

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
2 August 2007 (02.08.2007)

PCT

(10) International Publication Number
WO 2007/086705 A1

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

(21) International Application Number:
PCT/KR2007/000477

(22) International Filing Date: 26 January 2007 (26.01.2007)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:

60/763,031	27 January 2006 (27.01.2006)	US
60/764,458	1 February 2006 (01.02.2006)	US
60/765,471	3 February 2006 (03.02.2006)	US
60/771,225	7 February 2006 (07.02.2006)	US
60/772,474	10 February 2006 (10.02.2006)	US
60/774,252	15 February 2006 (15.02.2006)	US
60/774,284	16 February 2006 (16.02.2006)	US
60/779,755	6 March 2006 (06.03.2006)	US

(71) Applicant (for all designated States except US): **LG ELECTRONIC INC.** [KR/KR]; 20, Yoido-dong, Yong-dungpo-gu, Seoul 150-721 (KR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **YUN, Chan Phill** [KR/KR]; 404, 63-13, Juam-dong, Gwacheon-si, Gyeonggi-do 427-070 (KR). **RYU, Seung Hyup** [KR/KR]; Eulji Apt. 621-2502, Gwangjeong-dong, Gunpo-si, Gyeonggi-do 435-707 (KR). **YANG, Sook Hyun** [KR/KR]; Lemeilleur Gangnam2officetel 1211, 1061-18, Namhyeon-dong, Gwanak-gu, Seoul 151-080 (KR).

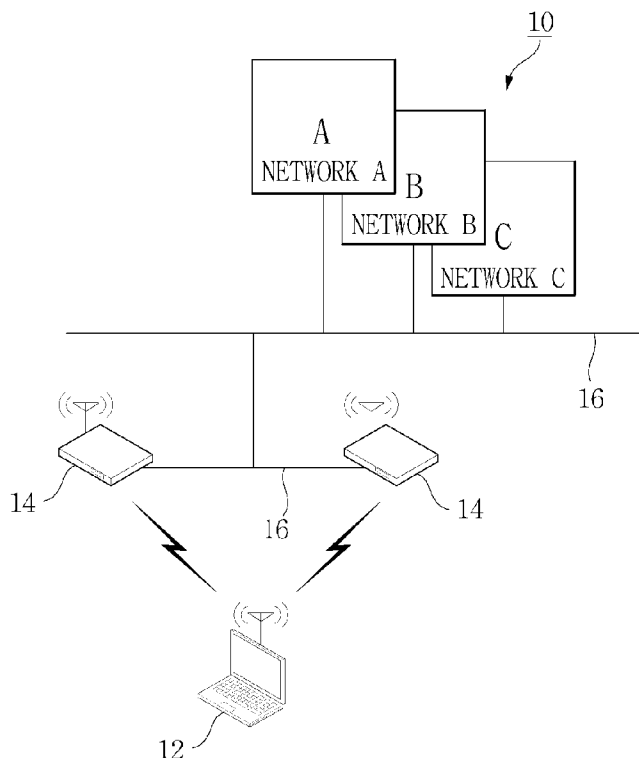
(74) Agent: **LEE, Soo Woong**; Baeklim Bldg. 101, 823-33, Yeoksam-dong, Gangnam-gu, Seoul 135-933 (KR).

(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, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) Title: COMMUNICATION METHOD FOR WIRELESS NETWORK AND WIRELESS NETWORK SYSTEM

(57) Abstract: The present invention relates to communication method for wireless network and wireless network system which transfer the information of service provider and protect MAC address.



WO 2007/086705 A1



(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).

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.

Published:

— *with international search report*

Description

COMMUNICATION METHOD FOR WIRELESS NETWORK AND WIRELESS NETWORK SYSTEM

Technical Field

- [1] The present invention relates to a communication method for a wireless network and a wireless network system which transfer the information of service providers and protect a MAC address.

Background Art

- [2] There are a lot of cases which need the information of service providers for a mobile terminal. There are a lot of method which acquire the information of service providers for the mobile terminal.
- [3] The wireless network also uses a MAC address for its communication. There need an more efficient usage of this MAC address.

Disclosure of Invention

Technical Solution

- [4] To one aspect, disclosed is a communication method its related method in wireless network comprising: processing an information of a service provider list using a specific function or algorithm, and transmitting a data comprising all or part of the processed information by a access point; and receiving the transmitted data from the access point, and processing the received data to decode the original information of the service provider list.
- [5] To another aspect, disclosed is a communication method and its related method in a wireless network comprising; transmitting the data comprising a request for a MAC address by a station; receiving the data comprising the request for the MAC address and transmitting to the station the other data comprising a random MAC address in accordance with the request for the MAC address by a access point; and transmitting a data comprising a real MAC address by the station.

Brief Description of the Drawings

- [6] FIGs. 1 to 3 are schematic diagrams of wireless network systems according to the embodiments of the present invention.
- [7] FIG. 4 is a flow chart illustrating connection procedure for the data transmission in wireless LAN system of FIG. 3.
- [8] FIG. 5 is a flow chart of the communication method in the wireless network according to another embodiment of the present invention.
- [9] FIG. 6 is a flow chart of the communication method in the wireless network according to further embodiment of the present invention.

Mode for the Invention

[10] Hereinafter, embodiments of the present invention will be described in detail with reference to the accompanying drawings.

[11] These embodiments of the present invention describe the wireless LAN system among wireless network systems by way of example. These embodiments of the present invention are equally or substantially equally applied to various available or permitted wireless network system aside from the wireless LAN system.

[12] In addition, terms and words used in embodiments of the present invention may be used with other terms and words in various wireless network systems. The present invention may comprise various wireless network systems with equivalence or similarity of the following embodiments in spite of a difference of terms and words.

[13]

[14] Wireless Network System

[15] FIGs. 1 to 3 are schematic diagrams of the wireless network systems according to the embodiments of the present invention. The same elements or components of FIGs. 1 to 3 use the same reference numbers respectively.

[16] Referring to FIG.3, the wireless network system, for example, a wireless LAN(10) comprises a plurality of stations or terminals(12), an access point or wireless base station, or a backbone network or distribution system (16).

[17] A plurality of stations or terminals(12) are equipped with a Network Interface Card for the wireless LAN and perform an operation of physical layer and MAC layer based on an IEEE 802.11 standard. A plurality of stations(12) are connected with the access point(14) on air and exchange the data frame in the wireless network as shown in FIG.1.

[18] The access point(14) functions as a wire or wireless bridge which can relay the data frame from one station to other. The access point has the same function as the bridge or the switch of Ethernet.

[19] In addition, because the access point(14) has the same physical layer and MAC layer as the above-described station(12), the access point(14) basically performs the same operation as the station(12). Therefore, it may be considered that the access point(14) is equal to the station(12) case by case.

[20] The distribution system(16) is a backbone network to connect a plurality of the access points(14). The ethernet may be generally used as the distribution system(16) and a plurality of various access points(14) are connected with each other, which is called a wireless distribution system. Broadly speaking, it is possible for the distribution system(16) to comprise a router or a switch connected with ethernet, or a plurality of servers connected with a wire or wireless internet network.

- [21] Referring to FIG.2, the wireless network system, for example, the wireless LAN(10), comprises a plurality of stations or terminals(12). In the wireless LAN(10), the plurality of stations(12) are directly connected with each other. Therefore, there may be no the extra access point(14) and the distribution system(16) in the wireless LAN(10) as shown in FIG.2 aside from FIG.1. The plurality of stations(12) may be substituted for access point(14) and the distribution system(16) as shown in FIG. 1. There may be omitted some of their functions in the wireless LAN(10) as shown in FIG.2.
- [22] The wireless LAN is described above referring to FIG.2, but the wireless network comprising the wireless LAN(10) according to the embodiment of the present invention is not limited thereon. The wireless network according to the embodiment of the present invention may be implemented by their combination or complete different systems. The wireless network according to the embodiment of the present invention not only exists by itself, but also interworks with an other wireless network system, a mobile communication network or wired/wireless internet network and so on.
- [23] For example, the wireless LAN system interworks with another disparate mobile communication network such as WCDMA(Wideband Code Division Multiple Access), which provides the roaming service for the terminal. In case the wireless LAN provides the voice service for the terminal for which both the wireless LAN and WCDMA is supported, the terminal makes a phone call using the WCDMA and automatically performs a seamless roaming operation with the wireless LAN in the area which is supported by the wireless LAN.
- [24] Not only the wireless LAN as shown in FIG.1 but also the wireless LAN as shown in FIG.2 need to associate the station(12) with the access point(14) or one station with other in order to exchange the data.
- [25] Referring to FIG. 3, the wireless network system, for example, the wireless LAN(10) equal to the wireless network system as shown in FIG.1 comprises a plurality of stations(12), the access point(14) and the distribution system(16). This wireless network system is connected to the wireless networks different from each other, for example, three wireless network(Network A, B, C). For example, these three wireless network(Network A, B, C) may be Subscription Service Provider Networks(SSPNs) different from each other. In other words, one of them may be a commercial network in which a RADIUS server was comprised, other of them may be web-based authentication network, and another of them may be VOIP(Voice Over IP) network.
- [26] Therefore, a user or subscriber can use the networks(Network A, B, C) different from each other through only one access point(14) with one station(14).

