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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 November 2004 (04.11.2004)

PCT

(10) International Publication Number
WO 2004/095863 A1

(51) International Patent Classification[7]: H04Q 7/24

(21) International Application Number:
PCT/US2004/002491

(22) International Filing Date: 29 January 2004 (29.01.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/458,189 27 March 2003 (27.03.2003) US

(71) Applicant *(for all designated States except US)*: **THOMSON LICENSING S.A.** [US/US]; 46, Quai A. Le Galo, F-92648 Boulogne (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ZHANG, Junbiao** [CN/US]; 20 Jenna Drive, Bridgewater, NJ 08807 (US). **MATHUR, Saurabh** [IN/US]; 4701 Quail Ridge Drive, Plainsboro, NJ 08536 (US). **RAMASWAMY, Kumar** [IN/US]; 71 Sayre Drive, Princeton, NJ 08540 (US).

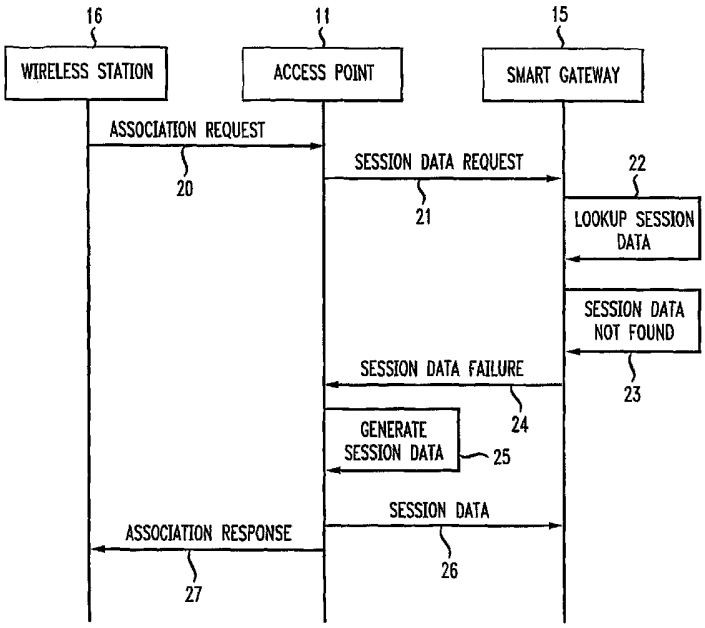
(74) Agents: **TRIPOLI, Joseph, S.** et al.; Two Independence Way, Suite #200, Princeton, NJ 08540 (US).

(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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, 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, 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, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SECURE ROAMING BETWEEN WIRELESS ACCESS POINTS



(57) Abstract: A system, method, and computer readable medium (fig.2) for enabling roaming of wireless client stations (16) among wireless access points (11) are disclosed. A gateway (15) programmed to receive session data requests (21) is provided in a network, which comprises access points (11) which are programmed to send session data requests (21) to the gateway. The gateway (15) sends session information setting commands to the requesting access point (11), or sends a session data failure (24) response to the access point.

WO 2004/095863 A1

Published:
— *with international search report*

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

SECURE ROAMING BETWEEN WIRELESS ACCESS POINTS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] Benefit of Provisional Application Serial No. 60/458189 filed March 27, 2003, is claimed.

[0002]

TECHNICAL FIELD

[0003] This invention relates to wireless local area networks, and particularly to methods and systems that facilitate roaming between wireless access points on a wireless access network.

[0004]

BACKGROUND OF THE INVENTION

[0005] IEEE 802.11-based wireless local area networks (WLANs) have become the focus of much research and development in recent years. WLANs offer simple, convenient to use, high throughput ways in which portable computer users can break away from the tethers of the wired world and move around freely with comparable network throughput. However, when a user moves from one access point to another, there is a need to provide seamless roaming. Present technology does not adequately meet this requirement.

