204-N decrypts the random key k using the shared key askey and uses k to decrypt the encryption key SEK. Having obtained the encryption key SEK, the authenticator 204-N may then proceed with a four-way handshake, which is represented in FIG. 2 for illustrative purposes as arrows 214 and 216, and allow secure data traffic between the client 208 and the network.

[0029] Advantageously, the authentication system illustrated in FIG. 2 enables a client 208 to roam efficiently from authenticator to authenticator by allowing the client 208 to keep the same encryption key SEK when transitioning between authenticators coupled to the same server 202. For example, the client 208 can move the SEK securely between authenticators by using a trusted third party (e.g. the server 202) that negotiates the distribution of the SEK without storing the SEK itself.

[0030] FIG. 3 is a block diagram illustrating an example of a WLAN system 300 including one or more authentication domains. In the example of FIG. 3, the WLAN system 300 includes a server 302, authentication domains 304-1 to 304-N (referred to hereinafter as authentication domains 304), and a network 306. The server 302 and the network 306 are similar to those described previously with reference to FIGS. 1 and 2. The authentication domains 304 include any WLANs, including virtual LANs, that are associated with individual authenticators similar to those described with reference to FIGS. 1 and 2.

[0031] The scope and boundary of the authentication domains 304 may be determined according to parameters such as geographic locations, load balancing requirements, etc. For illustrative purposes, the client 308 is depicted as roaming from the authentication domain 304-1 to the authentication domain 304-N. This may be accomplished by any known or convenient means, such as that described with reference to FIGS. 1 and 2.

[0032] FIGS. 4 to 6, which follow, serve only to illustrate by way of example. The modules are interchangeable in order and fewer or more modules may be used to promote additional features such as security or efficiency. For example, in an alternative embodiment, a client may increase security by generating and distributing a unique random key to each authenticator. In another alternative embodiment of the present invention, the authenticator employs a known or convenient encryption protocol (e.g. Otway-Rees, Wide-Mouth Frog, etc.) to obtain the encryption key.

[0033] FIG. 4 depicts a flowchart of an example of a method for secure network communication. In the example of FIG. 4, the flowchart starts at module 401 where a client sends an association request to an access point. The flowchart continues at decision point

403 where it is determined whether a preconfigured encryption key is used. If it is determined that a preconfigured encryption key is not to be used (403-NO), then the flowchart continues at module 405 with requesting an encryption key and at decision point 407 with waiting for the encryption key to be received.

[0034] In the example of FIG. 4, if a preconfigured encryption key is provided at module 403, or an encryption key has been received (407-YES), then the flowchart continues at module 409 with a four-way handshake. The flowchart then continues at module 411 where data traffic commences, and the flowchart continues to decision point 413 where it is determined whether the client is ready to transition to a new authentication domain.

[0035] In the example of FIG. 4, if it is determined that a client is ready to transition to a new authentication domain (413-YES), then the flowchart continues at module 415 when the client sends a cryptographic message to the new authenticator. In an alternative embodiment, the client sends the cryptographic message along with its initial association request and skips module 415.

[0036] The flowchart continues at module 417, where once the new authenticator receives the cryptographic message, the new authenticator sends a message to the server. If at decision point 419 the authenticator is not verified, the flowchart ends. Otherwise, the server sends a message to the authenticator at module 421. The flowchart continues at module 423 where the authenticator obtains an encryption key, at module 424 where the client and the authenticator enter a four-way handshake, and at module 427 where data traffic commences.

[0037] FIG. 5 depicts a flowchart of another example of a method for secure network communication. In the example of FIG. 5, the flowchart begins at module 501 where a client

makes an association request. The flowchart continues at decision point 503, where it is determined whether a preconfigured encryption key is available. If it is determined that a preconfigured encryption key is not available (503-NO) then the flowchart continues at module 505, where an encryption key is requested, and at decision point 507 where it is determined whether an encryption key is received. If it is determined that an encryption is not received (507-NO), the flowchart continues from module 505. If, on the other hand, it is determined that an encryption key is received (507-YES), or if a preconfigured encryption key is available (503-YES), then the flowchart continues at module 509 with a four-way handshake. In the example of FIG. 5, the flowchart continues at module 511, where data traffic commences, and at decision point 513, where it is determined whether a client is ready to transition. If it is determined that a client is not ready to transition (513-NO), then the flowchart continues at module 511 and at decision point 513 until the client is ready to transition (513-YES). The flowchart continues at module 515, where an authenticator obtains an encryption key using an established cryptographic protocol. The flowchart continues at module 517 with a four-way handshake, and at module 519 where data traffic commences.

[0038] FIG. 6 depicts a flowchart of a method to obtain an encryption key for secure network communication. In one embodiment, a client transitions from a first authenticator to a second authenticator, both of which coupled to the same server, and establishes secure communication with the first and the second authenticator using one encryption key.

[0039] At module 601, a client generates a first key. In one embodiment, the first key is randomly generated. In an alternative embodiment, the first key is generated according to a

preset value such as by requesting a value (e.g. password) from a user. In yet another alternative embodiment, the first key is a constant value such as a combination of the current date, time, etc.

