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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 April 2020 (16.04.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/074068 A1

(51) International Patent Classification:
H04B 7/024 (2017.01) *H04W 12/12* (2009.01)

(21) International Application Number:
PCT/EP2018/077485

(22) International Filing Date:
09 October 2018 (09.10.2018)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **NOKIA TECHNOLOGIES OY** [FI/FI]; Karakaari 7, 02610 Espoo (FI).

(72) Inventors: **SCHAEPPERLE, Joerg**; Nokia Solutions and Networks GmbH & Co. KG, Lorenzstrasse 10, 70435 STUTTGART (DE). **ZIRWAS, Wolfgang**; Rohrsängerplatz 7 b, 81249 MUNICH (DE).

(74) Agent: **NOKIA TECHNOLOGIES OY** et al.; Ari Aarnio, IPR Department, Karakaari 7, 02610 Espoo (FI).

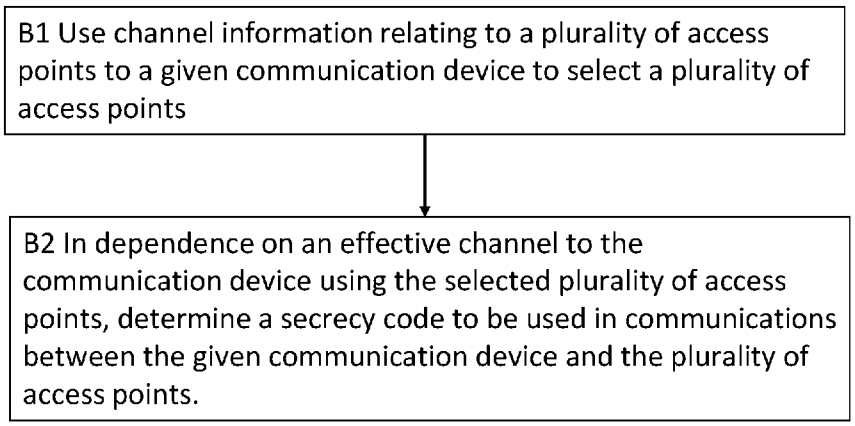
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

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

(54) Title: SECURE COMMUNICATION WITH A PLURALITY OF ACCESS POINTS

Figure 7



(57) Abstract: An apparatus comprises means for using channel information from a plurality of access points to a given communication device to select a plurality of access points. The means is for, in dependence on an effective channel to said communication device using said selected plurality of access points, determining a secrecy code to be used in communications between the given communication device and the plurality of access points.

WO 2020/074068 A1

SECURE COMMUNICATION WITH A PLURALITY OF ACCESS POINTS

Field

The present application relates to a method, apparatus and computer program and in particular but not exclusively to a method and apparatus for to be used in a network for providing secure communication in a network with a plurality of access points.

Background

A communication system can be seen as a facility that enables communication sessions between two or more entities such as communication devices, base stations/access points and/or other nodes by providing carriers between the various entities involved in the communications path. A communication system can be provided for example by means of a communication network and one or more compatible communication devices.

In a wireless communication system at least a part of a communication session between at least two stations occurs over a wireless link. This wireless link may be encrypted or otherwise secured.

A communication device is provided with an appropriate signal receiving and transmitting apparatus for enabling communications, for example enabling access to a communication network or communications directly with other communication devices. The communication device may access a carrier provided by a station or access point, and transmit and/or receive communications on the carrier.

The communication system and associated devices may operate in accordance with a given standard or specification which sets out what the various entities associated with the system are permitted to do and how that should be achieved. Communication protocols and/or parameters which shall be used for the connection are typically defined.

Summary

According to an aspect, there is provided an apparatus comprising means for: using channel information from a plurality of access points to a given communication device to select a plurality of access points; and in dependence on an effective channel to said communication

device using said selected plurality of access points, determining a code to be used in communications between said given communication device and said plurality of access points.

The channel information may relate to a plurality of beams from said plurality of access points, said means being for selecting a plurality of beams of said plurality of access points.

The means may be for estimating a channel quality to a potential eavesdropping device.

The means may be for estimating a limit on said channel quality to a potential eavesdropping device in dependence on one or more of channel information to one or more other devices, information about said effective channel, a security margin and potential location information associated with the potential eavesdropping device. The limit may be an upper limit.

The means may be for selecting said code in dependence on a secrecy rate.

The means may be for using channel quality information relating to said plurality of beams and channel quality information relating to a potential eavesdropping device to determine said secrecy rate.

The means may be for determining said secrecy rate in dependence on a difference between a mutual information between a signal which is transmitted to the given communication device and the signal which is received by that given communication device and mutual information between that transmitted signal and a signal potentially received by an eavesdropper.

The means may be for determining said secrecy rate in dependence on a difference between a mutual information between a signal which is transmitted from an access point to the given communication device and mutual information between that signal and a signal potentially received by an eavesdropper.

The means may be for determining first mutual information between a message to be transmitted and the message received by said given communication device and determining second mutual information between the message to be transmitted and the message received at an output of a channel corresponding to channel quality information associated with a potential eavesdropping device.

The secrecy rate may be dependent on a difference between the first and second mutual information.

The channel information may comprise one or more of: precoding weights for one or more beams; a beam direction for one or more beams; a transmit power for one or more beams; and one or more antenna orientations for one or more beams.

The means may be for receiving said channel information.

The means may be for determining channel quality information associated with said effective channel.

The means may be for providing one or more of transmit power information for one or more of said beams, a receive method for use by said given communication device; one or more beam directions for said beams; and precoding weights for one or more of said beams.

The means may be for using information about one or more of a location and an environment of said given device to determine said effective channel.

The means may be for using information about one or more of a location and an environment of a potential eavesdropping device to determine said effective channel.

The means may be for selecting one or more parameters of a code family to determine said code.

The means may be for causing different parts of said code to be distributed across different ones of said beams.

The effective channel may be such that a signal to interference noise ratio is relatively large in a region around said given communications device.

The region may be of an order of magnitude of a wavelength of a carrier frequency used for said effective channel.

The means may be for selecting at least three beams from at least three access points.

The means may be for selecting a physical layer code.

The means may be for causing information about said secrecy code to be provided to one or more of said plurality of access points and said given communication device.

The means may be for determining said secrecy code further in dependence on a required secrecy level.

According to another aspect, there is provided an apparatus comprising at least one processor and at least one memory including computer code for one or more programs, the at least one memory and the computer code configured, with the at least one processor, to cause the apparatus at least to: use channel information from a plurality of access points to a given communication device to select a plurality of access points; and in dependence on an effective channel to said communication device using said selected plurality of access points, determine a code to be used in communications between said given communication device and said plurality of access points.

The channel information may relate to a plurality of beams from said plurality of access points, the at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to select a plurality of beams of said plurality of access points.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to estimate a channel quality to a potential eavesdropping device.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to estimate a limit on said channel quality to a potential eavesdropping device in dependence on one or more of channel information to one or more other devices, information about said effective channel, a security margin and potential location information associated with the potential eavesdropping device. The limit may be an upper limit.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to select said code in dependence on a secrecy rate.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to use channel quality information relating to said

plurality of beams and channel quality information relating to a potential eavesdropping device to determine said secrecy rate.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to determine said secrecy rate in dependence on a difference between an mutual information between a signal which is transmitted to the given communication device and the signal which is received by that given communication device and mutual information between that transmitted signal and a signal potentially received by an eavesdropper.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to determine said secrecy rate in dependence on a difference between an mutual information between a signal which is transmitted from an access point to the given communication device and mutual information between that signal and a signal potentially received by an eavesdropper.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to determine first mutual information between a message to be transmitted and the message received by said given communication device and determining second mutual information between the message to be transmitted and the message received at an output of a channel corresponding to channel quality information associated with a potential eavesdropping device.

The secrecy rate may be dependent on a difference between the first and second mutual information.

The channel information may comprise one or more of: precoding weights for one or more beams; a beam direction for one or more beams; a transmit power for one or more beams; and one or more antenna orientations for one or more beams.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to receive said channel information.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to determine channel quality information associated with said effective channel.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to provide one or more of transmit power information for one or more of said beams, a receive method for use by said given communication device; one or more beam directions for said beams; and precoding weights for one or more of said beams.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to use information about one or more of a location and an environment of said given device to determine said effective channel.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to use information about one or more of a location and an environment of a potential eavesdropping device to determine said effective channel.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to select one or more parameters of a code family to determine said code.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to cause different parts of said code to be distributed across different ones of said beams.

The effective channel may be such that a signal to interference noise ratio is relatively large in a region around said given communications device.

