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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 January 2016 (14.01.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/007052 A1

(51) International Patent Classification:
*H04L 29/06* (2006.01) *H04W 12/02* (2009.01)
*H04W 28/02* (2009.01)

(21) International Application Number:
PCT/SE2014/050867

(22) International Filing Date:
7 July 2014 (07.07.2014)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors: **PERSSON, Fredrik**; Rönnvägen 9, S-195 44 Märsta (SE). **VIKBERG, Jari**; Svalsätersvägen 12, S-153 38 Järna (SE).

(74) Agent: **SJÖBERG, Mats**; Ericsson AB, Patent Unit Kista, RAN Implementation & Core (PU-KRIC), S-164 80 Stockholm (SE).

(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, LT, 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, 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).

**Declarations under Rule 4.17**:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *of inventorship (Rule 4.17(iv))*

**Published**:

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

(54) Title: A WIRELESS DEVICE, NETWORK NODE AND RESPECTIVE METHODS THEREIN FOR TRANSMITTING DATA THEREBETWEEN

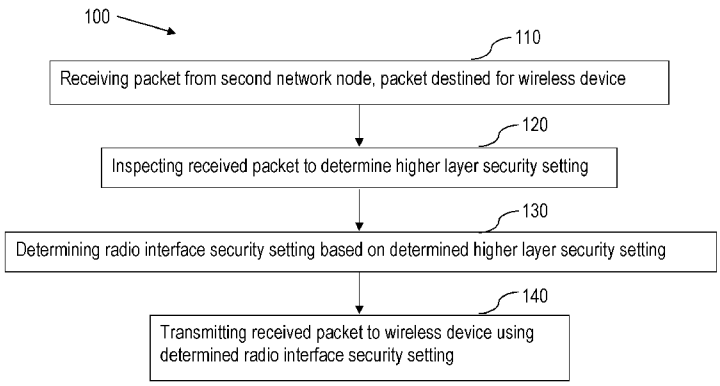


Fig. 1a

(57) Abstract: A first network node in a wireless communication network and a method in the first network node for transmitting data to a wireless device, as well as a first wireless device and a method in the first wireless device for transmitting data to a second wireless device or to a network node of a wireless communication network are provided. The method in the first network node comprises receiving (110) a packet from a second network node in the wireless communication network, the packet being destined for the wireless device; and inspecting (120) the received packet by performing a packet inspection to determine a higher layer security setting. The method 100 further comprises determining (130) a radio interface security setting based on the determined higher layer security setting; and transmitting (140) the received packet to the wireless device using the determined radio interface security setting.

WO 2016/007052 A1

# A WIRELESS DEVICE, NETWORK NODE AND RESPECTIVE METHODS THEREIN FOR TRANSMITTING DATA THEREBETWEEN

## Technical field

[0001] The present disclosure relates to wireless communication and in particular to a first network node for transmitting data to a wireless device and a first wireless device for transmitting data to a network node or a second wireless device.

## Background

[0002] Today's various communication systems and networks are becoming more and more interconnected. The different communication networks are of varying types, wireless, wired, employing different radio access technology, employing different levels and types of security.

[0003] When a wireless device is making use of a service that is not provided from within the wireless communication in which the wireless device is operating, the wireless device may receive e.g. data packets from a host or server being located in another network. The host or server may use different communication protocols, different transmission techniques, different levels and types of security.

[0004] Generally, in such scenarios, there are a multitude of different protocols being stacked on top of each other in order for the wireless device and the host or server running the application to communicate with each other.

[0005] Regarding security, the so-to-say complete security architecture may be divided into different security domains. Each domain may have its own set of security threats and security solutions. The 3rd Generation Partnership Project, 3GPP, Technical Specification, TS, 33.401 ("3GPP System Architecture Evolution, SAE; Security architecture") divides the security architecture into different groups or domains: 1) Network access security, 2) Network domain security, 3) User domain security, 4) Application domain security, and 5) Visibility and configurability of security.

[0006] The first group is specific to each access technology (e.g. Evolved Universal Terrestrial Radio Access Network, E-UTRAN, GSM EDGE Radio Access Network, GERAN, UTRAN, etc.), whereas the others are common for all accesses. By network access security is normally meant the security features that provide a user with a secure access to the network. This may include mutual authentication as well as privacy features. In addition, protection of signalling traffic and user plane traffic in the particular access is also included. This protection may provide confidentiality and/or integrity protection of the traffic.

[0007] The basic security concepts which are important in cellular networks are the following: **Authentication** is usually performed before a user is granted access to a network. During authentication the user proves that he or she is the one he/she claims to be. Typically, *mutual authentication* is desired, where the network authenticates the User Equipment, UE, and the UE authenticates the network. Authentication is in general done with a procedure where each party proves that it has access to a secret known only to the participating parties, for example, a password or a secret key.

[0008] The network also verifies that the subscriber is **authorized** to access the requested service, for example, to get access to Evolved Packet System, EPS, using a particular access network. This means that the user must have the right privileges (i.e. a subscription) for the type of services that is requested. Authorization for an access is often done at the same time as authentication.

[0009] Once the user has been granted access, there is a desire to protect the signalling traffic and user plane traffic between the UE and the network and between different entities within the network. **Ciphering** and/or **integrity protection** may be applied for this purpose. With ciphering (i.e. encryption and decryption) we ensure that the information transmitted is only readable by the intended recipients. To accomplish this, the traffic is scrambled so that it becomes unreadable for anyone who manages to intercept it, except for the entities that have access to the correct cryptographic keys. Integrity protection on the other hand is a means to detect whether traffic that reaches the intended recipient has not been modified, for example, by an attacker between the sender and the

receiver. If the traffic has been modified, the integrity protection ensures that the receiver is able to detect it. Ciphering and integrity protection serves different purposes and the need for ciphering and/or integrity protection differs depending on what traffic it is. Furthermore, the data protection may be done on different layers in the protocol stack.

[00010] In order to encrypt/decrypt as well as to perform integrity protection, the sending and receiving entities need **cryptographic keys**.

[00011] E-UTRAN should provide a security level, at least as high as that of UTRAN. Access security in E-UTRAN therefore consists of different components, similar to those that can be found in UTRAN: 1) Mutual authentication between UE and network, 2) Key derivation to establish the keys for ciphering and integrity protection, 3) Ciphering, integrity and replay protection of Network Access Stratum, NAS, signalling between UE and Mobility Management Entity, MME, 4) Ciphering, integrity and replay protection of Radio Resource Control, RRC, signalling between UE and evolved Node B, eNB, 5) Ciphering of the user plane. The user plane is ciphered between UE and eNB, and 6) Use of temporary identities in order to avoid sending the permanent user identity (International Mobile Subscriber Identity, IMSI) over the radio link.

[00012] The ciphering of the user plane in E-UTRAN, is performed on the Packet Data Convergence Protocol, PDCP, layer. The ciphering function in UTRAN is performed either in the Radio Link Control, RLC, sub-layer or in the Medium Access Control, MAC, sub-layer, according to the following rules: a) if a radio bearer is using a non-transparent RLC mode (Acknowledged Mode, AM, or Unacknowledged Mode, UM), ciphering is performed in the RLC sub-layer, and b) if a radio bearer is using the transparent RLC mode, ciphering is performed in the MAC sub-layer (MAC-d entity).

[00013] Ciphering when applied is performed in the Serving RNC and the UE and the context needed for ciphering (Ciphering Key, CK, Hyper Frame Number, HFN, etc.) is only known in Serving Radio Network Controller, RNC, and the UE.

[00014] The ciphering solution in the General Packet Radio Services, GPRS/EDGE case (i.e. the Packet Switched domain of GERAN) is somewhat different compared to UTRAN and E-UTRAN cases. In the GPRS/EDGE case ciphering is performed between the UE and the Serving GPRS Support Node, SGSN, in the core network in the Logical Link Control, LLC, protocol layer.

[00015] Internet Protocol Security, IPsec, is a protocol suite for securing Internet Protocol, IP, communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

[00016] IPsec is an end-to-end security scheme operating in the Internet Protocol, IP, of the Internet Protocol Suite (also known as Transmission Control Protocol, TCP/IP protocol suite), while some other Internet security systems in widespread use, such as Secure Sockets Layer, SSL, Transport Layer Security, TLS, and Secure Shell, SSH, operate on application layer on top of the TCP/IP layers. Hence, IPsec protects any application traffic across an IP network. Applications do not need to be specifically designed to use IPsec. Without IPsec, the use of TLS/SSL had to be inserted below the applications to protect the application protocols. IPsec is also supported as part of the security solution of the IP based GPRS Tunnelling Protocol, GTP, tunnel between the packet gateway (e.g. a Serving Gateway, SGW) and the radio access network (e.g. an eNodeB, eNB).

[00017] Some traffic in communication networks are transported, or transmitted, over secure links, and some traffic over unsecure links. By means of applying different security features or functions, the data being carried by the traffic may still be protected even if a link is insecure.

[00018] However, when a device in one security domain communicates with a device or node in another security domain, the two domains applying different security features, problems may arise due to the different technologies and also due to a lot of overhead leading to increasing demands of resources.

Summary

[00019] The object is to obviate at least some of the problems outlined above. In particular, it is an object to provide a first network node in a wireless communication network and a method performed by the first network node for transmitting data to a wireless device. It is a further object to provide a first wireless device and a method performed by the first wireless device for transmitting data to a second wireless device or to a network node of a wireless communication network. These objects and others may be obtained by providing a first network node and a first wireless device respectively, and a respective method performed by a first network node and a first wireless device according to the independent claims attached below.

[00020] According to an aspect, a method performed by a first network node in a wireless communication network for transmitting data to a wireless device is provided. The method comprises receiving a packet from a second network node in the wireless communication network, the packet being destined for the wireless device; and inspecting the received packet by performing a packet inspection to determine a higher layer security setting. The method further comprises determining a radio interface security setting based on the determined higher layer security setting; and transmitting the received packet to the wireless device using the determined radio interface security setting.

[00021] According to an aspect, a method performed by a first wireless device for transmitting data to a second wireless device or to a network node of a wireless communication network is provided. The method comprises comprising receiving, at a lower layer from a higher layer of a protocol stack used in the wireless device for communication towards the network node or the second wireless device, a packet to be transmitted to the network node or to the second wireless device. The

method further comprises determining a radio interface security setting based on a higher layer security setting; and transmitting the received packet to the network node or to the second wireless device using the determined radio interface security setting.

[00022] According to an aspect, a first network node in a wireless communication network for transmitting data to a wireless device is provided. The first network node is configured receive a packet from a second network node in the wireless communication network, the packet being destined for the wireless device; and to inspect the received packet by performing a packet inspection to determine a higher layer security setting. The first network node is further configured to determine a radio interface security setting based on the determined higher layer security setting; and to transmit the received packet to the wireless device using the determined radio interface security setting.

[00023] According to an aspect, a first wireless device for transmitting data to a second wireless device or to a network node of a wireless communication network is provided. The first wireless device is configured to receive, at a lower layer from a higher layer of a protocol stack used in the wireless device for communication towards the network node or the second wireless device, a packet to be transmitted to the network node or to the second wireless device. The first wireless device is further configured to determine a radio interface security setting based on a higher layer security setting; and to transmit the received packet to the network node or to the second wireless device using the determined radio interface security setting.

[00024] The first network node, the first wireless device and the respective method performed thereby may have several possible advantages. One possible advantage is unnecessary data overhead may be avoided. Another possible advantage is that wasting of resources relating to providing radio interface security when not needed may be reduced. Still a possible advantage is that latency may be reduced.

Brief description of drawings

[00025] Embodiments will now be described in more detail in relation to the accompanying drawings, in which:

[00026] Figure 1a is a flowchart of a method performed by a first network node for transmitting data to a wireless device according to an exemplifying embodiment.

[00027] Figure 1b is a flowchart of a method performed by a first network node for transmitting data to a wireless device according to yet an exemplifying embodiment.

[00028] Figure 1c is a flowchart sf a method performed by a first network node for transmitting data to a wireless device according to still an exemplifying embodiment.

[00029] Figure 1d is a flowchart of a method performed by a first network node for transmitting data to a wireless device according to another exemplifying embodiment.

[00030] Figure 1e is a flowchart of a method performed by a first network node for transmitting data to a wireless device according to a further exemplifying embodiment.

[00031] Figure 1f is a flowchart of a method performed by a first network node for transmitting data to a wireless device according to yet an exemplifying embodiment.

[00032] Figure 2a is a flowchart of a method performed by a first wireless device for transmitting data to a network node or a second wireless device according to an exemplifying embodiment.

[00033] Figure 2b is a flowchart of a method performed by a first wireless device for transmitting data to a network node or a second wireless device according to yet an exemplifying embodiment.

[00034] Figure 2c is a flowchart of a method performed by a first wireless device for transmitting data to a network node or a second wireless device according to still an exemplifying embodiment.

[00035] Figure 2d is a flowchart of a method performed by a first wireless device for transmitting data to a network node or a second wireless device according to a further exemplifying embodiment.

[00036] Figure 2e is a flowchart of a method performed by a first wireless device for transmitting data to a network node or a second wireless device according to another exemplifying embodiment.

[00037] Figure 2f is a flowchart of a method performed by a first wireless device for transmitting data to a network node or a second wireless device according to yet an exemplifying embodiment.

[00038] Figure 3 is a block diagram of a first network node adapted for transmitting data to a wireless device according to an exemplifying embodiment.

[00039] Figure 4 is a block diagram of a first wireless device adapted for transmitting data to a network node or a second wireless device according to an exemplifying embodiment.

[00040] Figure 5 is a block diagram of a first network node for transmitting data to a wireless device according to an exemplifying embodiment.

[00041] Figure 6 is a block diagram of a first wireless device for transmitting data to a network node or a second wireless device according to an exemplifying embodiment.

[00042] Figure 7 is a block diagram of an arrangement in a first network node for transmitting data to a wireless device according to an exemplifying embodiment.

[00043] Figure 8 is a block diagram of an arrangement in a first wireless device for transmitting data to a network node or a second wireless device according to an exemplifying embodiment.

[00044] Figure 9 is an illustration of a protocol stack for an application running on a UE and a host/server.

[00045] Figure 10 is another illustration of a protocol stack for an application running on a UE and a host/server also illustrating different security types being applied in different layers of the protocol stack.

Detailed description

[00046] Briefly described, a first network node and a method performed by the first network node for transmitting data to a wireless device are provided. Further, a first wireless device and a method performed by the first wireless device for transmitting data to a network node or to a second wireless device are provided. The first network node performs a packet inspection of a received packet being destined to the wireless device for determining if the packet is already protected by higher layer security. If so, there is no need to apply additional security in the form of radio interface security before transmitting the packet to the wireless device. However, if the packet is not already protected, then there is a need for applying radio interface security to the packet before transmitting it to the wireless device.

[00047] Exemplifying embodiments of a method performed by a first network node in a wireless communication network for transmitting data to a wireless device will now be described with reference to figures 1a-1f.

[00048] **Figure 1a** illustrates the method 100 comprising: receiving 110 a packet from a second network node in the wireless communication network, the packet being destined for the wireless device; and inspecting 120 the received packet by performing a packet inspection to determine a higher layer security setting. The method 100 further comprises determining 130 a radio interface security setting based on the determined higher layer security setting; and transmitting 140 the received packet to the wireless device using the determined radio interface security setting.

[00049] The first network node may be e.g. a Radio Base Station, RBS, or a Radio Network Controller, RNC, or another network node responsible for

transmitting the received packet to the wireless device. The first network node is also responsible for applying the radio interface security. The second network node may be e.g. a core network node for example a packet gateway such as a Serving gateway, SGW, Packet Data Gateway, PDN-GW, a SGSN or a Gateway GPRS Support Node, GGSN. The packet may have been generated and transmitted by an Over The Top, OTT, service or application, thereby providing a service to a user of the wireless device. Since such a service may be designed to run over, or being delivered by means of, unsecure data links, the OTT service or application may already have e.g. encrypted the packet.

