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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 March 2006 (02.03.2006)

PCT

(10) International Publication Number
WO 2006/021236 A1

(51) International Patent Classification[7]: H04L 12/28, H04Q 7/38, H04L 12/24

(21) International Application Number: PCT/EP2004/051918

(22) International Filing Date: 26 August 2004 (26.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NTT DOCOMO, INC.** [JP/JP]; 11-1, Nagata-cho 2-chome, Chiyoda-ku, Tokyo (JP).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **PRASAD, Anand R.** [NL/DE]; Gotthardstrasse 101, 80689 Muenchen (DE).

(74) Agent: **Betten & Resch**; Theatinerstr. 8, 80333 Muenchen (DE).

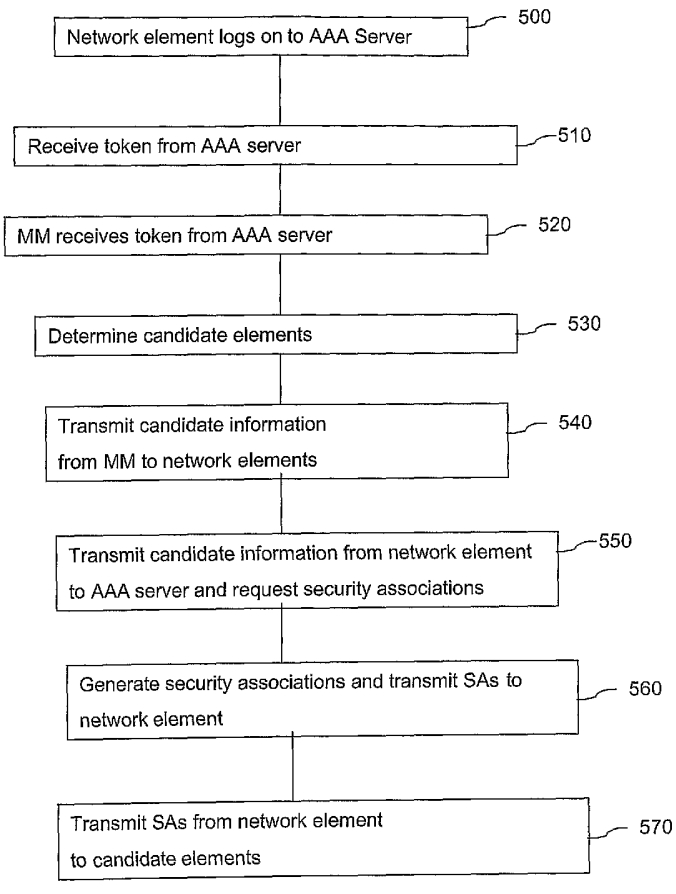
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, 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, 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, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *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.

(54) Title: METHOD AND APPARATUS FOR SUPPORTING SECURE HANDOVER



(57) Abstract: A method for supporting a secure handover of a mobile terminal from a first network element to another network element, said method comprising: automatically determining based on the topology of said network for said first network element candidate network elements which can be expected to act as candidates for the handover from said first network element; generating a security association between said candidate network elements and said first network element to support a handover based on said security association.

WO 2006/021236 A1

DCE 016 WO

METHOD AND APPARATUS FOR SUPPORTING SECURE HANDOVER

FIELD OF THE INVENTION

The present invention relates to a method and an apparatus for secure handover, and in particular it relates to the selection of handover candidates based on the network topology and the creation of trust with these candidates.

BACKGROUND OF THE INVENTION

In our days more and more communications links are implemented through wireless networks. Such wireless networks may comprise mobile phone communications networks, typically also referred to as so-called cellular networks, wireless computer networks such as wireless LANs, or hybrid networks which include a variety of different network technologies and corresponding terminals.

A typical property of wireless networks consists in the fact that usually they are organised in cells which means that terminals can access to the network through so-called access points which serve a certain range or area surrounding them. The communication between individual terminals which are not located in the same cell then is realised either through some backbone network which receives the information from the access point and delivers it to another access point close to the terminal device which is the intended recipient of the information, or the information may be transmitted from access point to access point until the access point is reached in the range of which the intended recipient terminal is located.

The great advantage of such types of network is that the user of a terminal device (a mobile phone, a PDA, a portable computer, or the like) may move while maintaining a communications link with another user through the network. However, one

of the problems arising with these types of networks is that the user may move out of the range of a certain cell, and then there must be provided some mechanism which still maintains the communications link despite the user and his terminal have moved out of the range of its access point or base station.

In order to maintain communications while moving out of the range of a certain cell the terminal must then make access and maintain the communications link through another cell the range of which covers the user's location after having moved. Such a procedure typically is labelled "handover". In order to perform a handover according to the conventional procedure there must be carried out an authentication and authorisation of the mobile terminal with respect to the new access point or base station. This is now schematically illustrated by referring to Fig. 1.

Fig. 1 shows a first access point AP1 having a certain range 100 within which it can communicate with mobile terminals, a mobile terminal MT1 located in this range, and moving to the coverage range 110 of another access point AP2. In order to prevent unauthorised access to the network and to ensure proper controlling of access and accounting and building of any services rendered by the network some kind of authentication and authorisation as well as accounting must be performed. Typically this kind of task is performed by an authentication, authorisation and accounting (AAA) server as shown in Fig. 1. The AAA server is in charge of performing authentication and authorisation checks when a terminal wishes to access a network, it typically is responsible for the general security environment like the generation and distribution of keys for communication sessions, the accounting of services rendered, and the like.

When a mobile terminal MT1 accesses the network through for example access point AP1, then AP1 contacts the AAA server in order to at first identify and authenticate the mobile terminal MT1 and then to negotiate some security environment such as encryption keys used during the communications session. When mobile terminal MT1 moves then to the range 110 of access point AP2, the same authentication and authorisation procedure has to be performed with respect to the new

access point AP2 by contacting the AAA server through access point AP2 to perform the authentication and authorisation.

This procedure is time consuming because for each secure handover the AAA server has to be contacted and a new security environment (which may also be labelled "security context" or "security association") has to be created by first checking the authentication and then negotiating a new security environment in a new cell.

Based on the foregoing it is an object of the present invention to provide a more efficient technique for performing a secure handover.

SUMMARY OF THE INVENTION

According to one aspect of the present invention there is provided a method for supporting a secure handover which employs the creation of a trust relation between neighbouring network elements to which the mobile device can handover. Once such a trust relationship has been created between neighbouring network elements such as access points, the handover can be performed in a faster and more efficient way by avoiding the need to re-authenticate the mobile device through contacting the AAA server.

According to one aspect the method includes the generation of a neighbour graph which is a data set which includes an identification of those neighbouring network elements (access points) to which a handover could be performed, as well as a security context, security association or security information which enables the direct handover without re-contacting the AAA server between neighbouring network elements.

According to one embodiment the neighbouring graph contains a list or set of the IDs of the access points to which a handover is possible, and a set of keys for the communication between the neighbouring access points or base stations. Such

keys may for example be encryption keys, integrity check keys, it may also include an identification of the encryption algorithm or a packet of authentication algorithm identification.

With such a neighbouring graph there is provided the necessary information in order to make possible a fast handover to those neighbouring networking elements which could possibly be the target of a handover.

According to one embodiment the generation of the neighbouring graph includes the selection or identification of those neighbouring networking elements which are candidates for a handover. In order to make such an identification or selection reference could be made to the network topology which may for example be stored in a management machine which maintains a description of the network topology.

According to one embodiment the method for supporting a the secure handover includes the transmission of the security context which has been generated for the neighbouring elements included in the neighbour graph to the candidate elements from the originating network element from which the handover should originate.

According to one embodiment the neighbour graph information including the candidates for handover and the corresponding security context can be transmitted to a network element as "piggyback" when it logs on to an AAA server. This means that no extra traffic in the network for distributing the neighbour graph will be needed. To implement this procedure, however, the network information and the relevant neighbour graph information must be available at the AAA server.

According to one embodiment the method of the invention enables the transmission of context parameters from one access point through the neighbouring element to which the handover should be performed. This may improve the quality of service during the handover by making use of the shortened secure channel directly between the relevant neighbouring access points without redirecting all the information through the mediation of the AAA server. Moreover, transmission of the context

parameters (which may be any parameters related to the user situation or the situation of the communication itself, such as location, used service, service configuration, or other parameters) may improve the handover quality by making sure that the handover of the service can be performed in a seamless manner by transferring all the relevant context information so that the communications session can be continued at the new access point in the same manner as it was conducted at the previous access point.