[0040] At module 603, the client obtains a second key. In one implementation, the generation of the second key relies on an existing protocol (e.g. 802.1X). In an alternative implementation, the second key is pre-configured (e.g. user password). In yet another alternative implementation, the second key is a combination of a pre-configured value and a randomly generated value.

[0041] At module 605, the client constructs a first message using the first key and the second key. In one embodiment, the message is a data packet comprising cryptographic data using the first and the second key. Furthermore, in one embodiment, the first message comprises the second key encrypted with the first key.

[0042] At module 607, the client sends the first message to an authenticator. In one embodiment, the authenticator is a second authenticator from which the client transitions from a first authenticator.

[0043] At module 609, the authenticator constructs a second message using data from the first message. In one implementation, the authenticator constructs the second message comprising the client's identity, and an encrypted portion having identity of the authenticator and the first key.

[0044] At module 611, the authenticator sends the second message to a server with which the authenticator is coupled. At module 613, the server decrypts an encrypted portion of the

second message. In one implementation, the encrypted portion of the second message comprises the identity of the authenticator and the first key.

[0045] Subsequently at module 615, the server verifies the authenticator with the decrypted identity information extracted from the second message. If the server cannot verify the authenticator according to the identification information, as shown at decision point 617, the client cannot communicate through the authenticator. If, on the other hand, the server verifies the authenticator, the server constructs a third message with the first key that it extracted from the second message at module 619. In one implementation, the third message comprises the first key encrypted with a third key that the server shares with the authenticator. The server then sends the third message to the authenticator at module 621.

[0046] After receiving the third message, the authenticator extracts the first key from the message at module 623. In one implementation, the authenticator extracts the first key using a third key it shares with the server. With the first key, the authenticator then decrypts the cryptographic data in the first message and extracts the second key at module 625. Having obtained the second key, the authenticator establishes secure data traffic/communication with the client using the second key. In one embodiment, the authenticator is a second authenticator to which the client transitions from a first authenticator coupled to the server, and the client communicates securely with both the first and the second authenticator using the second key.

[0047] As used herein, the term "embodiment" means an embodiment that serves to illustrate by way of example but not limitation. It may be noted that, in an embodiment, timestamps can be observed to measure roaming time.

[0048] It will be appreciated to those skilled in the art that the preceding examples and embodiments are exemplary and not limiting to the scope of the present invention. It is intended that all permutations, enhancements, equivalents, and improvements thereto that are apparent to those skilled in the art upon a reading of the specification and a study of the drawings are included within the true spirit and scope of the present invention. It is therefore intended that the following appended claims include all such modifications, permutations and equivalents as fall within the true spirit and scope of the present invention.

CLAIMS

What is claimed is:

1. A system comprising:

a first authenticator using an encryption key to ensure secure network communication;

a second authenticator using the encryption key to ensure secure network communication; and

a server coupled to the first authenticator and the second authenticator wherein the server distributes, to the first authenticator and the second authenticator, information to extract the encryption key from messages that a client sends to the first authenticator and the second authenticator.

2. The system of Claim 1, wherein the client maintains the encryption key that allows the client to communicate securely with authenticators coupled to the server.

3. The system of Claim 1, wherein the first authenticator is implemented in a network switch or an access point.

4. The system of Claim 1, wherein the second authenticator is implemented in a network switch or an access point.

5. The system of Claim 1, further comprising a first key that the client uses to encrypt the encryption key when the client sends a first message to the first authenticator.

6. The system of Claim 1, further comprising a first key that the client uses to encrypt the encryption key when the client sends a first message to the first authenticator; and a second key that the server and the client share, wherein the server uses the second key to decrypt and extract the portion of the first message comprising the first key and the identity of the first authenticator.

7. The system of Claim 1, further comprising

a first key that the client uses to encrypt the encryption key when the client sends a first message to the first authenticator;

a second key that the server and the client share, wherein the server uses the second key to extract the portion of the first message comprising the first key and the identity of the first authenticator;

a third key that the server and the first authenticator share, wherein the server uses the third key to encrypt the first key and sends the first key encrypted with the third key to the first authenticator, and wherein the first authenticator uses the third key to extract the first key which the first authenticator uses to extract the encryption key in order to establish secure communication with the client;

a fourth key that the client uses to encrypt the encryption key when the client sends a second message to the second authenticator;

a fifth key that the server and the client share, wherein the server uses the fifth key to extract the portion of the second message comprising the fourth key and the identity of the second authenticator; and

a sixth key that the server and the second authenticator share, wherein the server uses the sixth key to encrypt the fourth key and sends the fourth key encrypted with the sixth key to the second authenticator, and wherein the second authenticator uses the sixth key to extract the fourth key which the second authenticator uses to extract the encryption key in order to establish secure communication with the client.

8. A system comprising:

a first authentication domain using an encryption key to ensure secure network communication;

a second authentication domain using the encryption key to ensure secure network communication; and

a server coupled to the first authentication domain and the second authentication domain wherein the server acts as a trusted third party for a client that transitions from the first authentication domain to the second authentication domain.