[27]

[28] Connection Procedure

- [29] FIG. 4 is a flow chart illustrating connection procedure for the data transmission in the wireless LAN system of FIG.3. The wireless network systems of FIG.1 and FIG.2 and the above described various wireless network systems comprise the same or substantially same connection procedure as shown in FIG.4 in order to transmit the data. The more detailed explanation is abbreviated.
- [30] Referring to FIGs. 3 and 4, the connection procedure(20) for transmitting the data between the station(12) and the access point(14) comprises a scanning(S10), an authentication(S12) and an association(S14). Both the station(12) and the access point(14) apply to the data transmission(S16) via the above procedure.
- [31] The scanning(S10) is a process to find or identify the access point(14) around using beacon or probe message.
- [32] The scanning(S10) comprises the passive scanning and the active scanning procedure. In the passive scanning procedure, the station(12) finds the access point(14) receiving the beacon message which the access point(14) broadcast periodically. In the active scanning procedure, the station(12) broadcasts the probe request message or frame for each channel and receives the probe response message or frame which reports their network parameter such as SSID(Service Set ID) and supported rates. Therefore the station(12) finds the access point(14) in the area.
- [33] The beacon, the probe request and the probe response comprise the MAC header and the frame body respectively. For example, the MAC header and/or the frame body for the beacon message contains various capability information such as supported rates or encoding of the access point(14) and so on, and SSID(Service Set ID) which the access point belongs to.
- [34] The frame body of the beacon, the probe request or the probe response may contain any Action Management frame or Information Element(IE) so as to take any specific action or operation, or exchange some information.
- [35] The authentication(S12) is the process that the station(12) establishes its identity to the appropriate(right) access point(14) which the station(12) attaches to in the scanning(S10). In other words, the authentication(S12) is the process that the station(12) negotiates the validation and the encryption with the access point(14). Because most of the stations(12) perform Open-system authentication, the access point(14) accepts the station(12) at face value without verifying its identity. There are IEEE 802.1x based EAP-TLS, EAP-TTLS, EAP-FAST or PEAP and the like to bolster the authentication method.
- [36] The association(S14) is the process which the station(12) associates with the access point(14) to obtain full access to the wireless network(10), after the authentication has completed. After the association(14) completes, the access point(14) registers the station(12) on the wireless network(10) so frames for the station(12) are delivered to

the access point(14). After the association(14) is completed, one station(12) may communicate with other station(12) through the access point(14).

[37] In the authentication(S14), the station(12) sends an association request message or frame to the access point(14). The received access point(14) sends an association response message or frame which contains AID(association ID) to logically identify an other station.

[38] The station(12) and the access point(14) perform the data transmission(S16) via the above procedures(S10, S12, S14).

[39] A reassociation is almost the same as the association(S14). The reassociation is the process of changing an association from an old access point to a new one. The station(12) monitors the quality of the signal it receives from the old access point. When the quality of the signal is weaken, the station(12) initiates the reassociation with an other access point.

[40]

[41] Network selection

[42] The station(12) may obtain access to the disparate networks through a single access point(14) as described above, referring to FIG.3.

[43] To one aspect, the invention allows any number of SSPNs(Subscription Service Provider Networks) to be supported through a single access point. The invention specifies additional Information Elements(IEs) used in the beacon, the probe request and the probe response messages in order to provide information required by the station(12) as part of its network selection before the association(S14).

[44] According to one of methods which allow any number of SSPNs to be supported through a single access point, if the station(12) has credentials for a number of different realms, then it may send multiple probe request messages, each of which queries something about each of the realms.

[45] Although the above-described domain, realm or service provider network(SSPN) are mentioned differently from each other in this specification, but it may be understood that they have the same or almost the same meaning or the related words or terms. On the other hand, although the service provider may be described as realm string, NAI(Network Access Identifier), roaming ID, SSPN ID, service provider ID, or ESSID and so on, but it may be understood that they have the same or almost the same meaning, or the related words or terms to be modified by the ordinary person in this art in this specification. They may be broadly described as service provider information, SSPN information or realm information in this specification.

[46] As an alternative, multiple NAIs(Network Access Identifiers) could be included in a single probe request and in the probe response. however, this could lead to un-reasonably large probe messages.

- [47] Additional realm information could be made available in the probe response or the beacon, as part of the method described above.
- [48] Since, as previously described, the full realm strings may be quite long, a hash of the string instead of the full realm string may be used.
- [49] The need to reduce the amount of information in the messages particularly in the case of broadcast messages such as beacons creates a desire to use shorter hashes. Hash collisions (where two realms hash to the same value) are more likely to occur when shorter hashes are used. The effect of hash collisions is that the station(12) may believe a realm to be supported, when in fact the access point(14) does not support it but does support a different realm that is hashed to the same value.
- [50] In this case, the station(12) may attempt to perform the authentication using credentials for the realm it mistakenly believes to be supported, but the authentication will fail. It is, however, desirable to reduce the probability of such collisions where possible by using longer hashes.
- [51]
- [52] Adaptive hash
- [53] There may be a scheme using an adaptive hashing as one of schemes using hashing of realm strings.
- [54] Therefore, an adaptive hashing scheme is used, to allow the access point(14) to use a number of different hash lengths. The length of hash chosen might depend on the number of realms being advertised, or how busy the network is particularly in the case of beacons.
- [55] This scheme may manage all SSPN information which have roaming agreements in the Access Network(AN). As NAI of SSPN in this scheme gets longer, part of NAI of SSPN is hashed and the hashed result is contained in the beacon.
- [56] The Access network(AN) is commonly called as BSS(Basic Service Set) or ESS(Extended Service Set) and is a set of access points which a specific service provider manages. When the specific service provider supports the roaming service, the access points which belong to the AN include the information of service providers or SSPN.
- [57] The AN may be described as a single access point or a set of access points which a specific service provider manages in this specification. The access point is used in case of some action or operation, or the subject for the network. The AN or Access Network is used in case of management for the network in this specification.
- [58] When the information of SSPN accessible to the station(12), for example, the list of SSPN ID, is included in the hashed list, the station(12) sends the probe request to the access point(14) so as to gain the credential or the service information.
- [59] When the information of SSPN which the station would like to obtain access to is

not included in the hashed list, the station(12) doesn't send the probe request so that the station(12) determines by itself that it can not be served from the AN.

[60] Even if the information of SSPN which the station(12) would like to obtain access to may be included in the hashed list, it may not make a roaming agreement with the AN due to the characteristic of the hash(hash collision). The length of the hashed list used in the beacon will be set to 1-4 octets and is indicated into the beacon frame so as to reduce the hash collision.

[61] In addition, when the complete set of the hashed list is not included in one beacon, an other unadvertised SSPN available' bit or an 'unadv' bit are setup in the beacon to give notice of what there is the information of the SSPN not included into the beacon.

[62] In cases where the complete set of hashed list(realms) for the information of SSPN cannot be included in the message such as the beacon, an other unadvertised SSPNs available indicator is included in the message.

[63] In detail, a new Hashed Realms List IE is added, which can be used optionally in beacons and probe response messages.

[64] Table 1

Element ID	Length (octets)	Flags (1 octet)	Information (length)
TBD	1-?	Flags	Sequence of Hashed Realms

[65] The Element ID and the Length indicate the ID and the length of information element(IE). The Flags field indicates the Hashed Length as described in the table 2, etc. The final Information field includes the sequence of the hashed realms.

[66] Table 2

B0	B1	B2	B3	B4	B5	B6	B7	B8
Hash Length	Unadv	Reserved						

[67] As described in the table 2, initially, three flag bits are defined in the Flags field: Bits B0 and B1 indicate the hash length that is being used(00 = 1 octet, 01 = 2 octets, 10 = 3 octets, 11 = 4 octets). B2 indicates whether additional realms are available that are not included in the list of hashed realms in this IE.

[68] The reason to give notice of the SSPN list through the beacon is that the stations(12) wishing to connect to SSPN unavailable for the roaming prevent the unnecessary probe request from sending.

