

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
27 December 2007 (27.12.2007)

PCT

(10) International Publication Number
WO 2007/149014 A1

(51) International Patent Classification:

H04L 25/14 (2006.01) **H04L 9/12** (2006.01)
H04L 29/06 (2006.01) **H04Q 7/22** (2006.01)

(21) International Application Number:

PCT/SE2006/000744

(22) International Filing Date: 20 June 2006 (20.06.2006)

(25) Filing Language: English

(26) Publication Language: English

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

(72) Inventors; and

(75) Inventors/Applicants (for US only): **ANDERSSON, Mats** [SE/SE]; Ibsensgatan 16, S-417 19 Göteborg (SE).
GÖRANSSON, Bo [SE/SE]; Silverdalsvägen 67, S-191 38 Sollentuna (SE).

(74) Agent: **ALBIHNS GÖTEBORG AB**; Box 142, S-401 22 Göteborg (SE).

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

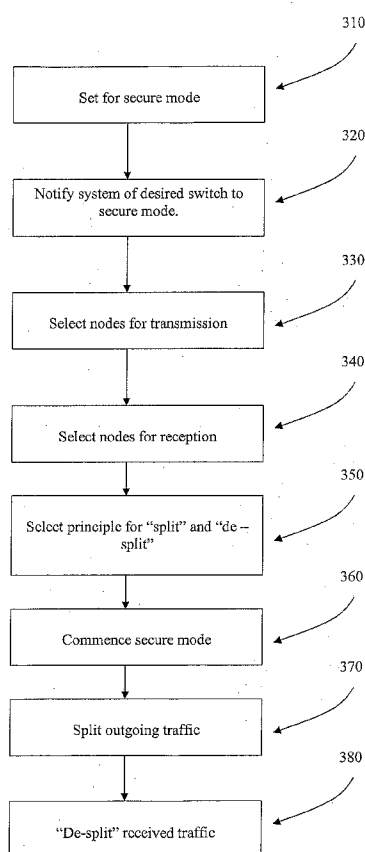
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— of inventorship (Rule 4.17(iv))

[Continued on next page]

(54) Title: A USER TERMINAL FOR ENHANCED SECURITY IN A WIRELESS COMMUNICATIONS SYSTEM, AND A SYSTEM FOR ITS USE



(57) Abstract: The invention discloses a user terminal (100) for use in a wireless communications system for voice calls and/or data sessions, which is equipped with means (140) for receiving and transmitting encrypted voice and/or data traffic to and from a second terminal in the system via a first node in the system. The user terminal is equipped with means (130) for splitting outgoing encrypted traffic during one and the same voice conversation and/or one and the same data session, so that a first part of the encrypted traffic to said second terminal is sent via said first node, and a second part is sent via a second node in the system.

WO 2007/149014 A1



Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TITLE

A user terminal for enhanced security in a wireless communications system, and a system for its use.

5 TECHNICAL FIELD

The present invention discloses a user terminal for use in a wireless communications system for voice calls and/or data sessions. The user terminal is equipped with means for receiving and transmitting encrypted voice and/or data traffic to and from a second terminal in the system via a
10 first node in the system.

The invention also discloses a wireless communications system and a method which employs the same principles as the user terminal of the invention.

15

BACKGROUND ART

Secure communications in wireless communications systems such as, for example, mobile telephony systems, has attracted a great amount of interest lately.

20

The traditional method of achieving secure communications in wireless or other systems has been to encrypt the traffic. Due to recent advances in cryptology, a high degree of communications security can be achieved using this method. However, unbreakable or nearly unbreakable encryption still
25 carries very high costs with it, if it can be achieved at all. Also, the demands for processor power in such systems is very high, both on the transmit and on the receive side.

DISCLOSURE OF THE INVENTION

30 As shown above, there is a need for a method and a system which could provide a high degree of communications security in a wireless

communications system at a reasonable cost, and without excessive demands on processor power.

Such a method is provided by the present invention, in that it discloses a user
5 terminal for use in a wireless communications system for voice calls and/or data sessions, the user terminal being equipped with means for receiving and transmitting encrypted voice and/or data traffic to and from a second terminal in the system via a first node in the system.

10 The user terminal is equipped with means for splitting encrypted traffic during one and the same voice conversation and/or one and the same data session, so that a first part of the encrypted traffic to said second terminal is sent via said first node, and a second part is sent via a second node in the system.

15 In one embodiment, the user terminal is additionally equipped with means for receiving split encrypted traffic from said second terminal in the system via at least two different nodes in the system, and for this purpose the user terminal is equipped with means for "de-splitting" the received traffic from said two nodes. Suitably, but not necessarily, said two nodes from which traffic is
20 received are the same as those nodes to which traffic is sent from the user terminal.