9. The system of Claim 8, further comprising

a first key that the client uses to encrypt the encryption key when the client sends a fist message to the first authenticator;

a second key that the server and the client share, wherein the server uses the second key to extract the portion of the first message comprising the first key and the identity of the first authenticator;

a third key that the server and the first authenticator share, wherein the server uses the third key to encrypt the first key and sends the first key encrypted with the third key to the first authenticator, and wherein the first authenticator uses the third key to extract the first key which the first authenticator uses to extract the encryption key in order to establish secure communication with the client;

a fourth key that the client uses to encrypt the encryption key when the client sends a second message to the second authenticator;

a fifth key that the server and the client share, wherein the server uses the fifth key to extract the portion of the second message comprising the fourth key and the identity of the second authenticator;

a sixth key that the server and the second authenticator share, wherein the server uses the sixth key to encrypt the fourth key and sends the fourth key encrypted with the sixth key to the second authenticator, and wherein the second authenticator uses the sixth key to extract the fourth key which the second authenticator uses to extract the encryption key in order to establish secure communication with the client.

10. The system of Claim 8, wherein the first authentication domain comprises a first authenticator coupled to the server and the second authentication domain comprises a second authenticator coupled to the server.

11. The system of Claim 8, wherein the first authentication domain comprises a first authenticator coupled to the server and the second authentication domain comprises a second authenticator coupled to the server, and the client maintains an encryption key that allows the client to communicate securely in authentication domains having authenticators coupled to the server.

12. A method comprising:

providing a first key;

providing a second key;

constructing a first message comprising cryptographic data using the first key and the second key;

sending the first message to an authenticator;

constructing a second message comprising cryptographic data included in the first message at the authenticator;

sending the second message to a server coupled to the authenticator;

decrypting the second message at the server;

verifying the identity of the authenticator at the server; and

if the authenticator is verified:

constructing a third message comprising the first key at the server;

sending the third message to the authenticator from the server;

extracting the first key from the third message at the authenticator;

extracting the second key from the cryptographic data at the authenticator; and

establishing secure data communication with the client using the second key.

13. The method of Claim 12, further comprising identifying an access point at a client.

14. The method of Claim 12, further comprising identifying a server at the authenticator.

15. The method of Claim 12, wherein the authenticator is not verified, further comprising refusing client authentication.

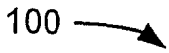
16. The method of Claim 12, wherein a client constructs and sends the first message comprising cryptographic data to the authenticator.

17. The method of Claim 12, wherein the first key is randomly generated.

18. The method of Claim 12, wherein the second key is defined by a user.

19. The method of Claim 12, wherein the authenticator is a second authenticator to which the client transitions from a first authenticator coupled to the server.

20. The method of Claim 12, wherein the authenticator is a second authenticator corresponding to an authentication domain to which the client transitions from a first authentication domain having a first authenticator coupled to the server.


100

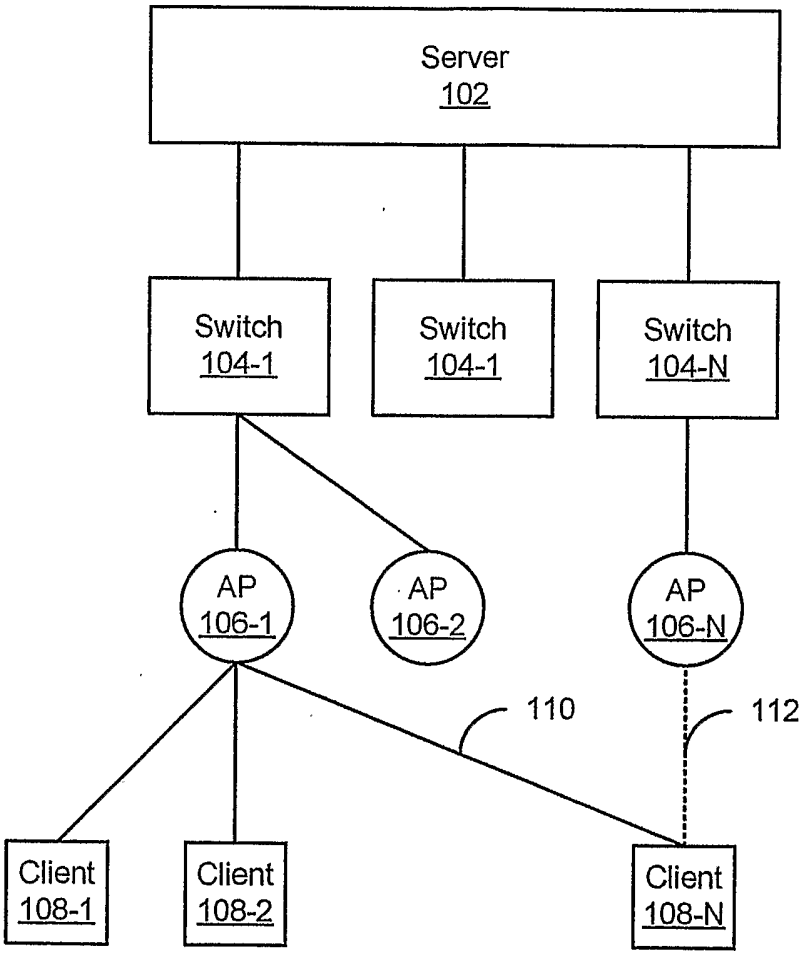

Server
102
Switch
104-1
Switch
104-1
Switch
104-N
AP
106-1
AP
106-2
AP
106-N
110
112
Client
108-1
Client
108-2
Client
108-N