[00050] The packet may alternatively have been generated and transmitted from a device, application or node wherein the packet is destined to be transmitted over secure radio links, such as those between an RBS and a wireless device in a wireless communication network, for example a Long Term Evolution, LTE, communication network, a Universal Mobile Telecommunication System, UMTS, communication network, or a Global System for Mobile communication, GSM, communication network.

[00051] Thus, when the first network node receives the packet from the second network node, the first network nodes inspects the packet in order to determine whether the packet is already protected as indicated by the higher layer security setting or if the packet is unprotected. The inspection may be done in different ways as will be described in more detail below.

[00052] Based on the result of the packet inspection, i.e. whether the packet is already protected as indicated by the higher layer security setting or if the packet is unprotected, the first network node determines the radio interface security setting to be used when transmitting the packet to the wireless device. For example, if the packet is already protected as indicated by the higher layer security setting then there may be little or no need for radio interface security, wherein the radio interface security setting may indicate no radio interface security. Alternatively, if the packet is unprotected, there may be a strong need to protect the packet when transmitting it to the wireless device. Thus the radio interface

security setting may indicate that the packet is to be protected by the radio interface security.

[00053] Then the first network node transmits the packet to the wireless device using the determined radio interface security setting.

[00054] In an example, the wireless device may be the so-to-say end point of the packet, but the wireless device may alternatively function as a modem, wherein another device may be the end point. No matter which it is, the first network node determines the radio interface security setting between itself and the wireless device based on the determined higher layer security setting, since whatever "happens" once the packet has been delivered to the wireless device is out of control of the first network node.

[00055] The method performed by the first network node may have several possible advantages. One possible advantage is unnecessary data overhead may be avoided. Another possible advantage is that wasting of resources relating to providing radio interface security when not needed may be reduced. Still a possible advantage is that latency may be reduced.

[00056] In an example, the radio interface security setting is associated with one of encrypting and non-encrypting of a radio bearer by means of which the packet is transmitted to the wireless device, or with encrypting and non-encrypting the received packet.

[00057] The radio interface security may be realised or implemented in different ways. An example is that the first network node and the wireless device may communicate by means of an encrypted radio bearer or by means of a non-encrypted radio bearer. Thus, the packet to be transmitted to the wireless device may either be transmitted on the encrypted radio bearer or on the non-encrypted radio bearer. Naturally, the encrypted radio bearer is a protected or secure radio bearer and thus a packet transmitted to the wireless device on the encrypted bearer is protected by means of the radio bearer itself. Likewise, the non-

encrypted radio bearer is unprotected and a packet transmitted to the wireless device on the non-encrypted radio bearer is thus unprotected by the bearer.

[00058] If the packet is already protected by the higher layer security, the packet may be transmitted on the non-encrypted radio bearer and if the packet is not already protected, it may be transmitted on the encrypted radio bearer in order to ensure it is transmitted in a protected manner to the wireless device.

[00059] The radio interface security setting may be associated with a level of encryption of a radio bearer by means of which the packet is transmitted to the wireless device.

[00060] In the examples above, the higher layer security setting has more or less indicated the presence or absence of higher layer security, and the radio interface security setting may likewise indicate the presence or absence of radio interface security, or the need for radio interface security. The higher layer security setting and the radio interface security setting may alternatively indicate a level of encryption (i.e. protection) that the higher layer security and the radio interface security respectively provide.

[00061] In a very simplified example, it can be said that if the higher layer setting is set to “1” the packet is already protected and if the higher layer setting is set to “0”, the packet is unprotected, and any value between “0” and “1” indicate a level of encryption of the packet. Merely as an equally simplified example, assume it is desirable to have so-to-say full security provided for each packet transmitted to the wireless device. Thus a packet being received by the first network node having a higher layer security setting indicating that the packet is protected to a level of 0.4, may require a radio interface security of about 0.6. Again this is a simplified example illustrating that a packet having a relatively low higher layer security may require a higher radio interface security than a packet having a relatively high higher layer security.

[00062] According to an embodiment, illustrated in **figure 1b**, when the higher layer security setting indicates that the packet is already protected by higher layer

security, then the method 100 comprises transmitting 140a the received packet to the wireless device by means of a non-encrypted radio bearer; and when the higher layer security setting indicates that the packet is not protected by higher layer security, then the method comprises transmitting 140b the received packet to the wireless device by means of an encrypted radio bearer.

[00063] As described above, when the higher layer security setting indicates that the packet is already protected by higher layer security, the packet is already protected. Thus there is no need to use a more resource demanding encrypted bearer to transmit the packet to the wireless device. Consequently, the packet is transmitted to the wireless device by means of a non-encrypted radio bearer.

[00064] However, if the higher layer security setting indicates that the packet is not protected by higher layer security, the packet still needs to be transmitted to the wireless device in a secure manner. In order to do so, the packet is transmitted to the wireless device by means of an encrypted radio bearer, wherein the encrypted radio bearer protects the packet by itself.

[00065] According to yet an embodiment, illustrated in **figure 1c**, if a non-encrypted radio bearer does not exist between the first network node and the wireless device, the method comprises setting up 140c a non-encrypted radio bearer between the first network node and the wireless device and transmitting 140a the received packet to the wireless device by means of the non-encrypted radio bearer.

[00066] It may be the case that there is no bearer of any kind established between the first network node and the wireless device. Alternatively, there may only be an encrypted radio bearer having been established between the first network node and the wireless device. Thus, if the packet should be transmitted to the wireless device by means of a non-encrypted bearer, the first network node sets up the non-encrypted radio bearer between the first network node and the wireless device and transmits the received packet to the wireless device by means of the non-encrypted radio bearer.

[00067] According to still an embodiment, illustrated in **figure 1d**, if a non-encrypted radio bearer doesn't exist between the first network node and the wireless device, the method 100 comprises refraining 140d from performing radio bearer level encryption, marking 140e the received packet with information that no radio bearer level encryption has been performed and transmitting 140f the packet to the wireless device by means of an encrypted radio bearer.

[00068] As described above, it may be the case that there is no bearer of any kind established between the first network node and the wireless device, or that there may only be an encrypted radio bearer having been established between the first network node and the wireless device. Setting up a new non-encrypted bearer may take some time and resources and in order to avoid that, the first wireless network node refrains from performing a radio bearer level encryption.

[00069] In this scenario, it is assumed that the radio interface security also, or alternatively, relates to an encryption of the packet itself. Thus, in this example, the packet is itself already encrypted and thus needs not to be further encrypted in order to obtain the radio bearer level encryption. The first network node thus refrains from further encrypting the packet, i.e. does not perform a radio bearer level encryption, but instead marks the packet with information that no radio bearer level encryption has been performed. By marking the packet in this manner, the wireless device is informed, when receiving the packet, that the packet is not encrypted on radio bearer level, and that the wireless device should not perform any decryption of the received packet. The first network node then transits the packet to the wireless device by means of the encrypted radio bearer. This also means that the encrypted radio bearer has additional capabilities to transport packets without performing encryption on radio bearer level and to convey the indication that no radio bearer level encryption has been performed.

[00070] According to another embodiment, illustrated in **figure 1e**, if a non-encrypted radio bearer doesn't exist between the first network node and the wireless device, the method 100 comprises modifying 140g an existing encrypted radio bearer to be non-encrypted and transmitting 140a the received packet to the wireless device by means of the non-encrypted radio bearer.

[00071] Alternatively to setting up a new non-encrypted bearer, the first network node may instead modify an existing encrypted bearer to making it a non-encrypted radio bearer. The modification may comprise signalling between the first network node and the wireless device to switch off an encryption function or algorithm running both on the first network node and on the wireless device, and in this manner switching off the encryption of the radio bearer thus making it a non-encrypted radio bearer. Once the radio bearer has been modified and operates as a non-encrypted radio bearer, the first network node transmits the packet to the wireless device by means of the non-encrypted radio bearer.

[00072] The packet inspection may be at least one of an Internet Protocol, IP, header classification, shallow inspection, deep packet inspection, and heuristic detection; or any other packet inspection mechanism.

[00073] There are different ways of inspecting the packet, or of performing packet inspection. The IP header classification typically inspects different information included in the IP header of the packet. It may also inspect protocol header related to other protocols such as TCP and UDP and it may also be known as the 5-tuple inspection. The 5-tuple inspection inspects the packet up to the so-called 5-tuple: source IP address, source TCP/UDP port, destination IP address, destination TCP/UDP port, and protocol (which runs on a transport layer, e.g. TCP, User Datagram Protocol, UDP, etc.).

[00074] The shallow inspection, also known as stateful inspection, analyses a transport level protocol state, by inspecting the current protocol header (TCP, UDP, etc.). For example, the shallow inspection analyses the sequence of TCP header flags like SYN, ACK and FIN which tell the state of the connection.

[00075] Deep packet inspection analyses the content on the application layer signalling, e.g. hypertext transfer protocol, HTTP, state, video frame content etc.

[00076] Heuristic detection comprises pattern detection or statistical identification methods on application layer data and is typically needed for classification of services with encrypted content.

[00077] The different types of packet inspection are more or less advanced and/or resource demanding. For example, deep packet inspection goes much "deeper" into the packet than e.g. shallow inspection. Consequently, deep inspection is more resource demanding than shallow inspection and also takes longer time to perform.

[00078] The packet inspection may be performed by using just one of the above, or by using a combination of different types of packet inspections.

[00079] In an example, illustrated in **figure 1f**, the method 100 further comprises storing 121 information relating to the received packet obtained from the packet inspection, receiving 110a a further packet destined for the wireless device, performing 120a a packet inspection on the received further packet to determine the higher layer security setting also using the stored information, and transmitting the received packet to the wireless device according to the previously determined radio interface security setting.

[00080] Generally, during a session, e.g. a data file transfer within the wireless communication network or downloading of information from the Internet, the session comprises a vast plurality of individual packets. Thus, the first network node may store information relating to the received packet obtained from the packet inspection (also referred to as the first packet inspection) to be used when receiving a next packet. When the next packet arrives at the first network node, the first network node may use this information together with information obtained by a packet inspection (also referred to as the second packet inspection) in order to determine the higher layer security setting. It may be that the first packet inspection is of a more resource demanding type than the second packet inspection, and by storing information from the first packet inspection, the second packet inspection does not need to be as thorough, or deep, as the first packet inspection.

[00081] Merely as an example, assume the first packet inspection is done by means of a deep packet inspection. A lot of information may be obtained from this packet inspection and some, or all, of it may be stored in a memory of the first

network node. When the next packet arrives, the first network node may save time and resources by performing a less resource demanding packet inspection, e.g. shallow inspection. Since the shallow inspection may not obtain as much information as the deep packet inspection, the first network node uses the stored data obtained by the deep packet inspection, in order to determine the higher layer security setting.

[00082] In this manner, time and resources may be saved in the first network node.

[00083] The wireless communication network may be a LTE communication network, wherein the first network node is a radio base station such as an evolved Node B, eNB.

[00084] The wireless communication network may alternatively be a Wideband Code Division Multiple Access, WCDMA, communication network such as a UMTS communication network, wherein the first network node is a Radio network Controller, RNC; or radio base station such as an Node B, NB

[00085] Alternatively, the wireless communication network may be a GSM communication network, wherein the first network node is a radio base station, a base station controller, BSC, or a Serving General packet radio service Support Node, SGSN.

[00086] Embodiments herein also relate to a method performed by a first wireless device for transmitting data to a second wireless device or to a network node of a wireless communication network. Exemplifying embodiments of such a method will now be described with reference to figure 2a-2f.

[00087] **Figure 2a** illustrates the method 200 comprising receiving 210, at a lower layer from a higher layer of a protocol stack used in the wireless device for communication towards the network node or the second wireless device, a packet to be transmitted to the network node or to the second wireless device. The method further comprises determining 220 a radio interface security setting based on a higher layer security setting; and transmitting 230 the received packet to the

network node or to the second wireless device using the determined radio interface security setting.

[00088] Typically, when e.g. an application on the first wireless device is to communicate with another device or unit, the application so-to-say goes through layers of different protocols. The different layers are illustrated in figures 9 and 10 to have layers laying on top of other layers. The higher layers of the so-called protocol stack usually relate to the application itself or high level operating system, HLOS, e.g. Android, iOS etc. Examples of higher layers are HTTP, TLS, TCP, and IP. The lower layers usually relate to the transport protocols, e.g. handling the radio bearers. Examples of lower layers are RRC, PDCP, RLC and MAC. The lower layer may be implemented as a lower layer protocol and higher layer may be implemented as a higher layer protocol. These are defined in relation to each other i.e. that the lower layer protocol is defined as existing "below" the higher layer protocol in the protocol architecture. For example, International Organization of Standardization, ISO, has defined an Open Systems Interconnection, OSI, model consisting of seven different logical layers. The lowest layer is Layer 1, the physical layer and the highest layer is Layer 7, the application layer. In this context, a lower layer has a layer number below a higher layer, for example Layer 2 is a lower layer for all Layers 3 to 7. A lower layer may be for example used for communication between the wireless device and the network node and may be responsible for radio interface security. A higher layer protocol may be used between the wireless device and a host or server being located in another network than the network node.

[00089] Consequently, in the first wireless device, a lower layer receives the packet from the higher layer of a protocol stack used in the wireless device for communication towards the network node or the second wireless device. The packet is to be transmitted to the network node or to the second wireless device.

[00090] In order for the first wireless device to transmit the packet, the first wireless device has to know which type of bearer to use for transmitting the packet. Thus the first wireless device, having knowledge about whether the packet

is already protected by higher layer security and consequently, determines the radio interface security setting based on the higher layer security setting.

[00091] Thereafter, the first wireless device transmits the received packet to the network node or to the second wireless device using the determined radio interface security setting.

[00092] The method performed by the first wireless device has the same possible advantages as the method performed by the first network node. One possible advantage is unnecessary data overhead may be avoided. Another possible advantage is that wasting of resources relating to providing radio interface security when not needed may be reduced. Still a possible advantage is that latency may be reduced.

[00093] As described above, the radio interface security setting may be associated with one of encrypting and non-encrypting of a radio bearer by means of which the packet is transmitted to the network node or the second wireless device, or with encrypting and non-encrypting the received packet.

[00094] As explained above, the radio interface security may be realised or implemented in different ways. An example is that the first network node and the wireless device may communicate by means of an encrypted radio bearer or by means of a non-encrypted radio bearer. Thus, the packet to be transmitted to the wireless device may either be transmitted on the encrypted radio bearer or on the non-encrypted radio bearer. Naturally, the encrypted radio bearer is a protected or secure radio bearer and thus a packet transmitted to the wireless device on the encrypted bearer is thus protected by means of the radio bearer itself. Likewise, the non-encrypted radio bearer is unprotected and a packet transmitted to the wireless device on the non-encrypted radio bearer is thus unprotected by the bearer.

[00095] Also, the higher layer security setting and the radio interface security setting may alternatively indicate a level of encryption (i.e. protection) that the higher layer security and the radio interface security respectively provide.

[00096] According to an embodiment, illustrated in **figure 2b**, when the higher layer security setting indicates that the packet is already protected by higher layer security, then the method 200 comprises transmitting 230a the packet to the network node or to the second wireless device by means of a non-encrypted radio bearer; and when the higher layer security setting indicates that the packet is not protected by higher layer security, then the method comprises transmitting 230b the packet to the network node or to the second wireless device by means of an encrypted radio bearer.