DESCRIPTION OF THE DRAWINGS

Fig. 1 schematically illustrates a network configuration according to the prior art.

Fig. 2 schematically illustrates a network configuration used in connection with an embodiment of the invention.

Fig. 3 schematically show a flowchart schematically illustrating an embodiment of the invention.

Fig. 4 schematically show a flowchart schematically illustrating a further embodiment of the invention.

Fig. 5 schematically illustrates a message sequence of an embodiment of the present invention compared to the prior art.

Fig. 6 schematically illustrates a message sequence of a further embodiment of the present invention.

DETAILED DESCRIPTION

Fig. 2 shows schematically a configuration of a network used in connection with an embodiment of the invention. Like in Fig. 1 there is shown an AAA server responsible for the security tasks. Several access points AP1 to AP7 are shown with their respective coverage. Furthermore there is shown a management machine MM

which has the task of generally managing the network, e.g. by maintaining a list of the network elements, managing the access and removal of network elements, and the like. The management machine is aware of the network topology, i.e. knows which network elements are located at which location and which range is covered by which network element. Typically the management machine is a secure location protected by limiting access thereto by keys and/or other security measures because the information about the network elements is security relevant.

The AAA server has (or generates on request) security related information for each network element such as keys, identities, etc.. When a network element switches on, it has to log-on to the AAA server. The AAA server keeps a list of network elements, it keeps track which elements are trusted or not, logged-on or not, and further their shared keys and Security Association (SA).The security association here means any security relevant information necessary to establish a communications session with a network element, this may include encryption keys, integrity check keys, it may also include an identification of the encryption algorithm or a packet of authentication algorithm identification.

In case of the present embodiment it is assumed that the AAA server and the management machine have a or can built up a secure communication channel. This can be provided for during network deployment by suitable configuration of the AAA server and the management machine.

In the following it will now be described how using the system of Fig. 2 a method for enabling a secure handover according to an embodiment of the invention is performed.

Since the management machine MM is aware of the topology of the network it knows for each network element which are its neighbours, or at least the management machine is capable to figure out the neighbouring elements of a certain network element. According to one embodiment as shown in Fig. 3 in step 300 the management machine for a certain network element determines which are the can-

didates for a handover from this network element. Typically such candidates are the neighbouring elements, i.e. those network elements whose coverage lies adjacent to or overlaps with the certain network element. Then in step 310 there is created a security association between the certain network element from which the handover originates and the candidates.

In case of a network configuration as shown in Fig. 2 this could mean that for network element AP3 as the originating element network elements AP1, AP2, AP4, and AP6, are included in the set of candidates. Then a security association is generated between AP3 and the candidates AP1, AP2, AP4, and AP6. This means that after the security association having been generated a handover from AP3 to any of the candidates AP1, AP2, AP4, and AP6 has been enabled and may be performed without re-authenticating the mobile device at the AAA server because the security association which has been generated between AP3 and the candidates can be used when handing over the mobile device to any of the candidates.

The set of candidates for handover for a certain network element together with a corresponding security association between the certain network element and the candidates can be labelled as "neighbour graph". Such a neighbour graph as described before with respect to AP3 may be performed for all network elements in a manner as described before, and then this enables a faster and more efficient handover from any of the network elements to another one.

Now a method for enabling a secure handover by creating a neighbour graph according to a further embodiment will be described by referring to Fig. 4. In this embodiment at first in operation 400 the network element "wakes-up", e.g. by being switched on or by being newly added to the network, and then it logs on to the AAA server. Like shown in Fig. 2 also in this embodiment there is a secure channel and a "trust" between the AAA server and the management machine MM. Based thereupon the network element receives a token from the AAA server to communicate with the management machine (operation 410). The AAA server also sends the token to the management machine (operation 420).

The management machine checks the location of the network element and determines the candidates for a handover from the network element (operation 430). This could be only neighboring elements, like in the embodiment before. However, in a particular embodiment the candidates could also include network elements which are not direct neighbors but can only be reached through an "intermediate network element", this may be called a "multiple hop", and it may be included when determining the candidates for handover depending on the network policy and possibly also on other parameters.

It should be understood here that the term "hop" or "multihop" when used in the following relates to a case where in addition to direct neighboring network elements further network elements are involved which are "neighbors of neighbors" such that a handover to such a network element would then be performed via an intermediate network element, and we in the following refer to this situation as a multiple hop. It should further be noted here that the generation of a neighbor graph may include network elements which are not direct neighbors of the originating network element.

In one embodiment the number of hops may be fixed. However, in a particular embodiment the number of hops could also be determined on certain parameters, e.g. the expected speed of the user and the location of the network. E.g. the network elements close to the rails of a train may often serve users moving at high speed, and then a multihop neighbor graph could be advantageous. The number of hops may also depend on the coverage of the individual network element (the cell size), which itself may depend on the allowed data rates.

After the candidate elements for a handover from a certain network element have been determined this information (the "candidate information") is sent to the network element from which the handover should originate (operation 440). The thus transmitted candidate information may comprise e.g. the ID of the candidate network elements, depending on availability of technology their location (which may e.g. be taken from a GPS system if the move and are not fixed), their capabilities (e.g. the available services, bandwidths, and other service related parameters) and

also the number of hops from the originating network element. Most important among this information is the ID of the candidate elements.

Based on the received information about the candidate network elements for a handover the originating network element send this candidate element information to the AAA server and requests a security association with them to be generated (operation 450).

The AAA server then generates (or retrieves if already generated) the security associations and transmits them to the network element from which the handover should originate. A security association in this embodiment means e.g. encryption information such as keys related to the originating network element which then are encrypted respectively by keys belonging to respective candidate elements. A security association for e.g. between AP3 and AP4 with AP3 as originating network element may therefore consist in security relevant information belonging to AP3 (keys, encryption algorithms, and possibly authentication algorithms like e.g. hashing algorithms) which has been encrypted by a key or keys belonging to AP4. The thus encrypted information then forms a "security association" between AP3 and AP4. Such security associations are generated for all pairs between the originating network element and the candidate elements.

In general a security association may be regarded as the relationship between two or more entities (typically a computer, but it could also be a user or a software component) which describes how the entities will use security services such as encryption to communicate.

Then the network element sends the SAs, encrypted by individual candidate network element keys (carried out by AAA server), to the candidate network elements (operation 470). This can be a multicast or unicast (i. e. all security associations together are transmitted as a single large security association message, to each network element, however would be time consuming). Each network element can

decrypt its SA or its portion thereof. This means that each candidate element is now aware of the security relevant information(such as the keying materials, encryption algorithm, authentication algorithm like hash-algorithms, and the like) of the originating network element and vice versa, and this enables now the performing of a secure (direct) handover from the originating network element to any of the candidate elements based on the thus created "neighbor graph" without having to re-authenticate the mobile terminal at the AAA server.

In other words, the keying materials related to the originating network element are encrypted by the keying materials of a certain candidate network element and then forwarded to said candidate network element. The candidate network element can decrypt them by using its own keying elements for decryption and thereby receives the keying elements or security information necessary to communicate with the originating network element. Furthermore the originating network element receives the keying materials of the candidate element. For security reasons these keying elements before being transmitted to the originating network element are encrypted using the keying materials belonging to said originating network element. The originating network element then can decrypt them using its own keying materials which it has been provided when logging on to the network.

Therefore, in one embodiment the message sent to the originating network element may look like as follows:

$$((C_{cand}(Key_{orig}); C_{orig}(Key_{cand}))_{i=1}, \ldots\ldots, (C_{cand}(Key_{orig}); C_{orig}(Key_{cand}))_{i=n})$$

The message part $((C_{cand}(Key_{orig}); C_{orig}(Key_{cand}))_{i=1}$ here means the keying elements Key_{orig} of the originating network element encrypted by an encryption algorithm C_{cand} using the keying elements of candidate element i=1, and the keying materials Key_{cand} for candidate network element i=1 are encrypted using the keying materials C_{orig} of the originating network element. Such message parts are generated and transmitted to the originating network element for each pair consisting between the

originating network element and the respective n candidate elements, therefore the whole message contains n such message elements as shown above.

The keying materials typically are generated using a security server or any unit which is trusted and dedicated to the generation and maintenance of keying materials and possibly other security relevant information. The security server may e.g. be an AAA server.

Depending on the level of trust which the originating network element enjoys it may be allowed to perform the encryption of the above message by itself so that only the keying materials Key_{cand} are delivered to the originating network element. It may then perform the encryption by itself to obtain $((C_{cand}(Key_{orig})$, however, according to another embodiment the encryption is performed in a separate unit such as in the AAA server.