The region may be of an order of magnitude of a wavelength of a carrier frequency used for said effective channel.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to select at least three beams from at least three access points.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to select a physical layer code.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to cause information about said secrecy code to be

provided to one or more of said plurality of access points and said given communication device.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to determine said secrecy code further in dependence on a required secrecy level.

According to another aspect, there is provide an apparatus comprising means for: determining estimated channel quality information for a potential eavesdropping device; and determining a secrecy code to be used in communications between a given communication device and a plurality of access points in dependence on said estimated channel quality information.

According to another aspect, there is provided an apparatus comprising at least one processor and at least one memory including computer code for one or more programs, the at least one memory and the computer code configured, with the at least one processor, to cause the apparatus at least to: determine estimated channel quality information for a potential eavesdropping device; and determine a secrecy code to be used in communications between a given communication device and a plurality of access points in dependence on said estimated channel quality information.

According to another aspect, there is provided an apparatus comprising means for: causing channel information relating to a plurality of access points to be provided to a network node; and decoding a signal to which a secrecy code has been applied, said signal being received from said plurality of access points.

The channel information may relate to a plurality of beams from said plurality of access points, said signal being received from a plurality of beams of said plurality of access points.

The channel information may comprise one or more of: precoding weights for one or more beams; a beam direction for one or more beams; a transmit power for one or more beams; and one or more antenna orientations for one or more beams.

The means may be for receiving one or more of transmit power information for one or more beams, a receive method to be used; one or more beam directions for said beams; and precoding weights for one or more of said beams.

An effective channel for said signal such that a signal to interference noise ratio is relatively large in a region around said apparatus.

The region may be of an order of magnitude of a wavelength of a used carrier frequency.

The means may be for encoding one or more signals to be transmitted to said access points using a secrecy code.

This secrecy code may be the same as the secrecy code used for the received signals, be related to the secrecy code used for the received signals are be different to the secrecy code used for the received signals.

The means may be for causing information on a required secrecy level to be provided to an access node.

The means may be for receiving one or more secrecy codes used for one or more of decoding received signals and encoding signals to be transmitted.

According to another aspect, there is provided an apparatus comprising at least one processor and at least one memory including computer code for one or more programs, the at least one memory and the computer code configured, with the at least one processor, to cause the apparatus at least to: cause channel information relating to a plurality of access points to be provided to a network node; and decode a signal to which a secrecy code has been applied, said signal being received from said plurality of access points.

The channel information may relate to a plurality of beams from said plurality of access points, said signal being received from a plurality of beams of said plurality of access points.

The channel information may comprise one or more of: precoding weights for one or more beams; a beam direction for one or more beams; a transmit power for one or more beams; and one or more antenna orientations for one or more beams.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to receive one or more of transmit power information for one or more beams, a receive method to be used; one or more beam directions for said beams; and precoding weights for one or more of said beams.

An effective channel for said signal such that a signal to interference noise ratio is relatively large in a region around said apparatus.

The region may be of an order of magnitude of a wavelength of a used carrier frequency.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to encode one or more signals to be transmitted to said access points using a secrecy code.

This secrecy code may be the same as the secrecy code used for the received signals, be related to the secrecy code used for the received signals are be different to the secrecy code used for the received signals.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to cause information on a required secrecy level to be provided to an access node.

The at least one memory and the computer code may be configured, with the at least one processor, to cause the apparatus at least to receive one or more secrecy codes used for one or more of decoding received signals and encoding signals to be transmitted.

According to another aspect, there is provide a method comprising: determining estimated channel quality information for a potential eavesdropping device; and determining a secrecy code to be used in communications between a given communication device and a plurality of access points in dependence on said estimated channel quality information.

According to another aspect, there is provided a method comprising: using channel information relating to a plurality of access points to a given communication device to select a plurality of access points; and in dependence on an effective channel to said communication device using said selected plurality of access points, determining a secrecy code to be used in communications between said given communication device and said plurality of access points.

The method may comprise estimating a channel quality to a potential eavesdropping device.

The method may comprise estimating a limit on said channel quality to a potential eavesdropping device in dependence on one or more of channel information to one or more

other devices, information about said effective channel, a security margin and potential location information associated with the potential eavesdropping device. The limit may be an upper limit.

The method may comprise selecting said code in dependence on a secrecy rate.

The method may comprise using channel quality information relating to said plurality of beams and channel quality information relating to a potential eavesdropping device to determine said secrecy rate.

The method may comprise determining said secrecy rate in dependence on a difference between a mutual information between a signal which is transmitted to the given communication device and mutual information between that signal and a signal potentially received by an eavesdropper.

The method may comprise determining said secrecy rate in dependence on a difference between a mutual information between a signal which is transmitted from an access point to the given communication device and the signal which is received by that given communication device and mutual information between that transmitted signal and a signal potentially received by an eavesdropper.

The method may comprise determining first mutual information between a message to be transmitted and the message received by said given communication device and determining second mutual information between the message to be transmitted and the message received at an output of a channel corresponding to channel quality information associated with a potential eavesdropping device.

The secrecy rate may be dependent on a difference between the first and second mutual information.

The channel information may comprise one or more of: precoding weights for one or more beams; a beam direction for one or more beams; a transmit power for one or more beams; and one or more antenna orientations for one or more beams.

The method may comprise receiving said channel information.

The method may comprise determining channel quality information associated with said effective channel.

The method may comprise providing one or more of transmit power information for one or more of said beams, a receive method for use by said given communication device; one or more beam directions for said beams; and precoding weights for one or more of said beams.

The method may comprise using information about one or more of a location and an environment of said given device to determine said effective channel.

The method may comprise using information about one or more of a location and an environment of a potential eavesdropping device to determine said effective channel.

The method may comprise selecting one or more parameters of a code family to determine said code.

The method may comprise causing different parts of said code to be distributed across different ones of said beams.

The effective channel may be such that a signal to interference noise ratio is relatively large in a region around said given communications device.

The region may be of an order of magnitude of a wavelength of a carrier frequency used for said effective channel.

The method may comprise selecting at least three beams from at least three access points.

The method may comprise selecting a physical layer code.

The method may comprise causing information about said secrecy code to be provided to one or more of said plurality of access points and said given communication device.

The method may comprise determining said secrecy code further in dependence on a required secrecy level.

According to another aspect, there is provided a method comprising: causing channel information relating to a plurality of access points to be provided to a network node; and

decoding a signal to which a secrecy code has been applied, said signal being received from said plurality of access points.

The channel information may relate to a plurality of beams from said plurality of access points, said signal being received from a plurality of beams of said plurality of access points.

The channel information may comprise one or more of: precoding weights for one or more beams; a beam direction for one or more beams; a transmit power for one or more beams; and one or more antenna orientations for one or more beams.

The method may comprise receiving one or more of transmit power information for one or more beams, a receive method to be used; one or more beam directions for said beams; and precoding weights for one or more of said beams.

An effective channel for said signal such that a signal to interference noise ratio is relatively large in a region around said apparatus.

The region may be of an order of magnitude of a wavelength of a used carrier frequency.

The method may comprise encoding one or more signals to be transmitted to said access points using a secrecy code.

This secrecy code may be the same as the secrecy code used for the received signals, be related to the secrecy code used for the received signals are be different to the secrecy code used for the received signals.

The method may comprise causing information on a required secrecy level to be provided to an access node.

The method may comprise receiving one or more secrecy codes used for one or more of decoding received signals and encoding signals to be transmitted.

According to another aspect, there is provided an apparatus comprising means for: causing channel information relating to a communication with a given communications device to be provided to a network node; receiving secrecy code information; and causing said secrecy code to be applied to a signal which is transmitted to said given communications device.

According to another aspect, there is provided an apparatus comprising at least one processor and at least one memory including computer code for one or more programs, the at least one memory and the computer code configured, with the at least one processor, to cause the apparatus at least to: cause channel information relating to a communication with a given communications device to be provided to a network node; receive secrecy code information; and cause said secrecy code to be applied to a signal which is transmitted to said given communications device.

According to another aspect, there is provided a method comprising: causing channel information relating to a plurality of access points to be provided to a network node; and decoding a signal to which a secrecy code has been applied, said signal being received from said plurality of access points.

In another aspect there is provided a computer program embodied on a non-transitory computer-readable storage medium, the computer program comprising program code for providing any of the above methods.

In another aspect there is provided a computer program product for a computer, comprising software code portions for performing the steps of any of the previous methods, when said product is run.

A computer program comprising program code means adapted to perform the method(s) may be provided. The computer program may be stored and/or otherwise embodied by means of a carrier medium.