[0006] In most of the current deployment, IEEE 802.11 uses static Wired Equivalent Privacy (WEP) keys and does not support per user session keys, thus, the wireless stations, usually clients, and all access points participating in roaming can have the same static WEP key. However, the security problem with static WEP keys has been highly publicized. Further, static WEP key protocols do not solve the distribution of authorization information to a large number of access points. To solve this problem, the IEEE 802.11 standard is trying to develop an Inter Access Point Protocol (IAPP).

[0007] The IEEE 802.1x standard addresses the security problem in IEEE 802.11 by using port controlled access control. In a large 802.1x installation, a backend authentication server authenticates the user. In order to secure the wireless link, the wireless station must go through an authentication process involving the station, the access point and the authentication server. If authentication is successful, a session key is agreed upon between the wireless station and the access point. This solution enables roaming, but with high overhead, i.e., each time a station is associated with a different access point, for example because of signal

fluctuation, the whole authentication process has to be carried through. This is highly undesirable, especially when the authentication server is far away from the wireless LAN, e.g., in an inter-working environment where the WLAN is in, for example, JFK airport but the authentication server belongs to, for example, SBC in California.

[0008] There is a need to provide seamless roaming when a wireless user (client) wishes to switch to an access point with better signal strength.

[0009] There is also a need to move per-user session keys and authorization information from one access point to another when a client roams between wireless access points.

[00010]

SUMMARY OF THE INVENTION

[00011] These needs and others, which will become apparent from the following disclosure are met by the present invention which comprises in one aspect a wireless local area network comprising gateway to control multiple access points. The access points reside in a wired or other type of network. The gateway is programmed to receive session data requests from access points, look up session data, and send session data back to the requesting access points. The access points are programmed to send requests for session data to the gateway and to receive and process session information setting commands from the gateway. The system comprising such a gateway moves the "intelligence" of the wireless network into such gateway and results in very simple access points, which enables easier control and more economical installation for large deployments.

[00012] In another aspect, the invention comprises a method of, and computer readable medium for, enabling roaming of wireless clients among wireless access points in a network comprising providing a gateway in the network, sending session data requests from access points to the gateway, looking up session data stored in the gateway, reporting session data failure if session data is not found, and sending a session data response from the gateway to the access points if session data is found or is generated by the gateway.

[00013] The present invention can compliment the IEEE 802.1x protocol and greatly reduce the complexity of the protocol.

[00014] The basic architecture of the system of the invention is illustrated in Fig. 1 wherein a gateway is used to control a number of access points with simple functions. The access points can be directly connected to the gateway or can be connected to the gateway through a network. Besides the normal IEEE 802.11 physical layer and MAC layer functions, these access points need only to support the following additional functions:

[00015] Per station session key;

[00016] An interface to accept session information (e.g. session key and authorization information) setting commands from the gateway; and

[00017] The capability to query the gateway about session information and transfer session information from the gateway.

[00018] Among these things, the first function is already widely available on many access points on the market presently. The other two functions are novel.

[00019] The invention also provides methods to deal with session information on the access point the wireless station (client) previously associated with, after the client roams to a different access point. In a first method, the gateway informs the previous access point to remove the information. In a second method, the access point sets up a timer to remove all idle wireless station entries after a certain time period of inactivity. The second method is preferred because the gateway does not have to send an extra command to remove the entry and the AP may maintain the entry to deal with "thrashing" scenarios in which the wireless station oscillates between two or more access points rather quickly. Because the entry is already there, the access point may just inquire the gateway about the "freshness" of the information instead of transferring all the session information. This may not seem to be significant if the session information only contains the session key, but with large session information, this could be potentially faster and save bandwidth.

[00020] There are differences in handling, or transferring, session information generated at the access point versus session information generated at the gateway.

[00021] The session information must be transferred to the gateway, thus the gateway must provide an interface for accepting session information, and the access point must be enhanced with the capability of transferring session information to the gateway. This is illustrated in Figure 3.

[00022] When session information is generated at the gateway, the session information need be transferred to the access point that the wireless station is associated with. There are no additional functionalities required at the access point beyond the basic functions mentioned earlier.

[00023] For the scheme to be secure, it must be ensured at any time that the connection between the gateway and each AP is trusted. This can be ensured through either physical security or encryption.