FIG. 1

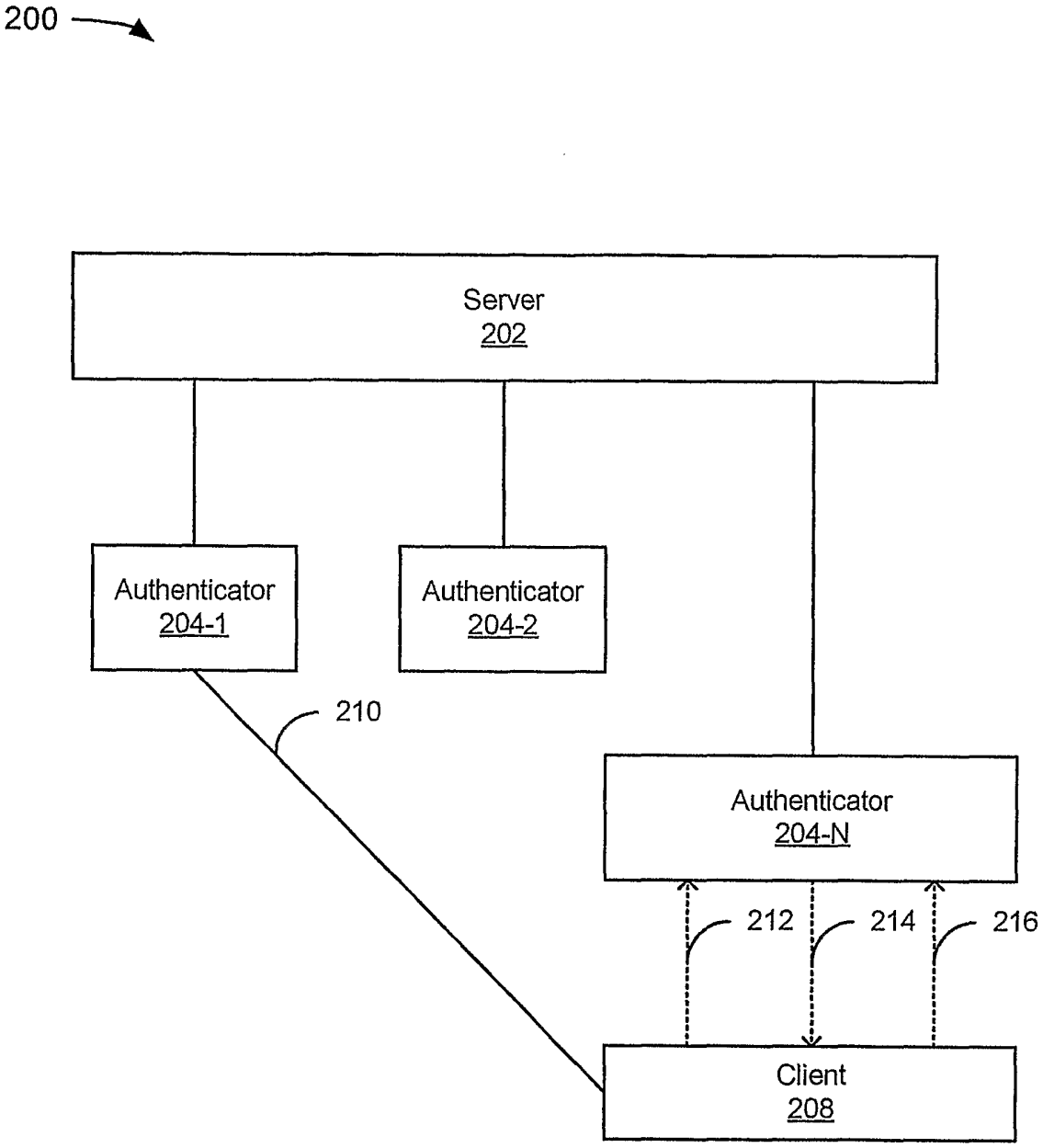

200
Server
202
Authenticator
204-1
Authenticator
204-2
210
Authenticator