Once each of the candidate elements has received the security association which enables it to communicate with the originating network element the neighbor graph has been completed for the originating network element. It will be understood that preferably for all network elements a neighbor graph is generated in the manner described before.

The above procedure to create a secure neighbor graph may be repeated in predefined intervals. This may enable an update of the neighbor graph in case of new network elements have been added to the network.

As an alternative or additionally the neighbor graph may be re-generated in case a new network element is added to the network. Such an addition will be noted by the management machine which may then be configured to trigger the re-generation of the neighbor graph in such a case. On the other hand, in case a network element remains idle for a certain predetermined time period which may be set as a network parameter it may be removed from the neighbor graph.

In the following some embodiments are described which focus on variations how the neighbor graph, is transferred to its target, namely the originating network element for which the neighbor graph should enable communication with its corresponding candidate elements for handover.

According to one embodiment AAA server has the network configuration information and sends a neighbor graph (or the list of candidate elements for a handover) to a new network element on log-on of the new network element. This avoids then the need for a management machine, however, it means that the AAA server must be configured to be aware of the network topology and it must further be configured to be able to determine the candidate elements for handover which correspond to a certain originating network element.

According to one further embodiment the AAA server communicates with the management server on log-on of a network element and sends the candidate elements to the AAA server. This corresponds to the embodiment described in very detail already before.

According to one further embodiment the AAA server sends respective tokens with SA (security association) information to the originating network element and the management machine. This is possible under the condition that there exists trust between the AAA server and the management machine as well as between the AAA server and the originating network element, respectively. The distribution of the tokens may consist in keying elements so that the management machine and the originating network can communicate directly in a secure manner, in other words trust has been established between them. The originating network element can then communicate with the management machine and get the set of candidate elements for the handover. The creation of the neighbor graph may then proceed as already described in detail before.

According to one embodiment the generation of the neighbor graph may be performed as follows. On request by a network element (e.g. when logging on) the list

of candidate elements is determined, either by the management machine of directly by the AAA server. The AAA server then based on the set of candidate elements creates security associations for each of the candidate elements comprising the keying materials of the originating network element and the respective candidate element. The respective security associations are then directly sent from the AAA server to the respective candidate elements to thereby enabling communication between the candidate elements and the originating network element, respectively.

In the following it will be described in somewhat more detail how the candidate elements for a handover are determined.

In order to determine the candidate elements the following information is needed:

- The network element ID used as log-on. This information is enough for fixed network, because in case of a fixed network (where no network element moves) this information is sufficiently to determine the neighboring network elements
- The network element location is needed when the network element can be mobile and may move.

Once the network element ID is received by the management machine, the management machine determines the neighbor elements based on the network configuration. For that purpose there are different methods that can be used depending on the embodiment.

According to one embodiment the management machine simply checks the ID of the network element and finds its location in the network configuration which it maintains. It then sends the ID of all the network elements in the neighborhood till the number of hops defined by the network policy.

According to a further embodiment the management machine checks the network elements available in the neighborhood as mentioned before. However, in this embodiment it also checks if there are walls or other materials that might distort the signal; thus the mobile device will not be able to handover to such network ele-

ments. Based on such external influences it then determines the ID of network elements that can be practically used for handover as neighbor graph. In this embodiment also the number of hops according to the network policy is checked and the candidate elements are determined accordingly.

According to an even further embodiment the candidate elements are determined similar to any of the previous two methods, however in this embodiment the number hops is dependent on the direction of the mobile terminal or the network element. If the direction is towards the inside of a building then it can be assumed that the user will walk and only one hop information is enough because the speed of the user doesn't make more than one hop necessary. However, if the direction of the mobile terminal or the network element is towards the street then it is possible that the user is driving and in this embodiment the candidate elements then are determined such that multiple hops are included. Alternatively to or in addition to the direction of movement the number of hops may also be determined depending on the location of the user or the network element and possibly based on the environmental conditions at such a location. If e.g. the location is close to a train rail, then the user may have entered a train and possibly may move fast so that multihops could be preferable and should be included into the candidate elements. The details about how many hops should be selected depending on which environmental condition may be chosen appropriately when defining the network parameters.

According to a further embodiment the network element has the ability to find its location (e.g. GPS based), and then it sends its ID and coordinates e.g. to the management machine. This is particularly useful for situations where the topology can change, i.e. if the network element itself (and not only the user with his mobile device) can move. The management machine then determines the IDs and coordinates of neighboring network elements based on the location of the originating network element. This includes the determination of candidates up to the number of hops defined by the network policy and possibly also based on the direction of the movement.

According to a further embodiment an improved determination can be made if the management machine has site survey information. Site survey information may e.g. include information how the signal strength looks like if a network element is placed in a given location. Alternatively or additionally a determination can be made based on geographical information. Geographical information may e.g. include information indicating which network elements will make no sense to use as handover candidate. This may take into account environmental influences which can be determined based on said geographical information and which may affect the possibility or the likelihood that a handover is performed to a certain candidate element. E.g. if the position information of a user indicates that he is located most likely in a train because his position coincides with the location of the rails of a train, then it makes no sense to include such candidate elements which are neighboring elements of the originating elements but which do not cover the geographical area in which the rails are located and hence the train and the user will move. However, in such a condition it may be useful to increase the number of hops in the direction of the rails because the train may move fast and therefore a fast sequence of handovers may be required.

In the foregoing embodiment preferably each network element on change of location sends its new coordinates to the management server. In case of a location change then preferably a new neighbor graph is generated. Alternatively based on the location change the management machine or the unit responsible for determining the candidate elements will perform a significance check in order to check whether the movement is so significant that a new neighbor graph should be generated. If e.g. the location change means that the set of neighboring network elements has changed then in one embodiment this could be regarded as significant enough to create a new neighbor graph. On the other hand, as long as the movement does not lead to a change in the set of neighboring elements in one embodiment it may be determined that the movement is not so significant that a new neighbor graph need to be generated.

According to one embodiment the invention can be applied to mesh networks, e.g.

to fixed wireless mesh network. By this there is meant a wireless mesh network with no change in topology. The methods described before can be used for cheap deployment or extension of networks. E.g. if a new network element is to be added to a LAN, then it is added at first by the network administrator to the network. Thereafter when it logs on to the network it may trigger the (re-) creation of a neighbor graph in on of the manners as described before. Because the network topology will not change in time no adjustments of the neighbor graph due to network element location changes are necessary.

In case of a wireless mesh network which may be subject to topology change the situation is somewhat different. A change in topology makes the system slightly more complex because in such case the location information becomes necessary. Location information can e.g. be found by using GPS or other positioning technologies that are available. In this embodiment the network elements preferably inform the management machine or the unit responsible for the determination of the candidate elements about their location every time they move. In one such embodiment each movement will mean a new neighbor graph. In this case the network element can send the location information together with a neighbor graph request.
In one particular embodiment there may be provided a unit for checking whether the movement is significant enough to make a creation of a new neighbor graph necessary. This unit can be implemented in the management machine, in the AAA server, or even in the network element itself.

According to the embodiments described hereinbefore there is created a neighbor graph which enables a secure communication between a first network element and candidate elements for a handover. According to one embodiment the thus created secure communications channel may be used for the transmission of context parameters from one access point through the neighbouring network element (access point) to which the handover should be performed. This may improve the quality of service during the handover by making use of the shortened secure channel directly between the relevant neighbouring access points without redirecting all the information through the mediation of the AAA server. Moreover, transmission of the

context parameters (which may be any parameters related to the user situation or the situation of the communication itself, such as location, used service, service configuration, or other parameters) may improve the handover quality by making sure that the handover of the service can be performed in a seamless manner by transferring all the relevant context information so that the communications session can be continued at the new access point in the same manner as it was conducted at the previous access point. Just as an example the context information being transferred may involve information about the quality of service or the available services such as the bandwidth or data rate, and then the communications session after handover may be continued in an appropriate manner based on these context parameters.

A system according to an embodiment of the present invention and its advantageous effects will now be explained in connection with Fig. 5. Fig. 5 on the left-hand side shows a message sequence for a handover procedure in a wireless LAN system according to the standard IEEE 802.11. In this message sequence there is shown a station STA which has been connected to an old access point AP and which now is about to perform a handover to a new access point APnew. At first as illustrated on the top of this diagram there are sent probe requests and responses in three different channels by the station STA. While the standard itself does not require three channels it should be mentioned here that a good implementation will use three channels. This is for just looking around which new access point might be suitable or available for handover. For this purpose the station STA sends around these requests in three channels different from the channel of the ongoing present communication. Any access point ready for handover sends a corresponding response, as illustrated in the sequence diagram.