[00024] Physical security requires directly attaching the access points to the gateway or through a managed network.

[00025] Encryption requires that upon initial installation and configuration, the gateway and access points share a secret, or the gateway shares a secret with each access point. The communication between the gateway and the access points are encrypted with the secret(s).

[00026] For large deployment of this invention and to facilitate faster roaming, multiple gateways can be organized in a hierarchy. Each gateway is responsible for a number of access points. When the wireless station roams among the access points belonging to the same gateway, session transfer is controlled by this gateway. Only when the station associates with the WLAN the first time or when it roams across access points belonging to different gateways, would it be necessary for the gateway to fetch session information from the gateway in the higher hierarchy.

[00027]

BRIEF DESCRIPTION OF DRAWINGS

[00028] Fig. 1 illustrates an embodiment of a system of the invention having a gateway in the wired network, the wired network comprising access points.

[00029] Fig. 2 illustrates a flow chart of a first example of an authentication and association process among a wireless station, an access point, and a gateway according to the invention.

[00030] Fig. 3 illustrates a second example of an authentication and association process among a wireless station, an access point, and a gateway according to the invention.

[00031] Fig. 4 illustrates a third example of an authentication and association process among a wireless station, an access point, and a gateway according to the invention.

[00032]

DETAILED DESCRIPTION

[00033] Referring first to Fig. 1, an embodiment of a system according to the invention is illustrated wherein access points 11, 12, and 13 are connected to a wired network 14. There is no limit to the number of access points in the wired network. A smart gateway 15 is connected to the wired network 14. Wireless clients, such as laptop computers 16 and 17 and personal data assistants 18 and 19 are illustrated as communicating with the access points 11, 12, 13. Present generation clients and access points use 802.11 protocols.

[00034] Referring next to Fig. 2, a process is illustrated wherein a wireless station 16 requests an association with an access point 11 during step 20. The access point 11 which

relays the session data request to the gateway 15 during step 21. During step 22, the gateway 15 looks up the session data and if session data is not found during step 23, a session data failure signal is relayed during step 24 to the access point 11, which then generates session data during step 25 and sends the generated session data during step 26 to the gateway 15 and also sends an association response to the wireless station 16 during step 27.

[00035] The session information (including session key and authorization information) can be generated at the access points, as illustrated in Fig. 2, or at the gateway, as illustrated in Fig. 3, wherein the wireless station 16 requests an association with an access point 11 during step 20. The access point relays the session data request to the gateway 15 during step 21. The gateway 15 looks up the session data during step 22 and if session data is not found during step 23, the gateway generates the session data during step 28, and sends a session data response back to the access point 11 during step 29. The access point 11 loads the session data during step 30, and sends the association response back to the wireless station 16 during step 27.

[00036] As illustrated in the Fig. 2, Fig. 3, and Fig. 4, the access point first checks with the gateway to see if session information already exists for the wireless station. If session information does not already exist, as illustrated in Figs. 2 and 3, the wireless station is not authenticated by the WLAN yet or the previous authentication has expired. The normal authentication steps are carried out and session information (including the session key) is generated for the station and is set in both the currently associated access point and the gateway.

[00037] If session information already exists, for example, when the wireless station roams from one access point to another, the gateway returns it to the access point. The access point sets that information (including the session key) in the access point. An example of such a process is illustrated in Fig. 4 wherein the wireless station 16 sends the association request to access point 11 during step 20, which relays the session data request to the gateway 15, which in turn looks up the session data during step 22 and finds it. The access point sends a session data during step 29 to the access point 11 which then loads the session data during step 30 and sends an association response to the wireless station 16 during step 27.

[00038] This simple procedure ensures that session information travels with the wireless station from one access point to another without the station having to go through authentication all over again.

[00039] Thus the invention described herein provides a secure wireless local area network infrastructure for seamless roaming with smart gateways and simple access points.

[00040] While the invention has been described in detail herein, various alternatives, modifications, and improvements should become readily apparent to those skilled in theis art without departing from the spirit and scope of the invention.