204-N
212
214
216
Client
208

FIG. 2

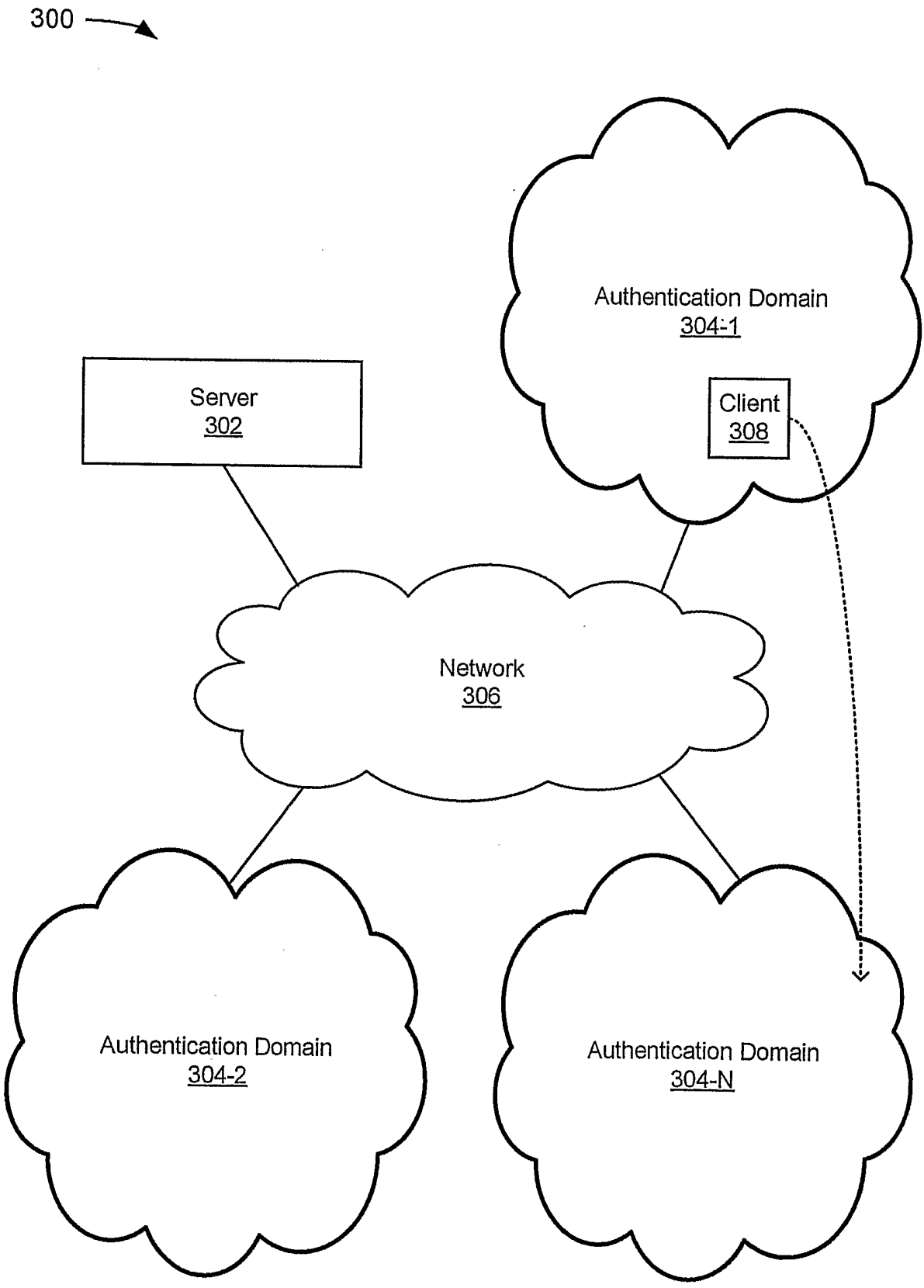
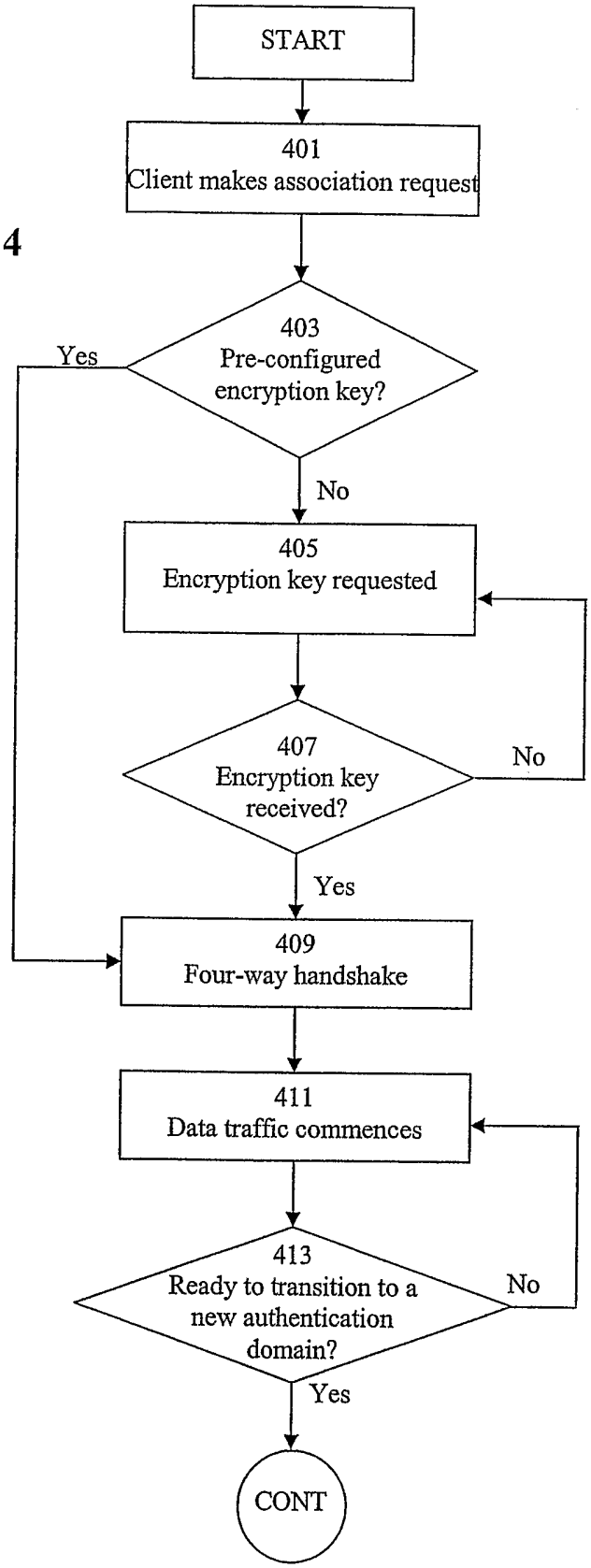