In the above, many different embodiments have been described. It should be appreciated that further embodiments may be provided by the combination of any two or more of the embodiments described above.

Description of Figures

Some embodiments will now be described, by way of example only, with reference to the accompanying Figures in which:

Figure 1 shows a schematic diagram of an example communication system comprising a plurality of base stations and a plurality of communication devices;

Figure 2 shows a schematic diagram of an example mobile communication device;

Figure 3 shows a schematic diagram of an example control apparatus;

Figure 4 shows a method of some embodiments;

Figure 5 schematically shows an embodiments with three access points and a communications device;

Figure 6 shows a signal flow of some embodiments;

Figure 7 shows a method performed by an apparatus in a network node;

Figure 8 shows a method performed by an apparatus in a communications device; and

Figure 9 shows a method performed by an apparatus in an access point.

Detailed description

Before explaining in detail the examples, certain general principles of a wireless communication system and mobile communication devices are briefly explained with reference to Figures 1 to 2 to assist in understanding the technology underlying the described examples.

In a wireless communication system 100, such as that shown in Figure 1, mobile communication devices or user equipment (UE) 102, 104, 105 are provided wireless access via at least one access point or similar wireless transmitting and/or receiving node or point. An access point or base station is referred to as a Node B or generally NB (for example an eNB in LTE and gNB in 5G NR). Base stations are typically controlled by at least one appropriate controller apparatus, so as to enable operation thereof and management of mobile communication devices in communication with the base stations. The controller apparatus may be located in a radio access network (e.g. wireless communication system 100) or in a core network (CN) (not shown) and may be implemented as one central apparatus or its functionality may be distributed over several apparatus. The controller apparatus may be part of the base station and/or provided by a separate entity such as a radio network controller. In Figure 1 control apparatus 108 and 109 are shown to control the respective macro level base stations 106 and 107. In some systems, the control apparatus may additionally or alternatively be provided in a radio network controller.

In Figure 1 base stations 106 and 107 are shown as connected to a wider communications network 113 via gateway 112. A further gateway function may be provided to connect to another network.

Smaller base stations (or relay nodes or RN) 116, 118 and 120 may also be connected to the network 113, for example by a separate gateway function and/or via the controllers of the macro level stations.

The base stations 116, 118 and 120 may be pico or femto level base stations or the like. In the example, station 118 is connected via a gateway 111 whilst station 120 connects via the controller apparatus 108. The station 116 may be connected via station 107. In some embodiments, the smaller stations may not be provided.

In some embodiments, a communication device may communicate with one, two or more base stations. In some embodiments, an effective wireless channel from the transmitter to the receiver is formed by using methods such as beamforming and/or CoMP (coordinated multipoint) or the like joint transmission. For example, a node may communicate simultaneously on a plurality of carriers. Multipoint schemes such as coordinated multi-point transmission (CoMP) provide this. Coordinated multipoint transmission (CoMP) is a technique where combined results of reception by a plurality of stations from a communication device or reception of a transmission based on signals transmitted from a plurality of sources can be utilised.

A possible communication device will now be described in more detail with reference to Figure 2 showing a schematic, partially sectioned view of a communication device 200. Such a communication device is may be a user equipment (UE) or terminal. An appropriate communication device may be provided by any device capable of sending and receiving radio signals. Non-limiting examples comprise a mobile station (MS) or mobile device such as a mobile phone or what is known as a 'smart phone', a computer provided with a wireless interface card or other wireless interface facility (e.g., USB dongle), personal data assistant (PDA) or a tablet provided with wireless communication capabilities, machine type devices, an IoT (Internet of Things) type device or any combinations of these or the like.

The communication device 200 may receive signals over an air or radio interface 207 via appropriate apparatus for receiving and may transmit signals via appropriate apparatus for transmitting radio signals. In Figure 2 transceiver apparatus is designated schematically by block 206. The transceiver apparatus 206 may be provided for example by means of a radio part and associated antenna arrangement. The antenna arrangement may be arranged internally or externally to the mobile device.

A communication device is typically provided with at least one data processing entity 201, at least one memory 202 and other possible components 203 for use in software and hardware aided execution of tasks it is designed to perform, including control of access to and communications with access systems and other communication devices. The data processing,

storage and other relevant control apparatus may be provided on an appropriate circuit board and/or in chipsets. This feature is denoted by reference 204.

A user may control the operation of the device by means of a suitable user interface such as key pad 205, voice commands, touch sensitive screen or pad, combinations thereof or the like. This may be optional in some embodiments. In some embodiments, the device may be controlled via a remote entity.

A display 208, a speaker and a microphone may be also provided. Again this may be optional.

An example control apparatus is shown in Figure 3. Figure 3 shows an example of a control apparatus provided in a base station or network entity or node. The control apparatus 300 comprises at least one memory 301, at least one data processing unit 302, 303 and an input/output interface 304. For example the control apparatus 300 or processor 302/303 can be configured to execute an appropriate software code to provide the control functions.

In wireless communication systems the signals transmitted over the air interface should be protected against eavesdropping. The air interface is typically provided between a base station and a communications device. In current mobile communication systems this is done by cryptographic methods which may use the assumption that the eavesdropper has limited computational power. These method may require the exchange of a cryptographic key via an additional secure channel before the communication takes place.

In some scenarios, the key exchange via the additional secure channel may not always be practical. For example, this may be in the context of the Internet of Things (IoT), where a large number of small devices is connected to a network. Another context may be where so called machine type devices are connected to a network.

Some embodiments may provide one or more cryptographic methods which do not require key exchange via a second secure channel. It should be appreciated that some embodiments may be in conjunction with a second secure channel to provide an enhanced level of security.

In some embodiments a cryptographic key is exchanged secretly over the unsecure wireless channel. In some embodiments communication is done in such a way that no cryptographic key is required for that key exchange. However, in some embodiments, for further security, one or more cryptographic keys may be used.

Thus in some embodiments, there is a secure wireless communication provided between a communication device such as UE or IOT device and a network which does not require an additional secure channel for cryptographic key exchange before data communication. Some embodiments may have no requirement to know the exact position and/or the exact channel state of a potential eavesdropper.

Some embodiments may address the issue that for example in the downlink direction, the generation of a zone around a legitimate receiver of a message where decoding of that message is not only difficult or erroneous due to bad channel quality but also difficult because the message received by an eavesdropper does not contain any information about the transmitted message

Some current proposals have secret communication based on cryptography. This requires exchange of a cryptographic key over a secure channel before secret communication over the unsecure channel,

Physical Layer Security has been proposed. In this, there is an achievable secrecy rate between a sender (Alice) and a receiver (Bob) is known as a function of the channel to Bob and a potential eavesdropper (Eve). First codes for PHY Layer security which guarantee decodability for Bob and secrecy towards Eve are available. Physical layer security is a technique which makes sure that no information about the transmitted signal is included in the signal received by a potential eavesdropper. For this, the channel to the eavesdropper is known. The rate at which communication can be regarded as perfectly secret is called secrecy rate and depends on the difference $IB - IE$ between the mutual information IB between the signal transmitted by Alice and that received by Bob and the mutual information IE between the transmitted signal and the signal received by the eavesdropper Eve. So called perfectly secret communication is possible, if the secrecy rate is positive. Codes that currently achieve this security approximately are based on a combination of a universal hash function and an error correction code.

The concept of physical space security has been proposed. This approach endeavours to ensure that a transmitted signal cannot be decoded without error outside a region around the legitimate receiver. The region around the legitimate receiver where the signal can be decoded without error may be minimized in order to make it unlikely for an eavesdropper to be in this region. Outside this region it may be possible to decode the signal with some errors or even some parts of the signal without error.

Some embodiments may provide secrecy in a whole area by using multiple access points. Some embodiments may provide an estimation of a potential eavesdropper's channel quality which may be used to determine a secrecy code to use.

In some embodiments, the size of a region around the inner zone around the legitimate receiver may be increased. In this region, it may be impossible for an eavesdropper to decode any of the useful information in the transmitted signal. Thus in some embodiment, a region between a transmitter and a receiver is provided. In this region, it may not be possible for a potential eavesdropper to decode the signal without error. Further, it may not be possible for a potential eavesdropper to decode any of the useful information in the signal. One or more parameters may influence the size of the region. The parameters may be one or more of the transmission method (for example one or more of selection of the involved access points and antennas, precoding weights, selection of the beam number in a grid of beams, and/or transmit power per antenna), the receive method at the legitimate receiver and the secrecy code with its parameters.

In some embodiments, being able to communicate information securely may requires a positive secrecy rate and/or appropriate coding of the signal.

