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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 April 2010 (15.04.2010)

PCT

(10) International Publication Number
WO 2010/040420 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/EP2008/063687

(22) International Filing Date:
10 October 2008 (10.10.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MELÉN, Jan** [FI/FI]; Malminhaankuja 1 C 2, FIN-02280 Espoo (FI). **SALMELA, Patrik** [FI/FI]; Kuninkaantie 5-7 B20, FIN-02400 Kirkkonummi (FI). **YLITALO, Jukka** [FI/FI]; Heinjoenpolku 1 C 27, FIN-02140 Espoo (FI).

(74) Agent: **LIND, Robert**; Marks & Clerk LLP, 4220 Nash Court, Oxford Business Park South, Oxford Oxfordshire OX4 2RU (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, 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, LY, MA, MD, ME, 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, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, 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 (Art. 21(3))*

(54) **Title**: SECURITY PARAMETER INDEX MULTIPLEXED NETWORK ADDRESS TRANSLATION

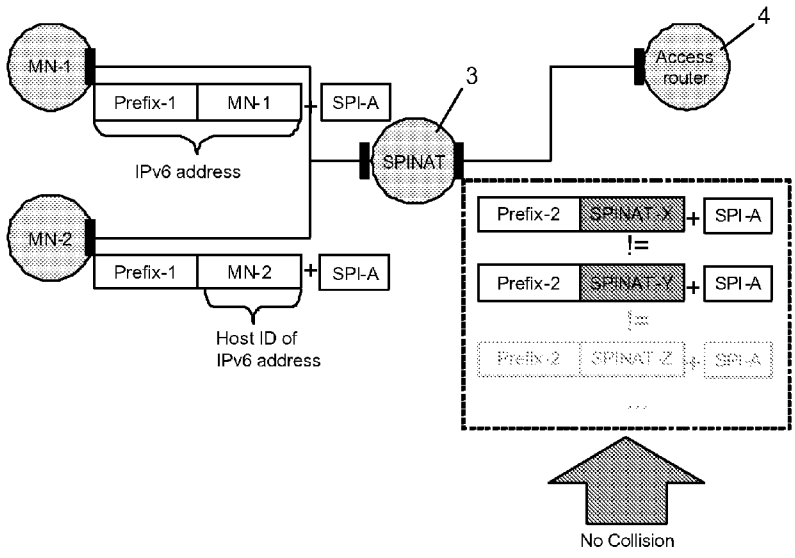


Figure 2

(57) **Abstract**: A security parameter index, SPI, network address translation, NAT, node, or SPINAT node, in an IP communications network is disclosed. The SPINAT node is configured to identify a potential collision arising from the specification of the same SPI value for use in communications by two or more client nodes of the SPINAT node. The SPINAT node assigns different IP-addresses for the SPINAT node for use by peer nodes communicating respectively with each of the client nodes.

WO 2010/040420 A1

Security Parameter Index Multiplexed Network Address Translation

Field of the Invention

The present invention relates to a Security Parameter Index Multiplexed Network Address Translation (SPINAT).

Background to the Invention

Internet Protocol (IP) communication systems allow multimedia services to provide a dynamic combination of voice, video, messaging, data, etc. within a communication session. IP Multimedia services are provided over IP-based mobile communication networks using the IP Multimedia Subsystem (IMS), which is the technology defined by the Third Generation Partnership Project (3GPP).

Internet Protocol Security (IPsec) is a suite of protocols for securing IP communications by authenticating and/or encrypting the packets of IP data that are sent between communicating peers over an IP-based network. The data packets are defined as IP Encapsulating Security Payload (ESP) packets as described in the 3GPP Internet Engineering Task Force (IETF) Request for Comments (RFC 2406). IPsec involves the establishment of Security Associations (SAs) between the network entities – an SA is a logical group of security parameters that allows the sharing of security information by the network entities, thereby allowing them to send and receive the data in a secure manner. For example, an SA may include cryptographic keys, initialisation vectors or digital certificates.

A Security Parameter Index (SPI) is an identification tag added to the header of an ESP data packet using IPsec. This tag enables the network entity (node) that controls the data traffic to distinguish between two traffic streams where different SAs have been established. The SPI is an integral part of an IPsec SA because it enables the receiving entity to select the SA under which a received packet will be processed. An SPI only

has local significance, because it is defined by the creator of the SA. However, the creator of an SA may interpret the bits in an SPI to facilitate local processing.

Network Address Translation (NAT) is the process of modifying network address information in data packet headers while the data is in transit across the network, so that a given address space can be mapped onto another address space. In NAT methods, client nodes of a "private" network are all represented to the outside world by the NAT node's IP address. SPI multiplexed NAT (SPINAT) is a NAT method of using the SPI values of ESP packets to demultiplex multiple IP addresses onto a single IP address. In other words it is a method of performing network address translation for ESP packets using IPsec. Thus, all connections made by the clients of the SPINAT node's private network appear to peers outside the private network to be terminated at the SPINAT node. An incoming ESP data packet received at the SPINAT node is mapped to the correct IP address of one of its clients using the SPI value in the ESP header of the packet. That is to say there is a state in the SPINAT node, which contains a SPI-IP address mapping. However, unless the system is configured to prevent it, it is possible for a collision condition to arise if two (or more) client nodes provide the same SPI value for the ESP packets that they are to receive. In that case the SPINAT node would not be able to resolve which of the IP addresses of the client nodes the packet is destined for.