[69] When the B2 of the Flags field in the table 2 is set to 'Unadv' bit, the station(12)

determines that the access point(14) may provide the SSPN wishing to be connected for the station(12), although the hashed value of SSPN wishing to be connected is not included in the hashed list. In this case, as all stations(12) send the probe request, the meaning to send the beacon comes to disappear. Therefore, when the beacon is sent, a list of all SSPN which support the roaming services in the AN(or AP) must be sent.

[70] As the hashed list becomes longer in this case, so there increases the possibility that the station(12) which is not supported in AN sends the probe request due to the hash collision.

[71]

[72] Hashed list diversity

[73] A method for selecting a network according to another embodiment of the present invention relates not to send all the same beacon in which the hashed roaming list is included, but to send the beacon or the probe response frame including the different hashed roaming list which is generated from the hash function with the different hash key value. Therefore, this method supports the diverse beacon.

[74] A new Hashed Realms List IE is added, which can be used optionally in beacons and probe response messages as shown in the table 3.

[75] Table 3

ID	Length (bytes)	Hash Length(1b)	Hash key	Hashed list
----	-------------------	--------------------	----------	----------------

[76] The Element ID and the Length indicate the ID and the length of information element(IE). The Hash length(1b) indicates the length of the result value hashed by the hash function. The Hash key indicates the hash key value used for the diversity of the hashed result. The Hashed list is the hashed result of the roaming list hashed by the hash function.

[77] As this occurs, the station(12) can receive the different hashed lists from the plurality of the access point(14) as shown in FIG.3. The station(12) can finally get the correct roaming list through the information from the plurality of the beacons such as the different hashed lists from the plurality of the access point(14).

[78]

[79] Hashed list truncation

[80] A method for selecting a network according to another embodiment of the present invention relates to what the truncated locations of the hashed result value are different, even if every access point(14) uses the same hash key for the hash function.

[81] For example, when the length of the hashed result value is 4bytes and the length of the hashed information wishing to send is 1byte, the first access point(AP1) sends the first 1byte among the 4bytes hashed result value and the second(AP2) sends the second

1byte among them, so that each of the access points sends the hashed lists different from each other. Therefore, while each of the access points(14) don't send the hash key different from each other, each of the access points(14) can send the different hashed list, without the complexity of the computation.

[82] A new Hashed Realms List IE is added, which can be used optionally in beacons and probe response messages as shown in the table 4.

[83] Table 4

ID		Length (bytes)	Hash Length (1b)		Hashed list		
B0	B1	B2	B3	B4	B5	B6	B7
Hash Length		Truncation Position		Un-adv	Reserved		

[84] Bits B0 and B1 in the Hash length field indicate the hash length that is being used: 00 = 1 octet, 01 = 2 octets, 10 = 3 octets, 11 = 4 octets. Bits B2 and B3 in the Hash length field indicate the location of the truncation.

[85] B4 in the Hash length field indicates whether additional realms are available that are not included in the list of hashed realms in this IE.

[86]

[87] Providing service provider ID no supported using NAK

[88] A method for selecting a network according to another embodiment of the present invention relates to transmit the list of the service provider ID which is frequently requested, but is not supported.

[89] In other words, if many stations(12) in the AN frequently broadcasts the probe request including the information of SSPN such as the service provider IDs without the roaming agreement, it leads to waste resources of the network.

[90] The AN manages the frequency of the service provider ID to which the stations(14) request the connection. The access points(14) belonging to the AN use this information such as the frequency of the requested service provider ID. The AN can give notice of the list of the service provider ID which is frequently requested, but is not supported through the beacon or the probe request as shown in the table 5. The stations(12) don't request the connection to the service provider ID.

[91] Table 5

ID	Length	Unsupported service provider ID list
----	--------	--------------------------------------

[92] Referring to the table 5, the Element ID and the Length indicate the ID and the length of information element(IE). The Unsupported service provider ID list indicates the list of the service provider ID which is frequently requested, but is not supported.

[93]

[94] Grouping of information

[95] A method for selecting a network according to another embodiment of the present invention relates to what after the information is grouped and then sent, the grouped information element is combined to be an original information.

[96] An information element including the total number of the grouped frames and the current number of a particular frames is included in the beacon, the probe request or the probe response and the like to be sent, as shown in the table 6. That combines the previous information with the present to make one information.

[97] Table 6

ID	Length	Total #	Current #
----	--------	---------	-----------

[98] Referring to the table 6, the Element ID and the Length indicate the ID and the length of information element(IE). The total number(Total #) indicates the total number of the grouped frame such as the beacon. The current number(Current #) indicates the turn of the particular grouped frame such as the beacon.

[99] The grouping of the IE information may apply to the probe request or the probe response. It is possible to combine the information received from the access points(14) different from each other inside the same ESS.

[100]

[101] Type field

[102] A method for selecting a network according to another embodiment of the present invention relates to what receives the type indicating the service domain and whether it supports roaming to confirm the accessibility to the network.

[103] We can remove to transmit a heavy beacon or probe response frame containing the hashed realm list by classifying 802.11 AN based on the policy of 802.11 AN.

[104] Table 7

Element ID	Length	Type (1 octet)	Information
TBD		Type	Additional subfield

[105] It can be classified based on two parameters: service domain and support of roaming as shown in the table 7. These 802.11 AN classification parameters are able to add newly using reserved bits at Type subfield. The first parameter, service domain, is distributed into "0(local)" and "1(global)". Local means that the station(12) cannot connect to servers at the other network domain and only get local domain network services. On the contrary, the station(12) is able to communicate with any correspondent nodes wherever correspondent nodes locate.

[106] The second parameter indicates whether the roaming is supported or not.

[107] Additional subfield is used to advertise which SSPNs can support to access 802.11AN.

[108] The table 8 indicates the service domain, the support of roaming and the combination of the additional subfields.

[109] Table 8

	Service domain	Supporting roaming or not	Additional subfield
1	0 (Local)	0 (not supporting)	Local domain's realm
2	0 (Local)	1 (supporting)	N/A
3	1 (Global)	0 (not supporting)	Local domain's realm
4	1 (Global)	1 (supporting)	Supported realm list

[110] The case 1 and 3 show only the local domain realm in the additional subfield. Because the case 1 is limited to the "Local" service domain and the case 3 doesn't support other SSPNs and roaming. The case 4 may be not existed, and the case 4 includes the supporting roaming lists in the additional subfield in case of supporting other SSPNs and roaming. The additional subfield may include several hashed roaming list as described above, and may include the not-hashed roaming list.

[111] These two bits or more are able to decrease sending the unnecessary probe request/response because the station(12) does not try to confirm whether or not SSPNs can supply access to 802.11 AN.

[112] If the station(12) locates Case 1, Case 2, Case 3 network, the station(12) only receives the beacon frame and knows whether the station(12) can obtain access to that 802.11 AN through two bits and additional subfield.

[113]

[114] Service provider grouping

[115] A method for selecting a network according to another embodiment of the present invention relates to what transmits the grouping information of the roaming service provider.

[116] As service providers share 802.11 AN by using virtual AP, service providers may have a lot of roaming agreement, and these roamed service providers may form a group with a globally unique name for business. The good example for grouping of service providers is an airline alliance: SkyTeam alliance, Star alliance, Oneworld alliance, etc.

[117] For reducing load of the beacon with heavy hashed realm list, the beacon frame or the probe request can include Service provider Group of unique name instead of realm list.

[118] Table 9

Element ID	Length	Flags	Information
TBD			Service Provider Group ID

- [119] Referring to the table 9, the Element ID and the Length indicate the ID and the length of Information Element(IE).
- [120] If a service provider makes the roaming agreement with the other service provider which does not belongs to any groups, the first bit of flags is set "1".
- [121] When a service provider is a member of several service provider groups, subfield information should consist of sequence of group IDs.
- [122]
- [123] Non-loss compression
- [124] The passive and the active method may be used to give notice of the list of SSPNs provided by the access point(14) to the station(12). The passive method is that the station(12) receives the beacon periodically sent by the access point(14), and knows the list of SSPNs included in the beacon.
- [125] As described above, the active method is that the station(12) requests the service provider list to the access point(14) through the probe request, and the access point(14) sends the list of SSPNs to the station(12) through the probe response.
- [126] There can be a problem at the scalability to send the list in itself through the beacon or the probe response by means of indicating each service provider(SSPN), for example Realm, NAI, Roaming ID or ESSID, especially when there are a lot of the service provider(SSPN).
- [127] As described above, although there may be a method to reduce the size of the service provider list using the hash function, the hash function lead to a hash collision. In other words, even if the hash function is $H(x)$ and the inputs x_1 and x_2 are not equal, there may occur the same results $H(x_1)$ and $H(x_2)$ from the hash function.
- [128] A method for selecting a network according to another embodiment of the present invention relates to what uses not-loss compression and compaction of the service provider list.
- [129] The Information Element(IE) defined by the method for selecting a network according to another embodiment of the present invention may be applied to the beacon and the probe response. It may be applied to the action management frame by a similar method.
- [130] The commercial wireless LAN appliance includes the non-loss compression feature to compress the data without lowering its quality. The problem of the compression is what needs the decoding time to decompress the compressed data.
- [131] However, because the service provider list is requested in the network selection

step, the constraint to the decoding time for the station(12) is very low. Because the compression rate of most compression algorithms is high, the constraint to the decoding time for the station(12) is lower.