[00097] As described above, when the higher layer security setting indicates that the packet is already protected by higher layer security, the packet is already protected. Thus there is no need to use a more resource demanding encrypted bearer to transmit the packet to the wireless device. Consequently, the packet is transmitted to the second wireless device or to the network node by means of a non-encrypted radio bearer.

[00098] However, if the higher layer security setting indicates that the packet is not protected by higher layer security, the packet still needs to be transmitted to the second wireless device or the network node in a secure manner. In order to do so, the packet is transmitted to the second wireless device or the network node by means of an encrypted radio bearer, wherein the encrypted radio bearer protects the packet by itself.

[00099] According to still an embodiment, illustrated in **figure 2c**, if a non-encrypted radio bearer does not exist between the network node and the first wireless device or the second wireless device, the method 200 comprises requesting 230c the network node to set up a non-encrypted radio bearer between the first wireless device and the network node or between the first wireless device and the second wireless device and transmitting 230a the packet to the network node or to the second wireless device by means of the non-encrypted radio bearer once the non-encrypted radio bearer is set up.

[000100] It may be the case that there is no bearer of any kind established between the first wireless device and the second wireless device or the network

node. Alternatively, there may only be an encrypted radio bearer having been established between the first wireless device and the second wireless device or the network node. Thus, if the packet should be transmitted to the second wireless device or the network node by means of a non-encrypted bearer, the first wireless device requests the network node to set up a non-encrypted radio bearer between the first wireless device and the network node or the second wireless device. The first wireless device may not itself set up a radio bearer, only the network node may set up the different radio bearers. Hence, the first wireless device requests the network node to do so.

[000101] Once the non-encrypted radio bearer is set up between the first wireless device and the network node or between the first wireless device and the second wireless device, the first wireless device transmits the packet to the network node or to the second wireless device by means of the non-encrypted radio bearer.

[000102] In an example, illustrated in **figure 2d**, wherein the packet is to be transmitted from the first wireless device to the second wireless device, wherein if a non-encrypted radio bearer does not exist between the two, the method 200 comprises setting up 230d the non-encrypted radio bearer between the first and the second wireless device and transmitting 230aa the packet to the second wireless device.

[000103] In the case the first wireless device is to transmit the packet to the second wireless device, and not the network node, and there is no non-encrypted radio bearer between the two, the first wireless device sets up such a non-encrypted radio bearer between the first and the second wireless device and then transmits the packet to the second wireless device by means of the non-encrypted radio bearer.

[000104] The way in which the first wireless device sets up the non-encrypted radio bearer is out scope of this disclosure. However, the first wireless device may in an alternative request the network node to set up the non-encrypted radio bearer between the first wireless device and the second wireless device, and in another alternative, the first wireless device itself sets up the non-encrypted radio

bearer according to a protocol known to both the first and the second wireless device.

[000105] The higher layer security setting may be determined by inspecting the received packet; or by receiving an indication from the higher layer that higher layer encryption is being used.

[000106] The first wireless device may perform, at the lower layer, a packet inspection in the same or similar manner as described above for the first network node. Alternatively, the lower payer may receive an indication form the higher layer that the encryption is being used. Since the higher layer is responsible for applying the higher layer security, e.g. by means of encryption, the higher layer may inform the lower layer that the encryption has been done. Thus, there is no need for the lower layer to also perform encryption, but instead, the first wireless device may transmit the packet on the non-encrypted radio bearer since the packet is already protected.

[000107] In an example, illustrated in **figure 2e**, if a non-encrypted radio bearer doesn't exist between the first wireless device and the network node or the second wireless device, the method 200 comprises refraining 230e from performing radio bearer level encryption, marking 230f the received packet with information that no radio bearer level encryption has been performed and transmitting 230g the packet by means of an encrypted radio bearer.

[000108] As described above, it is assumed in this scenario that the radio interface security also, or alternatively, relates to an encryption of the packet itself. Thus, in this example, the packet is itself already encrypted and thus needs not to be further encrypted in order to obtain the radio bearer level encryption. The first wireless device thus refrains from further encrypting the packet, i.e. does not perform a radio bearer level encryption, but instead marks the packet with information that no radio bearer level encryption has been performed. By marking the packet in this manner, the network node or the second wireless device is informed, when receiving the packet, that the packet is not encrypted on radio bearer level, and that the wireless device should not perform any decryption of the

received packet. The first wireless device then transits the packet to the wireless device by means of the encrypted radio bearer, assuming that such a radio bearer exists. If not, such a bearer is first set up and then the packet is transmitted. This also means that the encrypted radio bearer has additional capabilities to transport packets without performing encryption on radio bearer level and to convey the indication that no radio bearer level encryption has been performed.

[000109] In still an example, illustrated in **figure 2f**, if a non-encrypted radio bearer doesn't exist between the first wireless device and the network node or the second wireless device, the method 200 comprises modifying 230h an existing encrypted radio bearer to be non-encrypted and transmitting 230a the received packet to the network node or to the second wireless device by means of the non-encrypted radio bearer.

[000110] The manner in which the first wireless device modifies the existing encrypted radio bearer to be non-encrypted may be done in the same manner as for the first network node described above in conjunction with figures 1a-1f.

[000111] The modification may comprise signalling from the first wireless device to either the network node or the second wireless device to switch off an encryption function or algorithm running on the first wireless device, the second wireless device and/or the network node, and in this manner switching off the encryption of the radio bearer thus making it a non-encrypted radio bearer. Once the radio bearer has been modified and operates as a non-encrypted radio bearer, the first wireless device transmits the packet to the network node or to the second wireless device by means of the non-encrypted radio bearer.

[000112] Embodiments herein also relate to a first network node adapted for transmitting data to a wireless device. The first network node has the same technical features, objects and advantages as the method performed by the first network node described above. The first network node will thus only be described in brief in order to avoid unnecessary repetition. The first network node will be described with reference to figures 3 and 5.

[000113] The first network node 300, 500 is configured to receive a packet from a second network node in the wireless communication network, the packet being destined for the wireless device; and to inspect the received packet by performing a packet inspection to determine a higher layer security setting. The first network node is further configured to determine a radio interface security setting based on the determined higher layer security setting; and to transmit the received packet to the wireless device using the determined radio interface security setting.

[000114] The first network node 300, 500 may be implemented or realised in different ways. An exemplifying implementation is illustrated in figure 3. **Figure 3** illustrates the first network node 300 comprising a processor 321 and memory 322, the memory comprising instructions, e.g. by means of a computer program 323, which when executed by the processor 321 causes the first network node 300 to receive a packet from a second network node in the wireless communication network, the packet being destined for the wireless device; to inspect the received packet by performing a packet inspection to determine a higher layer security setting; to determine a radio interface security setting based on the determined higher layer security setting; and to transmit the received packet to the wireless device using the determined radio interface security setting.

[000115] Figure 3 also illustrates the network node 300 comprising a memory 310. It shall be pointed out that figure 3 is merely an exemplifying illustration and memory 310 may be optional, be a part of the memory 322 or be a further memory of the network node. The memory may for example comprise information relating to the network node 300, to statistics of operation of the network node 300, just to give a couple of illustrating examples. Figure 3 further illustrates the network node 300 comprising processing means 320, which comprises the memory 322 and the processor 321. Still further, figure 3 illustrates the network node 300 comprising a communication unit 330. The communication unit 330 may comprise an interface through which the network node 300 communicates with other nodes or entities of the communication network as well as wireless device of the communication network. Figure 3 also illustrates the network node 300 comprising further functionality 340. The further functionality 340 may comprise hardware of software

necessary for the network node 300 to perform different tasks that are not disclosed herein. Merely as an illustrative example, the further functionality may comprise a scheduler for scheduling transmissions from the network node 300 and/or for transmissions from wireless devices with which the network node 300 communicates with.

[000116] An alternative exemplifying implementation of the first network node is illustrated in figure 5. **Figure 5** illustrates the first network node 500 comprising a receiving unit 503 for receiving a packet from a second network node in the wireless communication network, the packet being destined for the wireless device; and an inspection unit 504 for inspecting the received packet by performing a packet inspection to determine a higher layer security setting. The first network node 500 further comprises a determining unit 505 for determining a radio interface security setting based on the determined higher layer security setting; and a transmitting unit 506 for transmitting the received packet to the wireless device using the determined radio interface security setting.

[000117] The first network node has the same possible advantages as the method performed by the first network node described above. One possible advantage is unnecessary data overhead may be avoided. Another possible advantage is that wasting of resources relating to providing radio interface security when not needed may be reduced. Still a possible advantage is that latency may be reduced.

[000118] In an example, the radio interface security setting is associated with one of encrypting and non-encrypting of a radio bearer by means of which the packet is transmitted to the wireless device, or with encrypting and non-encrypting the received packet.

[000119] The radio interface security setting may be associated with a level of encryption of a radio bearer by means of which the packet is transmitted to the wireless device.

[000120] According to an embodiment, when the higher layer security setting indicates that the packet is already protected by higher layer security, then the first

network node 300, 500 is configured to transmit the received packet to the wireless device by means of a non-encrypted radio bearer; and when the higher layer security setting indicates that the packet is not protected by higher layer security, then the network node 300, 500 is configured to transmit the received packet to the wireless device by means of an encrypted radio bearer.

[000121] Referring to the two given implementation examples given above, according to the first implementation example, the memory 322 further comprises instructions, which when executed by the processor 321 causes the first network node 300 to transmit the received packet to the wireless device by means of a non-encrypted radio bearer when the higher layer security setting indicates that the packet is already protected by higher layer security, and to transmit the received packet to the wireless device by means of an encrypted radio bearer when the higher layer security setting indicates that the packet is not protected by higher layer security. According to the second implementation example, the transmitting unit 506 of the first network node 500 is further for transmitting the received packet to the wireless device by means of a non-encrypted radio bearer when the higher layer security setting indicates that the packet is already protected by higher layer security, and for transmitting the received packet to the wireless device by means of an encrypted radio bearer when the higher layer security setting indicates that the packet is not protected by higher layer security.

[000122] According to an embodiment, if a non-encrypted radio bearer does not exist between the first network node and the wireless device, the first network node 300, 500 is configured to set up a non-encrypted radio bearer between the first network node and the wireless device and to transmit the received packet to the wireless device by means of the non-encrypted radio bearer.

[000123] According to yet an embodiment, if a non-encrypted radio bearer doesn't exist between the first network node and the wireless device, the first network node 300, 500 is configured to refrain from performing radio bearer level encryption, to mark the received packet with information that no radio bearer level encryption has been performed and to transmit the packet to the wireless device by means of an encrypted radio bearer.

[000124] According to still an embodiment, if a non-encrypted radio bearer doesn't exist between the first network node and the wireless device, the first network node 300, 500 is configured to modify an existing encrypted radio bearer to be non-encrypted and to transmit the received packet to the wireless device by means of the non-encrypted radio bearer

[000125] As described above, the packet inspection is at least one of an IP header classification, shallow inspection, deep packet inspection, and heuristic detection; or any other packet inspection mechanism.

[000126] According to yet another embodiment, the first network node is further being configured to store information relating to the received packet obtained from the packet inspection, to receive a further packet destined for the wireless device, to perform a packet inspection on the received further packet to determine the higher layer security setting also using the stored information, and to transmit the received packet to the wireless device according to the previously determined radio interface security setting.

[000127] Embodiments herein also relate to a first wireless device adapted for transmitting data to a second wireless device or to a network node of a wireless communication network. The first wireless device has the same technical features, objects and advantages as the method performed by the first wireless device described above. The first wireless device will thus only be described in brief in order to avoid unnecessary repetition. The first wireless device will be described with reference to figures 4 and 6.

[000128] The first wireless device 400, 600 is configured to receive, at a lower layer from a higher layer of a protocol stack used in the wireless device for communication towards the network node or the second wireless device, a packet to be transmitted to the network node or to the second wireless device. The first wireless device 400, 600 is further configured to determine a radio interface security setting based on a higher layer security setting; and to transmit the received packet to the network node or to the second wireless device using the determined radio interface security setting.

[000129] Just as for the first network node described above, also the first wireless device may be implemented or realised in different ways. An exemplifying implementation is illustrated in figure 4. **Figure 4** illustrates the first wireless device comprising a processor 421 and memory 422, the memory comprising instructions, e.g. by means of a computer program 423, which when executed by the processor 421 causes the first wireless device 400 to to receive, at a lower layer from a higher layer of a protocol stack used in the wireless device for communication towards the network node or the second wireless device, a packet to be transmitted to the network node or to the second wireless device; to determine a radio interface security setting based on a higher layer security setting; and to transmit the received packet to the network node or to the second wireless device using the determined radio interface security setting.

[000130] Figure 4 also illustrates the wireless device 400 comprising a memory 410. It shall be pointed out that figure 4 is merely an exemplifying illustration and memory 410 may be optional, be a part of the memory 422 or be a further memory of the wireless device 400. The memory may for example comprise information relating to the wireless device 400, to statistics of operation of the wireless device 400, or to information received from the network node, just to give a couple of illustrating examples. Figure 4 further illustrates the wireless device 400 comprising processing means 420, which comprises the memory 422 and the processor 421. Still further, figure 4 illustrates the wireless device 400 comprising a communication unit 430. The communication unit 430 may comprise an interface through which the wireless device 400 communicates with other nodes or entities of the communication network as well as other wireless devices of the communication network. Figure 4 also illustrates the wireless device 400 comprising further functionality 440. The further functionality 440 may comprise hardware of software necessary for the wireless device 400 to perform different tasks that are not disclosed herein.

[000131] An alternative exemplifying implementation of the first wireless device is illustrated in figure 6. **Figure 6** illustrates the first network node 600 comprising a receiving unit 603 for receiving, at a lower layer from a higher layer of a protocol

stack used in the wireless device for communication towards the network node or the second wireless device, a packet to be transmitted to the network node or to the second wireless device; a determining unit 604 for determining a radio interface security setting based on a higher layer security setting; and a transmitting unit 605 for transmitting the received packet to the network node or to the second wireless device using the determined radio interface security setting.

[000132] The first wireless device has the same possible advantages as the method performed by the first wireless device described above. One possible advantage is that unnecessary data overhead may be avoided. Another possible advantage is that wasting of resources relating to providing radio interface security when not needed may be reduced. Still a possible advantage is that latency may be reduced.

[000133] The radio interface security setting may be associated with one of encrypting and non-encrypting of a radio bearer by means of which the packet is transmitted to the network node or the second wireless device, or with encrypting and non-encrypting the received packet.

[000134] According to an embodiment, when the higher layer security setting indicates that the packet is already protected by higher layer security, then the first wireless device 400, 600 is configured to transmit the packet to the network node or to the second wireless device by means of a non-encrypted radio bearer; and when the higher layer security setting indicates that the packet is not protected by higher layer security, then the first wireless device 400, 600 is configured to transmit the packet to the network node or to the second wireless device by means of an encrypted radio bearer.

[000135] According to yet an embodiment, if a non-encrypted radio bearer does not exist between the network node and the first wireless device or the second wireless device, the first wireless device 400, 600 is configured to request the network node to set up a non-encrypted radio bearer between the first wireless device and the network node or the second wireless device and to transmit the

packet to the network node or to the second wireless device by means of the non-encrypted radio bearer once the non-encrypted radio bearer is set up.

[000136] According to still an embodiment, wherein the packet is to be transmitted from the first wireless device to the second wireless device, wherein if a non-encrypted radio bearer does not exist between the two, the first wireless device 400, 600 is configured to set up the non-encrypted radio bearer between the first and the second wireless device and to transmit the packet to the second wireless device.

[000137] The higher layer security setting may be determined by inspecting the received packet; or by receiving an indication from the higher layer that higher layer encryption is being used.