Having a positive secrecy rate may require that the channel quality, e.g., in terms of effective SINR (signal to interference noise ratio) after receive processing is better for the legitimate receiver than for the eavesdropper.

Some embodiments may cause the channel to be designed with a goal of maximizing the secrecy rate. The maximum secrecy rate is sometimes referred to as secrecy capacity. Secrecy codes may be codes achieving or approaching the secrecy rate.

The required level of secrecy may influences the selection of the secrecy code. The required level of secrecy may need to be signalled between network nodes.

The channel may be formed in such a way that the SINR is high in a relatively small zone around the legitimate receiver. By way of example, the size of the small zone be of the order of magnitude of a wavelength of the carrier frequency. In other embodiments, the small zone may be larger or smaller than this size.

The SINR may be relatively low in a region around this inner zone. This region around the inner zone may be relatively large. By way of example, this region may cover a significant

fraction of the coverage area of the access points which is the area between the involved access points. The diameter of this area may be of the order of magnitude of the distance between access points (e.g. one half of that distance or more). This is typically much larger than the wavelength of the carrier frequency. In other embodiments, the region may be larger or smaller than this size,

Some embodiments may use relatively narrow beams. This may make the areas where the SINR is relatively high, relatively small. This may make eavesdropping impossible or difficult outside these beams. By way of example only, in a mmWave communication systems, there may be antenna arrays with tens of antennas both in horizontal and vertical directions. This means that the angular width of a beam may be as small as a few degrees. If the distance to the access point is about 10 m, the beam width at the receiver can be below 1 m. In other embodiments, the beam may be wider or narrower than this width. It should be appreciated that other embodiments may be used with wavelengths other than mm wavelengths.

Some embodiments may use two or more of these beams to increase the difference between the channel quality of the legitimate user and the potential eavesdropper. In embodiments, three beams may be used. In some embodiments, there may be more or less than three beams. By way of example only, more than three beams may be used an indoor scenario such as in an industrial context.

In some embodiments information about this effective channel may be reported to a network function. When transmitting via a plurality of wireless links, the signal to be transmitted is split at the transmit side into a plurality of signals that are then, e.g., transmitted by different transmit antennas, and on the receive side the signals from different wireless propagation paths are combined either in the air at the receive antenna or in the receiver, when multiple receive antennas are used. The combining is done, for example by determining a weighted sum of the received signals. The effective channel is the channel from the point before splitting to the point after combining the signals, i.e. including the processing in transmitter and receiver. It may have an improved quality if the signals combine constructively.

The network function may be provided in a core network. The network function may be a security server. The information reported to this network function may comprise one or more of precoding weights, beam directions, transmit powers and antenna orientations.

The network function, for example the security server may decide based on that information how many and/or which access points should be used in order to achieve a required level of security.

The network function may determine a resulting channel quality (e.g., SINR) of the legitimate receiver. The network function may estimate an upper bound of the channel quality of a potential eavesdropper.

Based on the channel quality values, the network function may determine the rate at which secret communication is possible. This may be the secrecy rate such as previously described.

The network function may define a suitable security code. This may be achieved by adapting the parameters of a code family to the channel. This code may be a FEC code, have an FEC as a component or any other suitable code. The secrecy code may be such that an eavesdropper cannot decode any information. This may ensure that with the maximum channel quality of the eavesdropper no information can be decoded. It should be appreciated that any suitable code may be used.

By way of example only, the codes discussed in Himanshu Tyagi and Alexander Vardy paper –"Explicit Capacity- Achieving Coding Scheme for The Gaussian Wiretap Channel" may be used in some embodiments. This discusses universal hashing for information-theoretic security secret-key agreement and secure communications using a family of 2-universal hash function. The resulting schemes are modular, and can be implemented by including an extra processing layer over existing transmission codes. (Proc. IEEE, Vol. 103, No. 10, October 2015). This or a similar scheme may be used in some embodiments. Of course other schemes and codes may be used in other embodiments.

If the maximum channel quality of an eavesdropper is assumed, for example, to be that which can be achieved by eavesdropping a single link (beam), an eavesdropper who cannot eavesdrop more than one link is not able to decode any information. This may be the case where the secrecy code is derived under the assumption of that maximum channel quality

In some embodiments, coding blocks of the security code may be distributed over two or more links to ensure that eavesdropping a single link is not sufficient.

Reference is made to Figure 4 which shows a method of some embodiments.

In step A1, a beam search is performed between a communication device and one or more access points. Some embodiments may be used in a 5G network. In that network the beam search may be performed between the communication device and one or more several distributed units (DUs) of one or more gNodeBs. The respective channel quality for the beams may be determined or measured. This beam search may be performed by an apparatus of the communication device or the communication device.

In step A2, the communications device or an apparatus of the communication device is configured to report information about the channels to a central node responsible for security. The central node can be located in the central unit of a gNodeB or can be a separate node connected to a plurality of gNodeBs or any other suitable central node.

In step A3, the central node determines which one or more access points (DUs) and which spatial precoding (beams) to use.

In step A4, the central node determines an effective channel to the receiver (Bob) in the communications point when two or more access points are involved. This may be determined such the secrecy rate as described earlier is maximized.

In step A5, the central node estimates an upper limit on the channel quality to a potential eavesdropper (Eve). It should be appreciated that the probability that Eve has a channel with similar quality as Bob decreases with as the number of access points and antennas increases. It should be appreciated that step A4 and A5 can take place at the same time or in any order.

In some embodiments, the estimation of the upper limit on the channel quality may comprise one or more of the following. The channel information to other users/IoT devices in the system is evaluated. The channel quality of the best channels may be used. Other information about potential eavesdroppers may be taken into account. For example, in a factory hall, it can be assumed that the eavesdropper has an additional penetration loss if he is outside the factory hall. A security margin may be added. The margin is added because the knowledge about the channel may not be complete. This may reduce the secrecy rate but maintains secrecy for communication at that rate.

In step S6, an appropriate secrecy rate is determined and in dependence on that rate a secrecy code rate is selected. Information theoretic considerations may be taken into account. A secrecy code with an appropriate code rate is selected. This may be done by adjusting parameters of the code. This code is then applied to the message to be transmitted before

transmitting. This secrecy code may reduce the data rate by adding suitable redundancy to that it can be ensured that there is a sufficient secrecy for the data transmission.

In step S7, an appropriate PHY Layer code is designed or selected. When the central node has determined the transmit method (e.g., the precoding weights and a receive method), the central node may determine the secrecy rate by applying information theoretic methods. The PHY layer aspect relates to selecting an appropriate modulation.

A parametrized family of codes is given. Designing a code may mean to select the parameters in such a way that the required/requested level of secrecy is maintained while the code rate meets the requirements given by the channel, i.e., the code rate for communication with the legitimate receiver is smaller or equal than the maximum rate allowed by the channel to the legitimate receiver and the assumed best channel to the eavesdropper. In other embodiments, pre-calculation or determination is performed providing a table of code parameters for different combinations (pairs) of channel qualities to the legitimate receiver and the eavesdropper. One entry may be selected from the table that fits to the current channel instantiations. In contrast to current proposal where such a table has only one dimension (the channel quality to the legitimate user) this table of some embodiments has an additional dimension (the channel quality to the eavesdropper.

In some embodiments, the secrecy code is based on information on a required secrecy level. This may come from the communication device or from another instance in the network that the communication device is communicating with. The secrecy level may be a property of practical codes and describes the reliability with which the code ensure that the eavesdropper cannot decode any information or in other words the (by design small) probability that that code cannot guarantee secrecy

Figure 5 shows an example where there are three access points 500, 502 and 504 which can be distributed units (DUs) of one or more gNodeBs. Each access point is equipped with multiple antennas and can transmit narrow beams. The access points are connected to a central node 506 (for example a security server), which is responsible for the security. The connections may include a DU and a CU of a gNodeB in a 5G system. In the area 510 where the three beams transmitted by the access points overlap the signal strength is higher than outside that area. A communications device is located in this area. This allows for encoding of the transmitted signals in such a way that it may be impossible to decode any information in a certain area between the UE and the access points. The shaded area referenced 508 represents an area which is covered by the respective nodes. However, outside the area of

overlap 510 of the beams from the different DUs, no information may be decoded due to a low channel quality and appropriate secure encoding.

Reference is made to Figure 6 which shows a signal flow in some embodiments.

In step S1, a DU is configured to send for example, channel information to the network node, which in this example is a security server.

In step S2, the security server provides information on the secrecy rate and/or code to the central unit CU.

In step S3, the CU sends information on the secrecy rate and/or code and/or encoded bits to the DU. (the CU and DU may be provided in a gNB. The CU and DU may be provided in different gNodeBs)

In step S4, the DU may provide information for decoding to the communication device. This communication may be unsecure.