[132] The compaction simplifies the decoding process and have advantages to reduce the list size of SSPNs, compared to the compression.

[133] Each access point(14) has the following MIB(Management Information Base) value for the above method: Dot11CompressionThreshold, Dot11CompressionGainThreshold.

[134] "Dot11CompressionThreshold" is the integer in the unit byte(s). It may not compress the list of which the size is bigger than the "Dot11CompressionThreshold". "Dot11CompressionGainThreshold" is equal to or more than "0", and less than or equal to "1". If the compression efficiency, which is equal to "the size of the compressed list"/"the size of the original list", would be more than the "Dot11CompressionGainThreshold", the original list is compressed and sent.

[135] There are many type of compression algorithms that may be used. For example, the compression algorithms used may be non-loss compression algorithms including one of ITU-T V.42bis(LZW), ITU-T V.44(LZJH), ANSI X3.241(LZS).

[136] On the other hand, the present invention can use the new compaction process that is not used previously. The Information Element(IE) which is loaded in the beacon and the probe response may be defined as the table 10.

[137] Table 10

ID	Length	Compression Algorithm	Compressed SSPN list
----	--------	-----------------------	----------------------

[138] The ID as shown in the table 10 is allocated to Information Element ID(Information Element ID) based on IEEE 802.11. The Length indicates the total size(octets) of the IE. The Compression Algorithm indicates the not-loss compression algorithm that is used for the compression of the SSPN list. The list of compressed SSPN is the list compressed by the compression algorithm.

[139] After a list of compressed SSPN becomes a string, it is compressed and decoded. If $SSPN = \{SSPN1ID, SSPN2ID, \dots, SSPNnID\}$ ($SSPNkID = ID$ of the k^{th} SSPN), the string of the list of SSPN is generated using delimiter to divide each SSPN ID. A list of generated compression SSPN becomes $SSPN1ID + \{Delimiter\} + SSPN2ID + \{Delimiter\} + \dots + \{SSPNnID\}$. The delimiter may use the proper value according to the method to express the SSPN ID. If the SSPN ID expresses as NAI realm, there is used the special character(e.g. '_', '/') that is not used as NAI realm.

[140] For example, when the supporting SSPN realm is lge.com, lginnotek.com, the string of "lg.org, lge.com_lginnotek.com_lg.org" is composed and the compressed string

becomes the value of the list of SSPNs. When the station(12) decodes it, it looks for the delimiter and recognizes the SSPN realm.

[141]

[142] MAC address anonymity

[143] Stations(12) are required to use their actual MAC address for communication with the access point(14).

[144] Within the local network, the station(12) is not required to use its MAC address as identifier. At the ESS(Extended Service Set, the set of BSSs connected with each other through one backbone) level, the station(12) uses an arbitrary MAC address: EMID "ESS MAC Identifier". At the BSS(Basic Service Set, the set of station connected with each other) level, the station(12) uses an arbitrary MAC address: AMID "AP MAC Identifier".

[145] In other words, while each station(12) such as communication device uses one fixed MAC address, the above-described EMID and AMID instead of the fixed MAC address is dynamically allocated to supply MAC address anonymity.

[146] AMID is exposed into only BSS. Only AMID is shown for the transmitted packet on air. After the station(12) generates the trial AMID, the probe request including the generated AMID value is transmitted to the access point(14). If AMID is unique in BSS which the access point(14) composes of, the access point(14) can send the probe response to confirm the validation of AMID. Either the new EMID or the previous EMID is sent to the station(12).

[147] If AMID which the station(12) send is being used, the access point(14) does not reply anymore. EMID is ensured through 4-way handshake (defined by IEEE 802.11i) for RSN(Robust Security Network) later. As AMID and EMID have the lease time, they are expired after the lease time.

[148] According to this method, EMID should be allocated through the EMID server which is not existing previously.

[149] The above-described method to protect a MAC address such as EMID has the following problems basically. (1)As EMID is uniquely allocated in ESS, it is not necessary for AMID separately. (2) There needs the new architecture such as the EMID server. (3)The requirement to use the real MAC address for other organization such as 3GPP is not satisfied.

[150] 3GPP requests the use of real MAC address so as to define the number of connection according to the subscription of a user. The number of connection may be calculated as the number of MAC address used at the same time according to the specific subscription. Some problems from the above-described method may occur because of possibility of using the same EMID for other ESSs.

[151] The present invention provides the communication method for the wireless network

to solve the above-described problem.

[152]

[153] Dynamic address only for BSS

[154] MAC address anonymity makes an identity of the station(12) not presumed through the MAC address. The transmitted packet on air uses an arbitrary MAC address('Dynamic MAC address') which is dynamically allocated. Because it is not necessary to protect the MAC address of the access point(14), the access point(14) may use its real MAC address in itself.

[155] A method for selecting a network according to another embodiment of the present invention relates to what protects the real MAC address of the station(12) using the arbitrary MAC address and communicates between the access point(14) and the station(12).

[156] Referring to FIG.5, the station(12) transmits the data including the MAC address request such as the probe request('Dynamic MAC address request') to the access points(14). After then, the access points(14) receive the dynamic MAC address request from the station(12), and transmit other data including the arbitrary MAC address such as the probe response('dynamic MAC address request') to the station(12) in responsive to the MAC address request of the station(12).

[157] After the station(12) is connected with the access point(12), it transmit its real MAC address to the the access point(14) through the secure method. One action management frame can be considered as a method to support this. Or other management frame is newly defined for use. The method to securely transmit the frame(STA_Real_MAC_Address) including the real MAC address from the station(12) to the access point(14) is described as follows.

[158] The access point(14) sends Public key(pub) to the station(12). As an transmission method, the Information Element(IE) including the public key may be broadcasted by the beacon. Instead of sending a real MAC address for the station(12), the station(12) may send to the access point(14) encryption "c = encrypt (Real MAC Address, pub)" encrypted by the Public key(pub) which is sent by the access point(14). The Real MAC address in the action management frame becomes "c". The access point(14) decrypts the Real MAC address with the private key(priv).

[159] The action management frame in which the station(12) transmits the real MAC address to the access point(14) may be the following table 11.

[160] Table 11

Category	Action	STA Real MAC Address
----------	--------	----------------------

[161] The category in the table 11 indicates protection of MAC address. The reserved action value for the action field is newly defined and is used in the action field.

Another information field includes the real MAC address of the station(12).

[162] The access point(14) has a map between the real MAC address and the dynamic MAC address. The packet from/to the station(12) via the layer 2 access point(14) is routed using the real MAC address. When the access point(14) requests an authentication to the authentication server, it uses the securely transmitted real MAC address of the station(12).

[163]

[164] EMID management method allocating a MAC address block

[165] In case of EMID/AMID, since an EMID server manages all EMIDs in ESS, the EMID server needs to manage more MAC addresses according to the bigger region of ESS.

[166] For this reason, the EMID server does not manage all EMIDs in ESS, but the access point(14) locally manages all EMIDs in BSS. The EMID server allocates the range of EMIDs to the access point(14) in ESS. The access point(14) allocates some EMIDs among the allocated EMIDs from the EMID server to the station(12) which belongs to one's BSS.

[167] The EMID server can allocate the range of EMIDs to the access point(14) in ESS using the concept of subnet mask of IP(internet protocol). In this case, the routing for the layer 2 bridge level became to be easy. When the station(12) moves one ESS to other, the new access point(14) allocates the new EMID to the station(12). Without this restriction requirement, the new access point(14) ascertains whether it is possible to use the EMID which the station(12) requests to the old access point(14) and receives information on the lease time, if the station(12) requests that the new access point(14) wants to use the previously used EMID.