300
Authentication Domain
304-1
Server
302
Client
308
Network
306
Authentication Domain
304-2
Authentication Domain
304-N

FIG. 3

Figure 4


START
401
Client makes association request
403
Pre-configured encryption key?
Yes
No
405
Encryption key requested
407
Encryption key received?
No
Yes
409
Four-way handshake
411
Data traffic commences
413
Ready to transition to a new authentication domain?
No
Yes
CONT

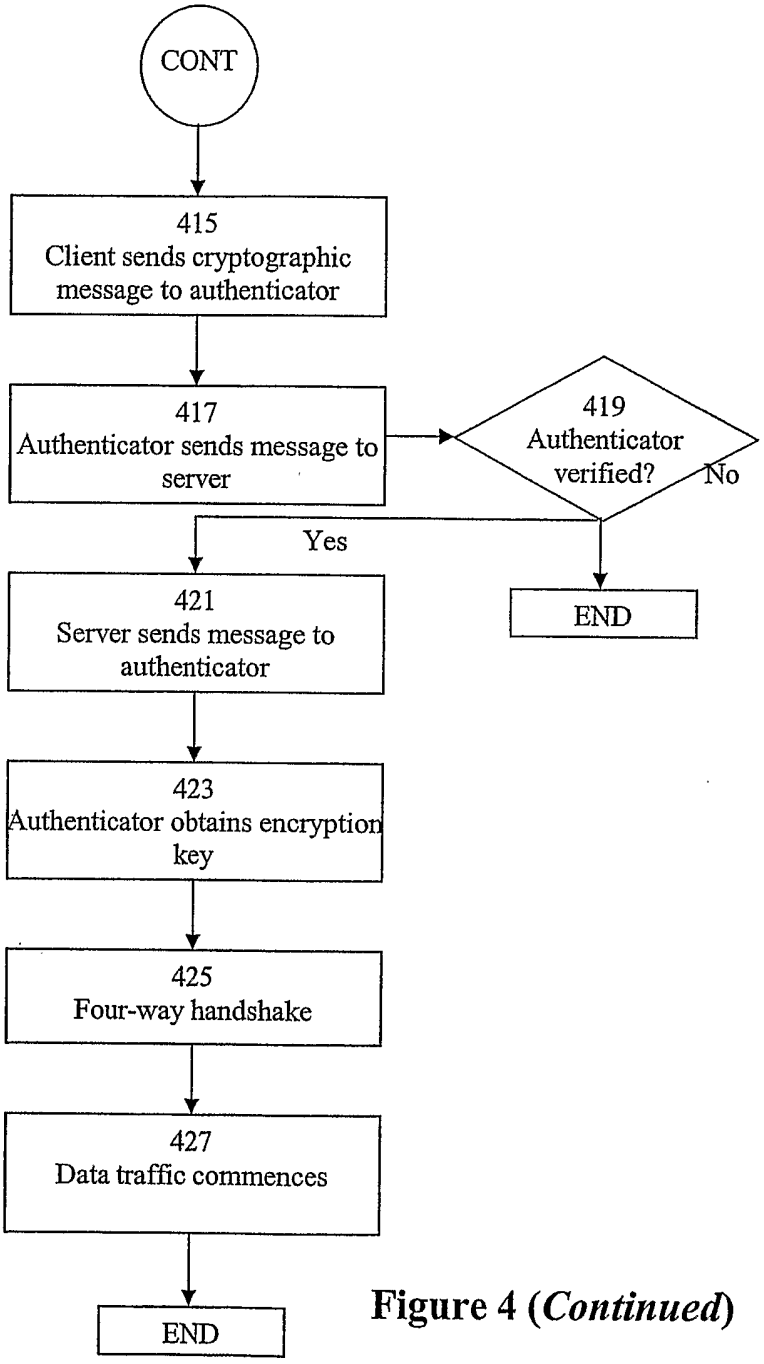
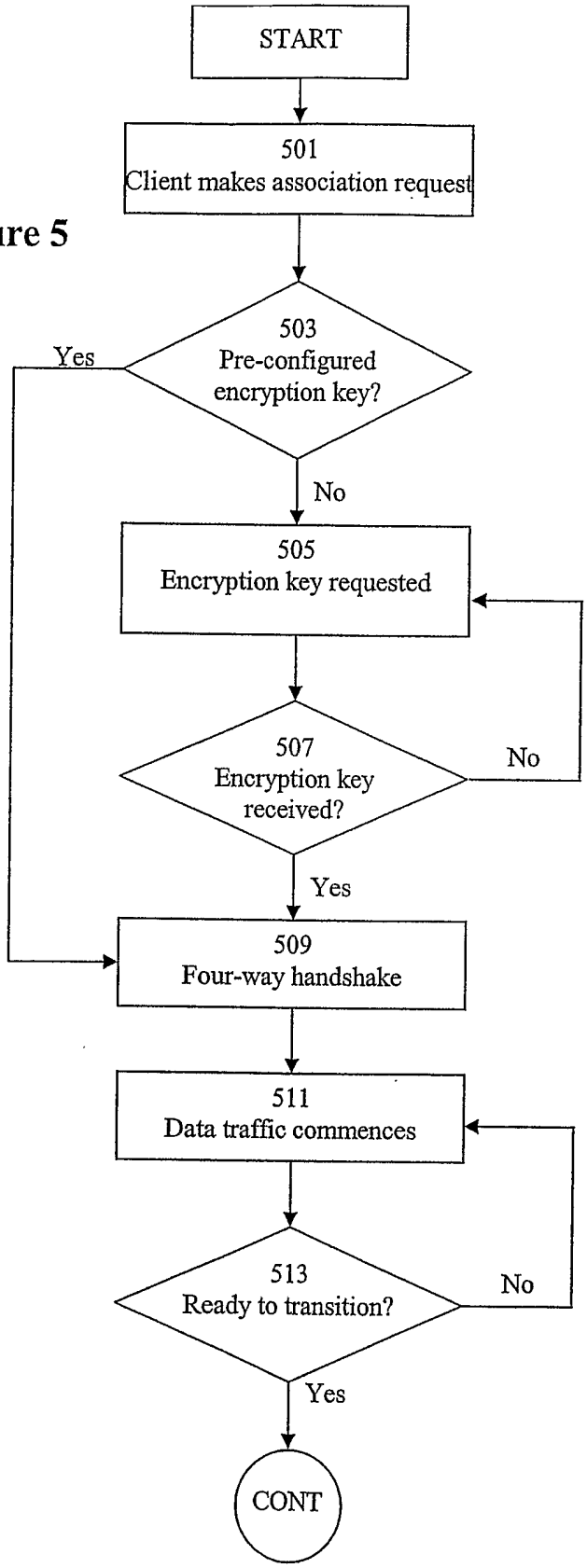