A collision condition is illustrated in Figure 1, where two clients, MN1 and MN2 are linked to a SPINAT node 3. MN1 and MN2 have both been assigned an IPv6 address from the prefix supplied by the SPINAT node 3, Prefix1. The address is completed by the host part of each of the nodes, MN-1 and MN-2, as indicated in the figure. Furthermore, the SPINAT node 3 has been assigned an outer IP address from the prefix, Prefix2, supplied by an Access Router 4 of the outer network. In this case, the SPINAT node 3 only has the one address ending with the host part, identified here by SPINAT. Note that this discussion relating to Figure 1, and further discussion below describe the use IPv6 addresses, but the same principles may be applied to other address formats, such as IPv4. If client MN1 initiates a connection to a peer (not shown) and decides to use the SPI value SPI-A as its identifier for the connection there will be a state in the

SPINAT node indicating that packets received with SPI-A should be sent to MN1 (IP address: Prefix1 + MN-1). If MN2 now also initiates a connection to some peer (not shown), and decides to use the same SPI value, SPI-A, there will be a collision in the SPINAT node because two of its clients want to have their traffic identified by SPI-A.

A SPINAT system and method that solves the collision problem has been proposed, in which the SPINAT node always translates the SPI value and itself assigns unique SPI values used between the SPINAT node and the peers. The translation of the SPI value for a client's ESP traffic ensures that incoming ESP packets can be uniquely translated to the correct client IP address. In this method a state is required in both the SPINAT node and in the peer node. The SPINAT node connects its private network to a public or Wide Area Network (WAN) in the same way that a traditional Network Address Port Translation (NAPT) node does. The NAPT method uses port values in TCP/UDP headers for multiplexing IP addresses, while the SPINAT method uses the SPI values in the ESP headers for that purpose.

However there are some important differences between the NAPT and SPINAT methods. In NAPT the port values in the TCP/UDP headers are not integrity protected, whereas in the SPINAT method the SPI values in ESP headers are integrity protected. This creates a problem for the SPI translation, because the related ESP integrity protection keys are only shared between the communicating peer end-points, not with the SPINAT nodes. Therefore, the SPINAT nodes cannot transparently translate SPI values in the same way that the traditional NAPT nodes translate port values. Thus, to sustain the integrity of ESP headers and to support SPI translation, the SPINAT nodes must inform the sending end-points about the translation.

When the Security Associations are set up between the communicating peer end-points, a separate control signalling (for example using Host Identity Protocol (HIP) control packets) is used to negotiate the SPI values to be used (unlike in NAPT where the destination port values are well-known). Additionally, the ESP header carries only the destination SPI value, and so cannot be used for state establishment at the SPINAT node. Therefore a separate control signalling (key-exchange) is needed for state

establishment at the SPINAT node. The SPINAT node that is in the forwarding path of the two peer nodes will create its state in two steps. The first step is to create a soft-state for the SPI-to-IP address mapping for ESP payload traffic based on the control signalling (key-exchange). The SPINAT node intercepts a control signalling message sent from a client in the private network and which carries a SPI value. The SPINAT adds a Type-Length-Value (TLV) field containing the SPI mapping information at the end of the intercepted message before forwarding the message to the WAN link. Next, the state is completed to a hard-state after receiving the first ESP payload packet that carries the SPI which corresponds to the SPI-to-IP address mapping.

This SPINAT operation does not require any modifications to the ESP processing at the client in the private network, but does require a modification at the communicating peer in the WAN to allow the SPINAT node to re-write the SPI value on the received ESP packets. The original SPI value is selected by the client in the private IP network, and the value is replaced with another SPI value by the SPINAT node. As a result of the key-exchange, both the SPINAT node and the peer host establish a translation state. The peer in the WAN implements the same SPI mapping as the SPINAT node for integrity protected ESP packets, but in a reverse order. The SPI translation must be made after the ESP integrity protection is computed using the original SPI values.

The system and method described above requires that the peers are aware of the SPINAT functionality, but this is a sub-optimal solution as it places restrictions on the configuration of peer user's equipment. Legacy NAT devices in today's internet are invisible to the communicating end-points, and it would be preferable for the same to be the case for a SPINAT node. Moreover, because the integrity check value of the ESP packet is determined before the SPI translation at the peer, this results in an incorrect integrity check value for the packet, at least until after the SPI value has been translated back again at the SPINAT node.

The present invention has been conceived with the foregoing in mind.

Summary of the Present Invention

According to a first aspect of the present invention there is provided a security parameter index, SPI, network address translation, NAT, node, or SPINAT node, in an IP communications network. The SPINAT node is configured to identify a potential collision arising from the specification of the same SPI value for use in communications by two or more client nodes of the SPINAT node, and to assign different IP-addresses for the SPINAT node for use by peer nodes communicating respectively with each of the client nodes.

In embodiments of the invention, the SPINAT node is configured to assign an extra IPv6 address for itself on detection of a potential collision. Alternatively, the SPINAT node may be configured to obtain an extra IP address from an address provider. The SPINAT node may be configured to issue a request to obtain the extra IP address using a configuration protocol, such as Dynamic Host Configuration Protocol, DHCP. As another alternative, the SPINAT node may be configured to obtain an extra IP-address from a pre-assigned address pool.

In embodiments of the invention, the SPINAT node, on receiving a data packet that includes an SPI value chosen by a client, may determine a local IP address of the client based on the SPI value and the public IP address of the SPINAT node used for sending the data packet.

According to a second aspect of the present invention there is provided a method of performing a security parameter index, SPI, network address translation, NAT for routing of data packets via a SPINAT node to and from clients of the SPINAT node. The method comprises: receiving a control data packet from a client, the control data packet including a SPI value; determining if the SPI value gives rise to a collision condition; and if it does, assigning a different public network address for the SPINAT node for use in data packets sent and received by the SPINAT node to/from a peer communicating with the client.

In embodiments of the invention, the method further comprises receiving a data packet destined for the client at the SPINAT node, the data packet including the SPI value, and determining a local IP address of the client based on the SPI value and the public IP address of the SPINAT node used for sending the data packet.

The different public IP address assigned by the SPINAT node may comprise an address already determined from identification of an earlier collision condition.