[168] This another embodiment defines APMEu and ESME as shown in FIG.6. APMEu, which is AP Management Entity for IEEE 802.11u, is the entity for AP management. ESME, which is ESS Server Management Entity, is the entity for ESS server management.

[169] APMEu sends MAC_address_range.request to ESME. When the access point(14) is connected to the ESS server through the ethernet, it can be transmitted by the IP packet. MAC_address_range.request may be defined as follows.

[170] MAC_address_range.request

[171] {

[172] Range_Size

[173] }

[174]

[175] The Range_Size indicates the size of MAC address block, which is interpreted as the same as the size of the subnet of IP address. If the Range_Size is n, the MAC

address block with the size of 2^n is requested. the detailed example of MAC_address_range.request is the same as follows.

[176] MAC_address_range.request

[177] {

[178] 4 // request of the MAC address block with the size of 2^n (=16).

[179] }

[180]

[181] The ESME allocates an EMID to the APMEu such as the access point(14) through MAC_address_range.confirm. The access point(14) allocates the EMID block which may be used in one's ESS. MAC_address_range.confirm is defined as follows.

[182] MAC_address_range.confirm

[183] {

[184] EMID_AP, // EMID which is allocated to AP.

[185] Range_Mask // the value equal to or less than the requested Range_Size. if it is allocated to zero, the allocation fails.

[186] }

[187]

[188] The detailed example of MAC_address_range.confirm is the same as follows.

[189] MAC_address_range.confirm

[190] {

[191] AB-CD-EF-00-11-CA,

[192] // Bit 47 = 0, Bit 46 = 1

[193] FF-FF-FF-FF-FF-C0

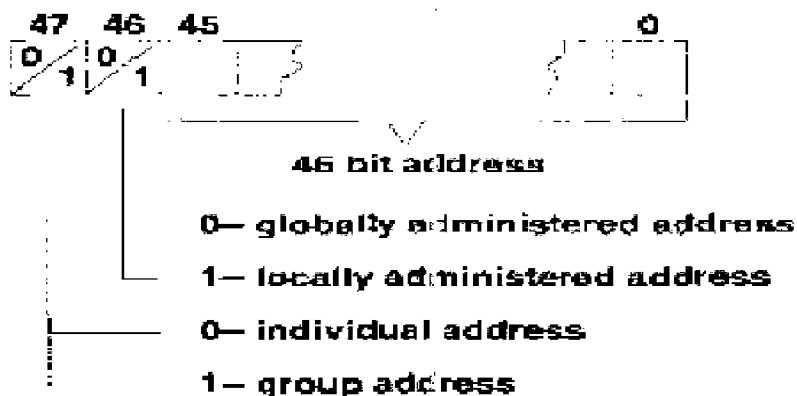
[194] // 4 bit range except for the last 2 bit is allocated. (C0h = 1100 0010b)

[195] }

[196]

[197] The table 12 is the definition of the MAC address. For example, Bit 47 and Bit 46 follows the definition of original MAC address for indicating that it is an individual & locally administered address.

[198] Table 12



[199]

[200] Distributed EMID block management method

[201] The communication method in wireless network according to another embodiment of the present invention may support the EMID function only by installing 802.11u AP.

[202] There needs a method to prevent an EMID conflict between a plurality of access points(14) for EMID management by a distributed method. This another embodiment provides this method to prevent the EMID conflict between them.

[203] Each access point(14) allocates an EMID to the station(12) inside one's BSS. The size of the EMID block which the access point(14) can allocate to the station(12) is fixed at the reasonable value. For example, it has very low possibility for the number of the stations(12) to be greater than 256 in 256/BSS. One access point(14) broadcasts/ multicasts an EMID and the range of EMID which wishing to use to the other access points(14) inside one's ESS. An MAC address which is used in order to request [EMID.request], [MAC_Addr_for_request], is separately allocated. [MAC_Addr_for_request] uses the random value within the predetermined range. If the requested EMID and EMID block from one access point(14) is being used, the other access point(14) which is using them sends the response. Without receiving the response after the EMID.request is sent, it is thought that this EMID is not used. In this case, the other access point(14) informs one access point(14) of using this EMID by itself.

[204] EMID.request is defined as follows.

[205] EMID.request

[206] {

[207] MAC_Addr_for_request // MAC address which is used for request. selected from the MAC address pool for request.

[208] requested_EMID // requesting EMID block

[209] }

[210] EMID.confirm is defined as follows.

[211] EMID.confirm

[212] {

[213] requested_EMID,

[214] Is_Conflict // True

[215] }

[216]

[217] Lease time negotiation

[218] According to current EMID/AMID technology, the valid lease time for EMID and AMID is allocated.

[219] The communication method in wireless network according to another embodiment of the present invention relates to negotiate a lease time for the station(12). The station(12) can request a lease time which it wishes to get. The lease time which the station(12) wishes to get is also assigned to it. The station(12) may request a lease time extension at an impending time before the expiration of the lease time. The station(12) transmits one's generating AMID and EMID to the access point(14) at the time of request for the initial address. AMID/EMID is transmitted by the method to transmit the probe request with IE(Information Element) including AMID and EMID.

[220] In another embodiment, the IE used for requesting AMID/EMID is modified as the table 13 to request the lease time. The access point(14) allocates the lease time to the station(12) within the requested lease time.

[221] Table 13

ID	Length	AMID	EMID	Requested Lease Time (AMID)	Requested Lease Time (EMID)
----	--------	------	------	-----------------------------	-----------------------------

[222] The access point(14) informs the station(14) of both the validity of the requested AMID, EMID value and the lease time which may be allocated. The EMID value may be either the confirmation for the requesting value of the station(12) or the newly allocated value. They may be transmitted by the probe response with the IE for allocating AMID/EMID as described in the table 14. It makes the condition, Allocated Lease Time $\leq$ requested Lease Time, satisfied.

[223] Table 14

ID	Length	AMID usability	EMID	Allocated Lease Time (AMID)	Allocated Lease Time (EMID)
----	--------	----------------	------	-----------------------------	-----------------------------

[224] Before the lease time allocated to the station(12) is expired, the station(12) may request the lease time extension. The access point may also extend the lease time allocated to the station(12) as needed. It may be requested through the action management frame or management frame which can be defined as follows. In case of

using the action management frame, Action field is defined as the table 15. Category ID is assigned by the IEEE 802.11. This ID is called as "MAC Addr Lease Time". The following explanation is based on the action frame.

[225] Table 15

Category	Action	Action Owner (= STA or AP)	EMID or AMID	Lease Time Extension
----------	--------	-------------------------------	-----------------	-------------------------

[226] One example of the Action Management frame in the table 15 is the same as follows.

[227] When the station(12) requests the lease time extension, the station(12) transmits to the access point(14) "MAC Addr Lease Time Action Frame" which indicates that Action Owner = STA, and Lease Time Extension = requested lease time extension. The station(12) informs the access point(14) whether the lease time for some MAC address is changed through the EMID or AMID field. The access point(14) transmits "MAC Addr Lease Time Action Frame" to the station(12) to inform the station(12) of the result of the lease time extension.

[228] The field of Action frame which the access point(14) sends to the station(12) indicates that Action Owner = AP, and Lease Time Extension is the assigned lease time additionally assigned to the currently remaining lease time. After the access point(14) transmits "MAC Addr Lease Time action frame", the lease time is the previous remained lease time + the lease time extension. If the access point(14) can extend the lease time without the station's request, this is applied by transmitting "MAC Addr Lease Time Action Frame" to the station(12).

[229] Although the example embodiments of the present invention have been described with reference to the Figures, the present invention is not limited to the examples disclosed in the Figures.

[230] Although the above-described embodiment is described that IEEE 801.11, IEEE 801.11i and IEEE 801.11u standard and the like are used, but the present invention is not limited to these standards.

[231] Although the above-described embodiment is described that each IE(Information Element) or Action Management frame is included in the beacon, the probe request or the probe response to be exchanged between the stations or between the station and the access point, but the present invention is not limited thereof. They may be included in any types of frames or frames, messages to be transmitted. For example, they may be included in any frames used for the authentication, the association, or the presence related service.

[232] This application claims benefit of U.S. Provisional patent Application (1)No. 60/763,031 filed in U.S. on Jan 27, 2006, (2) No. 60/764,458 filed in U.S. on Feb 01,

2006, (3) No. 60/765,471 filed in U.S. on Feb 03, 2006, (4) No. 60/771,225 filed in U.S. on Feb 07, 2006, (5) No. 60/772,474 filed in U.S. on Feb 10, 2006, (6) No. 60/774,252 filed in U.S. on Feb 15, 2006, (7) No. 60/774,284 filed in U.S. on Feb 16, 2006, (8) No. 60/779,755 filed in U.S. on Mar 06, 2006, which are hereby incorporated herein by reference.

