



(51) International Patent Classification:

H04W 12/02 (2009.01) *H04W 76/02* (2009.01)
H04L 29/06 (2006.01) *H04W 92/20* (2009.01)

(21) International Application Number:

PCT/EP2015/054825

(22) International Filing Date:

9 March 2015 (09.03.2015)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: **NOKIA SOLUTIONS AND NETWORKS OY** [FI/FI]; Karaportti 3, FI-02610 Espoo (FI).

(72) Inventors: **FREY, Jan**; Sophienstr. 30, 48145 Münster (DE). **DEISS, Thomas**; Berninghausstr. 88, 44625 Herne (DE).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: DYNAMIC SETUP OF SECURE COMMUNICATION

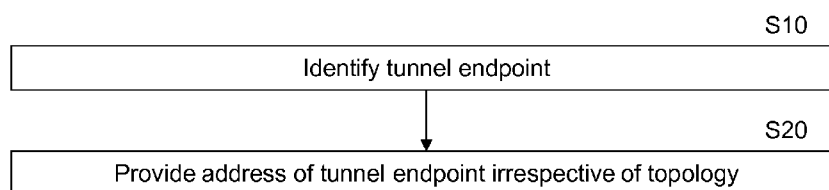


Fig. 3

(57) Abstract: It is provided a method, comprising identifying a first tunnel endpoint a communication device should use for securely communicating with an apparatus performing the method; providing an address of the first tunnel endpoint to the communication device, regardless of whether the address of the first tunnel endpoint is an address of the apparatus or an address of a gateway different from the apparatus.

Dynamic setup of secure communication

Field of the invention

5 The present invention relates to an apparatus, a method, and a computer program product related to secure communication. More particularly, the present invention relates to an apparatus, a method, and a computer program product related to dynamic setup of secure communication.

10

Abbreviations

	3GPP	3rd Generation Partnership Project
	BTS	Base Transceiver Station
15	CA	Carrier Aggregation
	CoMP	Coordinated MultiPoint (transmission)
	eCoMP	enhanced CoMP
	EDGE	Enhanced Data rates for GSM Evolution
	eNB	eNodeB
20	EPC	Evolved Packet Core
	E-UTRAN	Evolved UTRAN
	GPRS	Generic Packet Radio Service
	GSM	Global System for Mobile Communication
	IE	Information Element (ASN.1 term)
25	IETF	Internet Engineering Task Force
	IP	Internet Protocol
	IPsec	IP Security
	LTE	Long Term Evolution
	LTE-A	LTE Advanced
30	MME	Mobility Management Entity
	Rel	Release

RTT Round Trip Time

S1AP S1 Application Protocol

TLA Transport Layer Address (e.g.: an IP address)

5 TLS Transport Layer Security (a security protocol by the IETF)

TS Technical Specification

UMTS Universal Mobile Telecommunications System

UTRAN UMTS Terrestrial Radio Access Network

WiFi Wireless Fidelity

10 WLAN Wireless Local Area Network

X2AP X2 Application Protocol

Background of the invention

15 This application may relate to backhaul networks for LTE (E-UTRAN) deployments. For example, it may affect the inter-eNB connections (i.e. direct connection between neighbour base stations), the so-called X2 links. Two different network topologies/architectures are available, namely "X2 star" and
20 "X2 mesh". While the first one represents a more simple network architecture, basically by routing all inter-eNB traffic up to a central location and distributing it back from there (hub-and-spoke architecture), it is lacking performance for these connections due to the longer path.
25 Contrary, X2 mesh implements direct connections between the eNB, thus potentially offering reduced latency and higher capacity - at the cost of a more complex installation/configuration.

30 By adding IPsec for transport security to the scenario, the deployment of "X2 mesh" becomes even more complex, as it

requires dynamic management of IPsec tunnels between neighbouring base stations, while with X2 star a single IPsec tunnel from each eNB to a (central) security gateway is sufficient. In the context of the present application, a security gateway terminates the IPsec tunnel from a communication device such as an eNB, and may relay the communication to another IPsec tunnel to another communication device which is terminated at the security gateway, too. Thus, the security gateway enables secure communication between two communication devices via two IPsec tunnels which are terminated at the security gateway. The communication between the two communication devices may be via more than two IPsec tunnels if more than one security gateway is involved. In this case, there is a respective IPsec tunnel from the first communication device to the first security gateway, from there to the second security gateway, (from there to the third security gateway,...,) and from there to the second communication device.

Fig. 1 shows an example network deployment with IPsec tunnels. In Fig. 1, three eNBs 1001, 1002, and 1003 are shown. By physical layer connections (shown by thin solid lines), they are connected to a router 1011, such as a cell site router. A local security gateway 1012 is connected to the router 1011. The router 1011 is connected to the EPC 1040 (including MME) via a backhaul network 1020 and the corresponding edge router 1031. A central security gateway 1032 is connected on the physical layer to the edge router 1031.

The S1 connection between eNB 1001 and EPC 1040 is realized by connecting the eNB to the central security gateway 1032 by an IPsec tunnel 1a. The central security gateway 1032 may be

connected to the EPC 1040 by another IPsec tunnel (not shown). Alternatively, the central security gateway 1032 may be connected to the EPC by an unsecured connection (not shown), in particular, if the central security gateway and the EPC are both in the protected domain of the operator. I.e., the S1 connection between eNB 1001 and EPC 1040 is realized by two connections which are both terminated by the central security gateway 1032, which relays traffic from IPsec tunnel 1a to the connection to the EPC. In a conventional X2 star deployment (i.e. an X2 deployment in star topology), IPsec tunnel 1a between eNB 1001 and central security gateway 1032 is also used for X2 connections of eNB 1001. As an example, in Fig. 1, eNB 1004 (which is not connected to router 1011), has an IPsec tunnel 1b to the central security gateway, which is used for both its S1 connection and its X2 connection. Thus, eNB 1001 may communicate securely with eNB 1004 via IPsec tunnels 1a and 1b, and the communication is relayed between the tunnels 1a and 1b by the central security gateway 1032.

An example of a conventional X2 mesh deployment (i.e., an X2 deployment in mesh topology) is shown by X2 link between eNBs 1002 and 1003. The corresponding IPsec tunnel 2 runs directly between the two eNB 1002 and 1003. Within the present application, "directly" means that the IPsec tunnel is not interrupted (i.e., not terminated between the "directly" communicating entities); the physical layer connection may run via other network elements such as router 1011, as shown.

The X2 link between eNBs 1001 and 1003 combines advantages of X2 mesh and star topology. It runs over IPsec tunnel 3a between eNB 1001 and the local security gateway 1012, and IPsec tunnel 3b between local security gateway 1012 and eNB 1003. Both IPsec tunnels 3a and 3b are terminated at the local security gateway 1012 which relays traffic from one of

these tunnels to the other. Thus, performance and capacity are similar to X2 mesh topology, while the configuration simplicity and resource utilization (in particular as regards the number of IPsec tunnels) is comparable to X2 star topology. Note that, in general, cell site routers and local security gateways are expected to provide sufficient IPsec performance for all X2 traffic.

When IPsec is not in use, the implementation of X2 star vs. X2 mesh merely turns into routing configuration discussion - basically without any real impact on the end points (most of all eNBs). In such scenarios, it is trivial to configure network routers in a way that packets are routed on a short(est) path between eNBs instead of traversing the network up to a central hub such as the central security gateway 1032. However, this scenario cannot simply be applied for IPsec based deployments.

Regarding the selection of IPsec endpoints for X2 interfaces, either X2-star (using the same tunnel as S1 interface) or full X2-mesh (dedicated tunnel for each pair of eNBs) may be configured automatically (see 3GPP TS 36.413).

Summary of the invention

It is an object of the present invention to improve the prior art.

According to a first aspect of the invention, there is provided an apparatus, comprising identifying means adapted to identify a first tunnel endpoint a communication device should use for securely communicating with the apparatus; providing means adapted to provide an address of the first tunnel endpoint to the communication device, regardless of

whether the address of the first tunnel endpoint is an address of the apparatus or an address of a gateway different from the apparatus.