The data packet may be an encapsulating security payload, ESP, data packet, and the SPI value being specified as part of the packet header. The public network address of the SPINAT node may be specified in the header of the ESP packets received from communicating peers.

It is an advantage of the present invention that it provides a solution to the collision condition without requiring the peers to be made aware of the SPINAT node and its functionality. The previously proposed solution requires some extra functionality in the peers whereas this invention removes that requirement. As a consequence, the SPINAT node of the invention can be widely deployed. Furthermore, apart from the IP-address translation, the present invention provides a solution that does not tamper with the ESP data packet and so maintains a consistent integrity check value in the packet for the duration of its lifetime.

Brief Description of the Drawings

Figure 1 is a schematic illustration depicting a collision condition at a SPINAT node operating an IPsec system;

Figure 2 is a schematic illustration depicting the operation of a SPINAT node in accordance with an embodiment of the invention;

Figure 3 is a diagram illustrating signal flows in accordance with an embodiment of the invention;

Figure 4 is a functional block diagram of a SPINAT node in accordance with an embodiment of the invention;

Figure 5 is a flow diagram illustrating method steps in accordance with an embodiment of the invention.

Detailed Description of Certain Embodiments

Figure 2 illustrates a similar situation to that illustrated in Figure 1, where the two clients, MN1 and MN2 are linked to a SPINAT node 3. As before MN1 and MN2 each have an IPv6 address made up of the prefix, Prefix-1 supplied by the SPINAT node 3 and completed by the host part of each of the nodes, MN-1 and MN-2. Also, as before, the SPINAT node 3 has been assigned an outer IP address prefix, Prefix2, supplied by the Access Router 4. However, in this case, the SPINAT node is configured to identify a potential collision arising from the specification of the same SPI value in control packets sent by two or more client nodes. The SPINAT node assigns itself a different host part for its IP-address for use by the peer nodes communicating, respectively, with each of the client nodes.

For example, as illustrated in Figure 2, client MN1 initiates a connection to a peer (not shown) by sending a control packet (for example a Host Identity Protocol (HIP) control packet) to the SPINAT node 3 and decides to use the SPI value SPI-A as its identifier for the connection. As before there will be a state in the SPINAT node indicating that packets received with SPI-A should be sent to MN1 (IP address: Prefix1 + MN-1). However, the SPINAT node assigns itself the host part SPINAT-X for its address (IPv6 address: Prefix2 + SPINAT-X, as shown in Figure 2) for establishing the connection between MN1 and its peer (i.e. when forwarding the control packet to the peer over the external (WAN) link). Now, when MN2 initiates a connection to a peer and sends a control packet containing an SPI value SPI-A that would cause a collision, the SPINAT node 3 notices this conflict. As a result, the SPINAT node 3 allocates a new IP address for itself, using a new host part, SPINAT-Y (IPv6 address: Prefix2 + SPINAT-Y, as shown in Figure 2). The SPINAT node uses this new IP address as its address for the connection between MN2 and its peer.

This means that MN1's peer will send its data traffic destined for MN1 to the SPINAT node 3, using SPI-A in the ESP header, but sending it to the SPINAT-X address, while MN2's peer will send its data traffic, also using SPI-A in the ESP header, but sending it to the SPINAT-Y address. The data structure containing the SPI value also contains information about which local IP address the entry belongs to (i.e. the destination address for the packet). When an ESP packet is received at the SPINAT node 3 and sent to IPsec processing, the node will find two entries matching the SPI value SPI-A. To determine which SPI-IP address mapping the current packet belongs to, the destination IP address of the packet is inspected.. That is to say, if the destination IP address of an ESP packet received at the SPINAT node 3 is the SPINAT-X address, then the data structure containing SPI-A will be translated to the IPv6 address Prefix1 + MN-1, and the packet will be forwarded to MN1. However, if the destination IP address of the received packet is the SPINAT-Y address, then the data structure containing SPI-A will be translated to the IPv6 address Prefix1+MN-2 and the packet will be forwarded to MN2.

If yet another client tries to establish a connection using the same SPI value, SPI-A, then the SPINAT node 3 will allocate yet another IP address for itself (e.g. SPINAT-Z), and so on.

If the SPINAT node 3 has already allocated itself multiple addresses (e.g. because of an earlier SPI collision), it can use one of the already allocated "extra" addresses instead of allocating a new one. For example, if the SPINAT node 3 has already allocated itself the addresses SPINAT-X and SPINAT-Y, as described above, to prevent a collision condition caused by MN1 and MN2 both using SPI-A, and then two clients of the SPINAT node 3 wish to establish connections both using SPI-B as their SPI values, the SPINAT node can allocate the addresses SPINAT-X and SPINAT-Y for each of the clients (that is to say, the same extra address can be used for preventing a collision both for SPI-A and SPI-B). In other words, one "extra" address can be used for preventing multiple SPI collisions.

Alternatively, and, for example where network addresses are defined using IPv4, the SPINAT node 3, instead of allocating itself a new IP address (e.g. SPINAT-Y), is configured to obtain an extra address form another source. For example, this could be from a pre-assigned address pool, or from another address provider. This may involve using a suitable configuration protocol, such as the Dynamic Host Configuration Protocol (DHCP) to request a new IP address.

As a consequence of the use of "extra" addresses, the external peers do not have to be configured or made aware of the SPINAT node functionality. They no longer have to perform the SPI translation of the previously proposed method. Moreover, the collision prevention solution of the present invention does not tamper with the ESP packet headers, and so a consistent integrity check value is maintained for the ESP packet throughout as it is relayed through the SPINAT node.