CLAIMS

1. A system for enabling roaming of wireless clients among wireless access points comprising a gateway in a wired network which comprises access points, the gateway having means to (a) receive session data requests from access points, the session data including a session key associated with each wireless client and an associated access point, (b) look up session data, and (c) send session data back to the requesting access points, the access points having means to send requests for session data from the gateway and means to receive session information setting commands from the gateway.

2. The system of claim 1 wherein each access point has means to maintain a session key per associated client.

3. The system of claim 1 wherein the gateway has means to remove session information after a wireless client becomes disassociated with an access point comprising sending a command to the access point to remove the session information and/or to remove idle wireless client entires after a predetermined period of inactivity.

4. The system of claim 1 having means to ensure that a connection between the gateway and an access point is trusted.

5. The system of claim 4 wherein the means comprises physical security or encryption.

6. A method of enabling roaming of wireless clients among wireless access points in a network comprising the steps of (a) providing a gateway in the network, sending session data requests from access points to the gateway, the session data including a session key associated with each wireless client and an associated access point, (b) looking up session data stored in the gateway, reporting session data failure if session data is not found, and (c) sending a session data response from the gateway to the access point if session data is found or is generated by the gateway.

7. The method of claim 6 wherein an association request from a wireless station is received by an access point and, after receiving a session data response from the gateway, the access point loads session data and sends the session data to the wireless client.

8. The method of claim 6 wherein an association request from a wireless client is received by an access point and, after receiving a session data failure response from the gateway, the access point generates session data, reports the generated session data to the gateway and sends an association response to the wireless client.

9. The method of claim 6 comprising removing session information from the previously associated access point after a wireless client becomes associated with a new access point comprising the gateway sending a command to the prevoiusly associated access point to remove the session information or automatically removing idle wireless client entries after a predetermined period of inactivity.

10. The method of claim 6 wherein the gateway authenticates an access point to ensure that a connection between the gateway and the access point is trusted.

11. The method of claim 10 wherein the authentication is encrypted.

12. A computer readable medium containing instructions that, when executed by a processor in a gateway in a wired network which comprises access points, performs the steps of (a) receiving session data requests from access points to the gateway, the session data including a session key associated with each wireless client and an associated access point, (b) looking up session data stored in the gateway, reporting session data failure if session data is not found, and (c) sending a session data response from the gateway to the access point if session data is found or is generated by the gateway.

13. A computer readable medium comprising instructions that, when executed by a processor in a wireless access point in a network, performs the steps of receiving an association request from a wireless client and, after receiving a session data response from a gateway, loads session data and sends the session data to the wireless station, the session data including a session key associated with each wireless client and an associated access point.

14. The computer readable medium of claim 13 wherein after receiving a session data failure response from the gateway, performs the steps of generating session data, reporting the generated session data to the gateway nad sending an association response to the wireless station.

15. The computer readable medium of claim 13 which performs the steps of removing session information from a previously associated access point after a wireless client becomes associated with a new access point, sending a command to the previously associated access point to remove the session information or automatically removing idle wireless client entries after a predetermined period of inactivity.

16. The computer readable medium of claim 13, which performs the steps of authenticating an acess point to ensure that a connection between the gateway and the access point is trusted.