[000138] According to a further embodiment, if a non-encrypted radio bearer doesn't exist between the first wireless device and the network node or the second wireless device, the first wireless device 400, 600 is configured to refrain from performing radio bearer level encryption, to mark the received packet with information that no radio bearer level encryption has been performed and to transmitting the packet by means of an encrypted radio bearer.

[000139] According to another embodiment, if a non-encrypted radio bearer doesn't exist between the first wireless device and the network node or the second wireless device, the first wireless device 400, 600 is configured to modify an existing encrypted radio bearer to be non-encrypted and to transmit the received packet to the network node or to the second wireless device by means of the non-encrypted radio bearer.

[000140] In figure 5, the first network node 500 is also illustrated comprising a communication unit 501. Through this unit, the first network node 500 is adapted to communicate with other nodes and/or entities in the wireless communication network. The communication unit 501 may comprise more than one receiving arrangement. For example, the communication unit 501 may be connected to both a wire and an antenna, by means of which the first network node 500 is enabled to

communicate with other nodes and/or entities in the wireless communication network. Similarly, the communication unit 501 may comprise more than one transmitting arrangement, which in turn may be connected to both a wire and an antenna, by means of which the first network node 500 is enabled to communicate with other nodes and/or entities in the wireless communication network. The first network node 500 further comprises a memory 502 for storing data. Further, the first network node 500 may comprise a control or processing unit (not shown) which in turn is connected to the different units 503-506. It shall be pointed out that this is merely an illustrative example and the first network node 500 may comprise more, less or other units or modules which execute the functions of the first network node 500 in the same manner as the units illustrated in figure 5.

[000141] It should be noted that figure 5 merely illustrates various functional units in the first network node 500 in a logical sense. The functions in practice may be implemented using any suitable software and hardware means/circuits etc. Thus, the embodiments are generally not limited to the shown structures of the first network node 500 and the functional units. Hence, the previously described exemplary embodiments may be realised in many ways. For example, one embodiment includes a computer-readable medium having instructions stored thereon that are executable by the control or processing unit for executing the method steps in the first network node 500. The instructions executable by the computing system and stored on the computer-readable medium perform the method steps of the first network node 500 as set forth in the claims.

[000142] In figure 6, the first wireless device 600 is also illustrated comprising a communication unit 601. Through this unit, the first wireless device 600 is adapted to communicate with other nodes and/or entities in the wireless communication network. The communication unit 601 may comprise more than one receiving arrangement. For example, the communication unit may be connected to both a wire and an antenna, by means of which the first wireless device 600 is enabled to communicate with other nodes and/or entities in the wireless communication network. Similarly, the communication unit 601 may comprise more than one transmitting arrangement, which in turn may be connected to both a wire and an

antenna, by means of which the first wireless device 600 is enabled to communicate with other nodes and/or entities in the wireless communication network. The first wireless device 600 further comprises a memory 602 for storing data. Further, the first wireless device 600 may comprise a control or processing unit (not shown) which in turn is connected to the different units 603-605. It shall be pointed out that this is merely an illustrative example and the first wireless device 600 may comprise more, less or other units or modules which execute the functions of the first wireless device 600 in the same manner as the units illustrated in figure 6.

[000143] It should be noted that figure 6 merely illustrates various functional units in the first wireless device 600 in a logical sense. The functions in practice may be implemented using any suitable software and hardware means/circuits etc. Thus, the embodiments are generally not limited to the shown structures of the first wireless device 600 and the functional units. Hence, the previously described exemplary embodiments may be realised in many ways. For example, one embodiment includes a computer-readable medium having instructions stored thereon that are executable by the control or processing unit for executing the method steps in the first wireless device 600. The instructions executable by the computing system and stored on the computer-readable medium perform the method steps of the first wireless device 600 as set forth in the claims.

[000144] Figure 7 schematically shows an embodiment of an arrangement in a first network node 700. Comprised in the arrangement in the first network node 700 are here a processing unit 706, e.g. with a Digital Signal Processor, DSP. The processing unit 706 may be a single unit or a plurality of units to perform different actions of procedures described herein. The first network node 700 may also comprise an input unit 702 for receiving signals from other entities, and an output unit 704 for providing signal(s) to other entities. The input unit and the output unit may be arranged as an integrated entity or as illustrated in the example of figure 5, as one or more interfaces, or communication units, 501.

[000145] Furthermore, the first network node 700 comprises at least one computer program product 708 in the form of a non-volatile memory, e.g. an Electrically

Erasable Programmable Read-Only Memory, EEPROM, a flash memory and a hard drive. The computer program product 708 comprises a computer program 710, which comprises code means, which when executed in the processing unit 706 in the arrangement in the first network node 700 causes the first wireless device to perform the actions e.g. of the procedure described earlier in conjunction with figures 1a-1f.

[000146] The computer program 710 may be configured as a computer program code structured in computer program modules 710a-710e. Hence, in an exemplifying embodiment, the code means in the computer program of the first network node 700 comprises an receiving unit, or module, for receiving a packet from a second network node in the wireless communication network, the packet being destined for the wireless device .The computer program further comprises a inspecting unit, or module, for inspecting the received packet by performing a packet inspection to determine a higher layer security setting. Still further, the computer program comprises a determining unit, or module, for determining a radio interface security setting based on the determined higher layer security setting; and a transmitting unit, or module, for transmitting received packet to the wireless device using the determined radio interface security setting.

[000147] The computer program modules could essentially perform the actions of the flow illustrated in figure 1a, to emulate the first wireless device 500. In other words, when the different computer program modules are executed in the processing unit 706, they may correspond to the units 503-506 of figure 5.

[000148] Figure 8 schematically shows an embodiment of a first wireless device 800. Comprised in the first wireless device 800 are here a processing unit 806, e.g. with a Digital Signal Processor. The processing unit 806 may be a single unit or a plurality of units to perform different actions of procedures described herein. The first wireless device 800 may also comprise an input unit 802 for receiving signals from other entities, and an output unit 804 for providing signal(s) to other entities. The input unit and the output unit may be arranged as an integrated entity or as illustrated in the example of figure 6, as one or more interfaces, or communication units, 601.

[000149] Furthermore, the first wireless device 800 comprises at least one computer program product 808 in the form of a non-volatile memory, e.g. an Electrically Erasable Programmable Read-Only Memory, EEPROM, a flash memory and a hard drive. The computer program product 808 comprises a computer program 810, which comprises code means, which when executed in the processing unit 806 in the first wireless device 800 causes the first wireless device 800 to perform the actions e.g. of the procedure described earlier in conjunction with figures 2a-2f.

[000150] The computer program 810 may be configured as a computer program code structured in computer program modules 810a-810e. Hence, in an exemplifying embodiment, the code means in the computer program of the first wireless device 800 comprises a receiving unit, or module, for receiving, at a lower layer from a higher layer of a wireless communication protocol used between the wireless device and the network node or the second wireless device, a packet to be transmitted to the network node or to the second wireless device. The computer program further comprises a determining unit, or module, for determining a radio interface security setting based on a higher layer security setting; and a transmitting unit, or module, for transmitting the received packet to the network node or to the second wireless device using the determined radio interface security setting.

[000151] The computer program modules could essentially perform the actions of the flow illustrated in figure 2a, to emulate the first wireless device 600. In other words, when the different computer program modules are executed in the processing unit 806, they may correspond to the units 603-605 of figure 6.

[000152] Although the code means in the respective embodiments disclosed above in conjunction with figures 5 and 6 are implemented as computer program modules which when executed in the respective processing unit causes the first network node and the first wireless device respectively to perform the actions described above in the conjunction with figures mentioned above, at least one of the code means may in alternative embodiments be implemented at least partly as hardware circuits.

[000153] The processor may be a single Central Processing Unit, CPU, but could also comprise two or more processing units. For example, the processor may include general purpose microprocessors; instruction set processors and/or related chips sets and/or special purpose microprocessors such as Application Specific Integrated Circuits, ASICs. The processor may also comprise board memory for caching purposes. The computer program may be carried by a computer program product connected to the processor. The computer program product may comprise a computer readable medium on which the computer program is stored. For example, the computer program product may be a flash memory, a Random-Access Memory RAM, Read-Only Memory, ROM, or an EEPROM, and the computer program modules described above could in alternative embodiments be distributed on different computer program products in the form of memories within the first network node and the first wireless device respectively.

[000154] It is to be understood that the choice of interacting units, as well as the naming of the units within this disclosure are only for exemplifying purpose, and nodes suitable to execute any of the methods described above may be configured in a plurality of alternative ways in order to be able to execute the suggested procedure actions.

[000155] It should also be noted that the units described in this disclosure are to be regarded as logical entities and not with necessity as separate physical entities.

[000156] Figure 9 is an illustration of different protocol stacks in an LTE communication network. A UE, i.e. a wireless device, is making use of an application from a host or server. The host or server may be located in a network other than the LTE network, e.g. in the Internet. In order for the UE to be able to communicate with the host/server, several different protocols are used and they are put on top of each other. Assuming that the host/server is located in the Internet, the host/server may use a transport protocol called Internet Protocol, IP. Consequently, under the application, the IP protocol is present as illustrated in figure 9. Underneath the IP protocol, layer 2, L2, and layer 1, L1, protocols are implemented. The L1 and L2 protocols as well as the IP protocol may be referred

to as lower layer protocols. Not shown in figure 9 is that there may be one or more protocols present which generally is referred to as higher layer protocols (for example a TCP protocol layer between the application and the IP layers).

[000157] The host/server may communicate with the UE of the wireless communication network via a gateway e.g. a PDN-GW, a S-GW, and a RBS such as an eNodeB, eNB. The gateway and eNB must be able to communicate in-between themselves, which is illustrated a plurality of different protocols.

[000158] Figure 10 is a simplified example of a wireless device communicating with a host/server by means of two intermediate nodes, first and second network node. In figure 10, the higher layer protocol(s) may apply a higher layer security, e.g. by encrypting the packet generated by the application and to be transmitted to the wireless device. Thus, the higher layer protocol(s) encrypts the generated packet before handing it over to the lower layers, illustrated in figure 10 as layer 3, L3 and under L3, layer 2 and 1.The host/server transmits the packet via the second network node and the first network node to the wireless device. When the packet reaches the first network node, to be transmitted to the wireless device, the first network node inspects the packet to determine the higher layer security setting. Based on the result of the inspection, the first network node thus determines a radio interface security between the first network node and the wireless device. Then the first network node transmits the packet to the wireless device using the determined radio interface security setting.

[000159] It shall be pointed out that figures 9 and 10 are merely illustrative examples. Looking back at figure 2a and assuming that the first wireless device is to transmit the packet to the second wireless device, then the first network node of figure 10 would be the second wireless device. In such a case, the “Relay” that is depicted in figure 10 of the first network node would instead be the “Higher Layer “Security” and the “Application” of the protocol stack as for the first wireless device and the host/server, since the second wireless device would correspond to the host server.

[000160] While the embodiments have been described in terms of several embodiments, it is contemplated that alternatives, modifications, permutations and equivalents thereof will become apparent upon reading of the specifications and study of the drawings. It is therefore intended that the following appended claims include such alternatives, modifications, permutations and equivalents as fall within the scope of the embodiments and defined by the pending claims.

- - -

CLAIMS

1. A method (100) performed by a first network node in a wireless communication network for transmitting data to a wireless device, the method comprising:

- receiving (110) a packet from a second network node in the wireless communication network, the packet being destined for the wireless device,
- inspecting (120) the received packet by performing a packet inspection to determine a higher layer security setting,
- determining (130) a radio interface security setting based on the determined higher layer security setting, and
- transmitting (140) the received packet to the wireless device using the determined radio interface security setting.

2. A method (100) according to claim 1, wherein the radio interface security setting is associated with one of encrypting and non-encrypting of a radio bearer by means of which the packet is transmitted to the wireless device, or with encrypting and non-encrypting the received packet.

3. A method (100) according to claim 1, wherein the radio interface security setting is associated with a level of encryption of a radio bearer by means of which the packet is transmitted to the wireless device.

4. A method (100) according to claim 2 or 3, wherein when the higher layer security setting indicates that the packet is already protected by higher layer security, then the method comprises transmitting (140a) the received packet to the wireless device by means of a non-encrypted radio bearer; and when the higher layer security setting indicates that the packet is not protected by higher layer security, then the method comprises transmitting (140b) the received packet to the wireless device by means of an encrypted radio bearer.

5. A method (100) according to claim 4, wherein if a non-encrypted radio bearer does not exist between the first network node and the wireless device, the

method comprises setting up (140c) a non-encrypted radio bearer between the first network node and the wireless device and transmitting (140a) the received packet to the wireless device by means of the non-encrypted radio bearer.

6. A method (100) according to claim 4, wherein if a non-encrypted radio bearer doesn't exist between the first network node and the wireless device, the method comprises refraining (140d) from performing radio bearer level encryption, marking (140e) the received packet with information that no radio bearer level encryption has been performed and transmitting (140f) the packet to the wireless device by means of an encrypted radio bearer.

7. A method (100) according to claim 4, wherein if a non-encrypted radio bearer doesn't exist between the first network node and the wireless device, the method comprises modifying (140g) an existing encrypted radio bearer to be non-encrypted and transmitting (140a) the received packet to the wireless device by means of the non-encrypted radio bearer.

8. A method (100) according to any of claims 1-7, wherein the packet inspection is at least one of an Internet Protocol, IP, header classification, shallow inspection, deep packet inspection, and heuristic detection; or any other packet inspection mechanism.

9. A method (100) according to claim 8, further comprising storing (121) information relating to the received packet obtained from the packet inspection, receiving (110a) a further packet destined for the wireless device, performing (120a) a packet inspection on the received further packet to determine the higher layer security setting also using the stored information, and transmitting the received packet to the wireless device according to the previously determined radio interface security setting.

10. A method (200) performed by a first wireless device for transmitting data to a second wireless device or to a network node of a wireless communication network, the method comprising:

- receiving (210), at a lower layer from a higher layer of a protocol stack used in the wireless device for communication towards the network node or the second wireless device, a packet to be transmitted to the network node or to the second wireless device,
- determining (220) a radio interface security setting based on a higher layer security setting, and
- transmitting (230) the received packet to the network node or to the second wireless device using the determined radio interface security setting.

11. A method (200) according to claim 10, wherein the radio interface security setting is associated with one of encrypting and non-encrypting of a radio bearer by means of which the packet is transmitted to the network node or the second wireless device, or with encrypting and non-encrypting the received packet.

12. A method (200) according to claim 11, wherein when the higher layer security setting indicates that the packet is already protected by higher layer security, then the method comprises transmitting (230a) the packet to the network node or to the second wireless device by means of a non-encrypted radio bearer; and when the higher layer security setting indicates that the packet is not protected by higher layer security, then the method comprises transmitting (230b) the packet to the network node or to the second wireless device by means of an encrypted radio bearer.

13. A method (200) according to claim 12, wherein if a non-encrypted radio bearer does not exist between the network node and the first wireless device or the second wireless device, the method comprises requesting (230c) the network node to set up a non-encrypted radio bearer between the first wireless device and the network node or the second wireless device and transmitting (230a) the packet to the network node or to the second wireless device by means of the non-encrypted radio bearer once the non-encrypted radio bearer is set up.

14. A method (200) according to any of claims 10-12, wherein the packet is to be transmitted from the first wireless device to the second wireless device,

wherein if a non-encrypted radio bearer does not exist between the two, the method comprises setting up (230d) the non-encrypted radio bearer between the first and the second wireless device and transmitting (230aa) the packet to the second wireless device.

15. A method (200) according to claims 10-14, wherein the higher layer security setting is determined by inspecting the received packet; or by receiving an indication from the higher layer that higher layer encryption is being used.