The Internet Engineering Task Force (IETF) is establishing a more widespread use of the Host Identity Protocol (HIP) for control signalling. HIP uses a 4-way handshake base-exchange to authenticate the communicating peers. HIP provides a method of separating the end-point identifier and locator roles of IP addresses. It introduces a new Host Identity (HI) name space, based on public keys. The public keys are typically, but not necessarily, self generated. The specifications for the architecture and protocol details for these mechanisms are specified in the following IETF Requests For Comments (RFCs):

HIP Architecture (RFC 4423)
Host Identity Protocol (RFC 5201)

Figure 3 illustrates signal flows between client nodes MN1 1 and MN2 2, the SPINAT node 3 and peers 5 in the external network, with which MN1 and MN2 establish IPsec connections. In Figure 3 the signals involve a HIP base exchange of signals for establishing the connections for both MN1 and MN2, whereas in Figure 4 (described in more detail below), the signals for both MN1 and MN2 are HIP updates after connection has already been established. However, the principles would apply equally

if one of MN1 or MN2 was involved in a HIP base exchange, while the other was involved in a HIP update exchange.

As shown in Figure 3, at *301* client MN1 sends a control signal I1 to the SPINAT node 3, indicating that it wishes to establish connection with one of the external peers 5 and specifying its source IP address (3ffe::1). The SPINAT node 3 performs the network address translation and, utilising a first IP address (2001::1), forwards the packet to the destination peer at *302*. The destination peer returns a confirmation signal at *303* to the SPINAT node 3, and at *304* sends a response signal R1 to the client MN1. The SPINAT node inspects the Host identities from the HIP packets each packet (I1, R1, I2, R2) carries a source host identity tag and a destination host identity tag, each host identity tag being a hash calculated for the Host Identity. At *305*, MN1 sends a second control signal I2 to the SPINAT node 3, this time specifying its SPI value, SPI-MN1 to be used in ESP packets for IPsec communications. This is then simply forwarded to the peer (at *306*), again after performing the address translation so that the signal appears to originate from 2001::1, the address used by the SPINAT node. At *307*, the destination peer returns a response to the SPINAT node, using its IP address 2001::1, and this is returned in a response signal R2 to MN1 at *308*.

At *309* MN2 initiates a base exchange by sending a control signal I1 to the SPINAT node, and the signal exchanges at *310-312* proceed in the same way as described above for MN1, with the SPINAT node 3 using its IP address 2001::1. At *313* MN2 sends a second control signal I2 to the SPINAT node 3, specifying its SPI value SPI-MN2 to be used ESP packets for IPsec communications. If SPI-MN2 was different to SPI-MN1 there would be no collision condition and the signalling could proceed as above for MN1. However, as shown in Figure 3, SPI-MN1 is identical to SPI-MN2. The SPINAT node 3 recognises that this is a collision condition, and so assigns itself a second IP address, 2001::2, which it then uses at *314* for forwarding the control signal to the external peer. The external peer responds at *315* using the SPINAT node's second IP address. Now, even though the SPI values are the same, the SPINAT node can perform the network address translation to determine the correct client node, MN2, to forward the response R2 to at *316*. It can do this because there is a unique

association between the SPI value and client address for any ESP data packet it receives with the destination IP address 2001::2.

The equivalent situation is shown in Figure 4, where the signal exchange comprises HIP update signals, rather than a HIP base exchange. The sequence of signals at *401* to *406* occurs in the normal way, with the SPINAT node 3 receiving an update signal (at *401*) and an acknowledgement (at *405*), and after performing the address translation sending these on to the destination peer (at *402* and *406*). At *403*, the SPINAT node receives a signal from the destination peer, which, as before, uses the SPINAT nodes IP address 2001::1. At *407*, client MN2 sends an update signal destined for a peer, but including specification of an SPI value MN2. Now, as before, if the SPI value SPI-MN2 is the same as SPI-MN1, the SPINAT node detects the collision condition, and assigns itself the additional public IP address 2001::2, which it uses at *408* to forward the update signal to the destination peer. The remaining signalling (at *409* to *412*) proceeds as before, with the destination peer using the second IP address of the SPINAT node, so that there is no collision caused by the use of the same SPI value as MN1.

Figure 5 is a flow chart illustrating the method steps carried out in the SPINAT procedure described above. At step 501 a control packet is received from a client and its header is read by the SPINAT node. At 502 the SPINAT node, determines if there is a potential collision caused by use of the same SPI value as another client. If the determination is Yes, then at step 503 the SPINAT node assigns (or obtains) an extra public IP address for itself, and at step 504 it maps the SPI value to the local IP address of the client and it stores this in association with the extra public IP address it has obtained. Alternatively, if there is no collision detected, then at step 505 the SPINAT node maps the SPI value to the client address in association with the default, or existing, IP address of the SPINAT node. At step 506 the SPINAT node forwards the data packet to the peer in the external network, but uses either the new, extra public IP address (when a collision has been detected) or the existing default public IP address where no collision has been detected.

At step 507, a data packet is received at the SPINAT node from a peer in the external network, and the header of the data packet includes both the SPI value and the public IP address that the peer has used for the SPINAT node. Using these two pieces of information, the SPINAT node determines, at step 508, the correct local IP address of the client, and at step 509 forwards the data packet to the client.

Figure 6 illustrates, in a schematic block diagram format, the principal functional features of the SPINAT node 3. the SPINAT node 3 includes a transceiver module 31 which receives and transmits IP data packets to/from its clients 32 in a private network, and to/from peer entities 33 in an external, public network. The SPINAT node also includes various processing functions that include: a reader 34 for reading the headers of data packets it receives; a collision detector 35, which determines if the SPI value in a control packet received from a client is the same as an SPI value already being used by another client; and a public address module 36 that either assigns an IPv6 address, or obtains a public IP address (e.g. IPv4 address) by generating and sending a request for one. Finally the SPINAT node includes a memory 37 storing the NAT state data – in other words the mappings between the SPI values and the client local IP addresses. The memory is segmented into separate parts 27a, 37b, etc. for each public IP address that has been assigned.