17. The computer readable medium of claim 16 wherein the authentication is encrypted.

FIG. 1

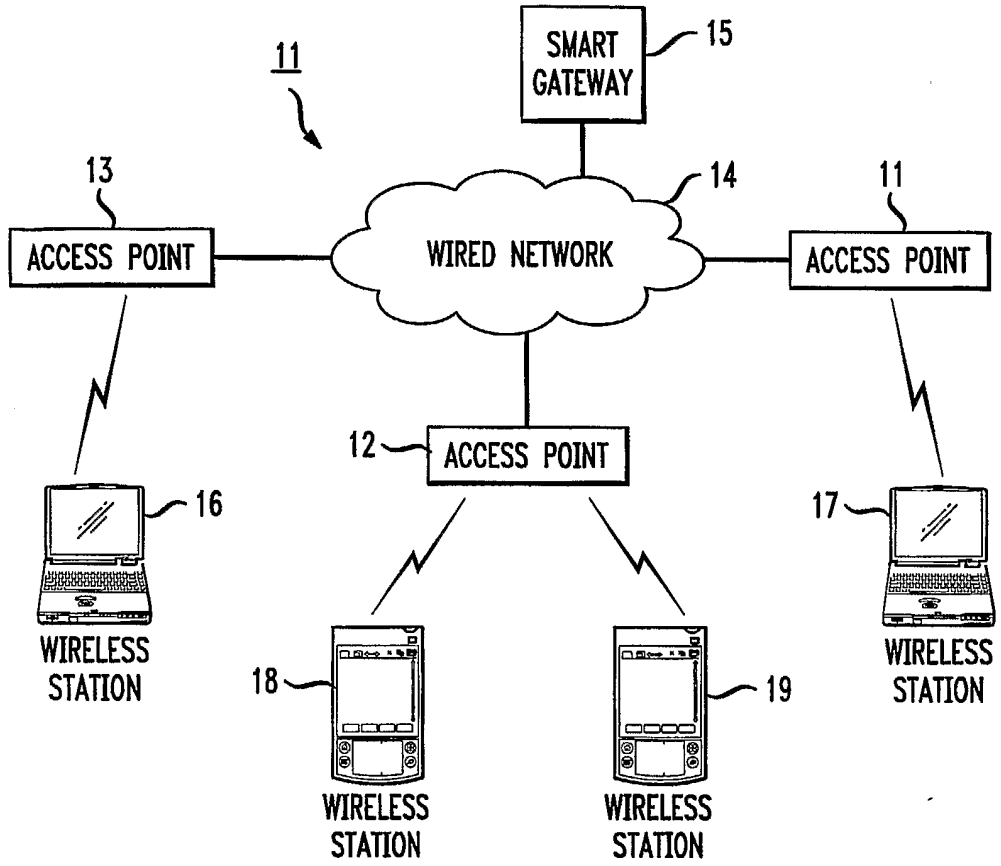

11
SMART GATEWAY
15
13
14
11
ACCESS POINT
WIRED NETWORK
ACCESS POINT
12
ACCESS POINT
16
17
WIRELESS STATION
18
19
WIRELESS STATION
WIRELESS STATION
WIRELESS STATION