Thus, a user terminal according to the invention can "spread" one and the same phone call or data session over a multitude of nodes, or in the case of
25 cellular telephony, a multitude of base stations. Not only is the traffic encrypted, so that intercepted traffic will be difficult to understand, a possible eavesdropper will also have to intercept traffic to and from more than one base station ("node"), which is much more difficult than intercepting traffic to and from one base station.

30

The splitting or spreading of traffic to and from the user terminal can be done in a variety of ways, or in a combination of ways. Some such ways which can

be mentioned are the use of different time slots, multiple transmit beams in an antenna of the user terminal, multiple polarizations in at least one antenna beam in an antenna of the user terminal, multiple frequency slots or multiple codes, or one or more steerable antenna beams

5

The invention also discloses a system and method which utilize the same fundamental principles as the user terminal of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

10 The invention will be described in more detail below, with reference to the appended drawings, in which

Fig 1 shows a schematic block diagram of a user terminal according to the invention, and

Fig 2 shows a system in which a terminal of the invention is employed, and

15 Fig 3 shows a basic flow chart of the function of a user terminal according to the invention.

EMBODIMENTS OF THE INVENTION

Fig 1 shows a basic block diagram of some functional components of a user
20 terminal 100 of the invention. The components shown are means 110 for encrypting and decrypting outgoing and incoming traffic respectively, as well as means 130 for splitting outgoing traffic and means 120 for "de-splitting" received traffic. The user terminal 100 also comprises means 140 for receiving and transmitting split encrypted traffic.

25

All of the above components of the user terminal 100 and their functions will be described in more detail below.

Fig 2 shows a schematic overview of a system 200 in which a user terminal
30 100 of the invention is employed. The system and the user terminal will be exemplified by means of a user terminal in a system for cellular telephony, but other kinds of user terminals and systems can also employ the invention.

Examples of other kind of user terminals are portable computers with cellular capabilities, or units with wireless LAN possibilities in a LAN.

5 The user terminal 100 can be used for voice calls and/or data sessions with other users (not shown) in the system 200. In order to enhance the communications security, the user terminal 100 is equipped with means for encrypting said voice and/or data traffic to and from other users (terminals) in the system, as well as means for decrypting received voice and/or data traffic from other users.

10

The encryption and corresponding decryption means can be of a wide variety of kinds, and can be either in hardware or software or a combination of those. Encryption algorithms or principles which are well known to those skilled in the art can be used with the invention, for which reason those principles will
15 not be elaborated upon here.

In traditional cellular telephony, a user terminal communicates with other users in the system via a radio base station (RBS). There is a plurality of base stations in the system, and all traffic to and from one and the same
20 terminal is routed via one RBS, usually the one with the best signal quality at the time. Thus, a user terminal will usually be listening to traffic not only from the base station through which its traffic is routed, it will also monitor signals from other base stations within range, in order to measure signal quality for use in deciding when the traffic should be routed through another base
25 station than the one currently used, a so called "hand-over". This situation is exemplified in fig 2 where there is one user terminal 100, in the vicinity of which there are three base stations, 210, 220, 230, with respective coverage areas, 211, 221, 231.

30 The user terminal 100 of the invention makes use of the principle mentioned above, i.e. that there is, at least in most environments, more than one RBS with signal strengths such that the terminal 100 could route its traffic via

them. In the example of fig 2, it is assumed that the signal quality is sufficient for this for all three of the base stations shown in the system 200.

According to the invention, the user terminal 100 is equipped with means 130
5 for splitting outgoing encrypted traffic during one and the same voice call or data session between two or more base stations, so that, in the case where two base stations are used, a first part of the encrypted traffic to another user is sent via a first base station, and a second part is sent via a second base station in the system.

10

In a corresponding manner, the user terminal 100 of the invention is also equipped with means 120 for "de-splitting" the received traffic from said first and second nodes

15 Some possible methods for use when splitting will be described below, but a possible scenario for use of the invention is as follows, with reference to the flow chart shown in fig 3. It should be pointed out that the steps shown in fig 3 and described below do not need to be carried out in the order shown in fig 3, the same result may be achieved with the steps taken in a different order.

20

A user sets his terminal 100 to work in the "secure mode" of the invention, block 310 of the flow chart, or, alternatively, this is the only mode in which the terminal can operate, in which case the step of block 310 corresponds to activation of the terminal. As a third alternative, the terminal can be notified
25 by the system, via at least one base station, that the system wants the terminal to use the secure mode.

Block 320 is used if the decision to use secure mode is taken at or by the user terminal: the user terminal notifies the system, via at least one base
30 station of the decision to use the secure mode.