CLAIMS:

1. A security parameter index, SPI, network address translation, NAT, node, or SPINAT node, in an IP communications network, wherein the SPINAT node is configured to identify a potential collision arising from the specification of the same SPI value for use in communications by two or more client nodes of the SPINAT node, and to assign different IP-addresses for the SPINAT node for use by peer nodes communicating respectively with each of the client nodes.

2. The SPINAT node of claim 1 configured to assign an extra IPv6 address for itself on detection of a potential collision.

3. The SPINAT node of claim 1 configured to obtain an extra IP address from an address provider.

4. The SPINAT node of claim 3 configured to issue a request to obtain the extra IP address using a configuration protocol, such as Dynamic Host Configuration Protocol, DHCP

5. The SPINAT node of claim 1 configured to obtain an extra IP-address from a pre-assigned address pool.

6. The SPINAT node of any preceding claim configured, on receiving a data packet that includes an SPI value chosen by a client, to determine a local IP address of the client based on the SPI value and the public IP address of the SPINAT node used for sending the data packet.

7. A method of performing a security parameter index, SPI, network address translation, NAT for routing of data packets via a SPINAT node to and from clients of the SPINAT node, the method comprising:

receiving a control data packet from a client, the control data packet including a SPI value;

determining if the SPI value gives rise to a collision condition, and if it does, assigning a different public network address for the SPINAT node for use in data packets sent and received by the SPINAT node to/from a peer communicating with the client.

8. The method of claim 7 further comprising receiving a data packet destined for the client at the SPINAT node, the data packet including the SPI value, and determining a local IP address of the client based on the SPI value and the public IP address of the SPINAT node used for sending the data packet.

9. The method of claim 7 or claim 8 wherein the SPINAT node assigns itself the different public IPv6 address on determination of a collision condition.

10. The method of claim 7 or claim 8, wherein the SPINAT node obtains an extra IP address from an address provider.

11. The method of claim 10 wherein the SPINAT node issues a request to obtain the extra IP address using a configuration protocol, such as Dynamic Host Configuration Protocol, DHCP.

12. The method of claim 7 or claim 8 wherein the SPINAT node obtains an extra IP-address from a pre-assigned address pool.

13. The method of any of claims 7 to 12 wherein the different public IP address assigned by the SPINAT node comprises an address already determined from identification of an earlier collision condition.

14. The method of any of claims 7 to 13 wherein the data packet is an encapsulating security payload, ESP, data packet, and the SPI value is specified as part of the packet header.

15. The method of claim 14 wherein the public network address of the SPINAT node is specified in the header of the ESP packets received from communicating peers.