Once then a new access point has been selected there is performed an open system authentication which is also a term according to the standard IEEE 802.11. This open system authentication just means that the station exchanges a message with the new access point. This open system of authentication does not yet involve any security parameters, it is not a "real authentication" in the sense that any se-

cure transmission or security check is involved in this authentication, it is therefore labeled "open system authentication".

After the open system authentication there follows a process of re-association, i.e. the station STA associates itself with the new access point. For this purpose at first there is sent a message from the station to the new access point Apnew. As a next step then the old access point contacts the AAA server to perform an authentication procedure to create a trust relationship between the old and the new access point. Then the old access point returns a message to the new access point to complete the establishment of a trust relationship between the two access points and to finally agree that the new access point will take over the mobile station. This procedure including the then two following steps which will be explained later is a so-called IAPP move producer between the old access point and the new access point. The exchange of these messages according to the inter-access point protocol (IAPP) move procedure has the purpose of first of all informing the old access point AP that the new access point APnew will now take over the mobile station STA and to perform an authentication (the first to fourth messages in the IAPP move procedure). The fifth and sixth messages may be used for the transfer of context information, for example context information related to the services and the features of the ongoing communications session.

After the re-association has been performed an authentication procedure is performed for which EAP-TLS is the most common implementation. Here EAP stands for extensible authentication protocol and TLS for transport layer security. The message sequences shown with respect to this authentication in the diagram follow the prescriptions of the standard IEEE 802.11i. As can be seen from the diagram this involves the exchange of a large number of messages, moreover, it involves two stages of message exchanges, namely from the station STA to the new access point APnew, from there to the AAA server, and back via the new access point to the station STA. All the messages together form the handover delay as indicated in the message sequence diagram of the left-hand side of Fig. 5, and the messages from the open system authentication to the EAP-TLS authentication form the re-

authentication delay involved with the re-authentication of the station at the new access point APnew.

In the following the advantageous effects of a method and system according to an embodiment of the present invention will be explained in connection with the message sequence diagram on the right-hand side of Fig. 5. As can be seen from this diagram, the probe request and response there is the same as in the diagram on the left-hand side of Fig. 5. Similarly, the open system authentication after the probe request and response also is the same as in the left-hand side of Fig. 5. Moreover, also the sequences involved with the re-association are in principle the same as in the left-hand side message sequence diagram. However, the transmission of context parameters in this embodiment (the last two messages in the IAPP move procedure) may involve the transmission of a security context, such as e.g. the key(s) and possibly other security related information such as an encryption algorithm, and/or an authentication algorithm like a hash-algorithm, necessary for the new access point to communicate with station STA.

As can be seen from the bottom part of the message sequence diagram on the right-hand side of Fig. 5 the actual re-authentication of the station STA at the new access point APnew is much faster than on the left-hand side, it merely involves the exchange of two authentication messages. This is because according to an embodiment of the present invention the security association between the station STA and the new access point has been created and delivered already in advance of the actual handover, e.g. by the transfer of the security context as described before in connection with the IAPP procedure.. For this reason merely the exchange of one pair of authentication messages (challenge and response) is necessary to perform the authentication of the station STA at the new access point. Moreover, as can be seen from the diagram on the right-hand side of Fig. 5 the authentication server AAA is not involved in this authentication procedure because all relevant security information has already in advance been delivered to the communication partners. As can be seen from a comparison of the message sequence diagrams on both sides of Fig. 5, the re-authentication delay and thereby the handover delay is sig-

nificantly reduced in an embodiment according to the present invention when compared with the prior art as shown on the left-hand side of Fig. 5.

In the following the advantageous effects according to a further embodiment of the present invention will now be described in connection with Fig. 6. Fig. 6 on the left-hand side shows a message sequence diagram which is identical to the one on the right-hand side of Fig. 5. It should be noted here that with respect to the IAPP move procedure the last two messages which are used for the transfer of context information may involve the transfer of the security context, i.e. the exchange of the relevant keys between the communications partners so that the station STA is enabled to communicate with the new access point APnew. Once this security context or security association has been transferred during the IAPP move procedure the actual authentication of the STA at the new access point APnew can be performed in the quick manner as shown on the right-hand side of Fig. 5 and the left-hand side of Fig. 6 without an involvement of the AAA server.

On the right-hand side there is shown a message sequence diagram according to a further embodiment of the present invention. In this embodiment it is assumed that the transfer of the security context parameters or the security associations has already been taken place, in other words the new access point APnew is already aware of the relevant keys enabling it to communicate with the station STA. This may be the result of the generation of a secure neighbor graph as has been described in connection with previous embodiments of the present invention.

Once such a secure neighbor graph has been created and the security context has already been transferred, the IAPP move procedure involves only the exchange of two messages in order to inform the old access point AP that the new access point APnew is to take over the communications session with the station STA. In a particular embodiment actually these two messages can be exchanged simultaneously (not in sequence) because a security association has been already generated between the old access point AP and the new access point APnew. This means that the exchange of these two messages does not need to involve any security check,

and for this reason the exchange of these two messages included in the IAPP move procedure may actually be sent simultaneously, thereby further decreasing the delay involved with the re-authentication.

After the IAPP move procedure then the actual authentication of the station STA at the new access point APnew may be performed as already explained in connection with the diagram shown on the left-hand side of Fig. 6. In summary, in the case of the embodiment illustrated in connection with the message sequence diagram on the right-hand side of Fig. 6 the total handover delay can be further decreased compared with the procedure of a handover according to the prior art.

One could mention here that the embodiments explained in connection with Figs. 5 and 6 are embodiments where the handover is performed in a wireless LAN. However, in principle the same procedure could also be performed in a fixed wired network. If in such a case of a fixed wired network there would be trust relationship between the access points, then the procedure would involve no delay in connection with an AP to AP communication because there is already a security association between the access points the network and therefore no security association has to be created first between different access points. Nevertheless the creation of a neighbor graph in such a case would be beneficial because it avoids the distribution of unnecessary security context information and therefore does not unnecessarily increase the load of the network. However, with the embodiment as shown on the right-hand side of Fig. 6 the response waiting time during the re-association procedure (the IAPP move procedure) has been reduced so drastically that it almost becomes negligible compared to the procedure in a wired network.

A further embodiment of the present invention will now be described in the following. According to this embodiment for the creation of a neighbor graph two types of security associations are generated. First of all, there is generated a security association between the originating access point and those candidate elements in the neighborhood of this originating access point which could possibly be the target of a handover procedure. For these candidate access points there is created a trust re-

lation or a security association between the originating access point and these candidate elements, as was described in connection with Fig. 5, right hand side, and Fig. 6, left hand side by referring to the first four messages in the IAPP move procedure. However, there is also a further security association or security context being transferred to fully create the neighbor graph, and this other security association being transferred relates to the security association between the mobile station STA and the originating access point AP. This security association is for example transferred by the fifth and sixth messages in the IAPP move procedure of the right hand side of Fig. 5 and the left hand side of Fig. 6.

According to one particular embodiment a certain access point which acts as an originating access point and for which the neighbor graph is generated not only determines the candidate elements based on which then the security context transfer between the originating access point and the candidate elements is performed, but also determines which mobile stations are served by this originating access point. For the mobile stations located and being served through the coverage area of this originating access point the security associations between these mobile stations and the originating access point are also transferred to the candidate elements to enable the fast handover as described before. In this embodiment the originating access point therefore transfers the security context or the security association to its neighboring candidate elements based on the individual mobile stations located in its coverage area.

According to a particular embodiment once a new mobile station enters the area of the originating access point this access point updates the neighbor graph by transferring the security association established between this new mobile station and the originating access point also to the other candidate elements included in the neighbor graph to enable the fast handover for this mobile station from the originating access point to one of the candidate elements after the new mobile station has entered the area of the originating access point. This may be regarded as an update of the neighbor graph.

The updating of the neighbor graph therefore involves the transfer of security associations between mobile stations and the originating access point. It may be triggered by the entering of a mobile station into the coverage area of a certain access point which then forms the originating access point for this newly entered mobile station and which therefore has to update its neighbor graph.

According to a further embodiment the updating of the neighbor graph may be dependent on the result of a status polling through which a certain access point checks by a polling which mobile stations are located in its coverage area. Such a polling may be performed at predefined moments in time or at predefined intervals.