In blocks 330 and 340, decisions are made regarding which nodes or base stations that should be used in receiving traffic from (330) and sending traffic to (340) the user terminal. It should be pointed out that if there is a sufficient amount of base stations with a sufficient signal strength in the area, the same
5 base stations need not be used for receiving traffic from the user terminal as are used for sending traffic to the user terminal.

Thus, outgoing traffic from the terminal can be split between a first and a second base station, and traffic can be received at the user terminal from two
10 different base stations, where said first and second base stations are not the same as said two different base stations.

The decisions in blocks 330 and 340 are preferably made at "system level", i.e. the system comprises a function which is able to coordinate the actions of
15 the base stations and which takes the decisions regarding which base stations to use. These decisions can preferably be based on parameters such as the signal levels received at the user terminal from the base stations, and the signal levels received at the base stations from the terminal, as well as the load at each individual base station.

20

The signal levels measured at the user terminal from the base stations, and at the base stations from the user terminal are parameters which are already measured today, in order to decide and prepare for hand over of user terminals between different base stations.

25

As an alternative to having the decision on which base stations to use taken at system level, the decision can be taken at one of the base stations which would then have a special function for this, using the parameters mentioned above, which could be received via the system from other base stations and
30 from the terminal, or from the terminal alone, in which case the terminal could pass on information from one base station to another.

It is also conceivable to have said decision taken at the user terminal, based on the criteria mentioned above. The decision would then be communicated by the user terminal to the base stations involved.

- 5 Also, if there is a large number of nodes detected in blocks 330 and 340 which meet the criteria for use, the decision can be to select only a sub-set of those nodes to be used for transmitting or receiving encrypted traffic to and from the user terminal respectively. Otherwise, what happens in the step of blocks 330 and 340 is that all of the available nodes are selected for use.

10

In block 350, a decision is made regarding the principle that is to be used for splitting the traffic from the user terminal to the base stations, and from the base stations to the terminal. Suitably, the same principle is used in both directions, although this need not be the case.

15

The user terminal is pre-programmed with the possibility of using a number of different principles for splitting outgoing traffic, and for de-splitting received or incoming traffic. The same principles can, if necessary, be programmed into the base stations of the system.

20

Although the same effect can conceivably be obtained with other principles, some examples of principles for split and "de-split" of the traffic to and from the user terminal, respectively, which are envisioned at present are:

- 25 • The use of different time slots. In other words, if, for example, two base stations are used for receiving the traffic from the user terminal, the user terminal will transit to the first base station in a first time slot or set of slots, and to the second base station in a second time slot or set of slots, and will repeat this. Similarly, if this principle is used for
- 30 reception at the terminal, it will be used for transmission by the base stations to the terminal, so that the first terminal will transmit to the

user terminal in a first time slot or set of slots, and the second base station in a second time slot or set of slots.

- The use of different transmit beams in an antenna of the user terminal.
5 According to this principle, the user terminal has an antenna that can generate multiple transmit beams, which is used so that a first beam directed towards a first node and a second beam towards a second node. Preferably, each beam covers only its respective node. Alternatively, if different base stations are used to transmit and receive
10 to and from the user terminal, these different base stations can be covered by different antenna beams.
- The use of different polarizations in at least one antenna beam in an antenna of the user terminal. In other words, if one and the same
15 antenna beam of the user terminal is used to cover, for example, two base stations, communication with one of the base stations can be in a first polarization, and with the other base station in a second polarization, the polarizations preferably being orthogonal to each other, for example horizontal and vertical polarization.
20
- The use of different frequency slots. This is similar to the use of different time slots, but instead, different frequencies are used, so that if, for example, two base stations are used for receiving the traffic from the user terminal, the user terminal will transmit to the first base station
25 on a first frequency or set of frequencies, and to the second base station on a second frequency or set of frequencies. Similarly, if this principle is used for reception at the terminal, it will be used for transmission by the base stations to the terminal, so that the first terminal will transmit to the user terminal on a first frequency or set of
30 frequencies, and the second base station on a second frequency or set of frequencies.