- 5 The providing means may be adapted to provide an address of the apparatus as the address of the first tunnel endpoint to the communication device if the identifying means identifies that the communication device should communicate securely directly with the apparatus.

10

The apparatus may further comprise first distance determining means adapted to determine a geographical distance to the communication device; wherein the identifying means is adapted to identify the tunnel end point based on the
15 geographical distance.

15

The first distance determining means may be adapted to determine the geographical distance based on a received information of a geographical location of the communication
20 device.

20

The apparatus may further comprise first roundtrip time determining means adapted to determine a total roundtrip time to the communication device; wherein the identifying means
25 may be adapted to identify the tunnel end point based on the total roundtrip time.

25

The apparatus may further comprise roundtrip time measuring means adapted to measure a first roundtrip time between the
30 apparatus and the first tunnel endpoint; wherein the first roundtrip time determining means may be adapted to determine the total roundtrip time based on the first roundtrip time

30

and a received information on a second roundtrip time between the communication device and the first tunnel endpoint.

The apparatus may further comprise first traffic determining means adapted to determine a previous traffic between the communication device and the apparatus; wherein the identifying means may be adapted to identify the tunnel endpoint based on the previous traffic.

The identifying means may be adapted to identify plural tunnel endpoints including the first tunnel endpoint, wherein the communication device should use one of the plural tunnel endpoints for the securely communicating with the apparatus; the providing means may be adapted to provide addresses of the plural tunnel endpoints to the communication device.

The apparatus may further comprise deciding means adapted to decide on a respective priority for each of the plural tunnel endpoints, wherein the providing means may be adapted to provide the respective priority along with the address of each of the plural tunnel endpoints.

The apparatus may further comprise second distance determining means adapted to determine a geographical distance to the communication device; wherein the deciding means may be adapted to decide on the priorities based on the geographical distance.

The apparatus may further comprise second roundtrip time determining means adapted to determine a respective total roundtrip time to the communication device for each of the plural tunnel endpoints; wherein the deciding means may be

adapted to decide on the priorities based on the respective total roundtrip times.

The apparatus may further comprise second traffic determining means adapted to determine a previous traffic between the communication device and the apparatus; wherein the deciding means may be adapted to decide on the priorities based on the previous traffic.

According to a second aspect of the invention, there is provided an apparatus, comprising determining means adapted to determine a first address of plural received addresses of respective tunnel endpoints, wherein the plural received addresses of the tunnel endpoints are received in one or more messages indicating that one of the tunnel endpoints should be used for securely communicating with a communication device; establishing means adapted to establish a first tunnel to a first tunnel endpoint of the tunnel endpoints for securely communicating with the communication device, wherein the first tunnel endpoint has the determined first address.

The determining means may be adapted to determine the first address based on received priorities for the plural received addresses.

25

The apparatus may further comprise monitoring means adapted to monitor if the establishing of the first tunnel fails; wherein the determining means may be adapted to determine, if the establishing of the first tunnel fails, a second address of the plural received addresses different from the first address; and the establishing means may be adapted to establish, if the establishing of the first tunnel fails, a second tunnel to a second tunnel endpoint of the tunnel

endpoints for securely communicating with the communication device, wherein the second tunnel endpoint has the determined second address.

- 5 The determining means may be adapted to determine the second address based on the received priorities.

The apparatus may further comprise location providing means adapted to provide an information on a geographical location
10 of the apparatus in response to a first configuration request.

The apparatus may further comprise roundtrip time measuring means adapted to measure a roundtrip time between the
15 apparatus and the first tunnel endpoint; roundtrip time providing means adapted to provide an information on the roundtrip time in response to a second configuration request.

The apparatus may further comprise comparing means adapted to
20 compare the first address with an address of an established tunnel endpoint of an established tunnel for securely communicating with an endpoint device; inhibiting means adapted to inhibit the establishing of the first tunnel different from the established tunnel if the first address
25 corresponds to the address of the established tunnel endpoint.

According to a third aspect of the invention, there is provided an apparatus, comprising comparing means adapted to
30 compare a received address of a first tunnel endpoint with an address of an established tunnel endpoint of an established tunnel for securely communicating with a communication device, wherein the received address of the first tunnel

endpoint is received in a message indicating that a first tunnel to the first tunnel endpoint should be established for securely communicating with a first communication device; inhibiting means adapted to inhibit establishing the first
5 tunnel different from the established tunnel if the received address corresponds to the address of the established tunnel endpoint.

According to a fourth aspect of the invention, there is
10 provided a base station apparatus, comprising base station means adapted to provide a base station functionality of a radio access technology; communicating means adapted to communicate securely with a base station device for providing the base station functionality; and an apparatus according to
15 any of the first to third aspects, wherein the base station device comprises the communication device; and the communicating means is adapted to use the first tunnel endpoint for the securely communicating with the base station device.

20
According to a fifth aspect of the invention, there is provided an apparatus, comprising identifying circuitry configured to identify a first tunnel endpoint a communication device should use for securely communicating
25 with the apparatus; providing circuitry configured to provide an address of the first tunnel endpoint to the communication device, regardless of whether the address of the first tunnel endpoint is an address of the apparatus or an address of a gateway different from the apparatus.

30
The providing circuitry may be configured to provide an address of the apparatus as the address of the first tunnel endpoint to the communication device if the identifying

circuitry identifies that the communication device should communicate securely directly with the apparatus.

The apparatus may further comprise first distance determining circuitry configured to determine a geographical distance to the communication device; wherein the identifying circuitry is configured to identify the tunnel end point based on the geographical distance.

10 The first distance determining circuitry may be configured to determine the geographical distance based on a received information of a geographical location of the communication device.

15 The apparatus may further comprise first roundtrip time determining circuitry configured to determine a total roundtrip time to the communication device; wherein the identifying circuitry may be configured to identify the tunnel end point based on the total roundtrip time.

20

The apparatus may further comprise roundtrip time measuring circuitry configured to measure a first roundtrip time between the apparatus and the first tunnel endpoint; wherein the first roundtrip time determining circuitry may be configured to determine the total roundtrip time based on the first roundtrip time and a received information on a second roundtrip time between the communication device and the first tunnel endpoint.

30 The apparatus may further comprise first traffic determining circuitry configured to determine a previous traffic between the communication device and the apparatus; wherein the

identifying circuitry may be configured to identify the tunnel end point based on the previous traffic.

5 The identifying circuitry may be configured to identify plural tunnel endpoints including the first tunnel endpoint, wherein the communication device should use one of the plural tunnel endpoints for the securely communicating with the apparatus; the providing circuitry may be configured to provide addresses of the plural tunnel endpoints to the
10 communication device.

The apparatus may further comprise deciding circuitry configured to decide on a respective priority for each of the plural tunnel endpoints, wherein the providing circuitry may
15 be configured to provide the respective priority along with the address of each of the plural tunnel endpoints.

The apparatus may further comprise second distance determining circuitry configured to determine a geographical
20 distance to the communication device; wherein the deciding circuitry may be configured to decide on the priorities based on the geographical distance.

The apparatus may further comprise second roundtrip time determining circuitry configured to determine a respective
25 total roundtrip time to the communication device for each of the plural tunnel endpoints; wherein the deciding circuitry may be configured to decide on the priorities based on the respective total roundtrip times.

30

The apparatus may further comprise second traffic determining circuitry configured to determine a previous traffic between the communication device and the apparatus; wherein the

deciding circuitry may be configured to decide on the priorities based on the previous traffic.

According to a sixth aspect of the invention, there is
5 provided an apparatus, comprising determining circuitry
configured to determine a first address of plural received
addresses of respective tunnel endpoints, wherein the plural
received addresses of the tunnel endpoints are received in
one or more messages indicating that one of the tunnel
10 endpoints should be used for securely communicating with a
communication device; establishing circuitry configured to
establish a first tunnel to a first tunnel endpoint of the
tunnel endpoints for securely communicating with the
communication device, wherein the first tunnel endpoint has
15 the determined first address.