According to a further embodiment the updating of a neighbor graph may also be based on a mobile station leaving the coverage area of a certain originating access point. After the mobile station has left the coverage area of the originating access point this originating access point may inform the candidate elements included in its neighbor graph about the leaving of this mobile station and about the fact that these candidate elements may delete their security associations related to this mobile station which just has left. In this manner an overflow or an over-accumulation of security associations which actually are not in use anymore at the different access point can be avoided.

However, it should be noted that in such a case it is preferable that then the neighbor graph is re-generated or updated at the access point into the coverage area of which the mobile station has moved. This avoids that the security association for this mobile station is deleted from such access points to which the mobile station actually could possibly hand over even after having moved into the new coverage area.

According to a particular embodiment the neighbor graph created for the certain access point (or originating access point) may depend also on the individual parameters or character of the mobile stations located in the coverage area of this access point. If for example in the coverage area of this access point there is lo-

cated one mobile station which may move relatively fast such that it requires a multi-hop neighbor graph, then due to this fact the neighbor graph for this originating access point may involve multi-hop candidate elements. Once this mobile station leaves the coverage area of this originating access point, however, the candidate elements which are included due to the multi-hop requirement may be cancelled from the neighbor graph of this originating access point.

According to one particular embodiment the individual candidate elements included in the neighbor graph of a certain originating access point may have corresponding identifiers which identify based on which mobile station they are included in the neighbor graph. As in case of the previous embodiment, for example, a certain candidate element may be included into the neighbor graph due to a first slowly moving mobile station and also due to a fast moving mobile station, in this case it will have two corresponding identifiers identifying these two mobile stations. If the fast moving mobile station leaves the coverage area, this candidate element will still be included in the neighbor graph because it is also included due to another mobile station. However, those candidate elements which are included into the neighbor graph only due to the fast moving mobile station (e.g. multihop stations which are not direct neighbors of the originating access point) may then by removed from the neighbor graph once this fast moving mobile station has left the coverage area of the originating access point.

The invention has been described in the foregoing by means of exemplary embodiments. It will be readily apparent to the skilled person that the methods according to the embodiments described may be implemented by computers or computer systems which are suitably programmed.

It will further be appreciated that the foregoing embodiments are for exemplary purposes only and may be modified by the skilled person.

CLAIMS

1. A method for supporting a secure handover of a mobile terminal from a first network element to another network element, said method comprising:
automatically determining based on the topology of said network for said first network element candidate network elements which can be expected to act as candidates for the handover from said first network element;
generating a security association between said candidate network elements and said first network element to support a handover based on said security association.

2. The method of claim 1, wherein the neighbouring network elements of said first network elements are determined as candidate network elements for a handover.

3. The method of one of the preceding claims, further comprising:
- generating a security association between one or more of the mobile stations located in the area of said first network element and said candidate network elements.

4. The method of one of the preceding claims, further comprising:
- updating said generated security associations based on the entering of a new mobile station into the area of said first network element or based on the addition, removal, and/or moving of a network element in said network.

5. The method of one of claims 3 or 4, further comprising:
- generating said security associations depending on the properties or parameters of the mobile stations located within the area of said first network element.

6. The method of one of the preceding claims, wherein said generation of said security association comprises:

generating by a security server a plurality of security associations, one for each pair of a candidate element and said first network element;
transmitting said plurality of security associations to said first network element;
sending said pairs of security associations from said first network element to said respective candidate elements.

7. The method of one of the preceding claims, wherein a security association for a certain pair consisting of said first network element and a candidate element comprises:
the keying materials associated with said first network element to communicate with said first network element:
the keying materials of said candidate network element necessary to communicate with said candidate network element.

8. The method of claim 7, wherein
said keying materials associated with said first network element to communicate with said first network element are encrypted by said keying materials of said candidate network element necessary to communicate with said candidate network element, and
said encrypted keying materials are sent to said candidate element to enable after decryption of said candidate element direct communication or a direct handover between said first network element and said candidate network element.

9. The method of one of the preceding claims, wherein
said method is performed repeatedly to update the security associations between said originating network element and said candidate elements.

10. The method of one of the preceding claims, wherein
performing said method is triggered by the addition of a new network element to said network.

11. The method of one of the preceding claims, wherein

a network element is removed from said neighbour graph if it remains idle for a predetermined period of time.

12. The method of one of the preceding claims, wherein
the determination of the candidate elements includes the selection of elements in addition to neighbouring elements of the first network element to obtain a multihop structure for the candidate elements.

13. The method of claim 12, wherein
the number of hops is determined by the network policy.

14. The method of one of the preceding claims, wherein
the determination of candidate elements and/or the number of hops is determined based on environmental influences which may affect the practical ability or the likelihood of the first network element handing over to a certain candidate element.

15. The method of one of the preceding claims, wherein
the determination of the candidate elements is based on the location of the first network element and/or the location of other network elements and the environmental conditions of these locations which may affect the ability and/or likelihood of a handover to a certain network element.

16. The method of one of the preceding claims, wherein
the determination of the candidate elements is based on the movement of the first network element and/or the movement of another network element and/or the movement of a user.

17. The method of one of the preceding claims, wherein
the determination of the candidate elements is based on site survey information indicating how the signal strength looks like if a network element is placed in a given location.

18. The method of one of the preceding claims, wherein
the determination of the candidate elements is based on geographical information indicating which network elements will make no sense to use as handover candidate.

19. The method of claim 18, wherein the geographical information take into account environmental influences which can be determined based on location information and which may affect the possibility or the likelihood that a handover is performed to a certain candidate element.

20. The method of one of the preceding claims, further comprising:
informing a unit responsible for the determination of the candidate elements about a movement of said first network element or any other network element to enable a re-determination of the candidate elements based on said movement.

21. The method of claim 20, further comprising:
determining whether the movement is sufficiently significant to justify the re-creation of the neighbour graph.

22. The method of claim 21, wherein said movement is judged to be significant enough if the set of neighbouring elements of said first network element has changed due to said movement.

23. The method of one of the preceding claims, further comprising:
transmitting context parameters between said first network element and one or more of said candidate network elements.

24. An apparatus for supporting a secure handover of a mobile terminal from a first network element to another network element, said apparatus comprising:

a module for automatically determining based on the topology of said network for said first network element candidate network elements which can be expected to act as candidates for the handover from said first network element;

a module for generating a security association between said candidate network elements and said first network element to support a handover based on said security association.

25. The apparatus of claim 24, wherein the neighbouring network elements of said first network elements are determined as candidate network elements for a handover.

26. The apparatus of one claims 24 or 25, further comprising:

- a module for generating a security association between one or more of the mobile stations located in the area of said first network element and said candidate network elements.

27. The apparatus of one of claims 24 to 26, further comprising:

- a module for updating said generated security associations based on the entering of a new mobile station into the area of said first network element or based on the addition, removal, and/or moving of a network element in said network.

28. The aparatus of one of claims26 or 27, further comprising:

- a module for generating said security associations depending on the properties or parameters of the mobile stations located within the area of said first network element.

29. The apparatus of one of claims 24 to 28, wherein said module for generation of said security association comprises:

a module for generating a plurality of security associations, one for each pair of a candidate element and said first network element;

a module for transmitting said plurality of security associations to said first network element;

a module for sending said pairs of security associations from said first network element to said respective candidate elements.

30. The apparatus of one of claims 24 to 30, wherein a security association for a certain pair consisting of said first network element and a candidate element comprises:

the keying materials associated with said first network element to communicate with said first network element;

the keying materials of said candidate network element necessary to communicate with said candidate network element.

31. The apparatus of claim 30, wherein

said keying materials associated with said first network element to communicate with said first network element are encrypted by said keying materials of said candidate network element necessary to communicate with said candidate network element, and

said encrypted keying materials are sent to said candidate element to enable after decryption of said candidate element direct communication or a direct handover between said first network element and said candidate network element.

32. The apparatus of one of claims 24 to 31, wherein

said candidate element determination module and said security association generation module are adapted to operate repeatedly to update the security associations between said originating network element and said candidate elements.

33. The apparatus of one of claims 24 to 32, further comprising

A module for triggering the operation of said candidate element determination module and said security association generation module by the addition of a new network element to said network.

34. The apparatus of one of claims 24 to 33, wherein
a network element is removed from said neighbour graph if it remains idle for a predetermined period of time.