- The use of different multiplexing codes. According to this principle, as used for example in the CDMA system (Code Division Multiple Access) communication between the user terminal and a first and a second base station is carried out by means of a first and a second set of multiplexing codes, respectively. The communication can thus, in principle, be on one and the same frequency to and from more than one base station.
- 10 It should be pointed out that the principle used for splitting traffic from the user terminal to the base station does not need to be the same as that used for splitting the traffic that is sent from the base stations to the user terminal, but in a preferred embodiment the same principle is used for traffic in both directions.
- 15 When the nodes to be used for communicating with the user terminal have been selected, blocks 330 and 340, and the principle/principles for use in splitting the traffic to/from the user terminal are chosen, block 350, the communication in "secure mode" can commence, block 360. As mentioned
- 20 previously, the enhanced security in this mode is obtained by use of encryption as well as by means of the use of more than one node for receiving traffic from the user terminal and for sending traffic to the user terminal during one and the same voice call or data session, or conceivably a call that involves the transfer of both voice and data.
- 25 Thus, somebody wishing to eavesdrop on a user terminal according to the invention would need to intercept traffic between the user terminal and at least two base stations, and would then need to "de-split" the traffic according to the principle used by the system, in addition to breaking the encryption
- 30 method used.

When the secure mode commences, block 360, this entails, as outlined above, splitting outgoing decrypted traffic at the user terminal, block 370, and "de-splitting" incoming decrypted traffic at the user terminal, block 380. Naturally, there are two alternatives here: either the traffic can first be split
5 and the encrypted, or first encrypted and then split, and similarly for incoming traffic. However, in a preferred embodiment, outgoing traffic is first split and then encrypted, in order to enable the use of different encryption for different "traffic splits", and incoming traffic is first decrypted and then "de-split". However, the reverse order is of course also possible.

10

The invention is not limited to the examples of embodiments shown above, but may be varied freely within the scope of the appended claims. As an example of such a variation, it would be perfectly possible to switch split principle during an ongoing voice or data session, or to combine principles
15 during one and the same session, provided that the standard of the system used permits this. For example, the GSM system would at present not permit a combination of time slot split and multiplex code split, but future systems such as, for example, systems beyond the 3G systems or WiMax might permit such combining.

20

Also, the number of RBS:s used by one and the same user terminal during one and the same session might be changed during an ongoing session.

In another embodiment of the invention, only one of the terminals involved in
25 a communication use the principle of splitting and de-splitting traffic. In such an embodiment, the first terminal would send split traffic via a number of nodes, and the system as such would comprise means for de-splitting the traffic before it is sent to the second terminal. Thus, the enhanced security would be offered at one end of the communication, but not at the other end.

30

The principle of letting the system de-split the traffic can also be used even if both of the user terminals utilize the invention: in such a system, the traffic

would be de-split by the system after being received from the first user terminal, and would then be split again before being sent to the second user terminal. Thus, four main cases can be discerned:

- 5 • Only one of the first and second user terminals splits outgoing encrypted traffic. The split traffic is de-split by the system.
- Both of the first and second user terminals split outgoing encrypted traffic. The split traffic is de-split by the system.
- Both of the first and second user terminals split outgoing encrypted traffic, and one of them can de-split received traffic. For the other
10 terminal, the split traffic is de-split by the system.
- Both of the first and second user terminals split outgoing encrypted traffic, and they can both de-split the received traffic.

15 It should also be noted that in those cases where the traffic is de-split by the system, this can take place at a more or less arbitrarily chosen node in the system, in other words the traffic does not need to be de-split at "RBS level".

CLAIMS

1. A user terminal (100) for use in a wireless communications system for voice calls and/or data sessions, said user terminal (100) being equipped
5 with means (140) for receiving and transmitting encrypted voice and/or data traffic to and from a second terminal in the system via a first node in the system, the user terminal being characterized in that it is equipped with means (130) for splitting outgoing encrypted traffic during one and the same voice conversation and/or one and the same data session so that a first part
10 of the encrypted traffic to said second terminal is sent via said first node, and a second part is sent via a second node in the system.
2. The user terminal of claim 1, additionally being characterized in that it is equipped with means (140) for receiving split encrypted traffic from said
15 second terminal in the system via at least two different nodes in the system, the user terminal (100) also being equipped with means (120) for "de-splitting" the received traffic from said at least two different nodes.
3. The user terminal (100) of claim 1, in which the means (130) for splitting
20 traffic to the second user is based on the use of different time slots.
4. The user terminal (100) of claim 1, in which the means (130) for splitting traffic to the second user is based on the use of different transmit beams in an antenna of the user terminal (100).
25
5. The user terminal (100) of claim 1, in which the means (130) for splitting traffic to the second user is based on the use of a steerable antenna beam, which is steered to the node which is used at each moment.
- 30 6. The user terminal (100) of claim 1, in which the means (130) for splitting traffic to the second user is based on the use of different polarizations in at least one antenna beam in an antenna of the user terminal.

7. The user terminal (100) of claim 1, in which the means (130) for splitting traffic to the second user is based on the use of different frequency slots.

5 8. The user terminal (100) of claim 1, in which the means (130) for splitting traffic to the second user is based on the use of different multiplexing codes.