The determining circuitry may be configured to determine the
first address based on received priorities for the plural
received addresses.

20

The apparatus may further comprise monitoring circuitry
configured to monitor if the establishing of the first tunnel
fails; wherein the determining circuitry may be configured to
determine, if the establishing of the first tunnel fails, a
25 second address of the plural received addresses different
from the first address; and the establishing circuitry may be
configured to establish, if the establishing of the first
tunnel fails, a second tunnel to a second tunnel endpoint of
the tunnel endpoints for securely communicating with the
30 communication device, wherein the second tunnel endpoint has
the determined second address.

The determining circuitry may be configured to determine the second address based on the received priorities.

5 The apparatus may further comprise location providing circuitry configured to provide an information on a geographical location of the apparatus in response to a first configuration request.

10 The apparatus may further comprise roundtrip time measuring circuitry configured to measure a roundtrip time between the apparatus and the first tunnel endpoint; roundtrip time providing circuitry configured to provide an information on the roundtrip time in response to a second configuration request.

15 The apparatus may further comprise comparing circuitry configured to compare the first address with an address of an established tunnel endpoint of an established tunnel for securely communicating with an endpoint device; inhibiting
20 circuitry configured to inhibit the establishing of the first tunnel different from the established tunnel if the first address corresponds to the address of the established tunnel endpoint.

25 According to a seventh aspect of the invention, there is provided an apparatus, comprising comparing circuitry configured to compare a received address of a first tunnel endpoint with an address of an established tunnel endpoint of an established tunnel for securely communicating with a
30 communication device, wherein the received address of the first tunnel endpoint is received in a message indicating that a first tunnel to the first tunnel endpoint should be established for securely communicating with a first

communication device; inhibiting circuitry configured to inhibit establishing the first tunnel different from the established tunnel if the received address corresponds to the address of the established tunnel endpoint.

5

According to a eighth aspect of the invention, there is provided a base station apparatus, comprising base station circuitry configured to provide a base station functionality of a radio access technology; communicating circuitry configured to communicate securely with a base station device for providing the base station functionality; and an apparatus according to any of the fifth to seventh aspects, wherein the base station device comprises the communication device; and the communicating circuitry is configured to use the first tunnel endpoint for the securely communicating with the base station device.

According to a ninth aspect of the invention, there is provided a method, comprising identifying a first tunnel endpoint a communication device should use for securely communicating with an apparatus performing the method; providing an address of the first tunnel endpoint to the communication device, regardless of whether the address of the first tunnel endpoint is an address of the apparatus or an address of a gateway different from the apparatus.

The providing may comprise providing an address of the apparatus as the address of the first tunnel endpoint to the communication device if it is identified that the communication device should communicate securely directly with the apparatus.

The method may further comprise determining a geographical distance to the communication device; wherein the tunnel end point is identified based on the geographical distance.

- 5 The geographical distance may be determined based on a received information of a geographical location of the communication device.

The method may further comprise determining a total roundtrip
10 time to the communication device; wherein the tunnel end point is identified based on the total roundtrip time.

The method may further comprise measuring a first roundtrip time between the apparatus and the first tunnel endpoint;
15 wherein the total roundtrip time may be determined based on the first roundtrip time and a received information on a second roundtrip time between the communication device and the first tunnel endpoint.

20 The method may further comprise determining a previous traffic between the communication device and the apparatus; wherein the tunnel end point may be identified based on the previous traffic.

25 The method may further comprise identifying plural tunnel endpoints including the first tunnel endpoint, wherein the communication device should use one of the plural tunnel endpoints for the securely communicating with the apparatus; providing addresses of the plural tunnel endpoints to the
30 communication device.

The method may further comprise deciding on a respective priority for each of the plural tunnel endpoints, and

providing the respective priority along with the address of each of the plural tunnel endpoints.

5 The method may further comprise determining a geographical distance to the communication device; and deciding on the priorities based on the geographical distance.

10 The method may further comprise determining a respective total roundtrip time to the communication device for each of the plural tunnel endpoints; and deciding on the priorities based on the respective total roundtrip times.

15 The method may further comprise determining a previous traffic between the communication device and the apparatus; and deciding on the priorities based on the previous traffic.

20 According to a tenth aspect of the invention, there is provided a method, comprising determining a first address of plural received addresses of respective tunnel endpoints, wherein the plural received addresses of the tunnel endpoints are received in one or more messages indicating that one of the tunnel endpoints should be used for securely communicating with a communication device; establishing a first tunnel to a first tunnel endpoint of the tunnel endpoints for securely communicating with the communication device, wherein the first tunnel endpoint has the determined first address.

25 The method may further comprise determining the first address based on received priorities for the plural received addresses.

The method may further comprise monitoring if the establishing of the first tunnel fails; determining, if the establishing of the first tunnel fails, a second address of the plural received addresses different from the first address; and establishing, if the establishing of the first tunnel fails, a second tunnel to a second tunnel endpoint of the tunnel endpoints for securely communicating with the communication device, wherein the second tunnel endpoint has the determined second address.

The determining of the second address may be based on the received priorities.

The method may further comprise providing an information on a geographical location of an apparatus performing the method in response to a first configuration request.

The method may further comprise measuring a roundtrip time between an apparatus performing the method and the first tunnel endpoint; providing an information on the roundtrip time in response to a second configuration request.

The method may further comprise comparing the first address with an address of an established tunnel endpoint of an established tunnel for securely communicating with an endpoint device; inhibiting the establishing of the first tunnel different from the established tunnel if the first address corresponds to the address of the established tunnel endpoint.

According to an eleventh aspect of the invention, there is provided a method, comprising comparing a received address of a first tunnel endpoint with an address of an established

tunnel endpoint of an established tunnel for securely communicating with a communication device, wherein the received address of the first tunnel endpoint is received in a message indicating that a first tunnel to the first tunnel endpoint should be established for securely communicating with a first communication device; inhibiting establishing the first tunnel different from the established tunnel if the received address corresponds to the address of the established tunnel endpoint.

Each of the methods of the ninth to eleventh aspects may be a method of dynamic setup of secure communication.

According to a twelfth aspect of the invention, there is provided a computer program product comprising a set of instructions which, when executed on an apparatus, is configured to cause the apparatus to carry out the method according to any of the ninth to eleventh aspects. The computer program product may be embodied as a computer-readable medium or directly loadable into a computer.

According to some embodiments of the invention, at least the following advantages are provided:

- short latency times may be realized when and where needed;
- low hardware requirements on eNB side;
- the solution may be backwards compatible for the interfaces;
- the number of established IPsec tunnels may be minimized for the desired X2 configuration;
- reliability of the network deployment is enhanced;
- higher user satisfaction;

- load on central security gateway is reduced; and
- manual administration effort may be alleviated or eliminated.

5 It is to be understood that any of the above modifications can be applied singly or in combination to the respective aspects to which they refer, unless they are explicitly stated as excluding alternatives.

10 Brief description of the drawings

Further details, features, objects, and advantages are apparent from the following detailed description of the preferred embodiments of the present invention which is to be
15 taken in conjunction with the appended drawings, wherein

Fig. 1 shows an example network deployment with IPsec tunnels;

Fig. 2 shows an apparatus according to an embodiment of the
20 invention;

Fig. 3 shows a method according to an embodiment of the invention;

Fig. 4 shows an apparatus according to an embodiment of the invention;

25 Fig. 5 shows a method according to an embodiment of the invention;

Fig. 6 shows an apparatus according to an embodiment of the invention;

Fig. 7 shows a method according to an embodiment of the
30 invention; and

Fig. 8 shows an apparatus according to an embodiment of the invention.

Detailed description of certain embodiments

35

Herein below, certain embodiments of the present invention are described in detail with reference to the accompanying drawings, wherein the features of the embodiments can be freely combined with each other unless otherwise described.