In step S5, the DU provides secrecy encoded bits to provide a secure channel to the communications channel. The communication device may be capable of decoding (and/or encoding) the secrecy code.

In some embodiments both sides of the communication may be involved when negotiating the required level of security/secrecy and the required data rate at which secret communication is intended.

The UE might verify the expected received SINR. If SINR falls below a certain threshold with respect to the assumed one, it may send a warning message back to the gNB or other access point. This may cause the secrecy rate to be re- evaluated.

In some embodiments the threshold and other related parameters may be controlled and sent by the gNB or other access point to the communications device.

In some embodiments, an appropriate channel may be defined by selecting access points for communication to/from a communications device and define precoding matrices or beam directions

In the downlink direction, there may be a transmission from two or more multiple base stations with narrow beams towards one communication device.

In the uplink direction, there may be transmission from the communication device of narrow beams to different base stations.

In some embodiments, the transmit precoding may be selected in such a way that receiving a single beam in the downlink direction or the uplink direction may not be sufficient for decoding.

The central node (security server) may provide a coordination function and may collect channel information. In some embodiments provided for example in a 5G system, communication over the interface (the F1 interface) between CU and DU is used. However it should be appreciate that other embodiments may be implemented in other systems which may have different entities between which information is communicated. In some embodiments the DU and CU functions may be provided by a single node.

The security server may decide on the number of access points required for secret communication and/or which access points should be used.

The security server may selects a secrecy-rate achieving code for the combined channel.

The security server may ensures that the signal from a single beam has zero information about the transmitted signal and the superposition of multiple beams has a positive secrecy rate. If the security server ensures that the SINR seen in an area where only one beam can be received, is smaller than at the legitimate receiver, it can select a secrecy code for which the mutual information between the transmitted message and that received from the single beam is zero.

The security server may determine a secrecy rate and code to be used based on number of beams used.

In some embodiments, in DL there are no locations where the eavesdropper could decode the signal except those close to the communications device.

In some embodiments, in UL the sender may be identified by its spatial signature.

In some embodiments, communication in the UL may be made secure by sending a cryptographic key in DL communication.

In some embodiments, alternatively or additionally information other than the radio channel state information can be used for estimating a “best” or similar case channel for the eavesdropper. For example the environment may be taken into account. Consider the example of a communications device in a factory where it can be assumed that that internally, the factory is secure. This may thus provide an additional penetration loss of, e.g., 20 dB. This information may for example be a provided by a configuration parameter of the communication system and/or can be obtained via an interface from one or more other sources.

In some embodiments, building vector data models or similar modes of an environment may be used. For factories there exist even full mirror plants. In some embodiments models for tracking of moving objects in such environments may be used. Any of this information may be used in some embodiments. This may allow a more accurate prediction of the pathloss values in the particular environment and surrounding that environment. This may enable more accurate estimations of the maximum secrecy rate to be obtained.

It should be appreciated that embodiments may be used for all communications with a communication device. Alternatively, the secure communication may be used to exchange for example a cryptographic key which may be used to secure further communications. In some embodiments, there may be a secure key exchange and the key is used in one or more of the previously described methods.

In contrast to classical cryptographic security which relies on the assumption that a potential eavesdropper has limited computational power, physical layer security is considered to provide good secrecy even when the eavesdropper has unlimited computational power. Such secrecy may be considered to be perfectly secret, in some embodiments.

Perfectly secret communication means that no information at all can be decoded and thus provides a higher level of secrecy in contrast with other methods that make error-free decoding of the whole information impossible while parts of the information may be decodable. In other words, there may be no degradation of decoding quality with a reduced channel quality but rather there may be a hard limit where no information can be decoded anymore.

Some embodiments may not require key exchange required over a second channel. However, some embodiments may be used in conjunction with a key exchange of a second channel.

In some embodiments secrecy with a relatively high probability may be provided.

Reference is made to Figure 7 which shows a method. The method may be performed by an apparatus. The apparatus may be in a node such as a security node.

In step B1, channel information relating to a plurality of access points to a given communication device is used to select a plurality of access points. The channel information may relate to a channel between the plurality of access points and the communication device.

In step B2, in dependence on an effective channel to the communication device using the selected plurality of access points, a secrecy code is determined. The secrecy code is to be used in communications between said given communication device and said plurality of access points.

Reference is made to Figure 8 which shows a method. The method may be performed by an apparatus. The apparatus may be in a communications device.

In step C1, channel information relating to a plurality of access points may be caused to be provided to a network node. The apparatus may cause the information to be provided to the network node via one or more of the access nodes.

In step C2, a signal to which a secrecy code has been applied is decoded, said signal being received from the plurality of access points.

Reference is made to Figure 9 which shows a method. The method may be performed by an apparatus. The apparatus may be in an access point.

In step D1, channel information relating to a communication with a given communications device is caused to be provided to a network node.

In step D2, secrecy code information is received.

In step D3, the secrecy code is caused to be applied to a signal which is transmitted to the given communications device.

It should be appreciated that the method of any of Figures 7 to 9 may be modified as set out in relation to any of the previously described embodiments.

It should be understood that each block of the flowchart of the Figures and any combination thereof may be implemented by various means or their combinations, such as hardware, software, firmware, one or more processors and/or circuitry.

It is noted that whilst embodiments have been described in relation to one example of a 5G network, similar principles maybe applied in relation to other examples of networks. It should be noted that other embodiments may be based on other standards other than 3GPP standards. Therefore, although certain embodiments were described above by way of example with reference to certain example architectures for wireless networks, technologies and standards, embodiments may be applied to any other suitable forms of communication systems than those illustrated and described herein.

It is also noted herein that while the above describes example embodiments, there are several variations and modifications which may be made to the disclosed solution without departing from the scope of the present invention.

Although the apparatuses have been described as one entity, different modules and memory may be implemented in one or more physical or logical entities.

In general, the various embodiments may be implemented in hardware or special purpose circuits, software, logic or any combination thereof. Some embodiments may be implemented in hardware, while other aspects may be implemented in firmware or software which may be executed by a controller, microprocessor or other computing device, although the invention is not limited thereto. While various aspects may be illustrated and described as block diagrams, flow charts, or using some other pictorial representation, it is well understood that these blocks, apparatus, systems, techniques or methods described herein may be implemented in, as non-limiting examples, hardware, software, firmware, special purpose circuits or logic, general purpose hardware or controller or other computing devices, or some combination thereof.

Some embodiments may be implemented by computer software executable by a data processor of the communications device, such as in the processor entity, or by hardware, or by a combination of software and hardware. Some embodiments may be implemented by computer software executable by a data processor of the control apparatus. Computer software or program, also called program product, including software routines, applets and/or macros, may be stored in any apparatus-readable data storage medium and they comprise program instructions to perform particular tasks. A computer program product may comprise

one or more computer-executable components which, when the program is run, are configured to carry out embodiments. The one or more computer-executable components may be at least one software code or portions of it.

Further in this regard it should be noted that any blocks of the logic flow as in the Figures may represent program steps, or interconnected logic circuits, blocks and functions, or a combination of program steps and logic circuits, blocks and functions. The software may be stored on such physical media as memory chips, or memory blocks implemented within the processor, magnetic media such as hard disk or floppy disks, and optical media such as for example DVD and the data variants thereof, CD. The physical media is a non-transitory media.

The memory may be of any type suitable to the local technical environment and may be implemented using any suitable data storage technology, such as semiconductor based memory devices, magnetic memory devices and systems, optical memory devices and systems, fixed memory and removable memory. The data processors may be of any type suitable to the local technical environment, and may comprise one or more of general purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs), application specific integrated circuits (ASIC), FPGA, gate level circuits and processors based on multi core processor architecture, as non-limiting examples.

Embodiments may be practiced in various components such as integrated circuit modules. The design of integrated circuits is by and large a highly automated process. Complex and powerful software tools are available for converting a logic level design into a semiconductor circuit design ready to be etched and formed on a semiconductor substrate.

The foregoing description has provided by way of non-limiting examples a full and informative description of the exemplary embodiments. However, various modifications and adaptations may become apparent to those skilled in the relevant arts in view of the foregoing description, when read in conjunction with the accompanying drawings and the appended claims. However, all such and similar modifications of the teachings of this invention will still fall within the scope of this invention as defined in the appended claims. Indeed there is a further embodiment comprising a combination of one or more embodiments with any of the other embodiments previously discussed.

CLAIMS

1. An apparatus comprising means for:

using channel information from a plurality of access points to a given communication device to select a plurality of access points; and

in dependence on an effective channel to said communication device using said selected plurality of access points, determining a secrecy code to be used in communications between said given communication device and said plurality of access points.