FIG. 2

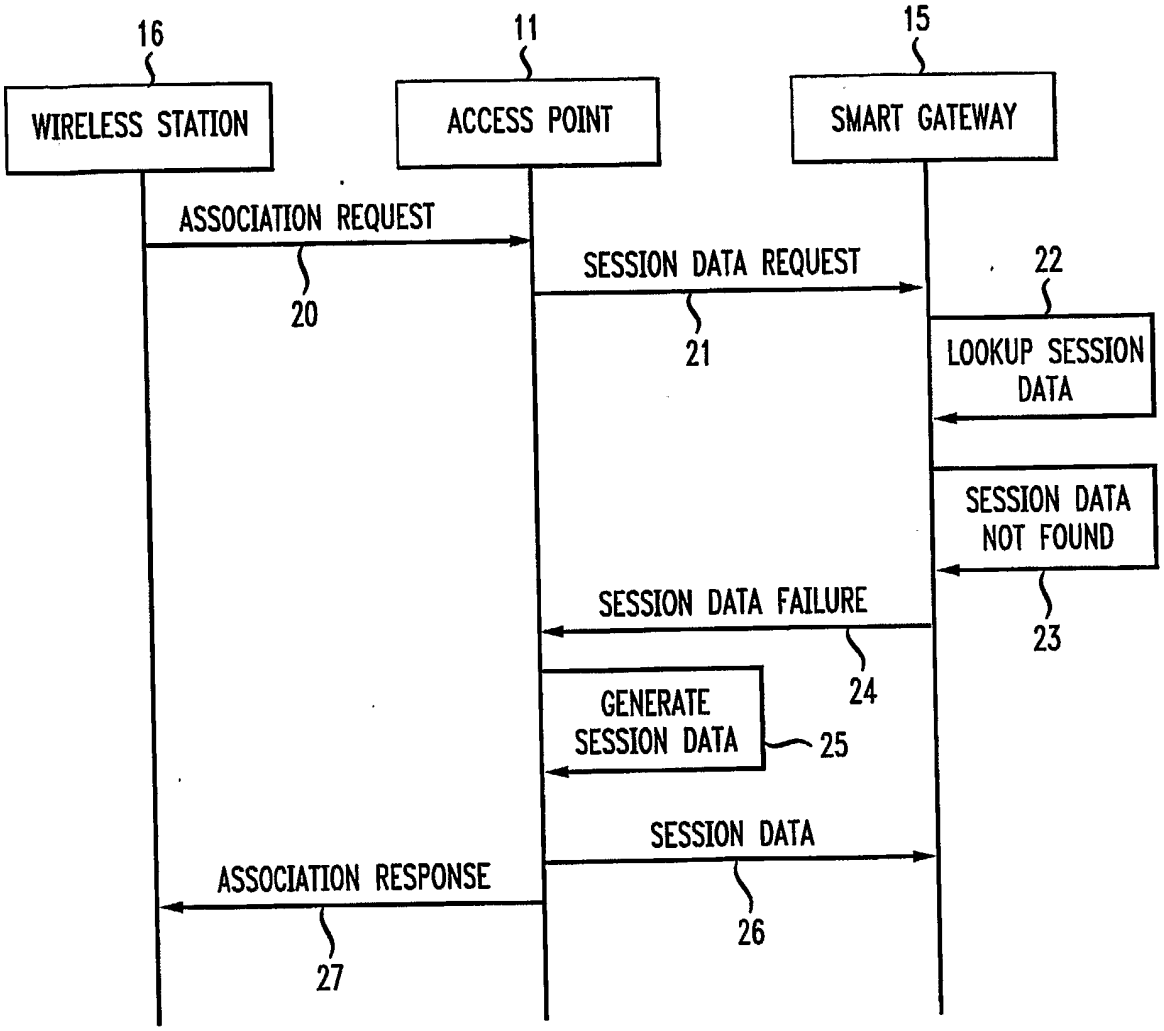

16
11
15
WIRELESS STATION
ACCESS POINT
SMART GATEWAY
ASSOCIATION REQUEST
20
SESSION DATA REQUEST
21
22
LOOKUP SESSION DATA
SESSION DATA NOT FOUND
23
SESSION DATA FAILURE
24
GENERATE SESSION DATA
25
SESSION DATA
26
ASSOCIATION RESPONSE
27