Figure 4 (*Continued*)

Figure 5


START
501
Client makes association request
503
Pre-configured encryption key?
Yes
No
505
Encryption key requested
507
Encryption key received?
No
Yes
509
Four-way handshake
511
Data traffic commences
513
Ready to transition?
No
Yes
CONT

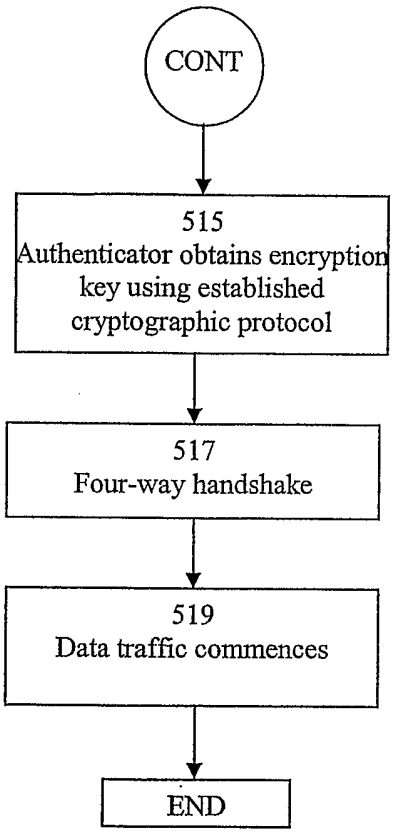


Figure 5 (*Continued*)