2. An apparatus as claimed in claim 1, wherein said channel information relates to a plurality of beams from said plurality of access points, said means being for selecting a plurality of beams of said plurality of access points.

3. An apparatus as claimed in claim 1 or 2, wherein said means is for estimating a channel quality to a potential eavesdropping device.

4. An apparatus as claimed in claim 3, wherein said means is for estimating a limit on said channel quality to a potential eavesdropping device in dependence on one or more of channel information to one or more other devices, information about said effective channel, a security margin and potential location information associated with the potential eavesdropping device.

5. An apparatus as claimed in any preceding claim, wherein said means is for selecting said secrecy code in dependence on a secrecy rate.

6. An apparatus as claimed in claim 5, wherein said means is for using channel quality information relating to said plurality of beams and channel quality information relating to a potential eavesdropping device to determine said secrecy rate.

7. An apparatus as claimed in claim 5 or 6, wherein said means is for determining said secrecy rate in dependence on a difference between a mutual information between a signal which is transmitted to the given communication device and the signal which is received by that given communication device and mutual information between that transmitted signal and a signal potentially received by an eavesdropper.

8. An apparatus as claimed in claim 5, 6 or 7, wherein said means is for determining first mutual information between a message to be transmitted and the message received by said

given communication device and determining second mutual information between the message to be transmitted and the message received at an output of a channel corresponding to channel quality information associated with a potential eavesdropping device.

9. An apparatus as claimed in claim 8, wherein said secrecy rate is dependent on a difference between the first and second mutual information.

10. An apparatus as claimed in any preceding claim, wherein said channel information comprises one or more of: precoding weights for one or more beams; a beam direction for one or more beams; a transmit power for one or more beams; and one or more antenna orientations for one or more beams.

11. An apparatus as claimed in any preceding claim, wherein said means is for determining channel quality information associated with said effective channel.

12. An apparatus as claimed in any preceding claim, wherein said means is for providing one or more of transmit power information for one or more beams, a receive method for use by said given communication device; one or more beam directions for said beams; and precoding weights for one or more of said beams.

13. An apparatus as claimed in any preceding claim, wherein said means is for using information about one or more of a location and an environment of said given device to determine said effective channel.

14. An apparatus as claimed in any preceding claim, wherein said means is for selecting one or more parameters of a code family to determine said secrecy code.

15. An apparatus as claimed in any preceding claim, wherein said means is for causing different parts of said secrecy code to be distributed across different ones of said access points.

16. An apparatus as claimed in any preceding claim, wherein said effective channel is such that a signal to interference noise ratio is relatively large in a region around said given communications device.

17. An apparatus as claimed in claim 15, wherein said region is of an order of magnitude of a wavelength of a carrier frequency used for said effective channel.

18. An apparatus as claimed in any preceding claim, wherein said means is for selecting at least three beams from at least three access points.

19. An apparatus as claimed in any preceding claim, wherein said means is for selecting a physical layer code.

20. An apparatus as claimed in any preceding claim, wherein said means is for causing information about said secrecy code to be provided to one or more of said plurality of access points and said given communication device.

21. An apparatus as claimed in any preceding claim, wherein said means is for determining said secrecy code further in dependence on a required secrecy level.

22. An apparatus comprising means for:

causing channel information relating to a plurality of access points to be provided to a network node; and

decoding a signal to which a secrecy code has been applied, said signal being received from said plurality of access points.

23. An apparatus as claimed in claim 22, wherein said channel information relates to a plurality of beams from said plurality of access points, said signal being received from a plurality of beams of said plurality of access points.

24. An apparatus as claimed in claim 22 or 23, wherein said channel information comprises one or more of: precoding weights for one or more beams; a beam direction for one or more beams; a transmit power for one or more beams; and one or more antenna orientations for one or more beams.

25. An apparatus as claimed in any of claims 22 to 24, wherein said means is for receiving one or more of transmit power information for one or more beams, a receive method to be used; one or more beam directions for said beams; and precoding weights for one or more of said beams.

26. An apparatus as claimed in any of claims 22 to 25, wherein an effective channel for said signal is such that a signal to interference noise ratio is relatively large in a region around said apparatus.

27. An apparatus as claimed in claim 26, wherein said region is of an order of magnitude of a wavelength of a used carrier frequency.

28. An apparatus as any of claims 22 to 27, wherein said means is for encoding one or more signals to be transmitted to said access points using a secrecy code.

29. An apparatus as claimed in any of claims 22 to 28, wherein said means is for causing information on a required secrecy level to be provided to an access node.

30. An apparatus as claimed in any of claims 22 to 29, wherein said means is for receiving one or more secrecy codes used for one or more of decoding received signals and encoding signals to be transmitted.

31. An apparatus comprising means for:

causing channel information relating to a communication with a given communications device to be provided to a network node;

receiving secrecy code information; and

causing said secrecy code to be applied to a signal which is transmitted to said given communications device.

32. A method comprising:

using channel information relating to a plurality of access points to a given communication device to select a plurality of access points; and

in dependence on an effective channel to said communication device using said selected plurality of access points, determining a secrecy code to be used in communications between said given communication device and said plurality of access points.

33. A method comprising:

causing channel information relating to a plurality of access points to be provided to a network node; and

decoding a signal to which a secrecy code has been applied, said signal being received from said plurality of access points.

34. A method comprising:

causing channel information relating to a communication with a given communications device to be provided to a network node;

receiving secrecy code information; and

causing said secrecy code to be applied to a signal which is transmitted to said given communications device.

35. A computer program comprising computer executable instructions which when run cause any of the methods of claims 32 to 34 to be performed.