35. The apparatus of one of claims 24 to 34, wherein
the determination of the candidate elements includes the selection of elements in addition to neighbouring elements of the first network element to obtain a multi-hop structure for the candidate elements.

36. The apparatus of claim 35, wherein
the number of hops is determined by the network policy.

37. The apparatus of one of claims 24 to 36, wherein
the determination of candidate elements and/or the number of hops is determined based on environmental influences which may affect the practical ability or the likelihood of the first network element handing over to a certain candidate element.

38. The apparatus of one of claims 24 to 37, wherein
the determination of the candidate elements is based on the location of the first network element and/or the location of other network elements and the environmental conditions of these locations which may affect the ability and/or likelihood of a handover to a certain network element.

39. The apparatus of one of claims 24 to 38, wherein
the determination of the candidate elements is based on the movement of the first network element and/or the movement of another network element and/or the movement of a user.

40. The apparatus of one of claims 24 to 39, wherein

the determination of the candidate elements is based on site survey information indicating how the signal strength looks like if a network element is placed in a given location.

41. The apparatus of one of claims 24 to 40, wherein
the determination of the candidate elements is based on geographical information indicating which network elements will make no sense to use as handover candidate.

42. The apparatus of one of claims 24 to 41,
the geographical information take into account environmental influences which can be determined based on location information and which may affect the possibility or the likelihood that a handover is performed to a certain candidate element.

43. The apparatus of one of claims 24 to 42, further comprising::
a module for informing a unit responsible for the determination of the candidate elements about a movement of said first network element or any other network element to enable a re-determination of the candidate elements based on said movement.

44. The apparatus of claim 43, further comprising:
a module for determining whether the movement is sufficiently significant to justify the re-creation of the neighbour graph.

45. The apparatus of claim 44, wherein said movement is judged to be significant enough if the set of neighbouring elements of said first network element has changed due to said movement.

46. The apparatus of one of claims 24 to 45 further comprising:
a module for transmitting context parameters between said first network element and one or more of said candidate network elements.

47. A computer program comprising computer program instructions which when being executed by a computer enable said computer to carry out a method according to one of claims 1 to 23.

48. A data carrier having recorded thereupon a computer program according to claim 47.

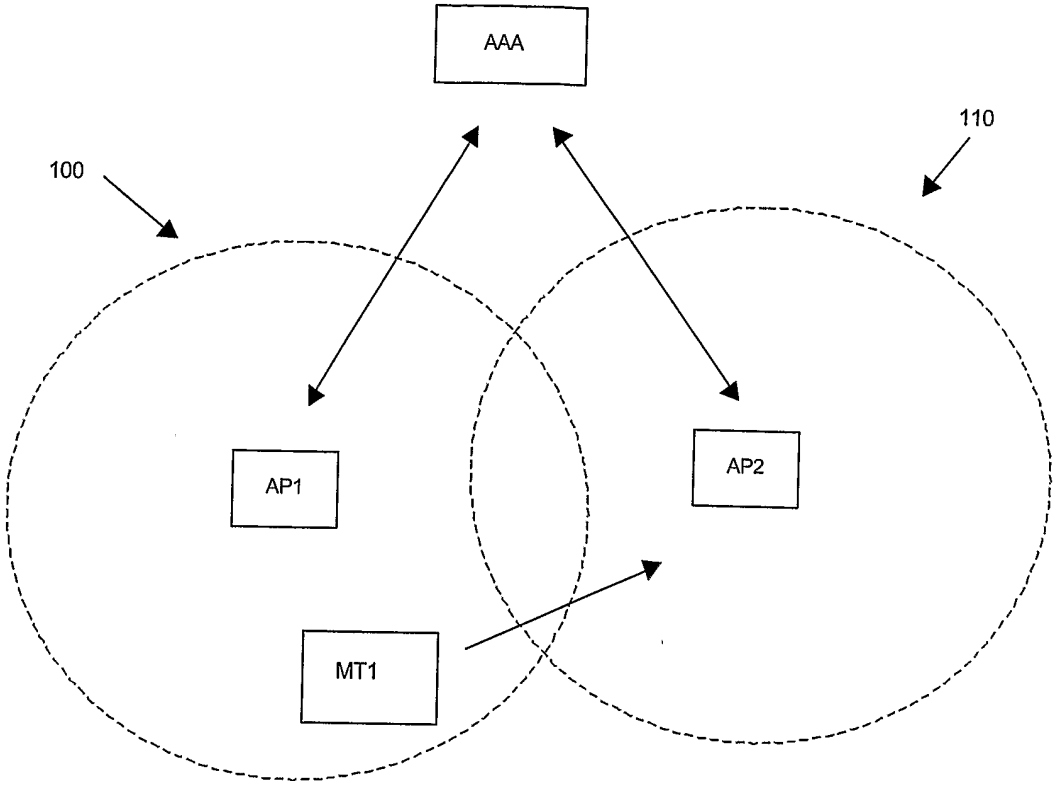


FIG. 1

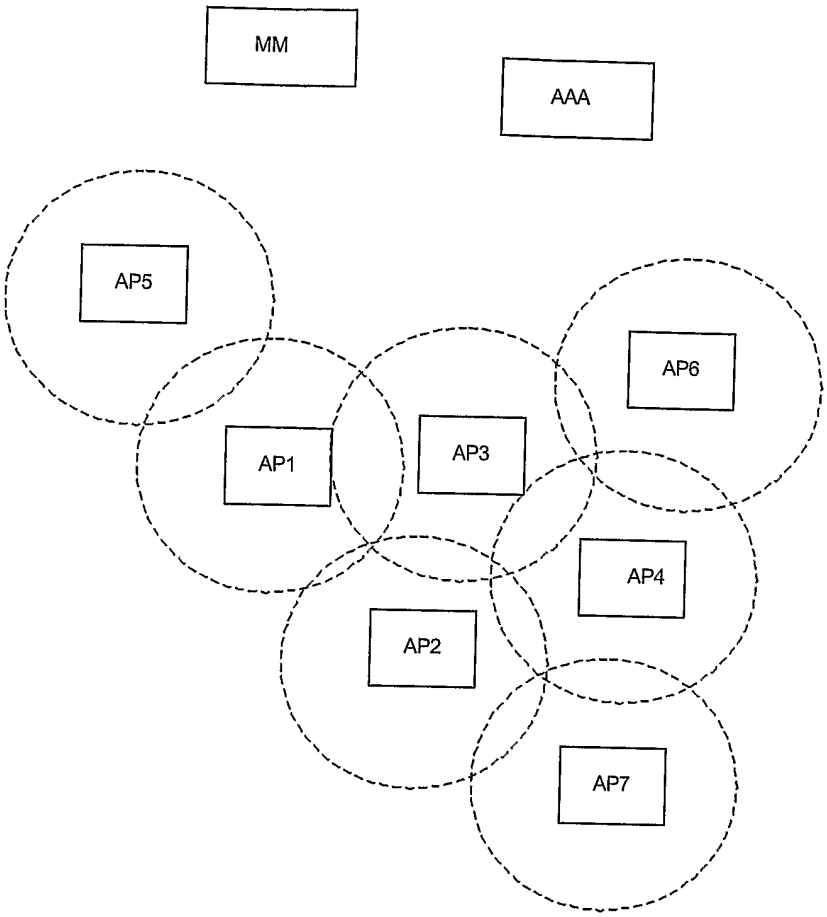


Fig. 2

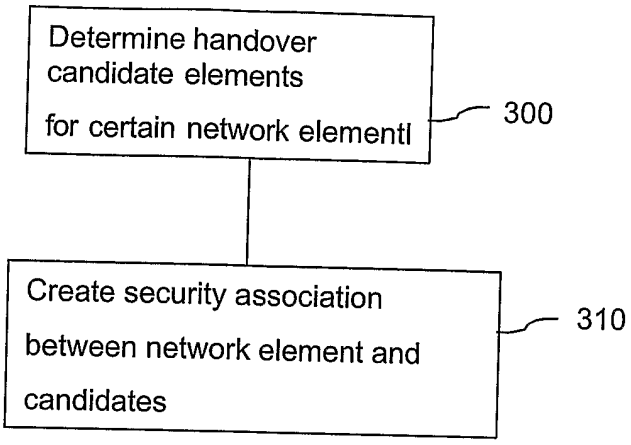

Determine handover candidate elements for certain network elementl
300
Create security association between network element and candidates
310