5 However, it is to be expressly understood that the description of certain embodiments is given for by way of example only, and that it is by no way intended to be understood as limiting the invention to the disclosed details.

10 Moreover, it is to be understood that the apparatus is configured to perform the corresponding method, although in some cases only the apparatus or only the method are described.

15 In backhaul networks based on X2 mesh architecture, the deployment of IPsec introduces several challenges for the overall network operation:

20 1. IPsec consumes significant resources in the endpoints (namely the two eNB terminating the X2 link). Based on the eNB type (and implementation) it is obvious, that in some cases the resources might be strictly limited (especially in eNB tailored for small cells) and an eNB
25 might not be able to establish another X2 link due to missing IPsec resources (even while all other resources needed, e.g. in the control plane processing, might still be available). A simple example for such resource constraints is the number of supported IPsec policies in
30 a certain eNB.

2. When an IPsec enabled X2 link fails to establish on the IPsec layer (that means, the tunnel does not come up), the requestor of the tunnel does not get any information

about why this process failed. This is an inherent issue of the IPsec approach, as without the tunnel no information can be transferred.

5 3. In some network scenarios, it may be desirable to implement a mixture of X2 star and X2 mesh deployments. For example, an X2 mesh topology might be employed only for X2 links considered important in general. In order to avoid huge impact on end user services, the operator
10 could also deploy an additional security gateway which is more local to the BTS site ("local" security gateway), such as local security gateway 1012 shown in Fig. 1. Note that, according to some embodiments of the invention, the local security gateway may be used as a
15 fallback in case no direct connections between the eNB could be established anymore (e.g. due to lack of processing resources).

In today's LTE networks, the X2 connections are receiving
20 minor attention, as they are used only for handover scenarios in a rather limited way. X2 mesh deployments might not be needed at all at this stage. However, based on upcoming LTE-A features (e.g., inter-eNB Carrier Aggregation/Dual Connectivity and eCoMP), communication via X2 will
25 dramatically increase and rather stringent performance requirements will apply (e.g., max. latency target between two eNBs is 5ms, which includes IPsec processing as well as the transmission delay in the transport network). Thus, efficient (but still secure) X2 links will be required in the
30 near future.

When a limited number of secured X2-mesh connections are possible only, it has to be decided for each eNB to which other eNB a secured X2-mesh connection is to be established.

Preferably, eNBs establish those X2-mesh links for which the benefit is largest compared to an X2-star link. For example, the benefit may be large for eNBs with high traffic volumes among them or where latency can be reduced most. Depending on
5 criteria, different X2-links might be the most suitable ones. In addition, operators might want to choose their preferred criteria.

Conventionally, a partial X2-mesh network (some eNBs are
10 connected directly to the eNB under consideration, while other eNBs are connected via one or more security gateways), the respective used X2 IPsec endpoints (i.e. the respective IPsec tunnel configurations) have to be configured manually, which is impractical and error prone. For example, on IPsec
15 level, one eNB may be connected directly to a first group of eNBs, via a local security gateway to a second group of eNBs, and via a central security gateway to a third group of eNBs.

According to some embodiments of the invention, S1 messages
20 are used to convey information from a first eNB (source eNB) to a second eNB (target eNB) whether it wants to communicate securely with the second eNB in a star configuration (via a security gateway) or directly (mesh or partial mesh configuration). Namely, the second eNB can get information of
25 the first eNB over the backhaul by using the S1-AP eNB configuration transfer procedure (from the first eNB to MME) and the S1-AP MME configuration transfer procedure (from MME to the second eNB).

Conventionally (see 3GPP TS 36.413, v 12.4.0, sections 8.15
30 and 8.16), the eNB configuration transfer message and MME configuration transfer message may comprise an IE IPsecTLA indicating the IP address of the tunnel endpoint to be used for X2 communication with the first eNB. If the second eNB is
35 configured to use the same IPsec tunnel for S1 and X2

communication (X2 star configuration according to tunnels 1a and 1b in Fig. 1), IE IPsecTLA is ignored.

According to some embodiments of the invention, the configuration transfer messages are not modified but differently interpreted by the eNBs. In case of an intended direct X2 communication (X2 mesh configuration or X2 partial mesh configuration), eNB fills its own IP address into the IPsecTLA address field. In case of an intended X2 communication via a security gateway (X2 star configuration or partial X2 mesh configuration), it fills the IP address of the respective security gateway into the IP address field. Thus, the first eNB may also select between different security gateways such as the local security gateway 1012 and the central security gateway 1032 of Fig. 1.

According to these embodiments of the invention, the second eNB establishes an IPsec tunnel to the address indicated in IPsecTLA.

According to some of these embodiments of the invention, the second eNB first checks if the IP address of the IPsecTLA is already used as tunnel endpoint. In this case, it refrains from establishing a new IPsec tunnel but uses the existing tunnel for X2 communication with the first eNB. Thus, establishment of another IPsec tunnel is avoided.

According to some embodiments of the invention, the eNB configuration transfer message and MME configuration transfer message may comprise plural IP addresses of tunnel endpoints (either in one modified IE IPsecTLA or in plural IEs, depending on the implementation). This allows specifying some or all the viable communication options per eNB. Consequently, the receiving eNB is enabled to choose from the offered IP address a most suitable option (e.g. based on

available resources, and/or based on the needs, and/or the current network status).

These embodiments allow for flexible X2 link creation that gives the eNBs the choice between resource consuming (but efficient) X2 mesh connections and simple (but less performant) X2 star connections for each X2 link to be established. The selection can be based on dynamic runtime information and does not have to be pre-configured by the operator.

The first eNB may also associate a priority with the signalled options. The second eNB may take these priorities into account when selecting the option for the secure communication with the first eNB. Priorities may be indicated in several different ways. E.g., they may be indicated by priority values, or they may be indicated implicitly by the sequence of the IP addresses in the configuration transfer messages.

In addition, if plural IP addresses are indicated, fallback mechanisms to mitigate (temporary) network failures can be implemented. For example, the target eNB may select one of the options and try to establish the corresponding IPsec tunnel. If this fails, it may select another option and try to establish the corresponding IPsec tunnel etc., until it succeeds or until it has tried all options. Also in this case, the communicated priorities may be taken into account for determining the sequence, according to which the options are tried.

For example, if a direct tunnel among two eNBs could not be established, the two eNBs could still establish a tunnel via the central security gateway. As another example, the two eNBs might fallback from the use of a local security gateway

to a central one, or from the use of a local (or central) security gateway to a direct connection.

Candidate sets for X2-mesh links (X2-star links) and also the preferred security gateways in case of a X2 star configuration may change over time. In case of such a change, a source eNB may use MME/eNB Configuration Transfer messages to indicate changed IP addresses to one or more other eNBs (peers). Thus, e.g. the source eNB may indicate that the X2-link has to be changed from X2-mesh to X2-star or vice versa, or from one security gateway to another security gateway. However, as each such change may interrupt the X2 link shortly, changes in the X2-links should be done rarely, i.e. more on a daily than on an hourly or minutely time scale.

Both eNBs of an X2 link may use one or more of the several criteria for X2 link configuration. More in detail, the source eNB may use one or more of these criteria to determine the tunnel endpoint in case it provides only one IP address of an IPsec tunnel endpoint in the configuration transfer message, In case the source eNB provides plural IP addresses of tunnel endpoints in the configuration transfer message, the same criteria may be used to determine the respective priorities, which may be provided to the target eNB.

On the other hand, the target eNB may use one or more of the several criteria to select one of the offered IP address options if the source eNB provides plural IP addresses of plural IPsec tunnel endpoints.

Some example criteria which may be used will be discussed at greater detail hereinafter. Namely, one, some, or all of the following criteria may be applied:

1. geographical distance between the eNBs;
2. round trip time between the eNBs;

3. capability of inter eNB carrier aggregation and/or eCoMP;
4. previous X2 traffic between the eNBs;
5. current network conditions; and
- 5 6. operator configured priorities.