Claims

- [1] A communication method in wireless network comprising:
processing an information of a service provider list using a specific function or algorithm, and transmitting a data comprising all or part of the processed information by a access point; and
receiving the transmitted data from the access point, and processing the received data to decode the original information of the service provider list.
- [2] The communication method of claim 1, wherein the specific function is a hash function, the access point processes the information of the service provider list using the hash function, and the data further comprises the hash key used by the hash function along with all of the processed service provider list.
- [3] The communication method of claim 1, wherein the specific function is a hash function, and if the access point transmits the data comprising part of the processed information, the data further comprises the location at which part of the processed information is located
- [4] The communication method of claim 1, wherein the specific algorithm is a compression algorithm, and the data comprises the used compression algorithm information for processing.
- [5] The communication method of one of claims 1 to 4, wherein the transmitted data is one of a beacon or a probe response.
- [6] A communication method of a access point in wireless network comprising:
processing an information of a service provider list using a specific function or algorithm; and
transmitting the data comprising all or part of the processed information.
- [7] The communication method of the access point of claim 6, wherein the specific function is a hash function, the access point processes the information of the service provider list using the hash function, and the data further comprises the hash key used by the hash function together with all of the processed service provider list.
- [8] The communication method of the access point of claim 6, wherein the specific function is a hash function, and if the access point transmits the data comprising part of the processed information, the data further comprises the location at which part of the processed information is located.
- [9] The communication method of the access point of claim 6, wherein the specific algorithm is a compression algorithm, and the data comprises the used compression algorithm information for processing.
- [10] The communication method of the access point of one of claims 6 to 9, wherein

- the transmitted data is one of a beacon or a probe response.
- [11] A station for a wireless network system comprising;
receiving the data comprising all or part of the information of a service provider list, which is processed using a specific function or algorithm and is transmitted from the access point, and
processing the received data to decode the original information of the service provider list.
- [12] A station for the wireless network system of claim 11, wherein the specific function is a hash function, the information of the service provider list is processed using the hash function, and the received data further comprises the hash key used by the hash function along with all of the processed service provider list.
- [13] A station for the wireless network system of claim 11, wherein the specific function is a hash function, and if the received data comprises part of the processed information, the data further comprises the location at which part of the processed information is located
- [14] A station for the wireless network system of claim 11, wherein the specific algorithm is a compression algorithm, and the data comprises the used compression algorithm information for processing.
- [15] A station for the wireless network system of claims 11 to 14, wherein the transmitted data is one of a beacon or a probe response.
- [16] A communication method in a wireless network comprising;
transmitting the data comprising an information on a provider for which a access point is not supported; and
receiving the transmitted data from the access point to a station, and the station performing a specific function or operation using the information included in the data or not.
- [17] The communication method of claim 16, wherein the data is one of a beacon or a probe response.
- [18] A communication method of a access point in wireless network comprising;
comprising an information on a provider for which the access point is not supported into a specific data; and
transmitting the specific data comprising an information on a provider for which a access point is not supported through the wireless network.
- [19] The communication method of a access point in wireless network of claim 18, wherein the specific data is one of a beacon or a probe response.
- [20] A station of a wireless network system comprising;
receiving from a access point the specific data comprising an information on a

provider for which a access point is not supported; and
performing a specific function or operation using the information included in the data or not.

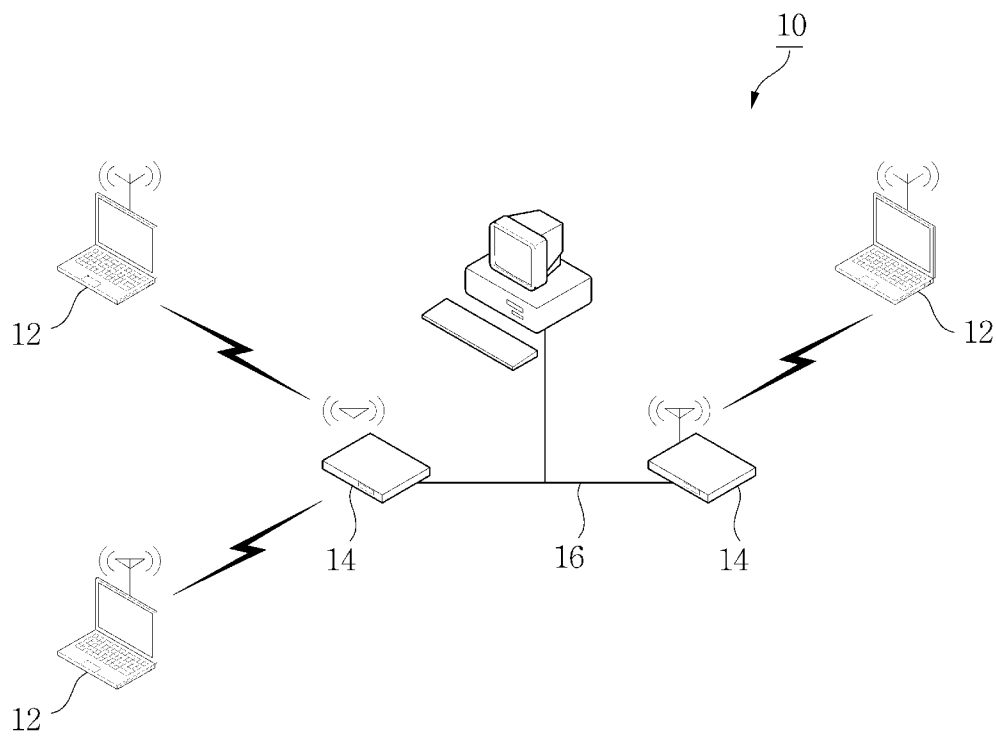
- [21] The station of the wireless network system of claim 20, wherein the specific data is one of a beacon or a probe response.
- [22] The station of the wireless network system of claim 20, wherein performing a specific function or operation using the information included in the data or not is not requesting a connection with the provider not supported by the access point.
- [23] A communication method in wireless network comprising;
transmitting a data comprising the total number of grouped information and one's turn among total information through the wireless network by a access point; and
receiving the transmitted data from the access point to the station and combining a specific information using the received data.
- [24] The communication method of claim 23, wherein the data is one of a beacon or a probe response.
- [25] A communication method of a access point in wireless network comprising;
grouping the specific information; and
transmitting a data comprising the total number of grouped information and one's turn among total information through the wireless network.
- [26] The communication method of claim 25, wherein the data is one of a beacon or a probe response.
- [27] A station of a wireless network system comprising;
receiving from a access point a data comprising the total number of grouped information and one's turn among total information through the wireless network;
and
combining a specific information using the received data.
- [28] The station of claim 27, wherein the data is one of a beacon or a probe response.
- [29] A communication method in wireless network comprising;
transmitting a data comprising one's network classification through the wireless network by a access point; and
receiving the transmitted data from the access point to the station and performing specific function or operation using the network classification of the access point included in the data or not.
- [30] The communication method of claim 25, wherein the type field with the network classification of the access point further comprises one of a service domain of the access point or a support for a roaming service.
- [31] A wireless network system comprising;
a access point transmitting a data comprising one's network classification

- through the wireless network by a access point; and
a station receiving the transmitted data from the access point and performing specific function or operation using the network classification of the access point included in the data or not.
- [32] A station of a wireless network system comprising;
receiving the transmitted data from the access point and performing specific function or operation using the network classification of the access point included in the data or not.
- [33] A communication method in wireless network comprising;
transmitting a data comprising the group information that a access point belongs to through the wireless network by the access point ; and
receiving the transmitted data from the access point and using the group information of the access point or not by a station .
- [34] A wireless network system comprising;
a access point transmitting a data comprising the group information that oneself belongs to through the wireless network; and
a station receiving the transmitted data from the access point and using the group information of the access point or not.
- [35] A communication method in a wireless network comprising;
transmitting the data comprising a request for a MAC address by a station;
receiving the data comprising the request for the MAC address and transmitting to the station the other data comprising a random MAC address in accordance with the request for the MAC address by a access point; and
transmitting a data comprising a real MAC address by the station.
- [36] The communication method of claim 35, wherein the data comprising the real MAC address is a action management frame.
- [37] The communication method of claim 36, wherein the real MAC address comprised in the action management frame is ciphered.
- [38] A communication method in a wireless network comprising;
allocating to station a random MAC address within a assigned range instead of a real MAC address of the station by a access point; and
communicating with the access point using the random MAC address by the station.
- [39] A communication method of a access point in a wireless network comprising;
being assigned from a specific server a random MAC address which a station uses within a predetermined range; and
assigning the random MAC address to the specific station instead of a real MAC address of the station within the assigned range.