9. The user terminal (100) of claim 1, in which the means for splitting traffic to the second user is based on a combination of at least two of the following principles :

- the use of different time slots.
- the use of different transmit beams in an antenna of the user terminal (100).
- the use of a steerable antenna beam, which is steered to the node which is used at each moment.
- the use of different polarizations in at least one antenna beam in an antenna of the user terminal.
- the use of different frequency slots.
- the use of different multiplexing codes.

20

10. The user terminal (100) of any of claims 2-8, in which the means (120) for "de-splitting" the received traffic is based on the same principle as the one used for transmitted traffic.

25 11. The user terminal (100) of any of claims 2-8, in which the means (120) for "de-splitting" the received traffic is one of the following:

- the use of different time slots.
- the use of different transmit beams in an antenna of the user terminal (100).
- the use of a steerable antenna beam, which is steered to the node which is used at each moment.

30

- the use of different polarizations in at least one antenna beam in an antenna of the user terminal.
- the use of different frequency slots.
- the use of different multiplexing codes.

5

12. A method for achieving enhanced communication security in a wireless communications system (200) for voice calls and/or data sessions, in which system (200) encrypted voice and/or data traffic is exchanged between at least a first (100) and a second user terminal via at least a first node (210, 220, 230) in the system, the method being characterized in that it comprises letting said first (100) and second user terminals split outgoing encrypted traffic during one and the same voice conversation and/or one and the same data session, so that a first part of the outgoing encrypted traffic from each of said terminals is sent via said first node, and a second part is sent via a second node in the system.

13. The method of claim 12, additionally comprising letting said first (100) and second user terminals receive said first and second parts of the encrypted traffic from the other terminal via said first and second nodes, and letting said user terminals "de-split" the received traffic.

14. The method of claim 13, according to which the first (100) and second user terminals split the outgoing encrypted traffic by using different time slots.

15. The method of claim 12, according to which the first (100) and second user terminals split the outgoing encrypted traffic by using different transmit beams in an antenna of the user terminal .

16. The method of claim 15, according to which the different antenna beams are employed to direct a first beam to the first node and a second beam to the second node.

17. The method of claim 12, according to which the first (100) and second user terminals split the outgoing encrypted traffic by using different polarizations in at least one antenna beam in an antenna of the user terminal
5 (100) .

18. The method of claim 12, according to which the first (100) and second user terminals split the outgoing encrypted traffic by using by using different frequency slots
10

19. The method of claim 12, according to which the first (100) and second user terminals split the outgoing encrypted traffic by using by using different multiplexing codes.

15 20. The method of claim 13, according to which the first and second user terminals (100) "de-split" the received traffic, based on the same principle as the one used for splitting transmitted traffic.

21. The method of claim 13, in which the principle for "de-splitting" the
20 received traffic is one of the following:

- the use of different time slots.
- the use of different transmit beams in an antenna of the user terminal (100).
- the use of a steerable antenna beam, which is steered to the node
25 which is used at each moment.
- the use of different polarizations in at least one antenna beam in an antenna of the user terminal.
- the use of different frequency slots.
- the use of different multiplexing codes.

30

22. A wireless communications system (200) for voice calls and/or data sessions, the system comprising at least a first (210, 220, 230) and a second (210, 220, 230) node for sending encrypted voice and data traffic to and receiving encrypted voice and data traffic from user terminals (100) in a geographical area covered by the system, the system in addition also comprising functionalities for:

- Receiving signals from a first user terminal (100) or sending signals to the first user terminal (100) that the terminal should or desires to commence sending and/or receiving traffic in a secure mode, the secure mode being a mode where traffic for one and the same voice call or data session is received from the first user terminal (100) by at least a first and a second node, the traffic being split between said nodes,
- Processing said split traffic before it is sent to a second, receiving user terminal in the system.

23. The system of claim 22, in which said functionality for processing the split traffic comprises a functionality for de-splitting the traffic.

24. The system of claim 22, in which said functionality for processing the split traffic comprises a functionality for forwarding the split traffic to the second user terminal.

25. The system of any of claims 22-24, further comprising functionalities for receiving split traffic from the second user terminal via at least two different nodes.

26. The system (200) of any of claims 21-25 additionally being equipped with a functionality for deciding which principle should be used for the splitting of the traffic, said principle being chosen from a plurality of predefined such principles.

27. The system (200) of claim 26, in which the principle for splitting the traffic is chosen from among the following:

- the use of different time slots,
- the use of different transmit beams in an antenna of the user terminal,
- 5 • the use of a steerable antenna beam, which is steered to the node which is used at each moment,
- the use of different polarizations in at least one antenna beam in an antenna of the user terminal,
- the use of different frequency slots,
- 10 • the use of different multiplexing codes.