5

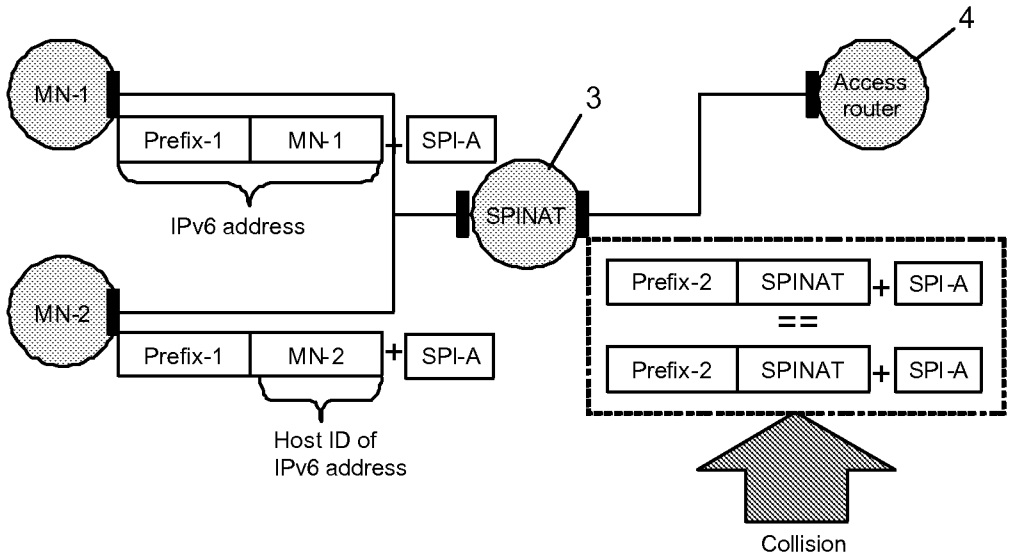


Figure 1

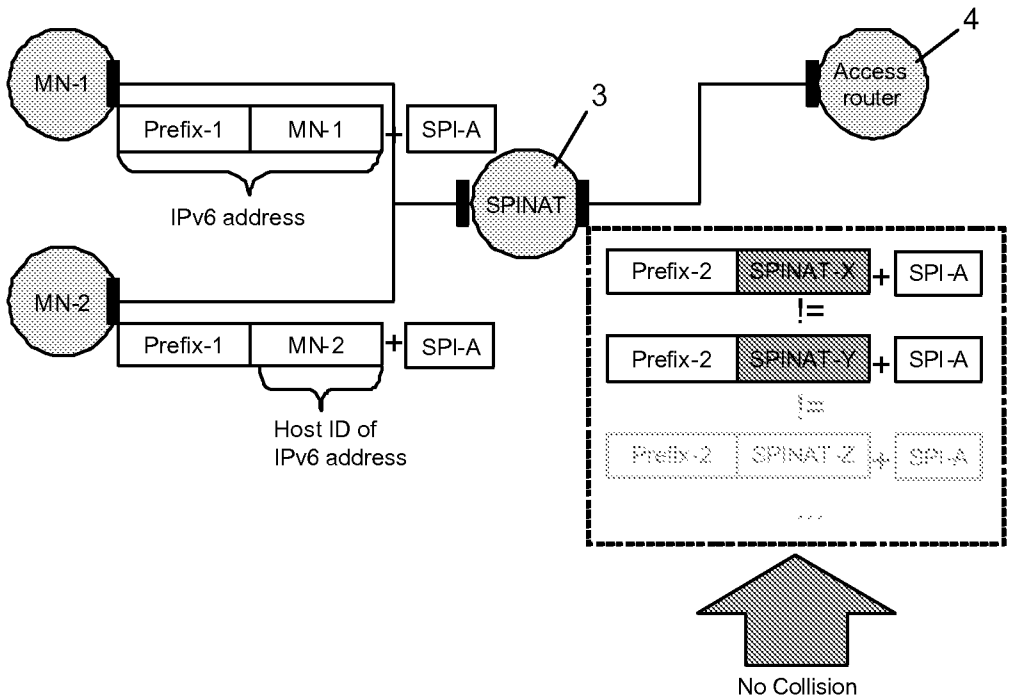
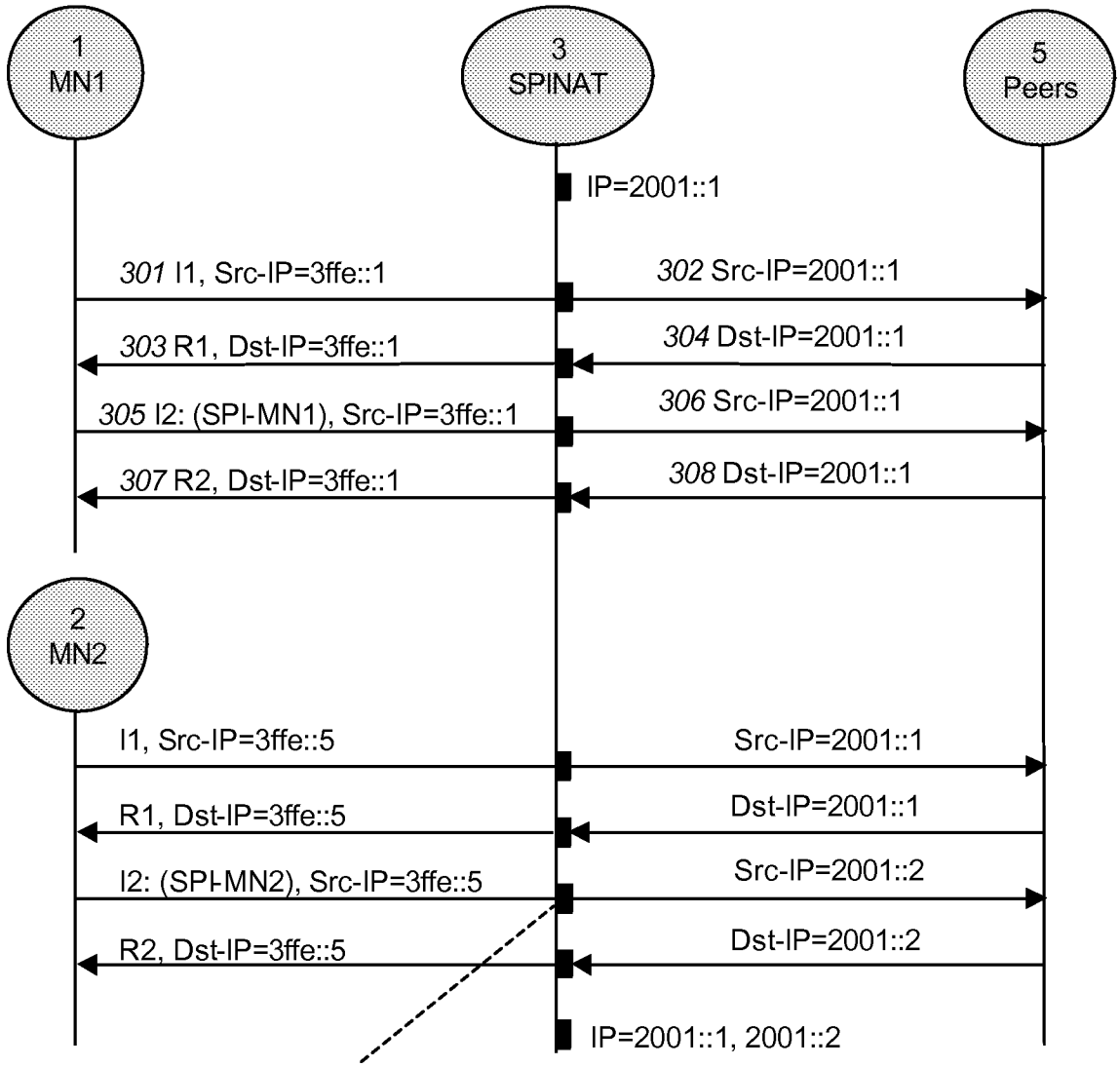


Figure 2



-SPI collision detected (SPI-MN1 == SPI-MN2)
- acquire new public address 2001::2
- forward message