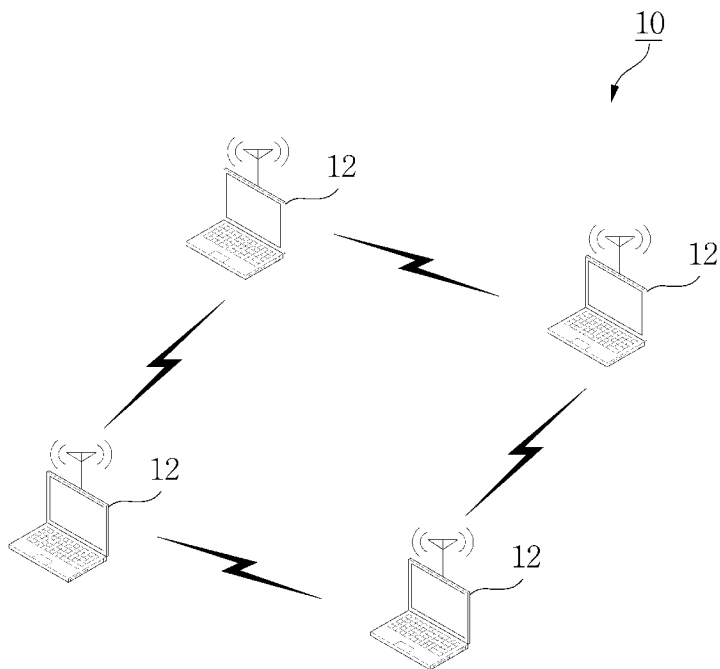
- [40] A communication method of a station in a wireless network comprising;
being assigned a random MAC address instead of a real MAC address of the
station from a access point within the assigned range; and
communicating with the access point using the random MAC address.
- [41] An access point in a wireless network comprising;
being assigned from a specific server a random MAC address which a station
uses within a predetermined range; and
assigning the random MAC address to the specific station instead of a real MAC
address of the station within the assigned range.
- [42] A station in a wireless network comprising;
being assigned a random MAC address instead of a real MAC address of the
station from a access point within the assigned range; and
communicating with the access point using the random MAC address.
- [43] A communication method in wireless network comprising;
transmitting the data comprising a random MAC address which oneself uses, and
the range for another random MAC addresses which oneself can assign, by one
of two or more access points;
receiving the data and, transmitting to the access point a response on the data, by
other of two or more access points, if at least one of the random MAC address
and the range for another random MAC addresses is used; and
receiving or not the response within a predetermined interval, and using the
random MAC address without receiving the response, by the former station.
- [44] The communication method of claim 43, further comprising;
informing the usage of the random MAC address and the usable range, by the
access point.
- [45] An wireless network system comprising;
one access point
transmitting the data comprising a random MAC address which oneself uses and
the range for another random MAC addresses which oneself can assign, and
receiving or not the response within a predetermined interval, and
using the random MAC address without receiving the response; and
the other access point
receiving the data, and
transmitting to the access point a response on the data, by other of two or more
access points, if at least one of the random MAC address and the range for
another random MAC addresses is used; and
- [46] The wireless network system of claim 45, wherein one access point informs the
usage of the random MAC address and the usable range, by the access point.

- [47] A communication method in wireless network comprising;
transmitting to a specific station the data comprising a random MAC address and the lease time of the station, by a access point; and
receiving the transmitted data from the access point, and communicating with the access point using the random MAC address before the lease time expiration.
- [48] The communication method of claim 47, further comprising; requesting the extension for the lease time.
- [49] The communication method of claim 48, wherein the requesting of the extension for the lease time is included in a action management frame.
- [50] A communication method of an access point in wireless network comprising;
transmitting to a specific station the data comprising a random MAC address and the lease time of the station; and
communicating with the station using the random MAC address before the lease time expiration.
- [51] The communication method of claim 50, further comprising; requesting the extension for the lease time.
- [52] The communication method of claim 51, wherein the requesting of the extension for the lease time is included in a action management frame.
- [53] A station of a wireless network system comprising;
receiving from a access point the data comprising a random MAC address and the lease time of a specific station; and
communicating with the access point using the random MAC address before the lease time expiration.
- [54] The station of claim 53, wherein the station further requests to the access point the extension for the lease time.
- [55] The station of claim 53, wherein the requesting of the extension for the lease time is included in a action management frame.

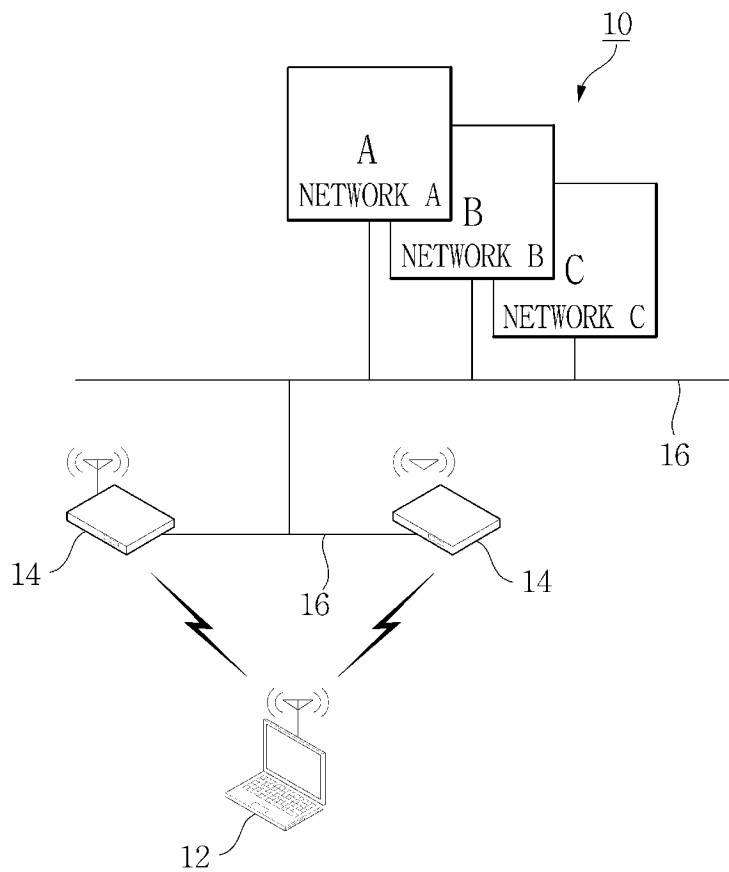
[Fig. 1]



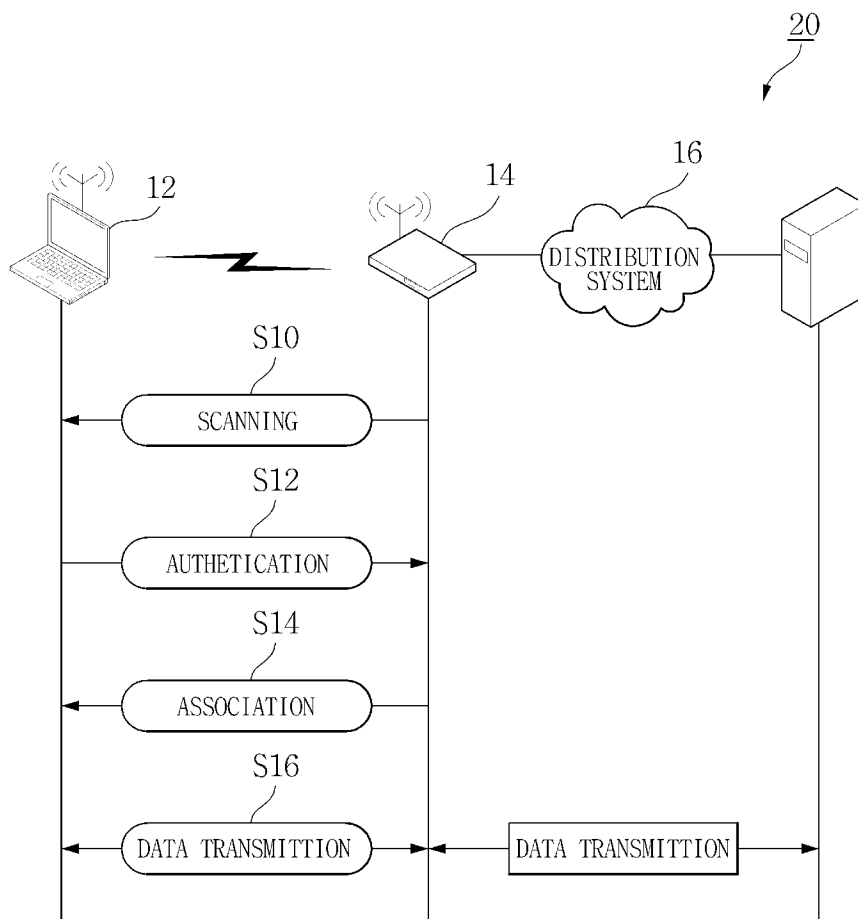
[Fig. 2]