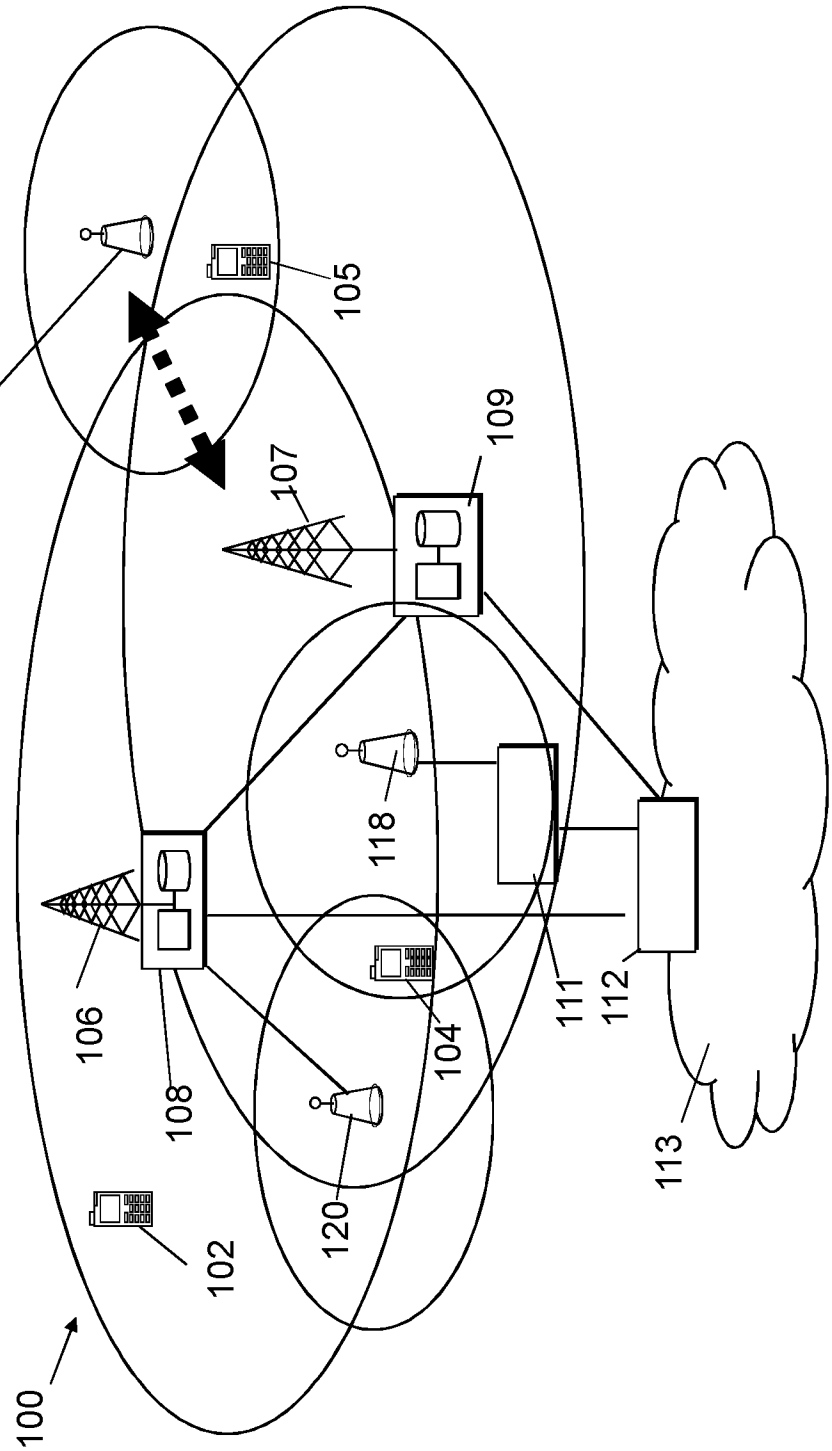


Figure 1

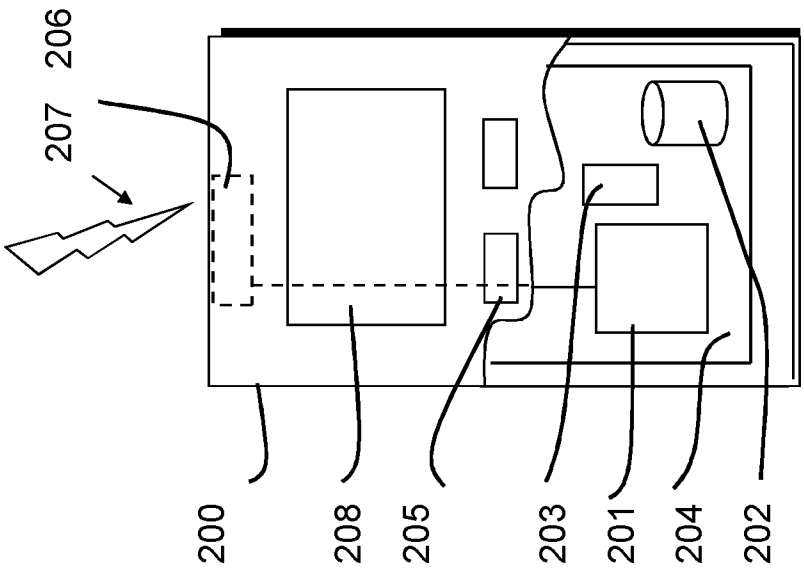


Figure 2

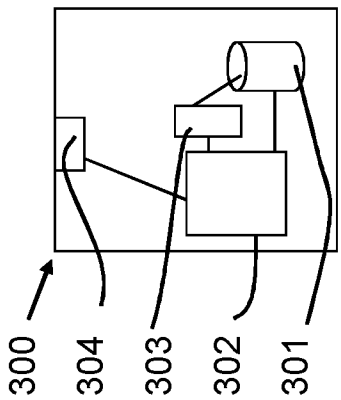


Figure 3


A1 Perform beam search and determine channel quality
A2 report information about the channels to a central node
A3 determine which DUs and which beams to use
A4 Determine effective channel to receiver
A5 Estimate upper limit on channel quality to potential eavesdropper
A6 – determine secrecy rate and select secrecy code rate
A7 – select PHY layer code

Figure 4

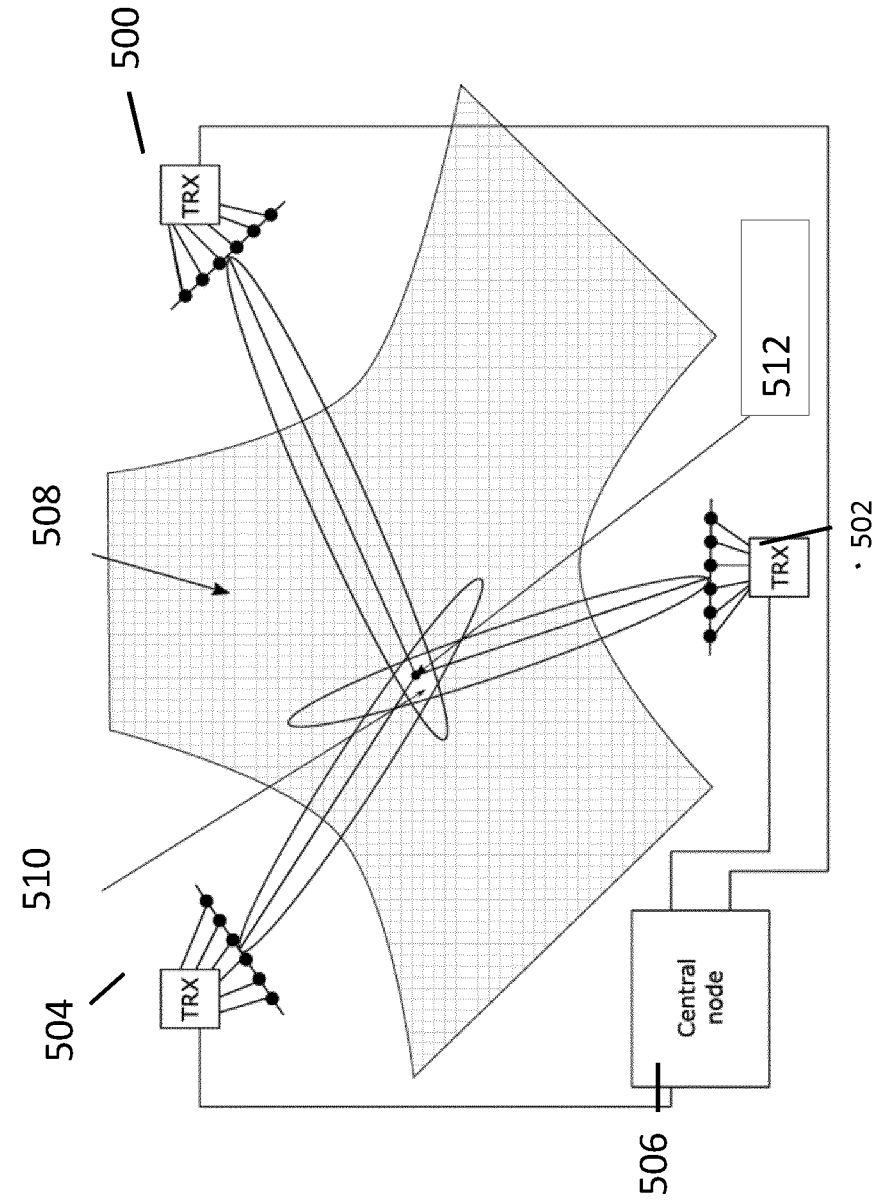


Figure 5

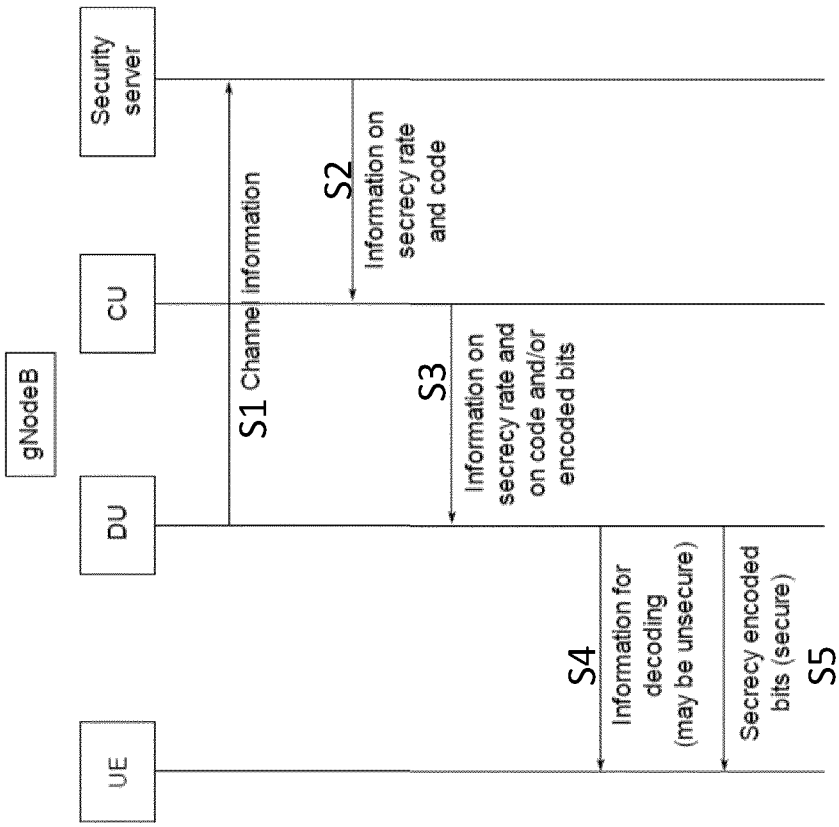

Security server
gNodeB
CU
DU
UE
S1 Channel information
S2
Information on secrecy rate and code
S3
Information on secrecy rate and on code and/or encoded bits
S4
Information for decoding (may be unsecure)
Secrecy encoded bits (secure)
S5