Figure 3

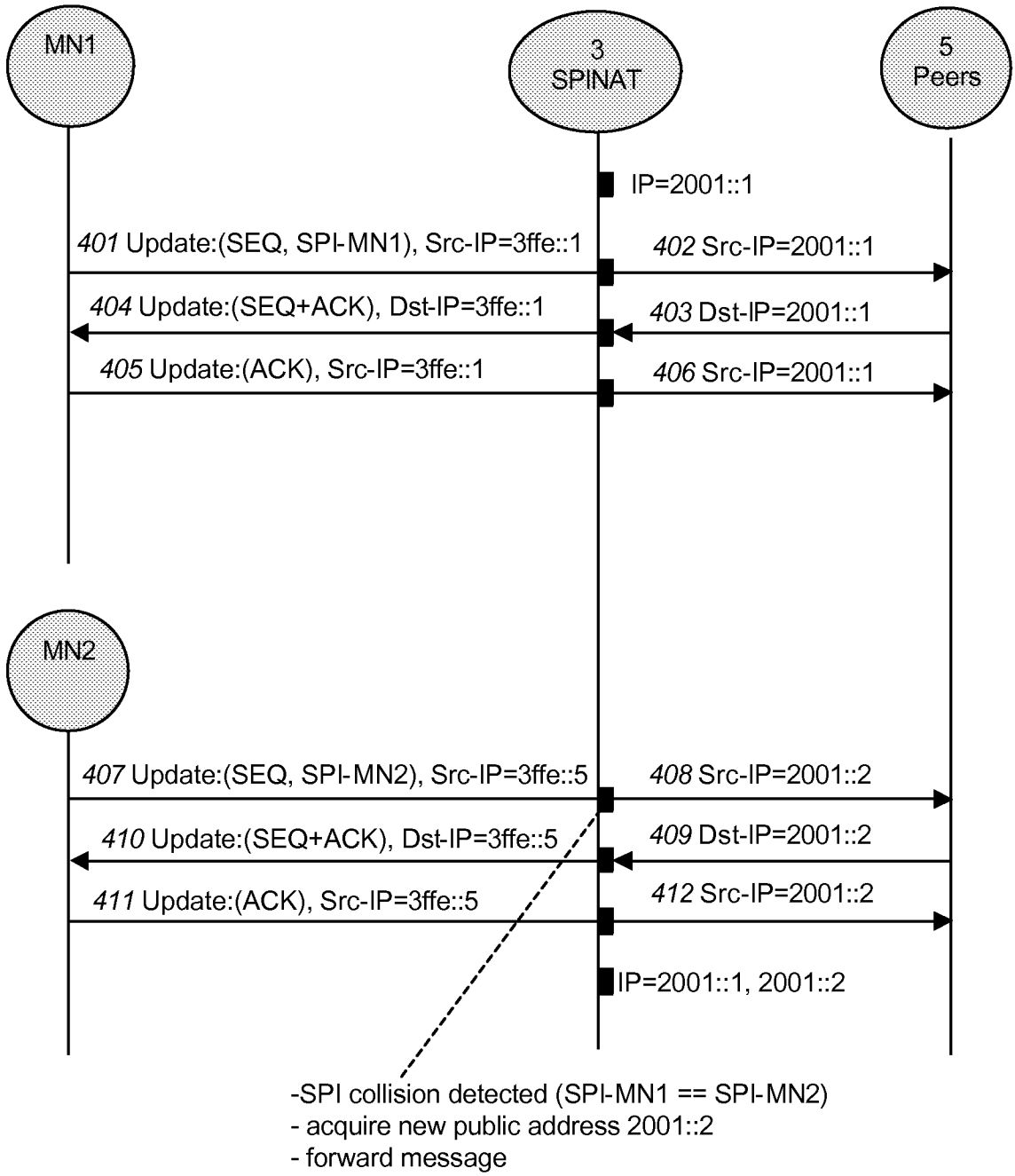

MN1
3
SPINAT
5
Peers
IP=2001::1
401 Update:(SEQ, SPI-MN1), Src-IP=3ffe::1
402 Src-IP=2001::1
404 Update:(SEQ+ACK), Dst-IP=3ffe::1
403 Dst-IP=2001::1
405 Update:(ACK), Src-IP=3ffe::1
406 Src-IP=2001::1
MN2
407 Update:(SEQ, SPI-MN2), Src-IP=3ffe::5
408 Src-IP=2001::2
410 Update:(SEQ+ACK), Dst-IP=3ffe::5
409 Dst-IP=2001::2
411 Update:(ACK), Src-IP=3ffe::5
412 Src-IP=2001::2
IP=2001::1, 2001::2
-SPI collision detected (SPI-MN1 == SPI-MN2)
- acquire new public address 2001::2
- forward message