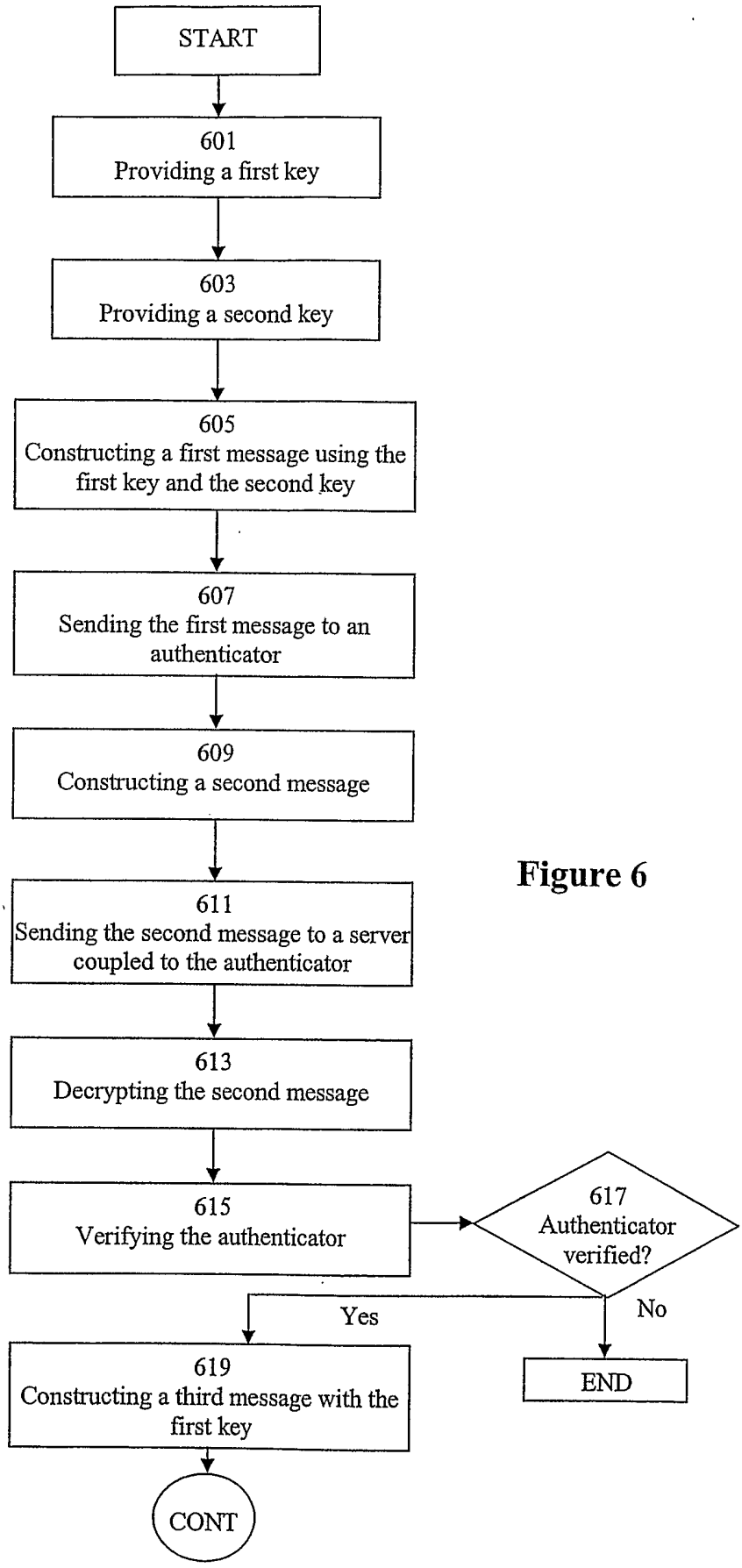

START
601
Providing a first key
603
Providing a second key
605
Constructing a first message using the first key and the second key
607
Sending the first message to an authenticator
609
Constructing a second message
611
Sending the second message to a server coupled to the authenticator
613
Decrypting the second message
615
Verifying the authenticator
617
Authenticator verified?
Yes
No
619
Constructing a third message with the first key
END
CONT

Figure 6

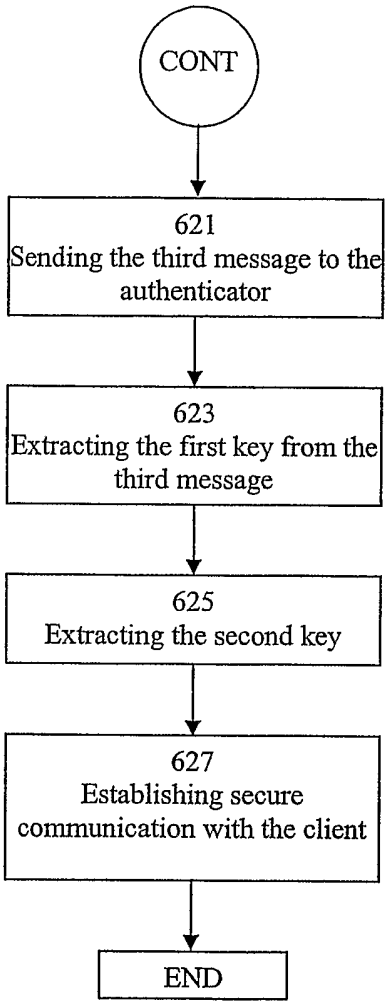


Figure 6 (*Continued*)