The considered criteria may be combined in one metric. Respective weights may be associated to each of the considered criteria.

10

As regards criterion 1, in general, co-located or closely located eNBs are expected to have low X2-latency. Thus, they are typically well suited for X2-mesh links.

- 15 In order to determine the geographical distance, according to some embodiments of the invention, one eNB requests the other eNB to provide its geographical location. Such request and the corresponding response may be conveyed by the S1 configuration transfer messages, which are to be enhanced
- 20 over nowadays 3GPP standards. The receiving eNB may then calculate the geographical distance from its known own position and the received location information.

As regards criterion 2, it might be worth to establish an X2-mesh link where the X2-star latencies are too large. An eNB (source eNB) might request another one (target eNB) to provide the RTT among the target eNB and the security gateway in an X2-star topology. The source eNB can combine this information with own information on RTTs among the source eNB

30 and the X2-star security gateway and (if available) the RTT among source eNB and target eNB to determine the benefit of using X2-mesh instead of X2-star.

For example, each of source eNB and target eNB may measure

35 RTT between itself and the security gateway. Target eNB

provides information on this RTT to source eNB, and source eNB calculates an approximate RTT between itself and target eNB in the star configuration by adding these RTTs. In addition, if available, it may compare the calculated RTT in
5 the star configuration with one or both of a measured RTT between itself and the target eNB in star configuration and a mesh configuration.

For example, mesh configuration may be prioritized only if
10 the gain of RTT is at least a certain percentage of the RTT of the mesh configuration. As another example, mesh configuration is prioritized only if a certain latency requirement can be fulfilled in mesh configuration but not in star configuration.

15 The request for information on RTT and the information on RTT may be conveyed by the S1 configuration transfer messages, which are to be enhanced over nowadays 3GPP standards.

20 As regards criterion 3, for carrier aggregation and/or eCoMP (e.g. of Release 12) quite stringent latency requirements for the X2 traffic are expected, which might be difficult to fulfill for inter-eNB carrier aggregation / inter-eNB eCoMP, if X2-star configuration is adopted. Therefore, according to
25 some embodiments of the invention, eNBs exchange information on their capability for inter-eNB CA and/or inter-eNB eCoMP. For example, if one of them is not capable of inter-eNB CA and inter-eNB eCoMP, X2-star configuration is preferred. As another example, if both eNBs are capable of at least one of
30 inter-eNB CA and inter-eNB eCoMP, X2-mesh configuration is preferred in order to fulfil more likely the latency requirements.

The request for information on inter-eNB CA capability and
35 the information on inter-eNB CA capability may be conveyed by

the S1 configuration transfer messages, which are to be enhanced over nowadays 3GPP standards.

As regards criterion 4, each of the eNB may determine the
5 previous traffic on the X2 interface to the other eNB.
"Previous" may mean the total or average traffic over a
predefined time such as the last minute, the last hour, the
last two hours, the last day etc. For example, if the
previous X2 traffic was higher than a certain threshold, X2-
10 mesh configuration may be preferred, otherwise, X2-star
configuration may be preferred.

As regards criterion 5, each of the eNBs may evaluate some
network conditions it is aware of (e.g. some RTT, some
15 jitter, etc.). Alternatively, or in addition, it may receive
information on network condition from some network monitoring
tool. For example, if the network conditions are "good", X2-
star configuration may be preferred. As another example, if
the network conditions are "poor", X2-mesh configuration may
20 be preferred because it consumes less network resources.

As regards criterion 6, the operator may configure a priority
or preference. The priority or preference may be configured
in each eNB, e.g. by O&M. As another option, the priority or
25 preference may be configured in MME, and conveyed to the eNBs
by S1 MME configuration transfer message. In this case, MME
configuration transfer message is to be enhanced over
nowadays 3GPP standards.

30 E.g., this criterion may be combined with one or more of the
other criteria are in one metric. Depending on his
preferences, the operator may construe the metric such that
there is a prevalence for one of X2-star and X2-mesh
configuration.

35

For example, a metric may be construed as $metric = operator-priority + sub-metric (criterion\ 1\ to\ criterion\ 5)$. X2-star configuration is used if $metric < K$, and X2-mesh configuration is used if $metric \geq K$. K is a predefined value.

5 $sub-metric (criterion\ 1\ to\ criterion\ 5)$ designates some numerical value which turns out from considering some or all of criteria 1 to 5. If *operator-priority* has a positive value, X2-mesh configuration is generally preferred, while, if *operator-priority* has a negative value, X2-star
10 configuration is generally preferred.

Fig. 2 shows an apparatus according to an embodiment of the invention. The apparatus may be communication entity or an element thereof. In particular, the apparatus may be a base
15 station such as an eNB, or an element thereof. Fig. 3 shows a method according to an embodiment of the invention. The apparatus according to Fig. 2 may perform the method of Fig. 3 but is not limited to this method. The method of Fig. 3 may be performed by the apparatus of Fig. 2 but is not limited to
20 being performed by this apparatus.

The apparatus comprises identifying means 10 and providing means 20.

25 The identifying means 10 identifies a tunnel endpoint a communication device should use for securely communicating with the apparatus (S10). For example, in order to identify the tunnel endpoint, it may apply one or more the criteria 1 to 6 discussed hereinabove. The communication device may be
30 another base station such as a eNB.

The providing means 20 provides an address of the tunnel endpoint to the communication device (S20). The providing means provides the address of the tunnel endpoint regardless
35 of whether the address of the tunnel endpoint is an address

of the apparatus (i.e., if a direct connection between the apparatus and the communication device is intended) or an address of a gateway different from the apparatus (i.e., if a X2-star connection via a gateway such as a security gateway is intended).

Fig. 4 shows an apparatus according to an embodiment of the invention. The apparatus may be communication entity or an element thereof. In particular, the apparatus may be a base station such as an eNB, or an element thereof. Fig. 5 shows a method according to an embodiment of the invention. The apparatus according to Fig. 4 may perform the method of Fig. 5 but is not limited to this method. The method of Fig. 5 may be performed by the apparatus of Fig. 4 but is not limited to being performed by this apparatus.

The apparatus comprises comparing means 110 and inhibiting means 120.

The comparing means 110 compares a received address of a first tunnel endpoint with an address of an established tunnel endpoint of an established tunnel for securely communicating with a communication device (S110). The received address of the first tunnel endpoint is received in a message indicating that a first tunnel to the first tunnel endpoint should be established for securely communicating with a first communication device. The communication device may be different from the first communication device. The communication device may be another base station such as an eNB.

The inhibiting means 120 inhibits establishing the first tunnel different from the established tunnel if the received address corresponds to the address of the established tunnel

endpoint (S120). "Corresponding" may mean "is equal to", or it may mean that the received address defines an address range and the established address is within the address range. If the addresses correspond to each other the
5 apparatus may securely communicate with the communication device via the established tunnel.

Fig. 6 shows an apparatus according to an embodiment of the invention. The apparatus may be communication entity or an
10 element thereof. In particular, the apparatus may be a base station such as an eNB, or an element thereof. Fig. 7 shows a method according to an embodiment of the invention. The apparatus according to Fig. 4 may perform the method of Fig. 7 but is not limited to this method. The method of Fig. 7 may
15 be performed by the apparatus of Fig. 6 but is not limited to being performed by this apparatus.

The apparatus comprises determining means 210 and
20 establishing means 220.

The determining means 210 determines a first address of plural received addresses of respective tunnel endpoints (S210). The plural received addresses of the tunnel endpoints are received in one or more messages indicating that one of
25 the tunnel endpoints should be used for securely communicating with a communication device. The communication device may be another base station such as an eNB. The determining means 210 may apply one or more of the criteria discussed hereinabove.

30 The establishing means 220 establishes a first tunnel to a first tunnel endpoint of the tunnel endpoints for securely communicating with the communication device (S220). The first tunnel endpoint has the determined first address.