28. The system (200) of claim 27, in which the principle for de-splitting the traffic is chosen from among the following:

- the use of different time slots,
- 15 • the use of different transmit beams in an antenna of the user terminal,
- the use of a steerable antenna beam, which is steered to the node which is used at each moment,
- the use of different polarizations in at least one antenna beam in an antenna of the user terminal,
- 20 • the use of different frequency slots,
- the use of different multiplexing codes.

100

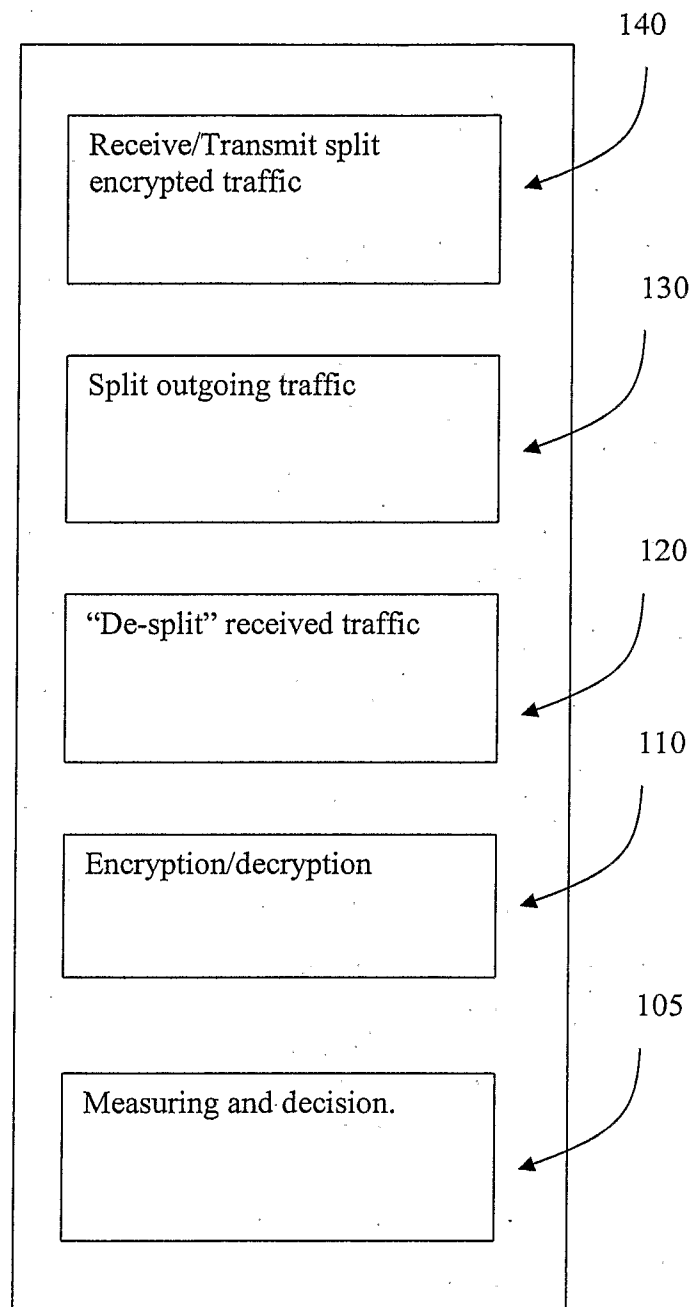


Fig 1

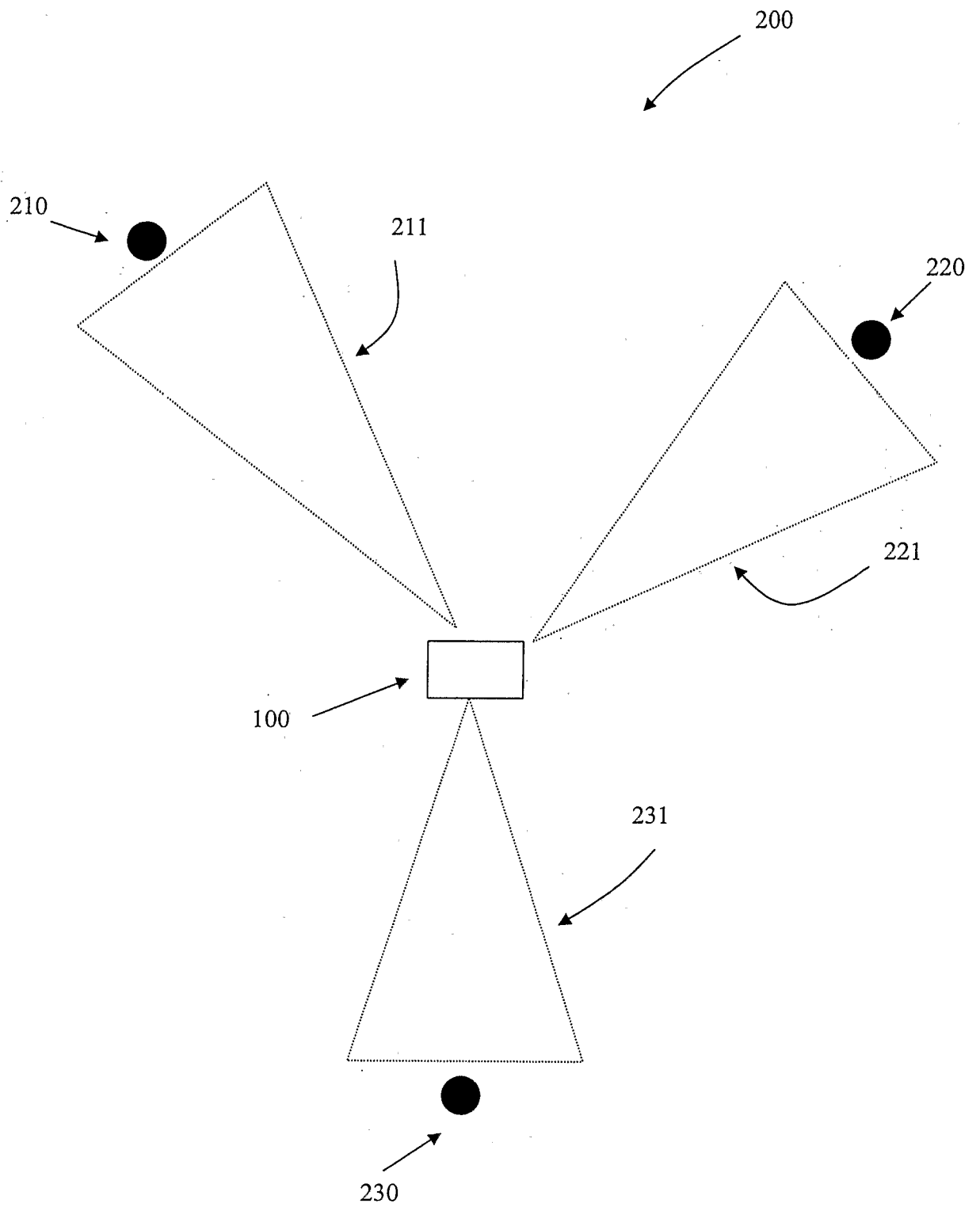


Fig 2

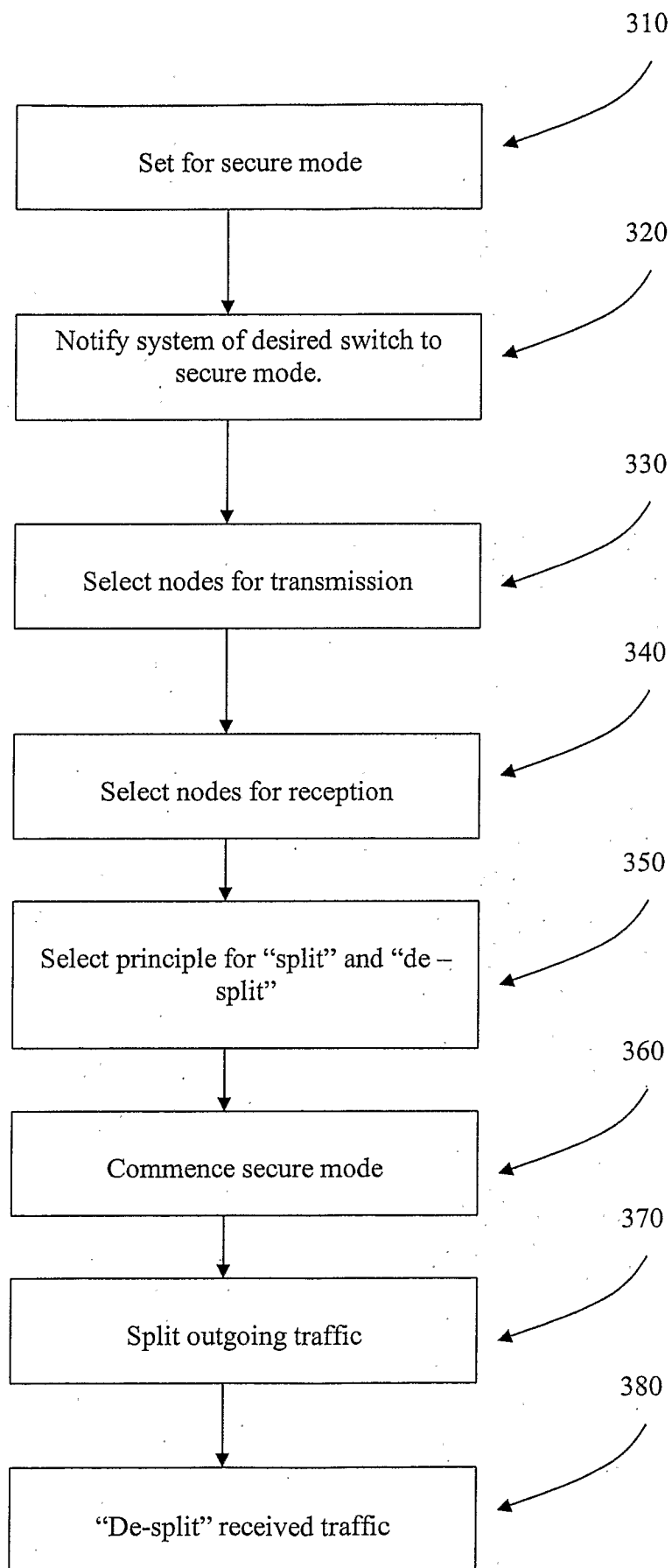


Fig 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE2006/000744

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04B, H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 20050163093 A1 (HARI KRISHNA GARG ET AL), 28 July 2005 (28.07.2005), abstract, claims 1-3, 6-7,10-18,22-27; [0003],[0008]-[0034], [0110]-[0111] --	1-28
A	US 4555805 A (ROBERT D. TALBOT), 26 November 1985 (26.11.1985), abstract --	1-28