16. A method (200) according to any of claims 10-12, wherein if a non-encrypted radio bearer doesn't exist between the first wireless device and the network node or the second wireless device, the method comprises refraining (230e) from performing radio bearer level encryption, marking (230f) the received packet with information that no radio bearer level encryption has been performed and transmitting (230g) the packet by means of an encrypted radio bearer.

17. A method (200) according to any of claims 10-12, wherein if a non-encrypted radio bearer doesn't exist between the first wireless device and the network node or the second wireless device, the method comprises modifying (230h) an existing encrypted radio bearer to be non-encrypted and transmitting (230a) the received packet to the network node or to the second wireless device by means of the non-encrypted radio bearer.

18. A first network node (300, 500) in a wireless communication network for transmitting data to a wireless device, the first network node (300, 500) being configured to:

- receive a packet from a second network node in the wireless communication network, the packet being destined for the wireless device,
- inspect the received packet by performing a packet inspection to determine a higher layer security setting,
- determine a radio interface security setting based on the determined higher layer security setting, and
- transmit the received packet to the wireless device using the determined radio interface security setting.

19. A first network node (300, 500) according to claim 18, wherein the radio interface security setting is associated with one of encrypting and non-encrypting of a radio bearer by means of which the packet is transmitted to the wireless device, or with encrypting and non-encrypting the received packet.

20. A first network node (300, 500) according to claim 18, wherein the radio interface security setting is associated with a level of encryption of a radio bearer by means of which the packet is transmitted to the wireless device.

21. A first network node (300, 500) according to claim 19, wherein when the higher layer security setting indicates that the packet is already protected by higher layer security, then the network node (300, 500) is configured to transmit the received packet to the wireless device by means of a non-encrypted radio bearer; and when the higher layer security setting indicates that the packet is not protected by higher layer security, then the network node (300, 500) is configured to transmit the received packet to the wireless device by means of an encrypted radio bearer.

22. A first network node (300, 500) according to claim 21, wherein if a non-encrypted radio bearer does not exist between the first network node and the wireless device, the first network node (300, 500) is configured to set up a non-encrypted radio bearer between the first network node and the wireless device and to transmit the received packet to the wireless device by means of the non-encrypted radio bearer.

23. A first network node (300, 500) according to claim 21, wherein if a non-encrypted radio bearer doesn't exist between the first network node and the wireless device, the first network node (300, 500) is configured to refrain from performing radio bearer level encryption, to mark the received packet with information that no radio bearer level encryption has been performed and to transmit the packet to the wireless device by means of an encrypted radio bearer.

24. A first network node (300, 500) according to claim 21, wherein if a non-encrypted radio bearer doesn't exist between the first network node and the

wireless device, the first network node (300, 500) is configured to modify an existing encrypted radio bearer to be non-encrypted and to transmit the received packet to the wireless device by means of the non-encrypted radio bearer.

25. A first network node (300, 500) according to any of claims 18-24, wherein the packet inspection is at least one of an Internet Protocol, IP, header classification, shallow inspection, deep packet inspection, and heuristic detection; or any other packet inspection mechanism.

26. A first network node (300, 500) according to claim 25, further being configured to store information relating to the received packet obtained from the packet inspection, to receive a further packet destined for the wireless device, to perform a packet inspection on the received further packet to determine the higher layer security setting also using the stored information, and to transmit the received packet to the wireless device according to the previously determined radio interface security setting.

27. A first wireless device (400, 600) for transmitting data to a second wireless device or to a network node of a wireless communication network, the first wireless device (400, 600) being configured to:

- receive, at a lower layer from a higher layer of a protocol stack used in the wireless device for communication towards the network node or the second wireless device, a packet to be transmitted to the network node or to the second wireless device,
- determine a radio interface security setting based on a higher layer security setting, and to
- transmit the received packet to the network node or to the second wireless device using the determined radio interface security setting.

28. A first wireless device (400, 600) according to claim 27, wherein the radio interface security setting is associated with one of encrypting and non-encrypting of a radio bearer by means of which the packet is transmitted to the network node or the second wireless device, or with encrypting and non-encrypting the received packet.

29. A first wireless device (400, 600) according to claim 28, wherein when the higher layer security setting indicates that the packet is already protected by higher layer security, then the first wireless device (400, 600) is configured to transmit the packet to the network node or to the second wireless device by means of a non-encrypted radio bearer; and when the higher layer security setting indicates that the packet is not protected by higher layer security, then the first wireless device (400, 600) is configured to transmit the packet to the network node or to the second wireless device by means of an encrypted radio bearer.

30. A first wireless device (400, 600) according to claim 29, wherein if a non-encrypted radio bearer does not exist between the network node and the first wireless device or the second wireless device, the first wireless device (400, 600) is configured to request the network node to set up a non-encrypted radio bearer between the first wireless device and the network node or the second wireless device and to transmit the packet to the network node or to the second wireless device by means of the non-encrypted radio bearer once the non-encrypted radio bearer is set up.

31. A first wireless device (400, 600) according to any of claims 27-29, wherein the packet is to be transmitted from the first wireless device to the second wireless device, wherein if a non-encrypted radio bearer does not exist between the two, the first wireless device (400, 600) is configured to set up the non-encrypted radio bearer between the first and the second wireless device and to transmit the packet to the second wireless device.

32. A first wireless device (400, 600) according to claims 27-31, wherein the higher layer security setting is determined by inspecting the received packet; or by receiving an indication from the higher layer that higher layer encryption is being used.

33. A first wireless device (400, 600) according to any of claims 27-29, wherein if a non-encrypted radio bearer doesn't exist between the first wireless device and the network node or the second wireless device, the first wireless device (400, 600) is configured to refrain from performing radio bearer level

encryption, to mark the received packet with information that no radio bearer level encryption has been performed and to transmitting the packet by means of an encrypted radio bearer.

34. A first wireless device (400, 600) according to any of claims 27-29, wherein if a non-encrypted radio bearer doesn't exist between the first wireless device and the network node or the second wireless device, the first wireless device (400, 600) is configured to modify an existing encrypted radio bearer to be non-encrypted and to transmit the received packet to the network node or to the second wireless device by means of the non-encrypted radio bearer.

35. A Computer program (710), comprising computer readable code means, which when run in a processing unit (706) comprised in an arrangement in a first network node (500, 700) according to claims 18-26 causes the first network node (500, 700) to perform the corresponding method according to claims 1-9.

36. A Computer program product (708) comprising the computer program (710) according to claim 35.

37. A Computer program (810), comprising computer readable code means, which when run in a processing unit (806) comprised in an arrangement in a first wireless device (600, 800) according to claims 27-34 causes the first wireless device (600, 800) to perform the corresponding method according to claims 10-17.

38. A Computer program product (808) comprising the computer program (810) according to claim 37.

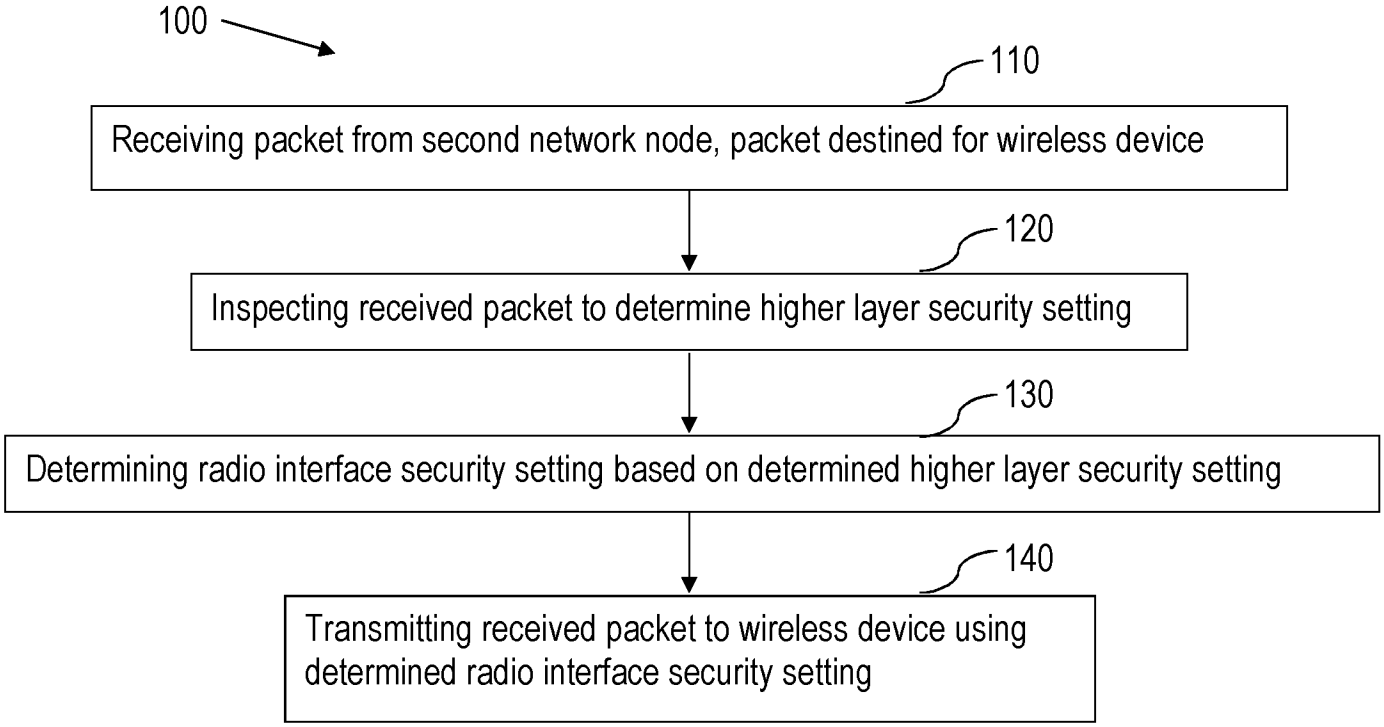
100
110
Receiving packet from second network node, packet destined for wireless device
120
Inspecting received packet to determine higher layer security setting
130
Determining radio interface security setting based on determined higher layer security setting
140
Transmitting received packet to wireless device using determined radio interface security setting

Fig. 1a

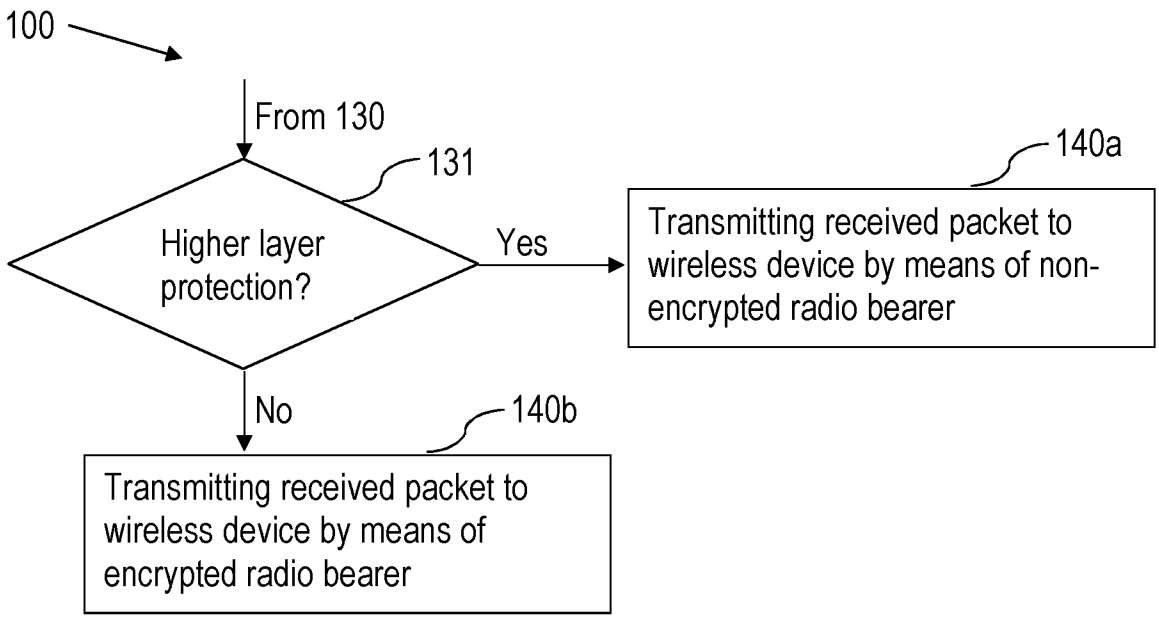
100
From 130
131
Higher layer protection?
Yes
140a
Transmitting received packet to wireless device by means of non-encrypted radio bearer
No
140b
Transmitting received packet to wireless device by means of encrypted radio bearer

Fig. 1b

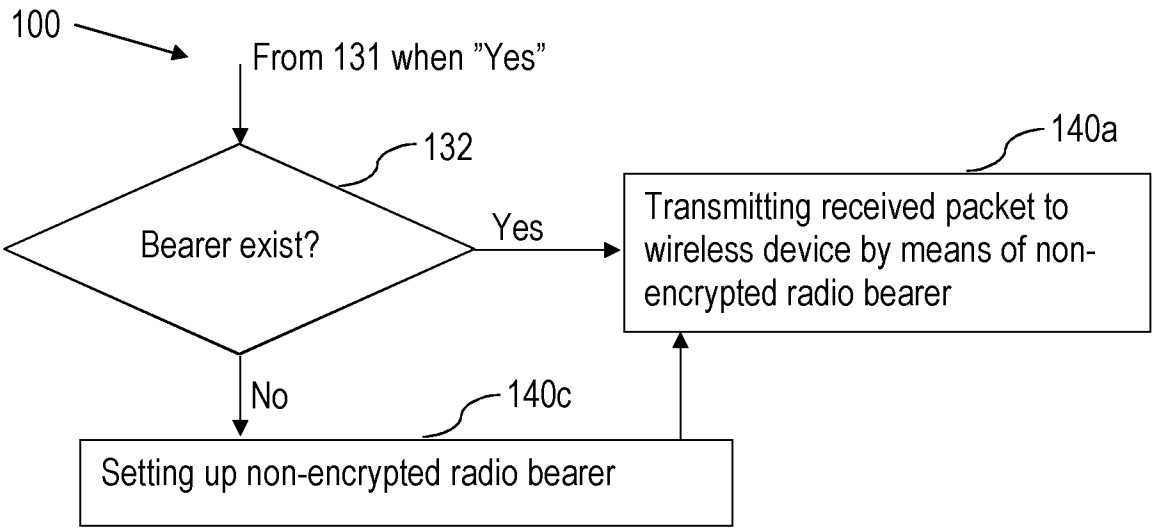
100
From 131 when "Yes"
132
Bearer exist?
Yes
140a
Transmitting received packet to wireless device by means of non-encrypted radio bearer
No
140c
Setting up non-encrypted radio bearer