Fig. 8 shows an apparatus according to an embodiment of the invention. The apparatus comprises at least one processor 310, at least one memory 320 including computer program code, and the at least one processor, with the at least one memory and the computer program code, being arranged to cause the apparatus to at least perform at least one of the methods according to Figs. 3, 5, and 7 and related description.

Embodiments of the invention may be employed in a fixed network and/or a mobile network, where secure communications between several entities (communication devices) may be performed in star topology, mesh topology, or a mixture of star and mesh topology. For example, they may be employed in a 3GPP network such as an LTE-A network. They may be employed also in other 3GPP and non-3GPP mobile networks such as Mobile adhoc networks (MANET) of 5th generation mobile networks, whenever there is direct exchange of messages among the communication devices. A communication device may be a base station of the respective radio technology (e.g. eNB for LTE-A). In general, a communication device may be any device capable of secure communication.

IPsec is a protocol enabling secure communication. However, embodiments of the invention are not restricted to IPsec but may be applied to other protocols enabling secure communication, too, such as TLS.

According to the described embodiments of the invention, information exchange between the eNBs on the configuration of the X2 link and on some of the criteria is performed by configuration transfer messages of S1AP. However, according to some embodiments of the invention, another message of S1AP may be accordingly modified, or a new message of S1AP may be created to convey some or all of this information.

A terminal may be a user equipment such as a mobile phone, a smart phone, a PDA, a laptop, a tablet PC, a wearable, a machine-to-machine device, or any other device which may be
5 connected to the respective network such as a 3GPP network. If not otherwise indicated or made clear from the context, the terms "UE" and "user" are synonymously used in the present application.

10 One piece of information may be transmitted in one or plural messages from one entity to another entity. Each of these messages may comprise further (different) pieces of information.

15 Names of network elements, protocols, and methods are based on current standards. In other versions or other technologies, the names of these network elements and/or protocols and/or methods may be different, as long as they provide a corresponding functionality.

20 If not otherwise stated or otherwise made clear from the context, the statement that two entities are different means that they perform different functions. It does not necessarily mean that they are based on different hardware.

25 That is, each of the entities described in the present description may be based on a different hardware, or some or all of the entities may be based on the same hardware. It does not necessarily mean that they are based on different software. That is, each of the entities described in the
30 present description may be based on different software, or some or all of the entities may be based on the same software.

According to the above description, it should thus be
35 apparent that example embodiments of the present invention

provide, for example a base station such as a eNodeB, or a component thereof, an apparatus embodying the same, a method for controlling and/or operating the same, and computer program(s) controlling and/or operating the same as well as
5 mediums carrying such computer program(s) and forming computer program product(s).

Implementations of any of the above described blocks, apparatuses, means, devices, units, systems, techniques or
10 methods include, as non-limiting examples, implementations as hardware, software, firmware, special purpose circuits or logic, general purpose hardware or controller or other computing devices, or some combination thereof.

15 It is to be understood that what is described above is what is presently considered the preferred embodiments of the present invention. However, it should be noted that the description of the preferred embodiments is given by way of example only and that various modifications may be made
20 without departing from the scope of the invention as defined by the appended claims.

Claims:

1. Apparatus, comprising

identifying means adapted to identify a first tunnel
5 endpoint a communication device should use for securely
communicating with the apparatus;

providing means adapted to provide an address of the
first tunnel endpoint to the communication device, regardless
of whether the address of the first tunnel endpoint is an
10 address of the apparatus or an address of a gateway different
from the apparatus.

2. The apparatus according to claim 1, wherein

the providing means is adapted to provide an address of
15 the apparatus as the address of the first tunnel endpoint to
the communication device if the identifying means identifies
that the communication device should communicate securely
directly with the apparatus.

20 3. The apparatus according to any of claims 1 to 2, further
comprising

first distance determining means adapted to determine a
geographical distance to the communication device; wherein

the identifying means is adapted to identify the tunnel
25 end point based on the geographical distance.

4. The apparatus according to claim 3, wherein

the first distance determining means is adapted to
determine the geographical distance based on a received
30 information of a geographical location of the communication
device.

5. The apparatus according to any of claims 1 to 4, further comprising

first roundtrip time determining means adapted to determine a total roundtrip time to the communication device;

5 wherein

the identifying means is adapted to identify the tunnel end point based on the total roundtrip time.

6. The apparatus according to claim 5, further comprising

10 roundtrip time measuring means adapted to measure a first roundtrip time between the apparatus and the first tunnel endpoint; wherein

the first roundtrip time determining means is adapted to determine the total roundtrip time based on the first
15 roundtrip time and a received information on a second roundtrip time between the communication device and the first tunnel endpoint.

7. The apparatus according to any of claims 1 to 6, further
20 comprising

first traffic determining means adapted to determine a previous traffic between the communication device and the apparatus; wherein

the identifying means is adapted to identify the tunnel
25 end point based on the previous traffic.

8. The apparatus according to any of claim 1 to 7, wherein

the identifying means is adapted to identify plural tunnel endpoints including the first tunnel endpoint, wherein
30 the communication device should use one of the plural tunnel endpoints for the securely communicating with the apparatus;

the providing means is adapted to provide addresses of the plural tunnel endpoints to the communication device.

9. The apparatus according to claim 8, further comprising
deciding means adapted to decide on a respective
priority for each of the plural tunnel endpoints, wherein
5 the providing means is adapted to provide the respective
priority along with the address of each of the plural tunnel
endpoints.

10. The apparatus according to claim 9, further comprising
10 second distance determining means adapted to determine a
geographical distance to the communication device; wherein
the deciding means is adapted to decide on the
priorities based on the geographical distance.

15 11. The apparatus according to any of claims 9 to 10, further
comprising
second roundtrip time determining means adapted to
determine a respective total roundtrip time to the
communication device for each of the plural tunnel endpoints;
20 wherein
the deciding means is adapted to decide on the
priorities based on the respective total roundtrip times.

12. The apparatus according to any of claims 9 to 11, further
25 comprising
second traffic determining means adapted to determine a
previous traffic between the communication device and the
apparatus; wherein
the deciding means is adapted to decide on the
30 priorities based on the previous traffic.

13. Apparatus, comprising

determining means adapted to determine a first address of plural received addresses of respective tunnel endpoints, wherein the plural received addresses of the tunnel endpoints are received in one or more messages indicating that one of
5 the tunnel endpoints should be used for securely communicating with a communication device;

establishing means adapted to establish a first tunnel to a first tunnel endpoint of the tunnel endpoints for securely communicating with the communication device, wherein
10 the first tunnel endpoint has the determined first address.

14. The apparatus according to claim 13, wherein

the determining means is adapted to determine the first address based on received priorities for the plural received
15 addresses.

15. The apparatus according to any of claims 13 to 14, further comprising

monitoring means adapted to monitor if the establishing
20 of the first tunnel fails; wherein

the determining means is adapted to determine, if the establishing of the first tunnel fails, a second address of the plural received addresses different from the first address; and

25 the establishing means is adapted to establish, if the establishing of the first tunnel fails, a second tunnel to a second tunnel endpoint of the tunnel endpoints for securely communicating with the communication device, wherein the second tunnel endpoint has the determined second address.

30

16. The apparatus according to claim 15 dependent on claim 14, wherein

the determining means is adapted to determine the second address based on the received priorities.

17. The apparatus according to any of claims 13 to 16,
5 further comprising

location providing means adapted to provide an information on a geographical location of the apparatus in response to a first configuration request.

10 18. The apparatus according to any of claims 13 to 17, further comprising

roundtrip time measuring means adapted to measure a roundtrip time between the apparatus and the first tunnel endpoint;

15 roundtrip time providing means adapted to provide an information on the roundtrip time in response to a second configuration request.

19. The apparatus according to any of claims 13 to 18,
20 further comprising

comparing means adapted to compare the first address with an address of an established tunnel endpoint of an established tunnel for securely communicating with an endpoint device;

25 inhibiting means adapted to inhibit the establishing of the first tunnel different from the established tunnel if the first address corresponds to the address of the established tunnel endpoint.