Figure 4

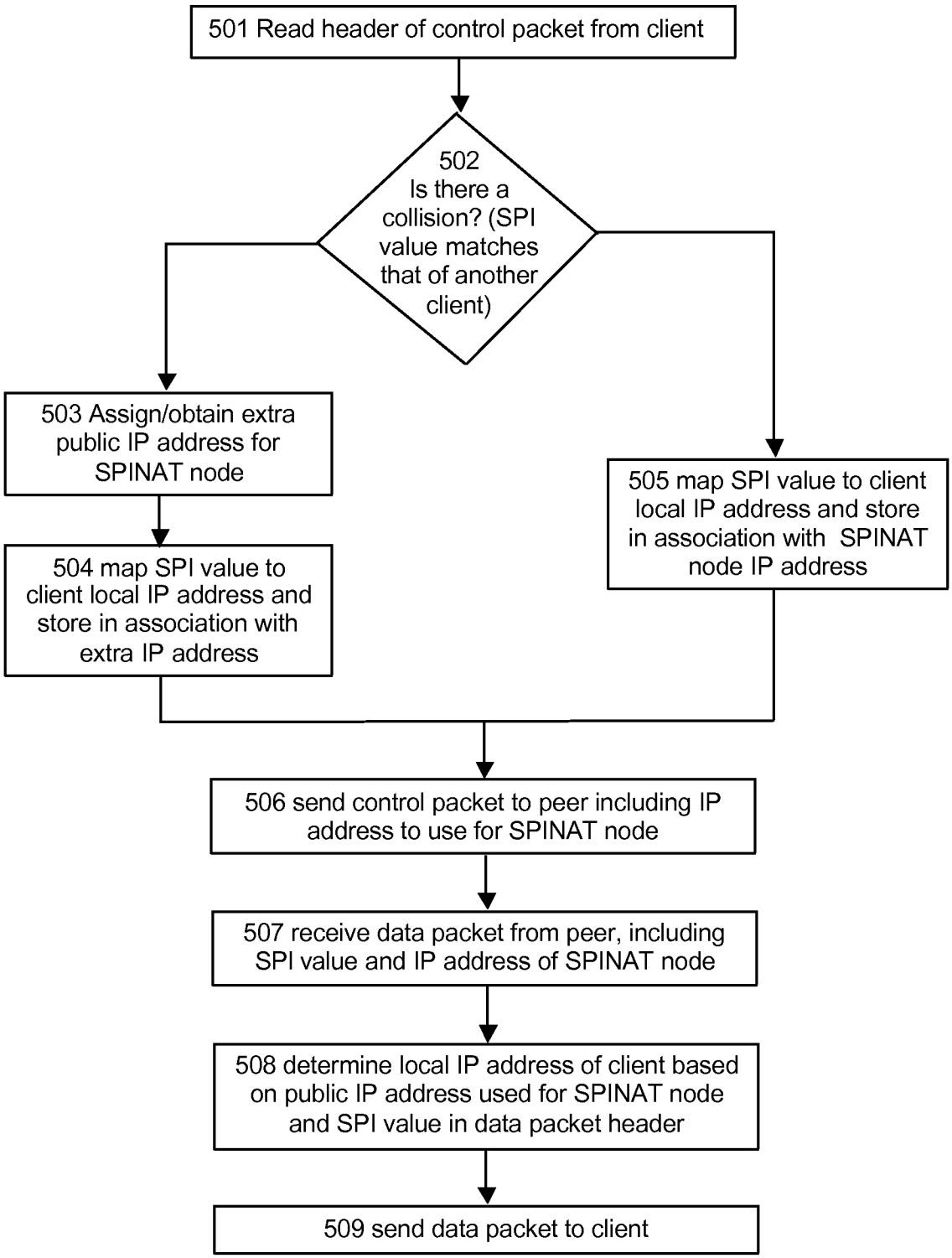

501 Read header of control packet from client
502 Is there a collision? (SPI value matches that of another client)
503 Assign/obtain extra public IP address for SPINAT node
504 map SPI value to client local IP address and store in association with extra IP address
505 map SPI value to client local IP address and store in association with SPINAT node IP address
506 send control packet to peer including IP address to use for SPINAT node
507 receive data packet from peer, including SPI value and IP address of SPINAT node
508 determine local IP address of client based on public IP address used for SPINAT node and SPI value in data packet header
509 send data packet to client

Figure 5

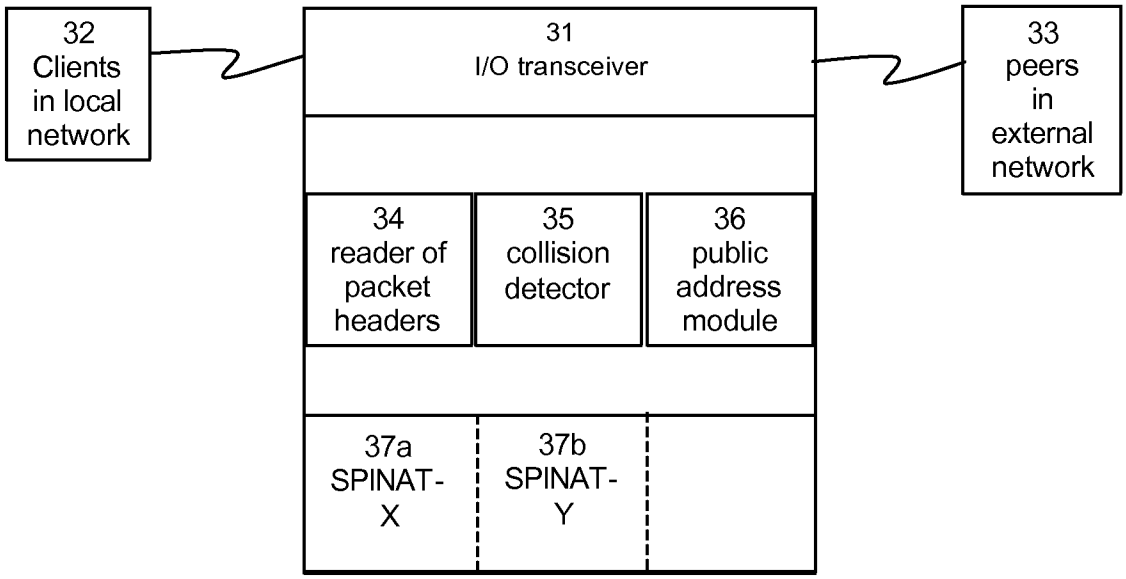

32
Clients
in local
network
31
I/O transceiver
33
peers
in
external
network
34
reader of
packet
headers
35
collision
detector
36
public
address
module
37a
SPINAT-
X
37b
SPINAT-
Y

Figure 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/063687

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06

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)
H04L

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, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SARELA M ET AL: "Applying host identity protocol to tactical networks" MILITARY COMMUNICATIONS CONFERENCE, 2004. MILCOM 2004. 2004 IEEE MONTEREY, CA, USA 31 OCT. - 3 NOV. 2004, PISCATAWAY, NJ, USA,IEEE, vol. 2, 31 October 2004 (2004-10-31), pages 834-840, XP010825757 ISBN: 978-0-7803-8847-5 page 838	1-15

-/--

[X] 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 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
4 December 2008	11/12/2008

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, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/063687

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	YLITALO J ET AL: "SPINAT: Integrating IPsec into Overlay Routing" SECURITY AND PRIVACY FOR EMERGING AREAS IN COMMUNICATIONS NETWORKS, 20 05. SECURECOMM 2005. FIRST INTERNATIONAL CONFERENCE ON ATHENS, GREECE 05-09 SEPT. 2005, PISCATAWAY, NJ, USA,IEEE, 5 September 2005 (2005-09-05), pages 315-326, XP010902901 ISBN: 978-0-7695-2369-9 page 318 - page 320 -----	1-15