Fig. 3

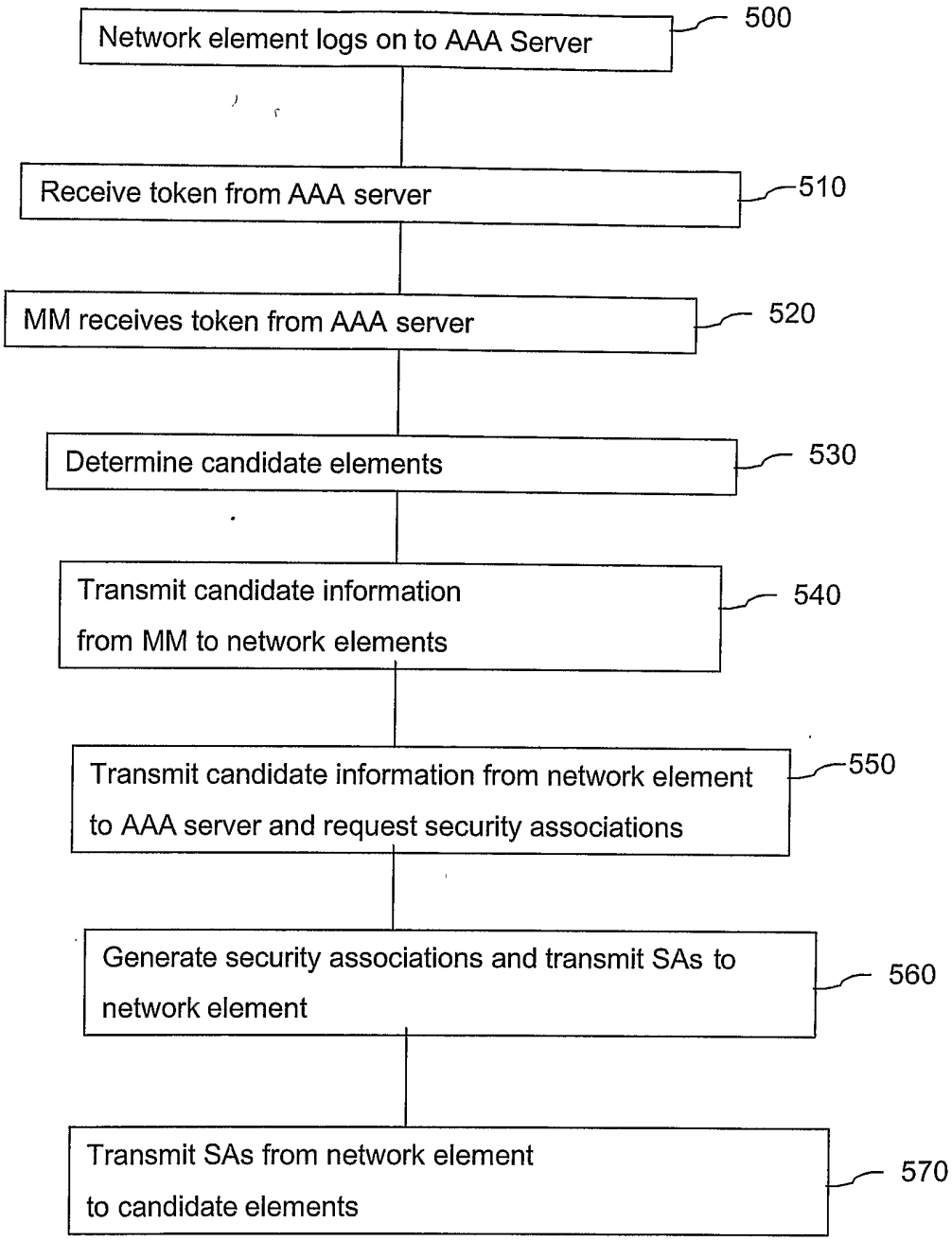

Network element logs on to AAA Server
500
Receive token from AAA server
510
MM receives token from AAA server
520
Determine candidate elements
530
Transmit candidate information from MM to network elements
540
Transmit candidate information from network element to AAA server and request security associations
550
Generate security associations and transmit SAs to network element
560
Transmit SAs from network element to candidate elements
570

Fig. 4

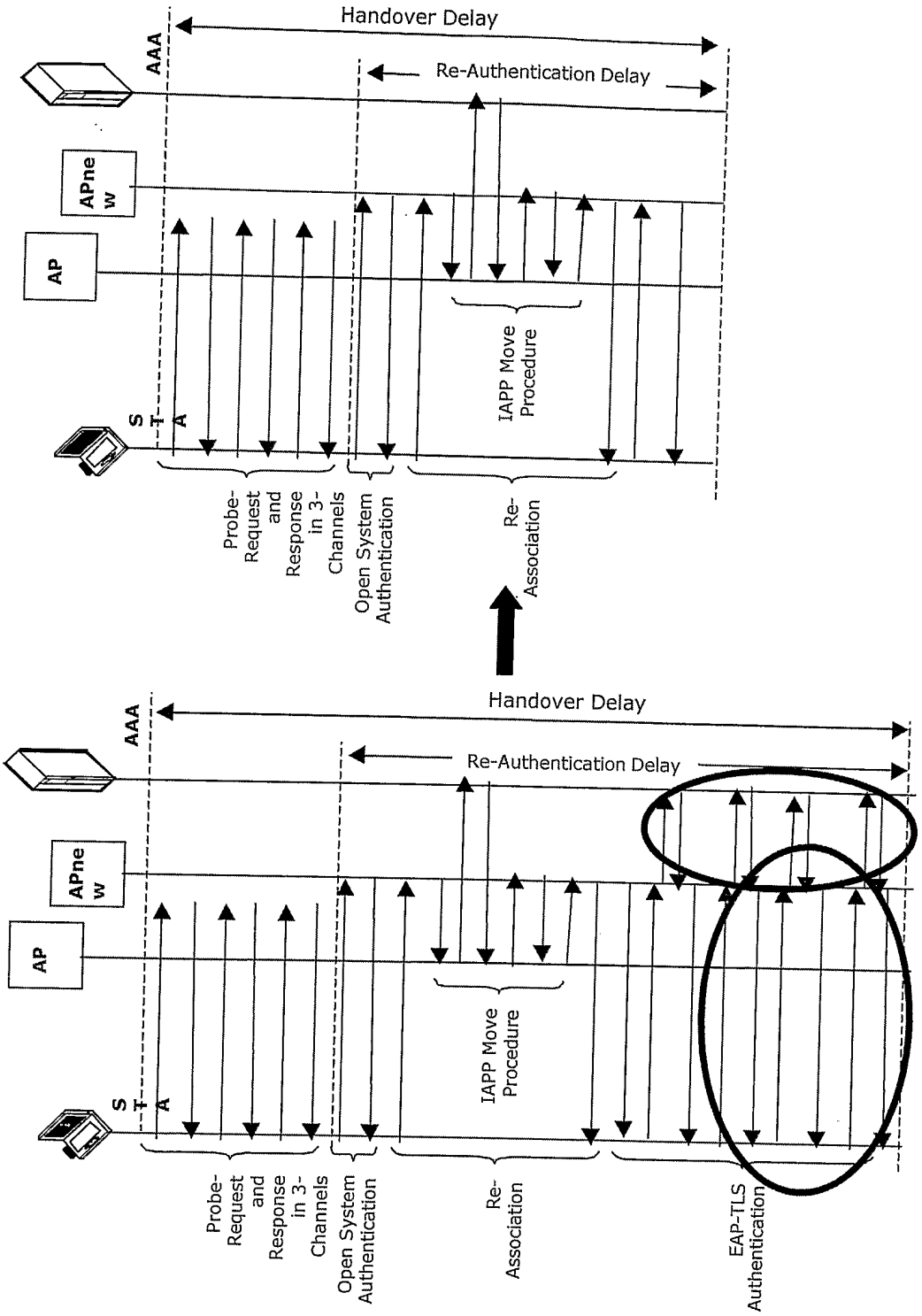

Handover Delay
Re-Authentication Delay
AAA
APnew
AP
STA
IAPP Move Procedure
Probe-Request and Response in 3-Channels
Open System Authentication
Re-Association
Handover Delay
Re-Authentication Delay
AAA
APnew
AP
STA
IAPP Move Procedure
Probe-Request and Response in 3-Channels
Open System Authentication
Re-Association
EAP-TLS Authentication