30 20. Apparatus, comprising

comparing means adapted to compare a received address of a first tunnel endpoint with an address of an established tunnel endpoint of an established tunnel for securely

communicating with a communication device, wherein the received address of the first tunnel endpoint is received in a message indicating that a first tunnel to the first tunnel endpoint should be established for securely communicating with a first communication device;

inhibiting means adapted to inhibit establishing the first tunnel different from the established tunnel if the received address corresponds to the address of the established tunnel endpoint.

21. Base station apparatus, comprising

base station means adapted to provide a base station functionality of a radio access technology;

communicating means adapted to communicate securely with a base station device for providing the base station functionality; and

an apparatus according to any of claims 1 to 20, wherein the base station device comprises the communication device; and

the communicating means is adapted to use the first tunnel endpoint for the securely communicating with the base station device.

22. Method, comprising

identifying a first tunnel endpoint a communication device should use for securely communicating with an apparatus performing the method;

providing an address of the first tunnel endpoint to the communication device, regardless of whether the address of the first tunnel endpoint is an address of the apparatus or an address of a gateway different from the apparatus.

23. The method according to claim 22, wherein

the providing comprises providing an address of the apparatus as the address of the first tunnel endpoint to the communication device if it is identified that the communication device should communicate securely directly
5 with the apparatus.

24. The method according to any of claims 22 to 23, further comprising

determining a geographical distance to the communication
10 device; wherein

the tunnel end point is identified based on the geographical distance.

25. The method according to claim 24, wherein

15 the geographical distance is determined based on a received information of a geographical location of the communication device.

26. The method according to any of claims 22 to 25, further
20 comprising

determining a total roundtrip time to the communication device; wherein

the tunnel end point is identified based on the total roundtrip time.

25

27. The method according to claim 26, further comprising

measuring a first roundtrip time between the apparatus and the first tunnel endpoint; wherein

the total roundtrip time is determined based on the
30 first roundtrip time and a received information on a second roundtrip time between the communication device and the first tunnel endpoint.

28. The method according to any of claims 22 to 27, further comprising

determining a previous traffic between the communication device and the apparatus; wherein

5 the tunnel end point is identified based on the previous traffic.

29. The method according to any of claim 22 to 28, further comprising

10 identifying plural tunnel endpoints including the first tunnel endpoint, wherein the communication device should use one of the plural tunnel endpoints for the securely communicating with the apparatus;

15 providing addresses of the plural tunnel endpoints to the communication device.

30. The method according to claim 29, further comprising

deciding on a respective priority for each of the plural tunnel endpoints, and

20 providing the respective priority along with the address of each of the plural tunnel endpoints.

31. The method according to claim 30, further comprising

25 determining a geographical distance to the communication device; and

deciding on the priorities based on the geographical distance.

32. The method according to any of claims 30 to 31, further comprising

30 determining a respective total roundtrip time to the communication device for each of the plural tunnel endpoints; and

deciding on the priorities based on the respective total roundtrip times.

33. The method according to any of claims 30 to 32, further comprising

determining a previous traffic between the communication device and the apparatus; and

deciding on the priorities based on the previous traffic.

34. Method, comprising

determining a first address of plural received addresses of respective tunnel endpoints, wherein the plural received addresses of the tunnel endpoints are received in one or more messages indicating that one of the tunnel endpoints should be used for securely communicating with a communication device;

establishing a first tunnel to a first tunnel endpoint of the tunnel endpoints for securely communicating with the communication device, wherein the first tunnel endpoint has the determined first address.

35. The method according to claim 34, further comprising

determining the first address based on received priorities for the plural received addresses.

36. The method according to any of claims 34 to 35, further comprising

monitoring if the establishing of the first tunnel fails;

determining, if the establishing of the first tunnel fails, a second address of the plural received addresses different from the first address; and

establishing, if the establishing of the first tunnel fails, a second tunnel to a second tunnel endpoint of the tunnel endpoints for securely communicating with the communication device, wherein the second tunnel endpoint has
5 the determined second address.

37. The method according to claim 36 dependent on claim 35, wherein

the determining of the second address is based on the
10 received priorities.

38. The method according to any of claims 34 to 37, further comprising

providing an information on a geographical location of
15 an apparatus performing the method in response to a first configuration request.

39. The method according to any of claims 34 to 38, further comprising

20 measuring a roundtrip time between an apparatus performing the method and the first tunnel endpoint;

providing an information on the roundtrip time in response to a second configuration request.

25 40. The method according to any of claims 34 to 39, further comprising

comparing the first address with an address of an established tunnel endpoint of an established tunnel for securely communicating with an endpoint device;

30 inhibiting the establishing of the first tunnel different from the established tunnel if the first address corresponds to the address of the established tunnel endpoint.

41. Method, comprising

comparing a received address of a first tunnel endpoint
with an address of an established tunnel endpoint of an
5 established tunnel for securely communicating with a
communication device, wherein the received address of the
first tunnel endpoint is received in a message indicating
that a first tunnel to the first tunnel endpoint should be
established for securely communicating with a first
10 communication device;

inhibiting establishing the first tunnel different from
the established tunnel if the received address corresponds to
the address of the established tunnel endpoint.

15 42. A computer program product comprising a set of
instructions which, when executed on an apparatus, is
configured to cause the apparatus to carry out the method
according to any of claims 22 to 41.

20 43. The computer program product according to claim 42,
embodied as a computer-readable medium or directly loadable
into a computer.