Fig. 1c

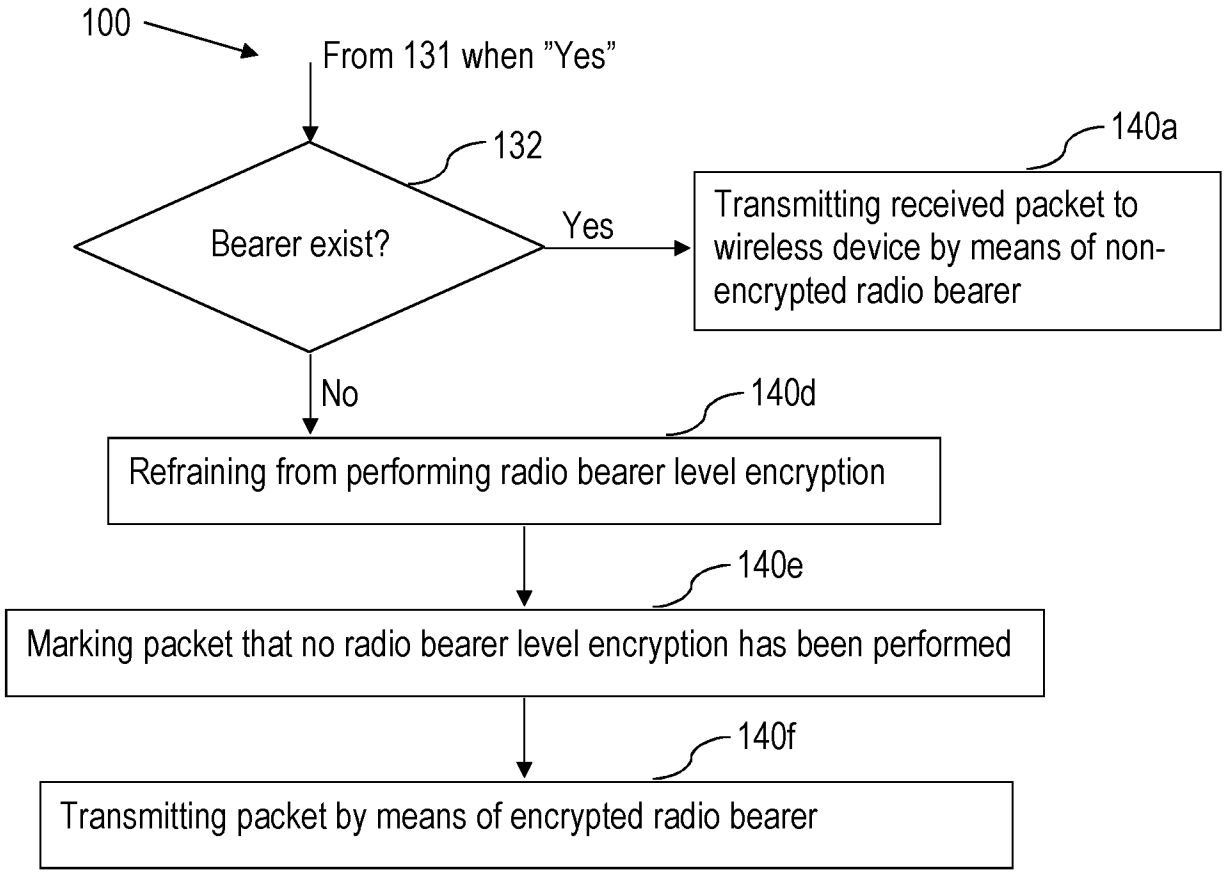
100
From 131 when "Yes"
132
Bearer exist?
Yes
140a
Transmitting received packet to wireless device by means of non-encrypted radio bearer
No
140d
Refraining from performing radio bearer level encryption
140e
Marking packet that no radio bearer level encryption has been performed
140f
Transmitting packet by means of encrypted radio bearer

Fig. 1d

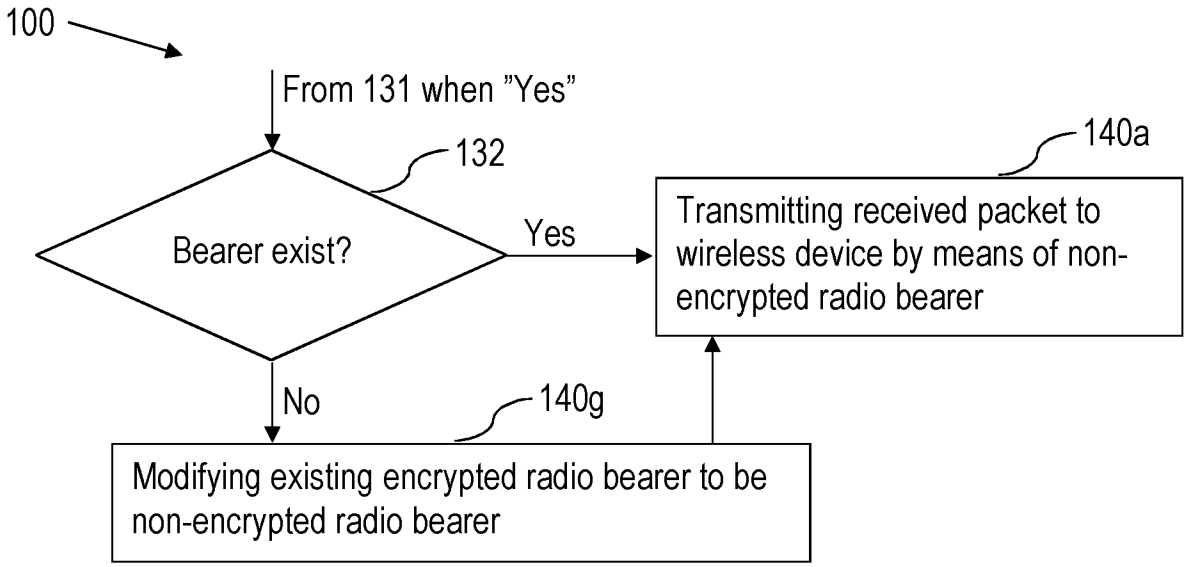
100
From 131 when "Yes"
132
Bearer exist?
Yes
No
140a
Transmitting received packet to wireless device by means of non-encrypted radio bearer
140g
Modifying existing encrypted radio bearer to be non-encrypted radio bearer

Fig. 1e

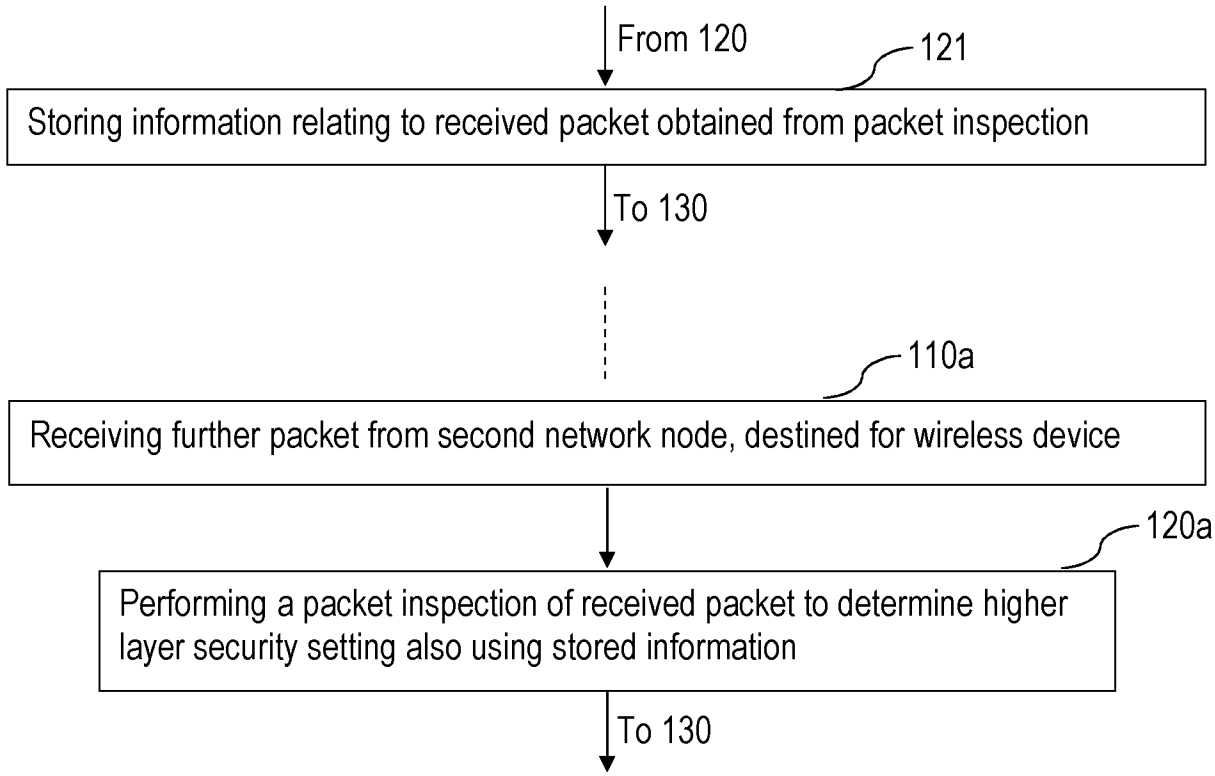
From 120
121
Storing information relating to received packet obtained from packet inspection
To 130
110a
Receiving further packet from second network node, destined for wireless device
120a
Performing a packet inspection of received packet to determine higher layer security setting also using stored information
To 130

Fig. 1f

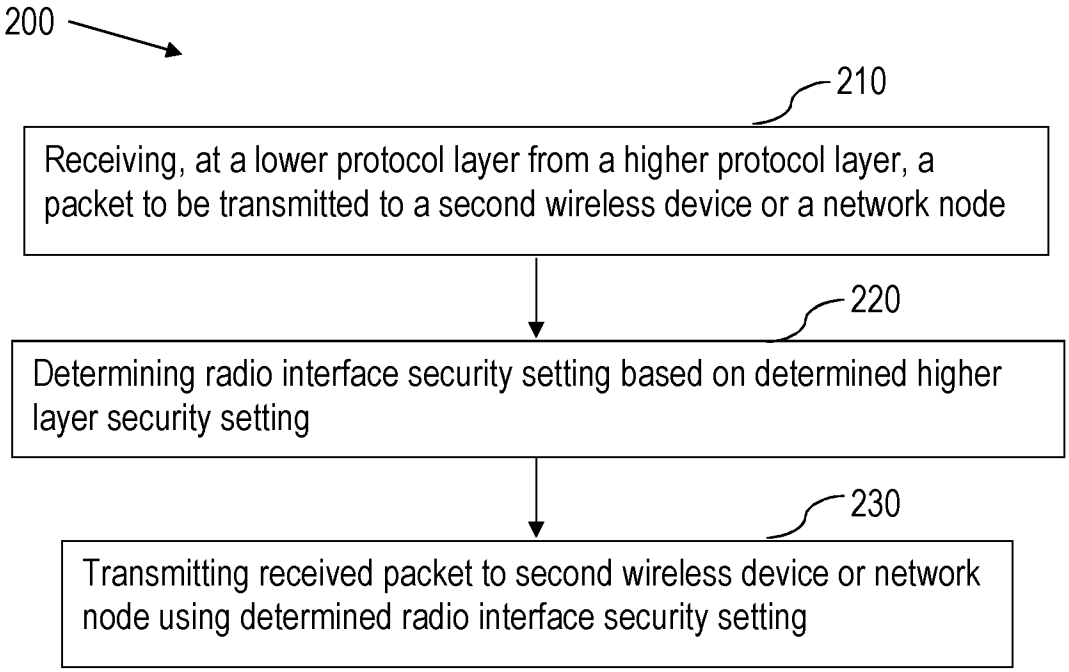
200
210
Receiving, at a lower protocol layer from a higher protocol layer, a packet to be transmitted to a second wireless device or a network node
220
Determining radio interface security setting based on determined higher layer security setting
230
Transmitting received packet to second wireless device or network node using determined radio interface security setting

Fig. 2a

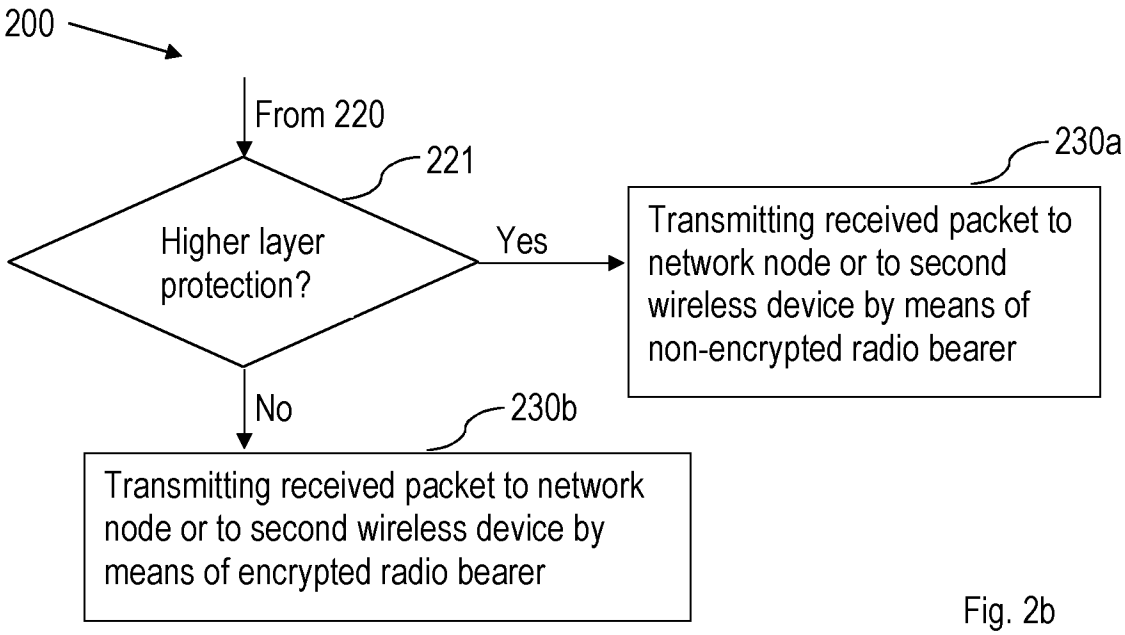
200
From 220
221
Higher layer protection?
Yes
230a
Transmitting received packet to network node or to second wireless device by means of non-encrypted radio bearer
No
230b
Transmitting received packet to network node or to second wireless device by means of encrypted radio bearer

Fig. 2b

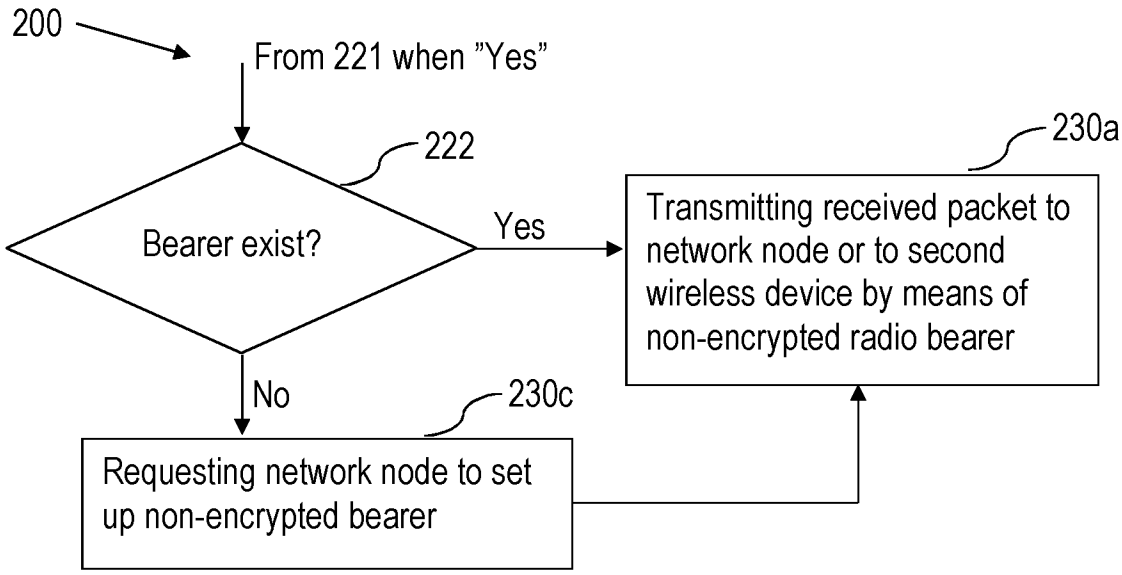
200
From 221 when "Yes"
222
Bearer exist?
Yes
No
230a
Transmitting received packet to network node or to second wireless device by means of non-encrypted radio bearer
230c
Requesting network node to set up non-encrypted bearer