FIG. 3

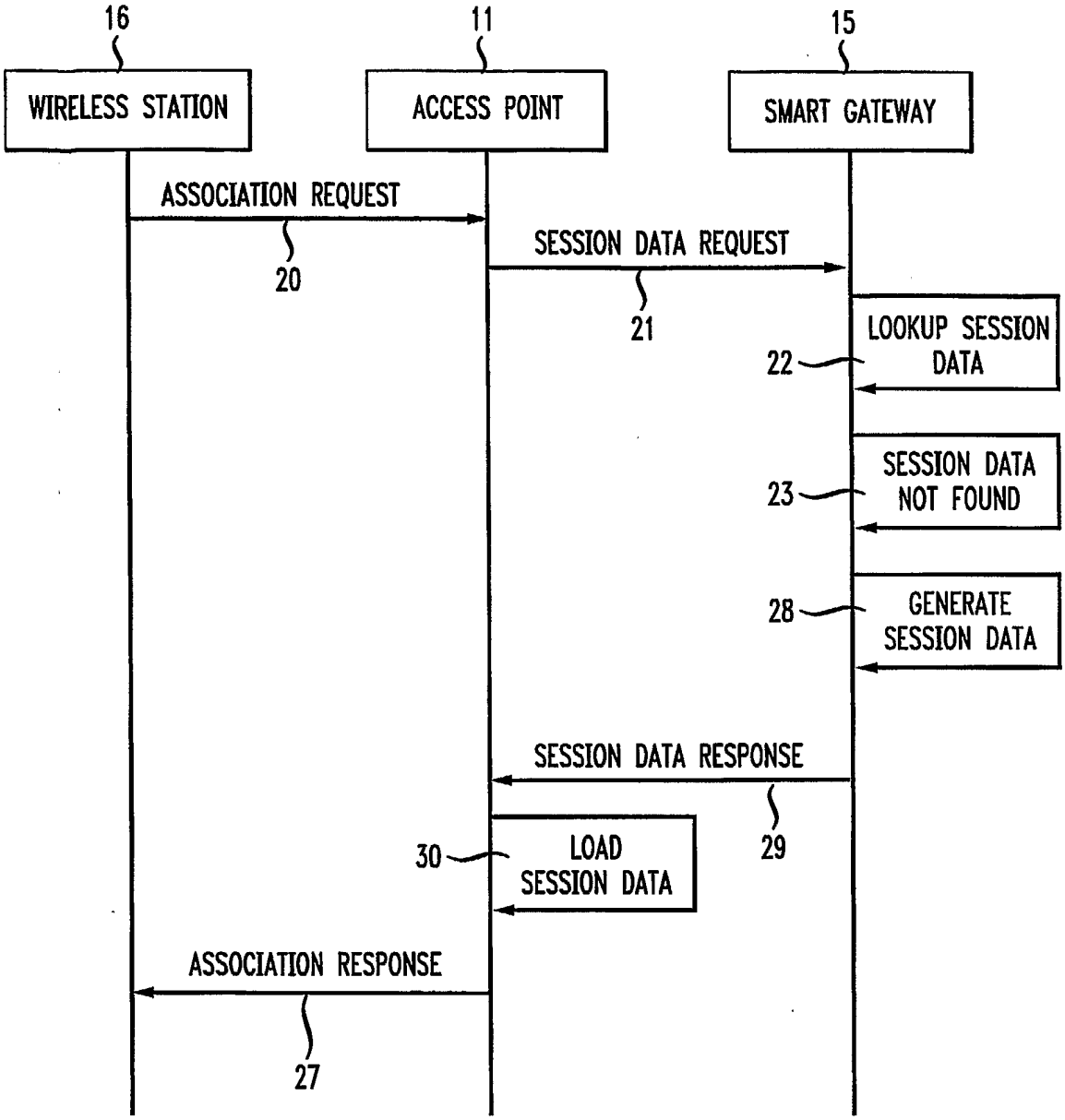
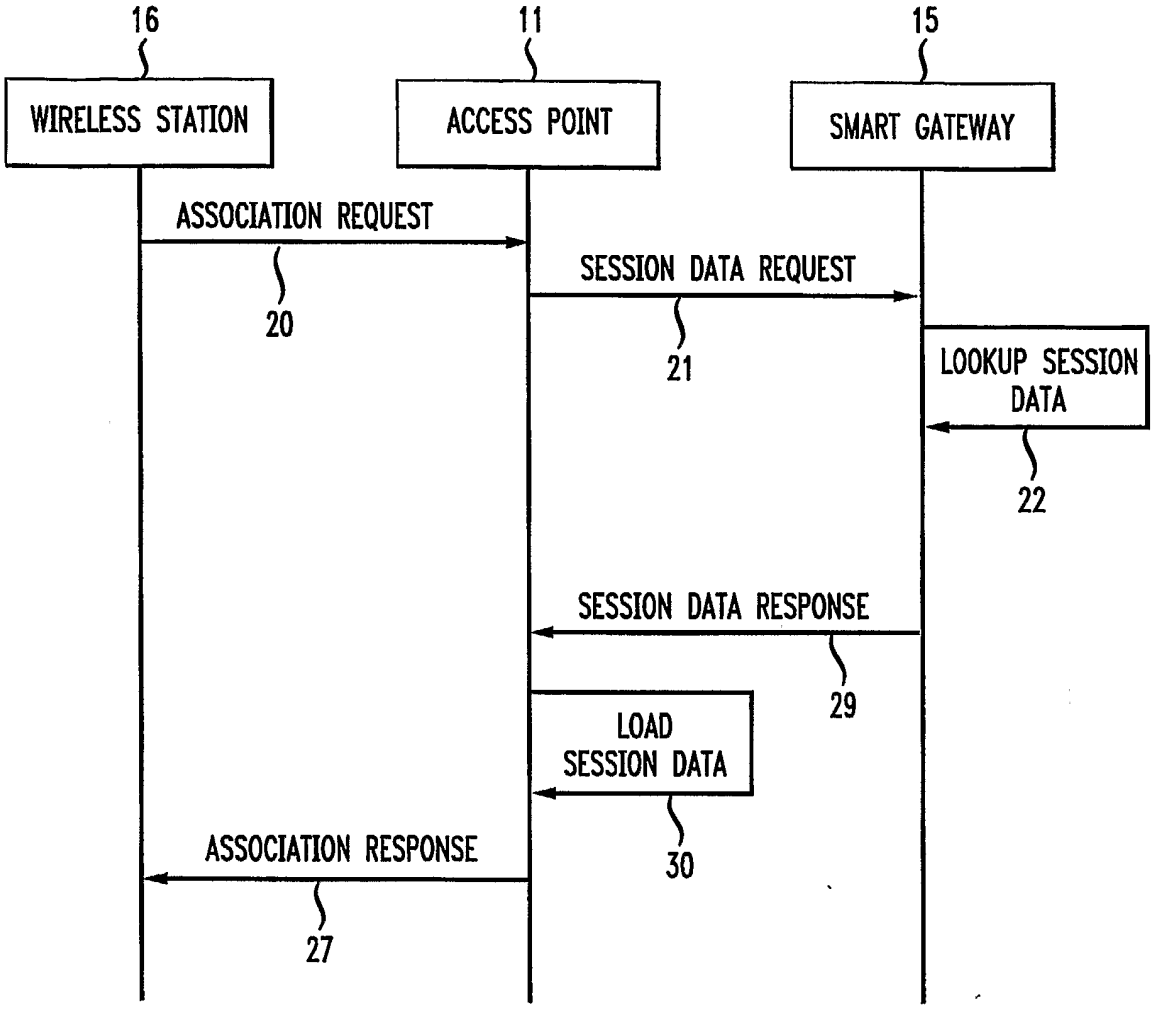