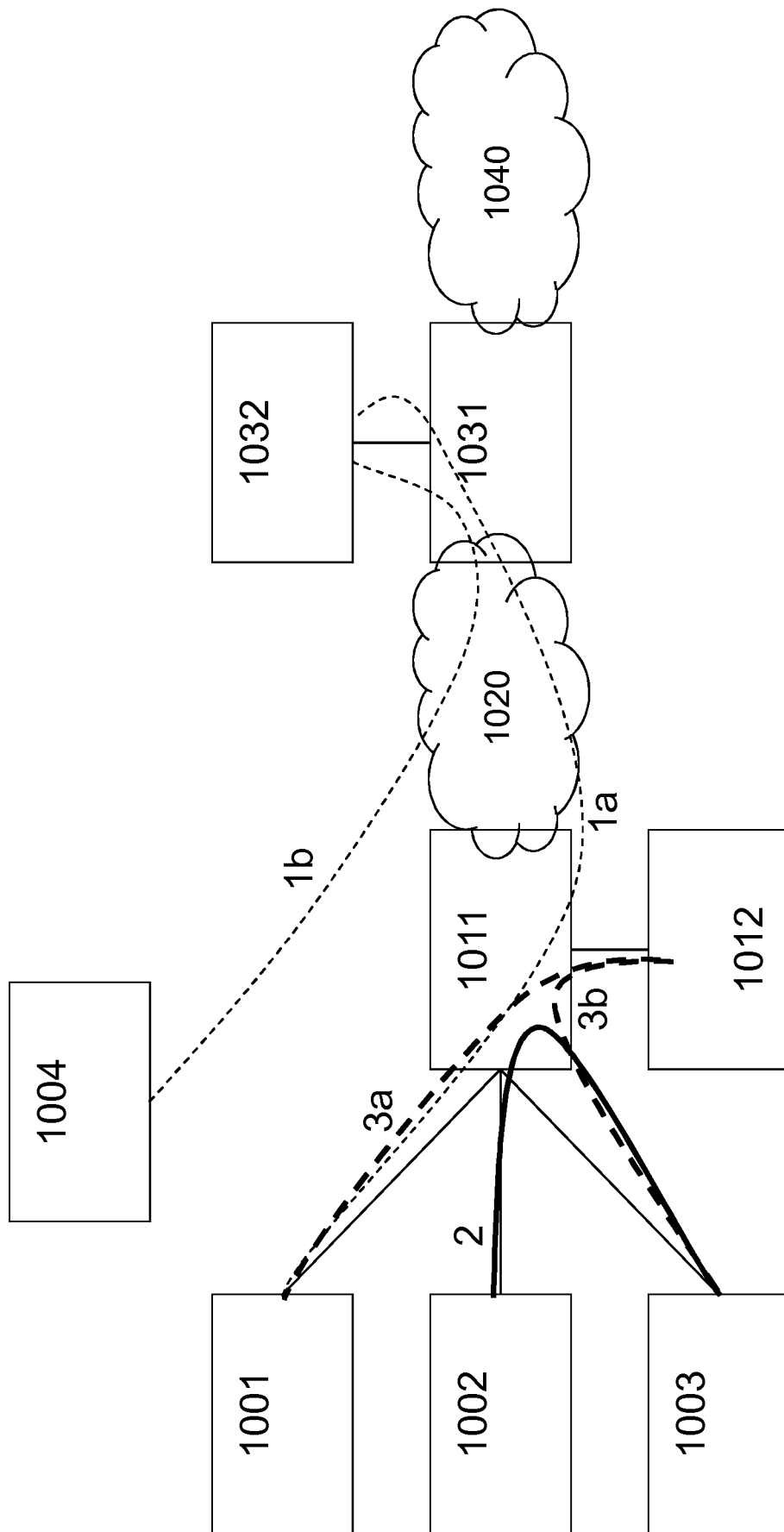


Fig. 1

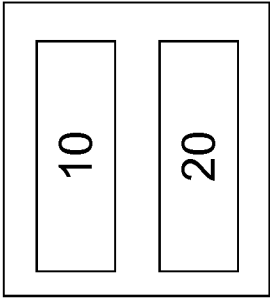


Fig. 2

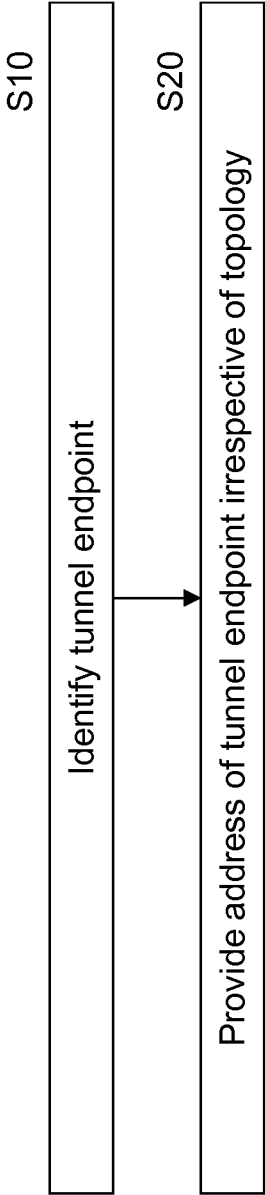


Fig. 3

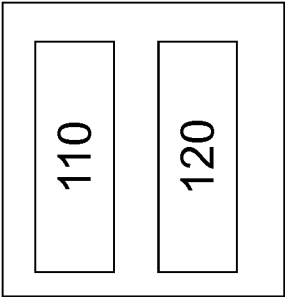


Fig. 4

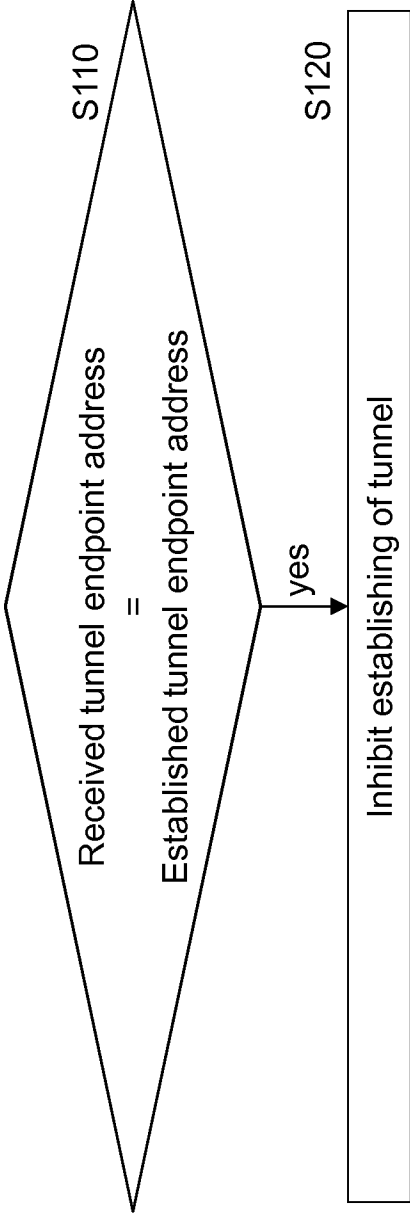


Fig. 5

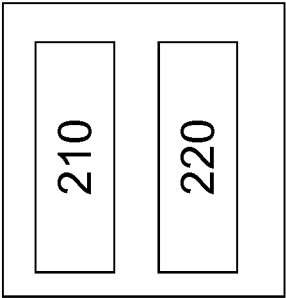


Fig. 6

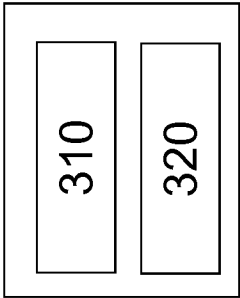


Fig. 8

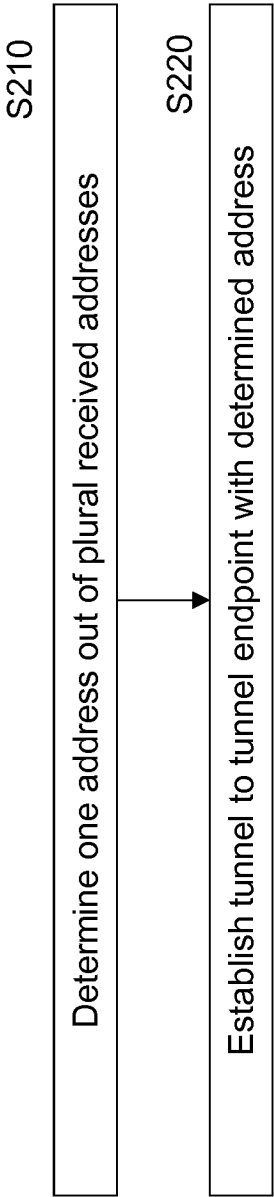


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/054825

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/02 H04L29/06 H04W76/02 H04W92/20
ADD.

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)
H04W 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 practicable, search terms used)

EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SAMSUNG: "Enhance TNL Address Discovery procedure for X2 GW", 3GPP DRAFT; R3-140137 TNL DISCOVERY, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. RAN WG3, no. Prague, Czech Republic; 20140210 - 20140214 31 January 2014 (2014-01-31), XP050755597, Retrieved from the Internet: URL: http://www.3gpp.org/ftp/tsg_ran/WG3_Iu/TSGR3_83/Docs/ [retrieved on 2014-01-31] paragraph [8.16] paragraph [9.2.2.29] ----- -/--	1-43



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

29 October 2015

Date of mailing of the international search report

05/11/2015

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Figiel, Barbara

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/054825

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CATT ET AL: "Discussion on Security Gateway for Small cell deployment", 3GPP DRAFT; R3-131709, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. RAN WG3, no. Venice, Italy; 20131007 - 20131011 28 September 2013 (2013-09-28), XP050719983, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg_ran/WG3_Iu/TSGR3_81bis/Docs/ [retrieved on 2013-09-28] the whole document -----	1-43
A	HUAWEI: "Security GW impact analysis for MSA", 3GPP DRAFT; R3-131652 SEC GW ANALYSIS, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. RAN WG3 27 September 2013 (2013-09-27), XP050719841, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg_ran/WG3_Iu/TSGR3_81bis/Docs/ [retrieved on 2013-09-27] the whole document -----	1-43