Fig. 2c

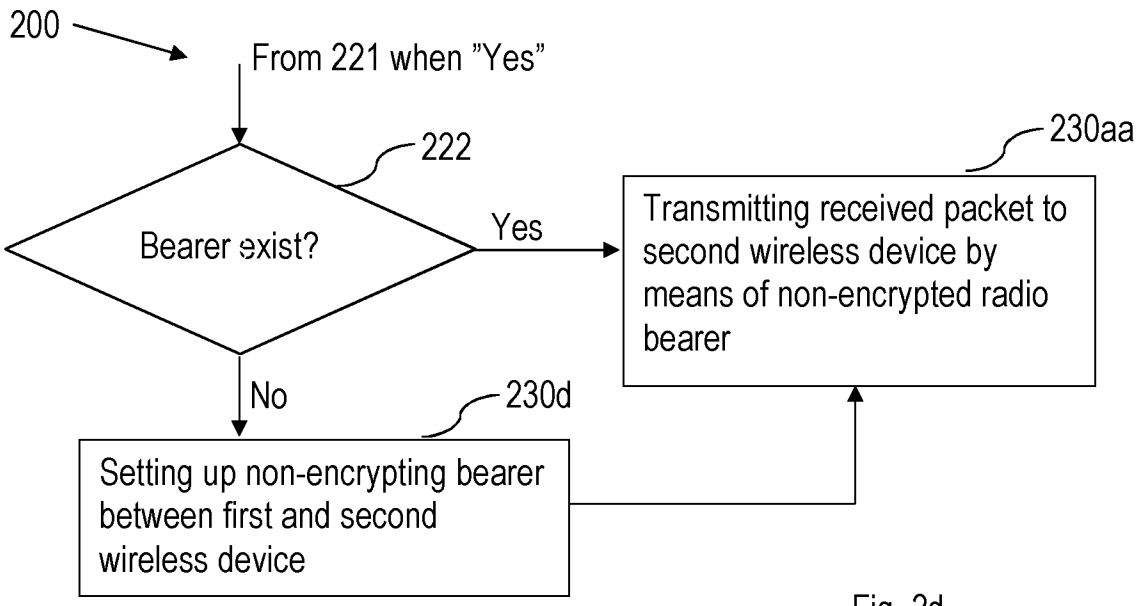
200
From 221 when "Yes"
222
Bearer exist?
Yes
No
230aa
Transmitting received packet to second wireless device by means of non-encrypted radio bearer
230d
Setting up non-encrypting bearer between first and second wireless device

Fig. 2d

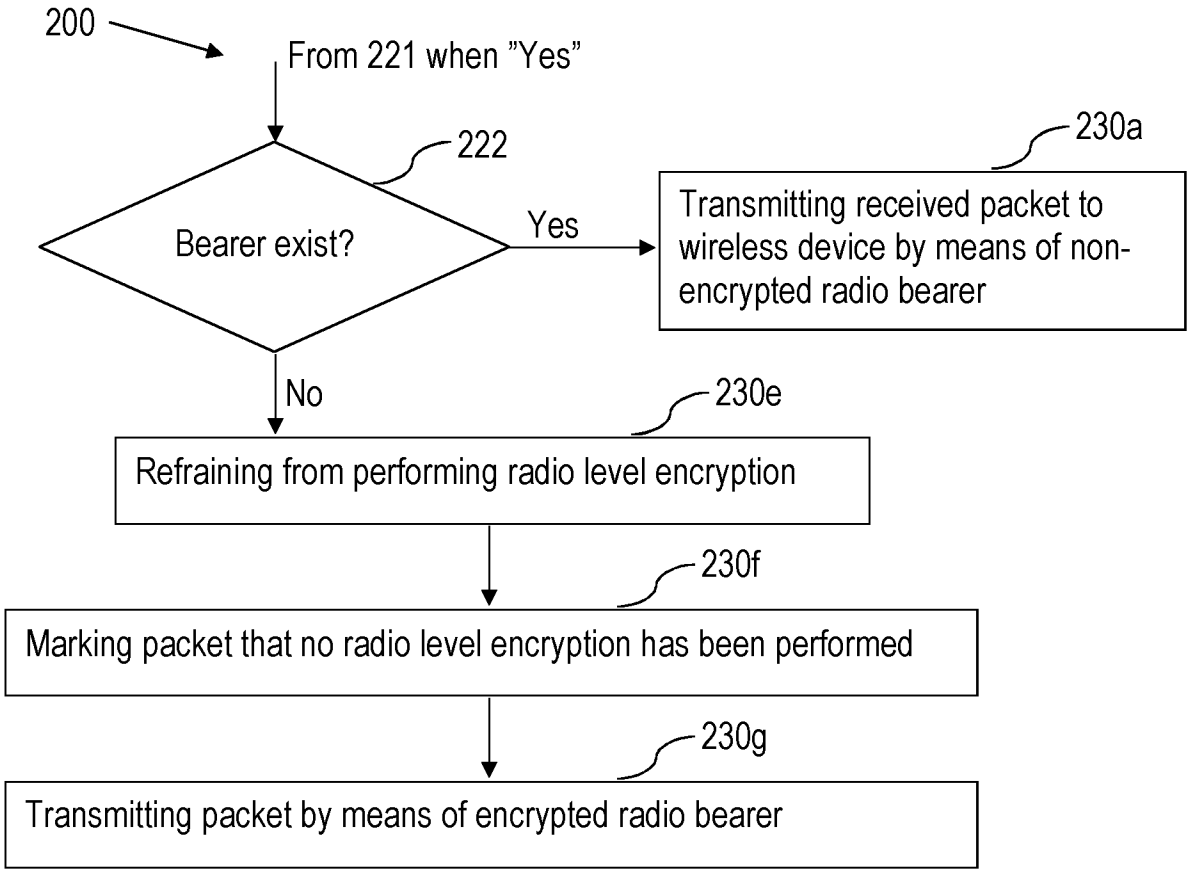
200
From 221 when "Yes"
222
Bearer exist?
Yes
230a
Transmitting received packet to wireless device by means of non-encrypted radio bearer
No
230e
Refraining from performing radio level encryption
230f
Marking packet that no radio level encryption has been performed
230g
Transmitting packet by means of encrypted radio bearer

Fig. 2e

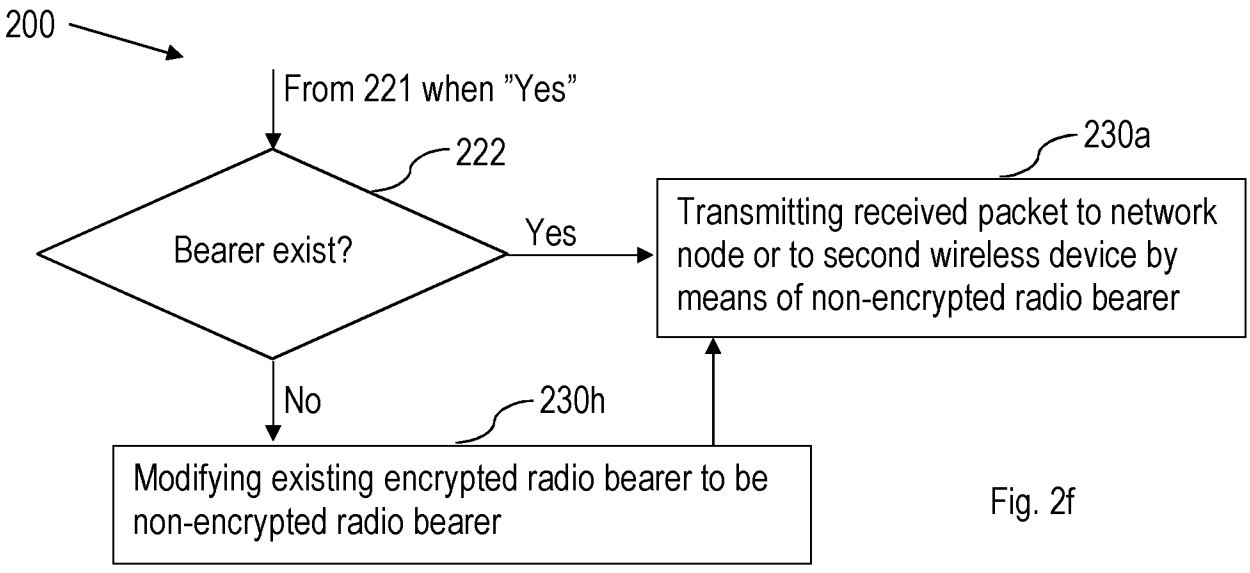
200
From 221 when "Yes"
222
Bearer exist?
Yes
230a
Transmitting received packet to network node or to second wireless device by means of non-encrypted radio bearer
No
230h
Modifying existing encrypted radio bearer to be non-encrypted radio bearer

Fig. 2f

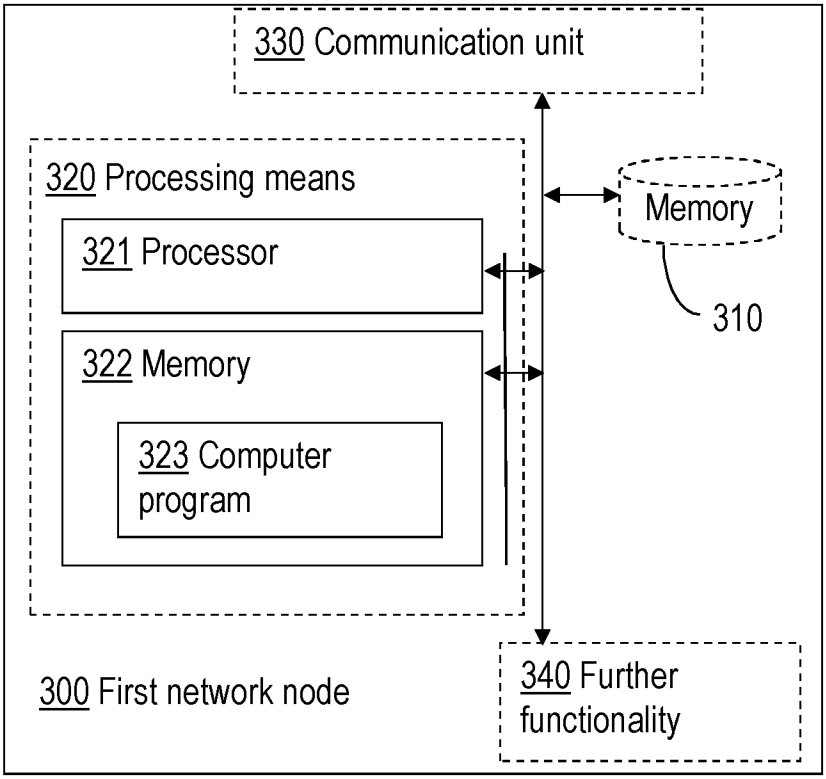
330 Communication unit
320 Processing means
321 Processor
322 Memory
323 Computer program
Memory
310
300 First network node
340 Further functionality

Fig. 3

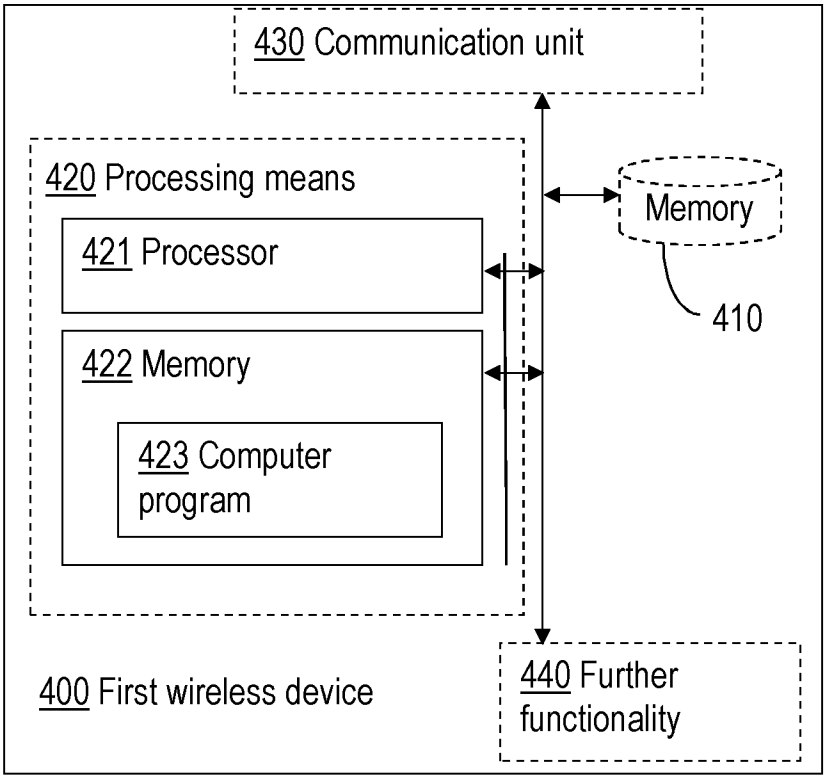
430 Communication unit
420 Processing means
421 Processor
422 Memory
423 Computer program
Memory
410
400 First wireless device
440 Further functionality

Fig. 4

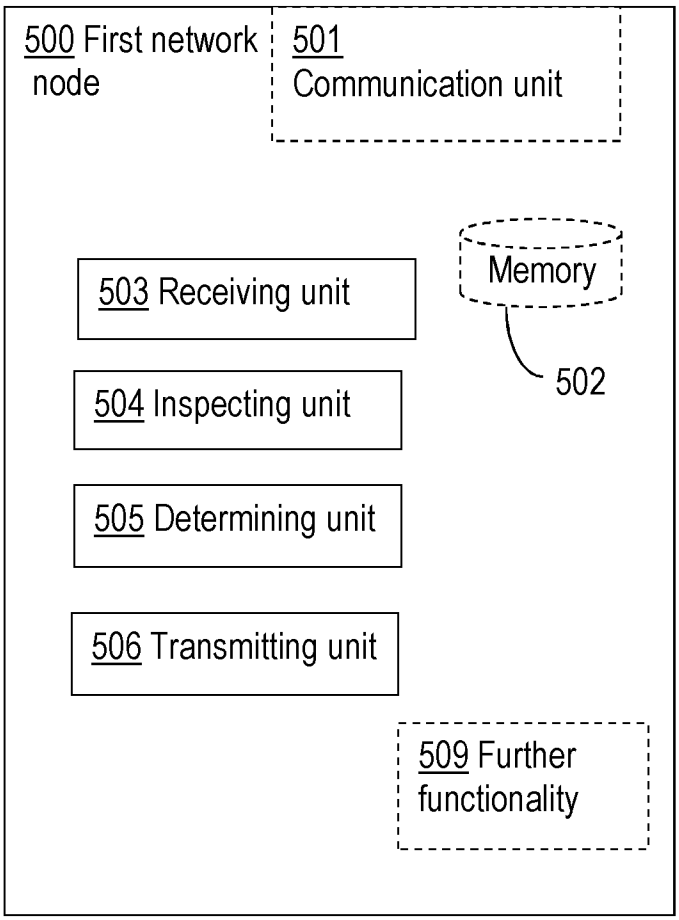
500 First network node
501 Communication unit
Memory
502
503 Receiving unit
504 Inspecting unit
505 Determining unit
506 Transmitting unit
509 Further functionality