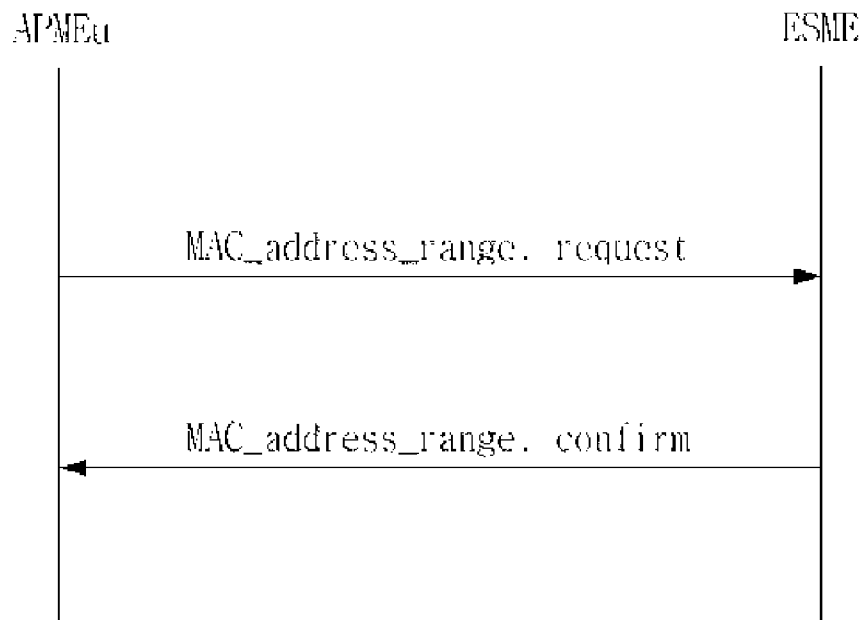
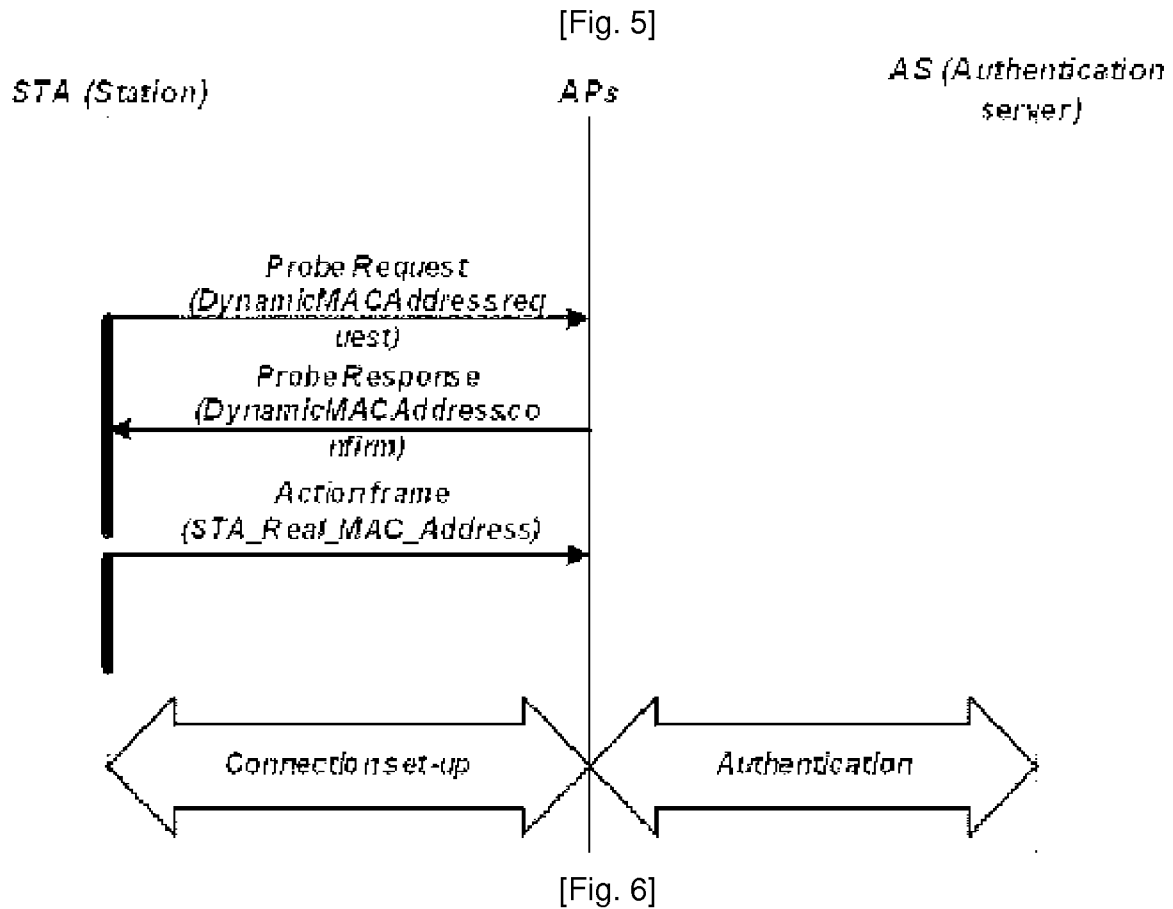


[Fig. 3]



[Fig. 4]





INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2007/000477**A. CLASSIFICATION OF SUBJECT MATTER****H04L 12/28(2006.01)i**

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)

IPC8: G06F, H04L

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

Korean Utility models and applications for Utility models since 1975

Japanese Utility models and application for Utility models since 1975

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

EKIPASS (KIPO internal), IEEE xplora

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	'IEEE 802.11 Wireless Local Area Networks', Crow, B.P.; Widjaja, I.; Kim, L.G.; Sakai, P.T.; Communications Magazine, IEEE, Volume 35, Issue 9, Sept. 1997 Page(s):116 - 126	35- 55
A	US 2003/0007464 A1 (Ram Jethannand Balani, Jan. 9, 2003) See the abstract, fig. 1a, and claim 1	1 - 15
A	US 2005/0060319 A1 (Bretton Douglas et al., Mar. 17, 2005) See the abstract, fig.1 and claim 1	1 - 15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

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

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of 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

11 MAY 2007 (11.05.2007)

Date of mailing of the international search report

11 MAY 2007 (11.05.2007)

Name and mailing address of the ISA/KR

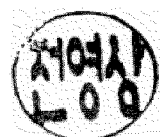
Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

JUN, Young Sang

Telephone No. 82-42-481-5653



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2007/000477**Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

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

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☒ Claims Nos.: 16-34
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
See the extra sheet
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

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

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

Claims 1-34 relate to transferring data including various information on 'processing' between AP and mobile stations
Claims 35-55 relate to allocating MAC address of AP and mobile stations.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

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

< Extra Sheet >

Claims 16-22 are unsearchable, because the expression 'provider for which an access point is not supported' is unclear. The claims could not be properly interpreted, although the description of the present invention is referred to.

Claims 23-28 are unsearchable, because the expression 'grouped specific information is unclear. The claims could not be properly interpreted, although the description of the present invention is referred to.

Claims 29-34 are unsearchable, because they are too broad to make meaningful search possible. According to claims 29-34, they simply disclose the technique for transmitting data including network group information between an AP and station in WLAN.

※ Claims 1-15 are unsearchable, because the expression 'processing information' is unclear. Nevertheless the search was performed, interpreting 'processing' as 'encoding' according to the description of the present invention

Claims 33-55 are unsearchable, because MAC address of a station and AP is described as being allocated in WLAN. It seems to mistake MAC identifiers (AMID and EMID) for the MAC address. Nevertheless the search was performed, assuming the MAC identifiers are allocated in claims 35-55 of the present invention.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2007/000477

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US2003/0007464A1	09.01.2003	CA2451668AA EP1400135A1	03.01.2003 24.03.2004
US2005/0060319A1	17.03.2005	W02006039087A2	13.04.2006