Figure 6

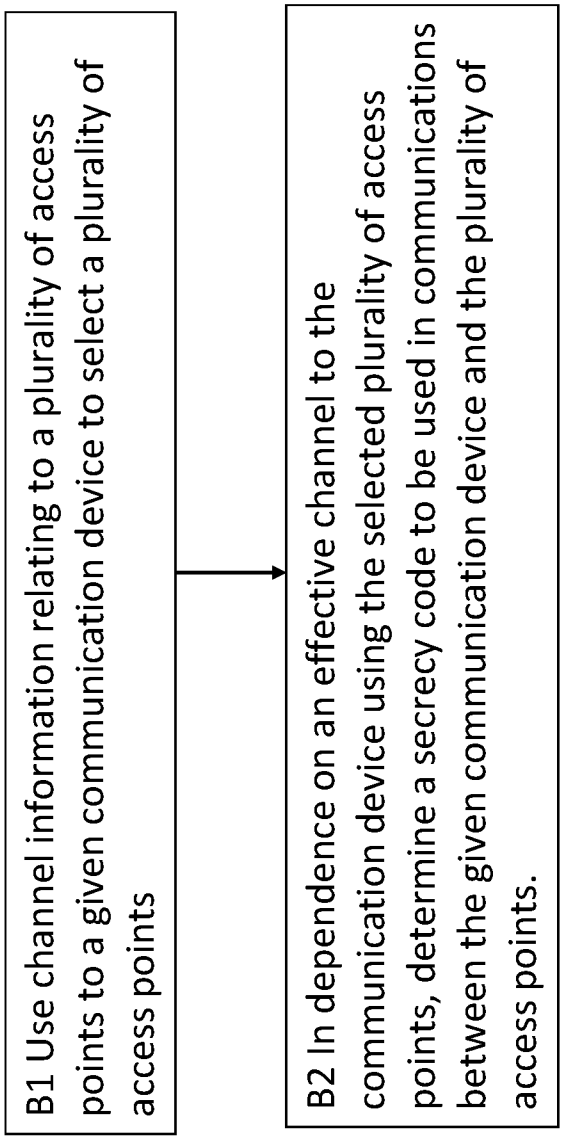

B1 Use channel information relating to a plurality of access points to a given communication device to select a plurality of access points
B2 In dependence on an effective channel to the communication device using the selected plurality of access points, determine a secrecy code to be used in communications between the given communication device and the plurality of access points.

Figure 7

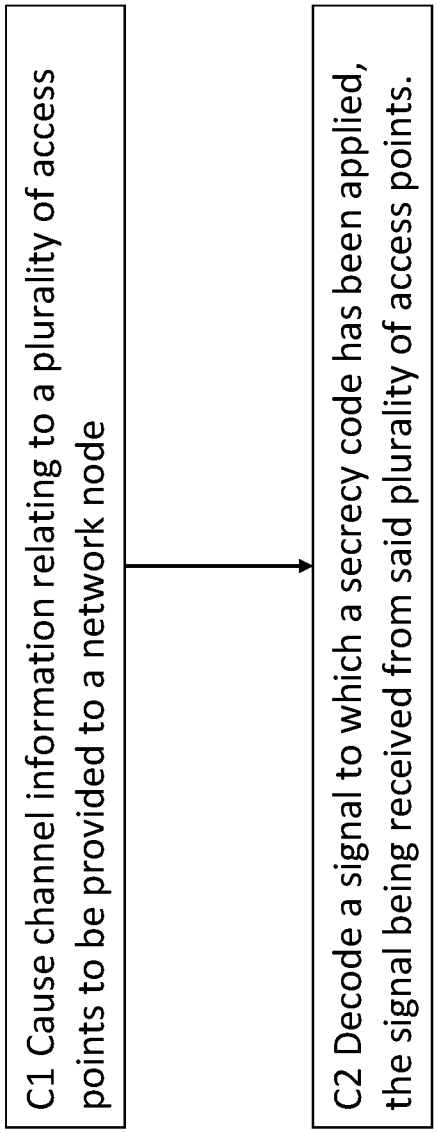

C1 Cause channel information relating to a plurality of access points to be provided to a network node
C2 Decode a signal to which a secrecy code has been applied, the signal being received from said plurality of access points.

Figure 8

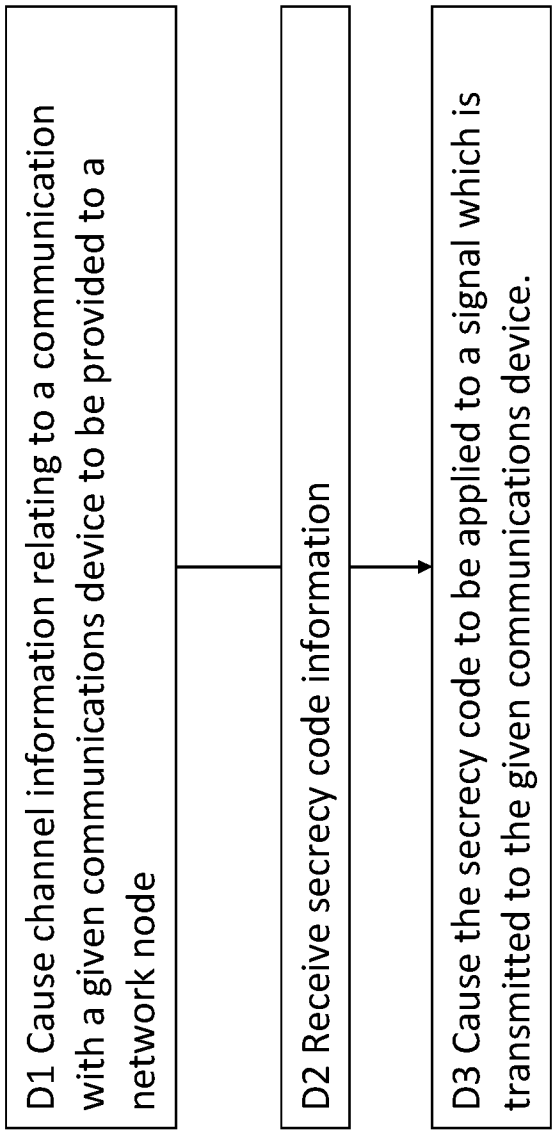

D1 Cause channel information relating to a communication with a given communications device to be provided to a network node
D2 Receive secrecy code information
D3 Cause the secrecy code to be applied to a signal which is transmitted to the given communications device.

Figure 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/077485

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04B7/024 H04W12/12
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)
H04B 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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KAMENI NGASSA CHRISTIANE L ET AL: "Combining artificial noise beam forming and concatenated coding schemes to effectively secure wireless communications", ANALOG INTEGRATED CIRCUITS AND SIGNAL PROCESSING, SPRINGER NEW YORK LLC, US, vol. 91, no. 2, 6 March 2017 (2017-03-06), pages 293-304, XP036205298, ISSN: 0925-1030, DOI: 10.1007/S10470-017-0942-2 [retrieved on 2017-03-06]	31,34,35
Y	page 293 - page 296 page 300 - page 303	1-30,32, 33

-/--

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents :

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

"E" earlier 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
14 June 2019	25/06/2019

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

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	LAKSHMANAN S ET AL: "Aegis: Physical Space Security for Wireless Networks With Smart Antennas", IEEE / ACM TRANSACTIONS ON NETWORKING, IEEE / ACM, NEW YORK, NY, US, vol. 18, no. 4, 1 August 2010 (2010-08-01) , pages 1105-1118, XP011298666, ISSN: 1063-6692 page 1105 - page 1110 page 1112 - page 1117	1-30,32, 33
A	WU YONGPENG ET AL: "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE SERVICE CENTER, PISCATAWAY, US, vol. 36, no. 4, 1 April 2018 (2018-04-01), pages 679-695, XP011686866, ISSN: 0733-8716, DOI: 10.1109/JSAC.2018.2825560 [retrieved on 2018-07-09] page 679 - page 684	1-35

1