16
11
15
WIRELESS STATION
ACCESS POINT
SMART GATEWAY
ASSOCIATION REQUEST
20
SESSION DATA REQUEST
21
LOOKUP SESSION DATA
22
SESSION DATA NOT FOUND
23
GENERATE SESSION DATA
28
SESSION DATA RESPONSE
29
LOAD SESSION DATA
30
ASSOCIATION RESPONSE
27

FIG. 4


16
11
15
WIRELESS STATION
ACCESS POINT
SMART GATEWAY
ASSOCIATION REQUEST
20
SESSION DATA REQUEST
21
LOOKUP SESSION DATA
22
SESSION DATA RESPONSE
29
LOAD SESSION DATA
30
ASSOCIATION RESPONSE
27

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/02491

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04Q 7/24
US CL : 370/338

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 370/338, 455/432.1-433, 436-443, 445-449, 456.1-456.6

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0191572 A1 (WEINSTEIN et al) 19 December 2002 (19.12.2002), paragraphs [0017-0021], [0050-0055], [0068-0077], [0085-0090], [0094-0098], [0107-0113].	1-2, 4-5, 13, 16-17
A	US 2001/0024953 A1 (BALOGH) 27 September 2001 (27.09.2001). See pages 2-4	1, 13
X	US 2002/0085719 A1 (CROSBIE) 04 July 2002 (04.07.2002), paragraphs [0013], [0016-0021], [0034-0044], [0066-0069]	1, 13
A, P	US 2003/0142641 A1 (SUMMER et al) 31 July 2003 (31.07.2003), pages 3-5.	1-17

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
01 July 2004 (01.07.2004)	04 AUG 2004
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Chi Pham Telephone No. (703) 305-4700

Form PCT/ISA/210 (second sheet) (July 1998)