Fig. 5

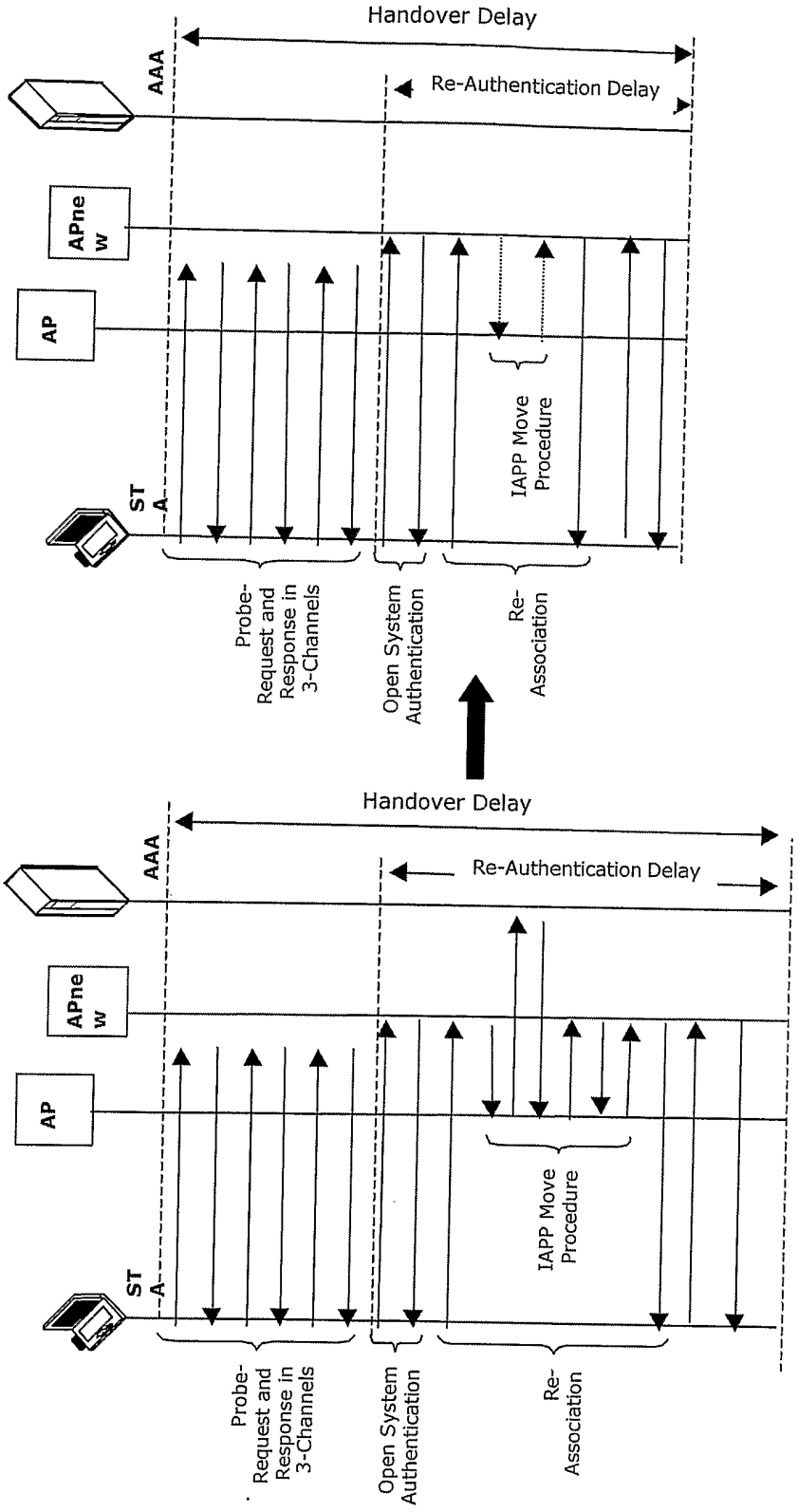

Handover Delay
Re-Authentication Delay
AAA
APnew
AP
STA
IAPP Move Procedure
Probe-Request and Response in 3-Channels
Open System Authentication
Re-Association
Handover Delay
Re-Authentication Delay
AAA
APnew
AP
STA
IAPP Move Procedure
Probe-Request and Response in 3-Channels
Open System Authentication
Re-Association

Fig. 6

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/051918

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/28 H04Q7/38 H04L12/24

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)
IPC 7 H04L H04Q

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 practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/047397 A (CISCO TECHNOLOGY, INC) 3 June 2004 (2004-06-03) abstract page 1, line 13 - page 2, line 24 page 4, line 1 - page 6, line 12 page 6, line 23 - page 7, line 31	1,2,4, 23-25, 27,46-48
A		3,6,7, 10,26, 29,30,33

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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 document 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 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
1 September 2005	08. 09. 2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Biyee, N

Form PCT/ISA/210 (second sheet) (January 2004)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 418 711 A (SAMSUNG ELECTRONICS CO., LTD; THE UNIVERSITY OF MARYLAND) 12 May 2004 (2004-05-12) abstract column 2, line 11 - line 40 column 3, line 9 - column 6, line 11 column 6, line 43 - column 12, line 32	1-10, 14-16, 18,19, 23-33, 37-39, 41,42, 46-48
Y	"DRAFT RECOMMENDED PRACTICE FOR MULTI-VENDOR ACCESS POINT INTEROPERABILITY VIA AN INTER-ACCESS POINT PROTOCOL acrOss distribution systems supporting IEEE 802.11 operation" IEEE P802.11F/D5, January 2003 (2003-01), pages 1-83, XP002275579 Page numbers refer to numbering in document page 1, line 29 - line 33 page 2, line 13 - line 16 page 3, line 29 - page 4, line 1 page 15, line 24 - line 28 page 17, line 19 - page 19, line 15 page 36, line 4 - page 38, line 37 page 39, line 7 - page 44, line 5 page 45, line 17 - page 48, line 25 page 52, line 23 - page 53, line 2	1-10, 14-16, 18,19, 23-33, 37-39, 41,42, 46-48
A	US 5 802 473 A (RUTLEDGE ET AL) 1 September 1998 (1998-09-01) abstract column 1, line 25 - column 3, line 17 column 4, line 10 - line 32 column 5, line 7 - column 6, line 51 column 9, line 51 - column 10, line 18 column 11, line 31 - column 13, line 18 column 14, line 28 - column 17, line 40	1,2,10, 12-19, 24,25, 33, 35-42, 47,48

-/--

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/051918

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KOODLI R ET AL: "FAST HANDOVERS AND CONTEXT TRANSFERS IN MOBILE NETWORKS" COMPUTER COMMUNICATION REVIEW, ASSOCIATION FOR COMPUTING MACHINERY. NEW YORK, US, vol. 31, no. 5, October 2001 (2001-10), pages 37-47, XP001115324 ISSN: 0146-4833 abstract page 43, left-hand column, line 15 - page 44, left-hand column, line 6 page 45, right-hand column, line 39 - page 46, left-hand column, line 7	1-10, 23-33, 46-48
A	US 2004/106408 A1 (BEASLEY JAMES ET AL) 3 June 2004 (2004-06-03) page 1, paragraph '0011! page 2, paragraph '0027! to page 3, paragraph '0038! page 4, paragraph '0051! to page 7, paragraph '0091!	1,2, 11-22, 24,25, 34-45, 47,48

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2004/051918

Box 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.:
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:

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 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:

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.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/051918

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004047397 A	03-06-2004	US 2004098586 A1	20-05-2004
		AU 2003290841 A1	15-06-2004
		CN 1505314 A	16-06-2004
		EP 1561331 A2	10-08-2005
		WO 2004047397 A2	03-06-2004
EP 1418711 A	12-05-2004	CN 1520107 A	11-08-2004
		EP 1418711 A2	12-05-2004
		EP 1526683 A2	27-04-2005
		EP 1521402 A2	06-04-2005
		EP 1521403 A2	06-04-2005
		JP 2004166277 A	10-06-2004
		JP 2005204341 A	28-07-2005
		US 2005143073 A1	30-06-2005
		US 2005083887 A1	21-04-2005
		US 2005141457 A1	30-06-2005
		US 2005117524 A1	02-06-2005
US 5802473 A	01-09-1998	GB 2290195 A	13-12-1995
		CA 2166539 A1	21-12-1995
		DE 69524850 D1	07-02-2002
		DE 69524850 T2	19-09-2002
		EP 0713632 A1	29-05-1996
		JP 2981519 B2	22-11-1999
		JP 9505196 T	20-05-1997
		WO 9535004 A1	21-12-1995
		CN 1129509 A	21-08-1996
US 2004106408 A1	03-06-2004	EP 1391100 A1	25-02-2004