A	WO 02052787 A2 (THE CHARLES STARK DRAPER LABORATORY, INC.), 4 July 2002 (04.07.2002), page 6, figures 1-5, abstract, claims 1-3,10-15, 19,23 --	1-28

☒ 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

3 April 2007

Date of mailing of the international search report

17 -04- 2007

Name and mailing address of the ISA/

Swedish Patent Office

Box 5055, S-102 42 STOCKHOLM

Facsimile No. +46 8 666 02 86

Authorized officer

Anders Edlund/MN

Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE2006/000744

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2005025179 A1 (BONA CSABA), 17 March 2005 (17.03.2005), page 3, line 25 - line 28; page 4, line 7, figure 1, claims 1-3,8-10, abstract --	1-28
A	WO 03003604 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V.), 9 January 2003 (09.01.2003), page 2, line 10 - line 15, abstract --	1-28
A	WO 03058984 A2 (LORANET NV ET AL), 17 July 2003 (17.07.2003), page 2 - page 4, abstract -- -----	1-28

International patent classification (IPC)**H04L 25/14** (2006.01)**H04L 29/06** (2006.01)**H04L 9/12** (2006.01)**H04Q 7/22** (2006.01)**Download your patent documents at www.prv.se**

The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.

The password is **LOTDOJCVPI**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT

Information on patent family members

24/02/2007

International application No.

PCT/SE2006/000744

US	20050163093	A1	28/07/2005	AU	2004314892	A	11/08/2005
				CA	2553668	A	11/08/2005
				EP	1709749	A	11/10/2006
				WO	2005074159	A	11/08/2005

US	4555805	A	26/11/1985	US	4411017	A	18/10/1983

WO	02052787	A2	04/07/2002	AU	2002253827	A	28/08/2002
				US	20020080888	A	27/06/2002
				US	20020120874	A	29/08/2002
				US	20030084020	A	01/05/2003
				WO	02062032	A	08/08/2002
				WO	02065292	A	22/08/2002

WO	2005025179	A1	17/03/2005	CH	694215	A	15/09/2004
				EP	1665712	A	07/06/2006

WO	03003604	A1	09/01/2003	CN	1520644	A	11/08/2004
				EP	1405429	A	07/04/2004
				GB	0115937	D	00/00/0000
				JP	2004533787	T	04/11/2004
				US	20030013468	A	16/01/2003

WO	03058984	A2	17/07/2003	AT	308044	T	15/11/2005
				AU	2003201413	A	24/07/2003
				CA	2435727	A	15/08/2002
				DE	60206880	D,T	20/07/2006
				EP	1358475	A,B	05/11/2003
				SE	1358475	T3	
				EP	1464189	A	06/10/2004
				GB	0200237	D	00/00/0000
				JP	2004518959	T	24/06/2004
				US	6805009	B	19/10/2004
				US	20040051539	A	18/03/2004
				US	20050059342	A	17/03/2005