Fig. 5

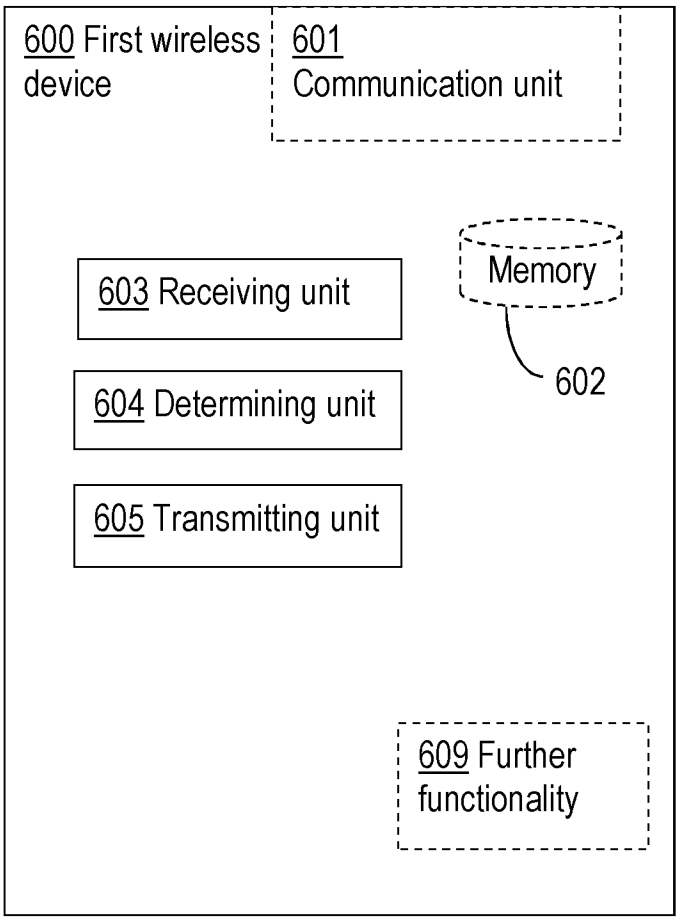
600 First wireless device
601 Communication unit
Memory
603 Receiving unit
602
604 Determining unit
605 Transmitting unit
609 Further functionality

Fig. 6

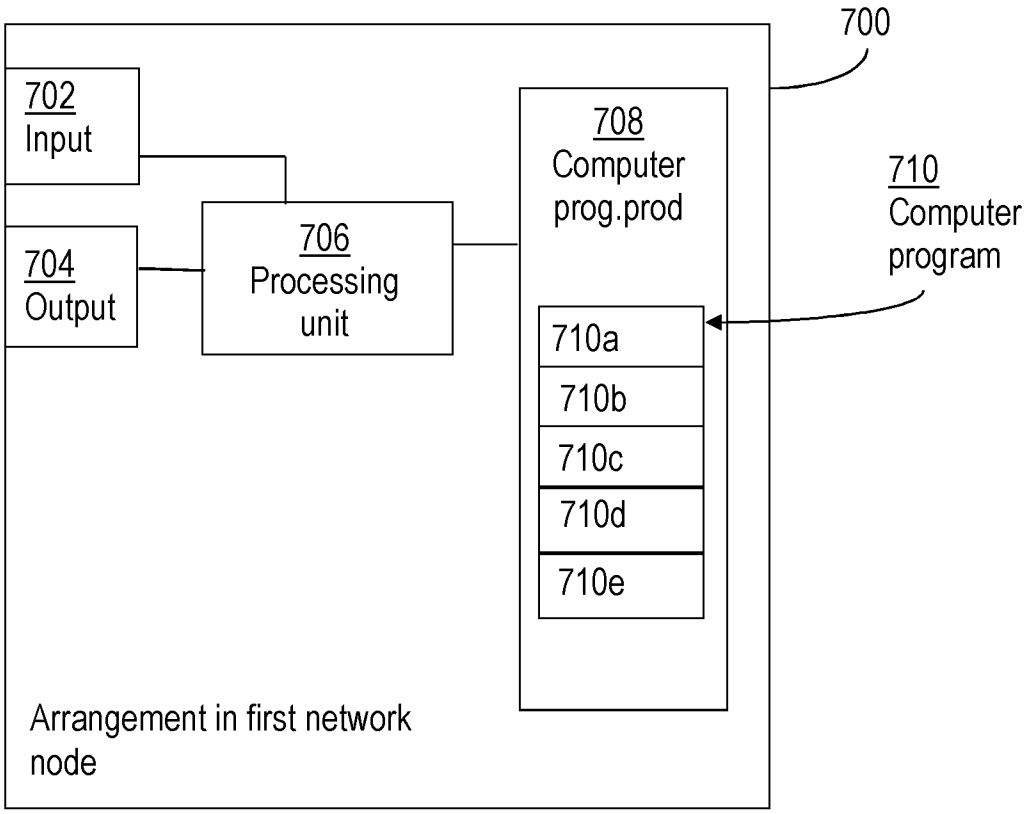
700
702
Input
704
Output
706
Processing
unit
708
Computer
prog.prod
710
Computer
program
710a
710b
710c
710d
710e
Arrangement in first network
node

Fig. 7

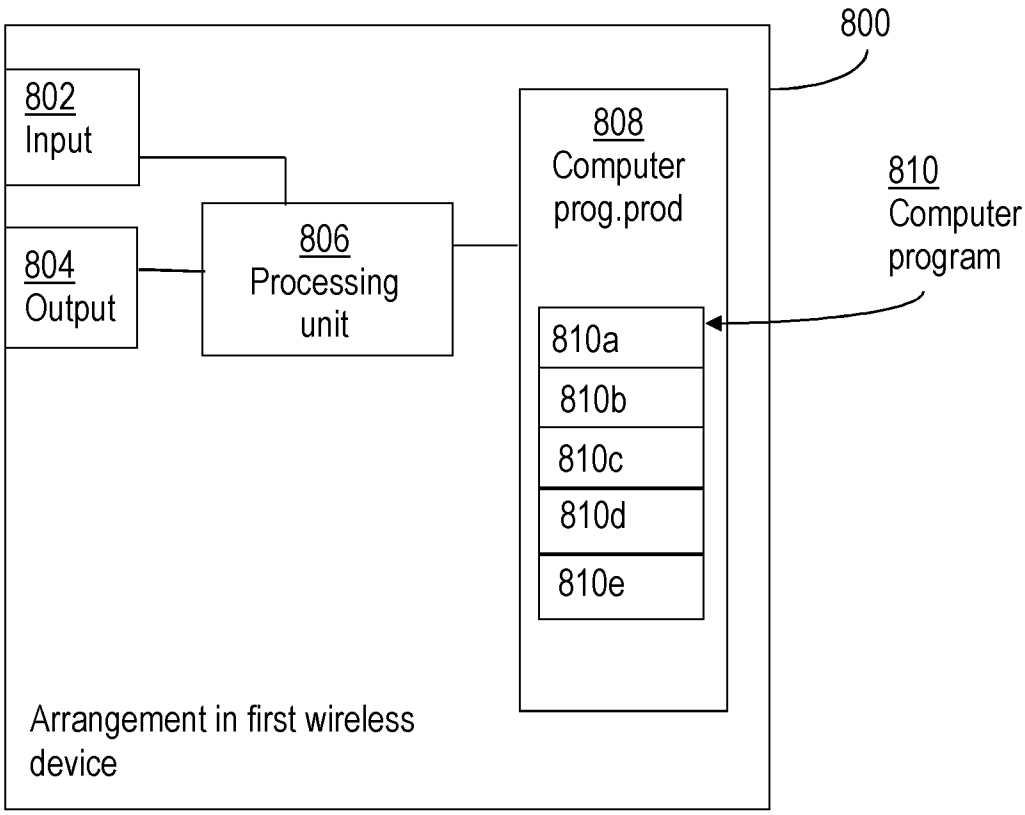
800
802
Input
804
Output
806
Processing
unit
808
Computer
prog.prod
810
Computer
program
810a
810b
810c
810d
810e
Arrangement in first wireless
device

Fig. 8

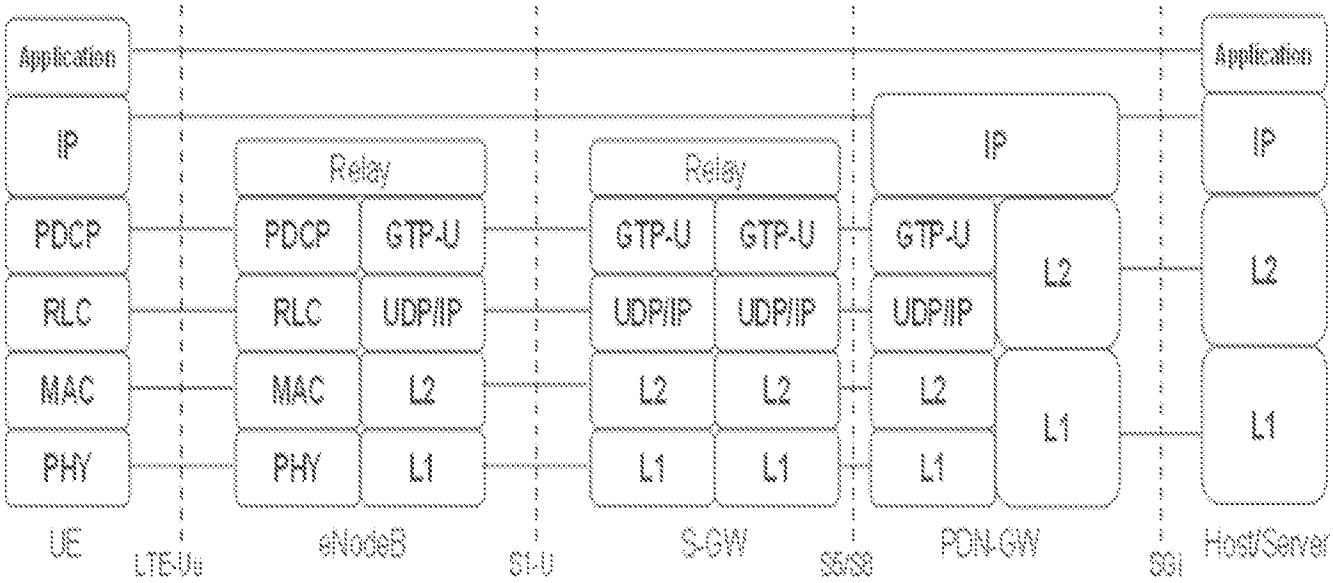
Application
IP
PDCP
RLC
MAC
PHY
Relay
PDCP
GTP-U
RLC
UDP/IP
MAC
L2
PHY
L1
Relay
GTP-U
GTP-U
UDP/IP
UDP/IP
L2
L2
L1
L1
IP
GTP-U
UDP/IP
L2
L2
L1
L1
Application
IP
L2
L1
UE
LTE-Uu
eNodeB
S1-U
S-GW
S5/S8
PDN-GW
SGi
Host/Server

Fig. 9

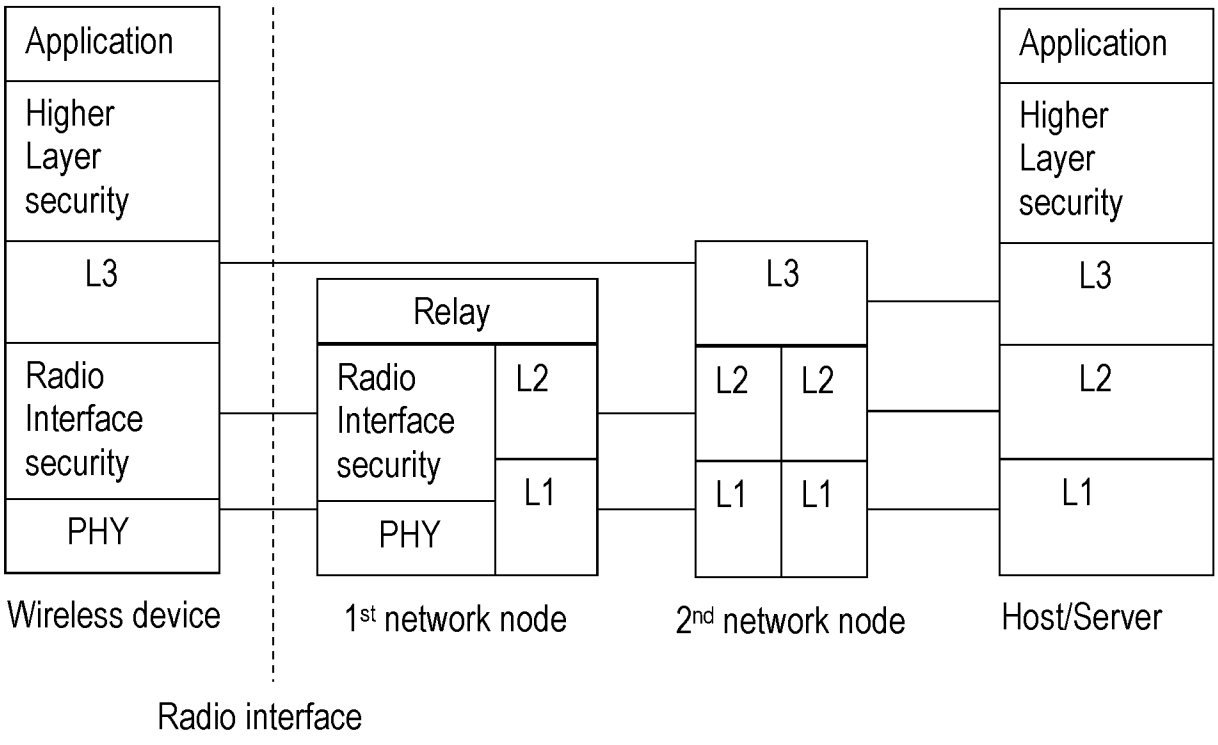
Application
Higher Layer security
L3
Radio Interface security
PHY
Relay
Radio Interface security
PHY
L2
L1
L3
L2
L2
L1
L1
Application
Higher Layer security
L3
L2
L1
Wireless device
1st network node
2nd network node
Host/Server
Radio interface

Fig. 10

# INTERNATIONAL SEARCH REPORT

International application No
PCT/SE2014/050867

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W28/02 H04W12/02
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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | EP 1 758 310 A1 (CIT ALCATEL [FR] ALCATEL LUCENT [FR]) 28 February 2007 (2007-02-28)<br>figures 1b, 1c<br>paragraphs [0006] - [0009]<br>paragraphs [0036] - [0040]<br>-----<br>-/-- | 1-38 |

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

[X] 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 | Date of mailing of the international search report |
|---|---|
| 26 February 2015 | 05/03/2015 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Kufer, Léna |

# INTERNATIONAL SEARCH REPORT

International application No
PCT/SE2014/050867

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | CARNEIRO G ET AL: "Cross-layer design in 4G wireless terminals", IEEE PERSONAL COMMUNICATIONS, IEEE COMMUNICATIONS SOCIETY, US, vol. 11, no. 2, April 2004 (2004-04), pages 7-13, XP011112433, ISSN: 1070-9916, DOI: 10.1109/MWC.2004.1295732 Section Security; page 8, right-hand column - page 9, left-hand column Section Security Plane; page 12, right-hand column<br>----- | 1-38 |
| A | WO 2014/077753 A1 (ERICSSON TELEFON AB L M [SE]) 22 May 2014 (2014-05-22) figure 5 page 7, line 11 - line 16 page 8, line 8 - page 9, line 14 page 11, line 18 - line 30<br>----- | 1-38 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/SE2014/050867

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 1758310 A1 | 28-02-2007 | AT 506785 T | 15-05-2011 |
| | | CN 1946233 A | 11-04-2007 |
| | | EP 1758310 A1 | 28-02-2007 |
| | | US 2007043940 A1 | 22-02-2007 |
| WO 2014077753 A1 | 22-05-2014 | NONE | |