(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 849 374 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.03.2015 Bulletin 2015/12

(51) Int Cl.:
H04K 1/02 *(2006.01)*

(21) Application number: **13290221.4**

(22) Date of filing: **16.09.2013**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(71) Applicant: **ALCATEL LUCENT**
92100 Boulogne-Billancourt (FR)

(72) Inventor: **Chen, Yejian**
70825 Stuttgart (DE)

(74) Representative: **Richardt Patentanwälte PartG mbB**
Wilhelmstraße 7
65185 Wiesbaden (DE)

(54) Secure communications system and method

(57) The invention relates to a communications method of securely transmitting an electronic message from at least one transmitter (1) to at least one intended receiver (2) over at least one public communications channel, comprising the steps of: selecting a predetermined pilot pattern (4) by a selecting means and advising said at least one transmitter (1) and said at least one intended receiver (2) of said selected pilot pattern;

transmitting a superimposed signal comprising of said electronic message (5) and said selected pilot pattern (4) over said at least one public communications channel by said at least one transmitter;

receiving said superimposed signal and extracting said electronic message by at least one of said intended receivers (1) from said superimposed signal using said selected pilot pattern.

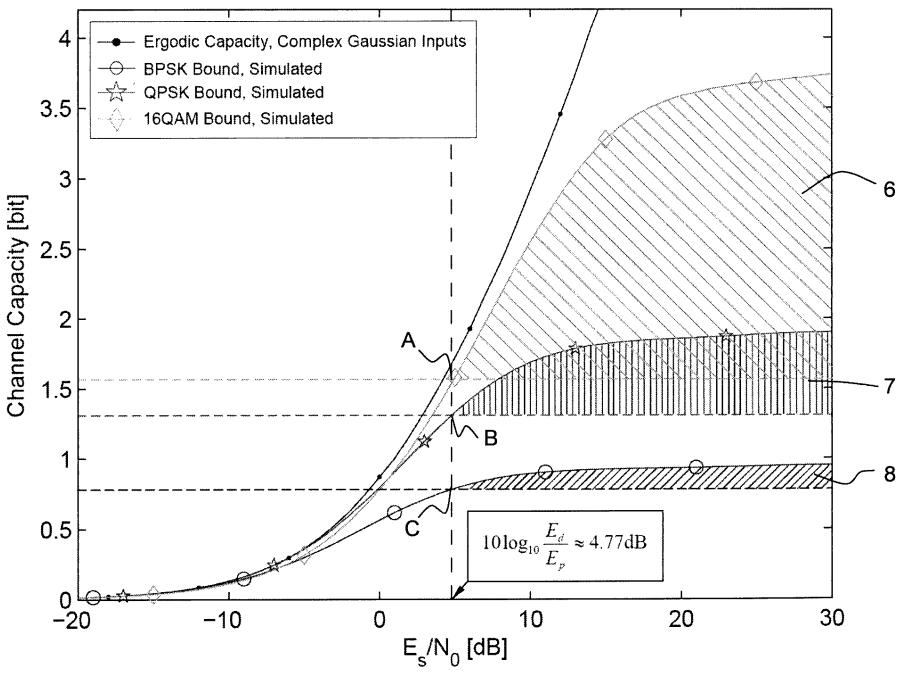

Fig. 2

EP 2 849 374 A1

Description

[0001] The present invention relates to secure communication and in particular to secure communication without use of encryption.

[0002] Methods for communicating secret data are known. These methods mainly rely on the exchange of encryption keys between transmitter and intended recipient. Once the secret message is encrypted by use of the encryption key it is protected at least to a certain extent from being read by third parties while being transmitted. However, encryption key-based systems necessitate an exchange of encryption keys and are thus rather awkward to handle.

[0003] Nevertheless, as Machine-to-Machine (M2M) communications, or alternatively Machine Type Communications (MTC), is becoming a more and more important player in future wireless communications standards, it is recognized at the very beginning that new technologies have to be investigated to combat against the M2M/MTC related security threats.

[0004] In Wyner, A.D.; "The wire-tap channel," Bell Syst. Tech. J., Vol. 54, pp. 1355-1387, 1975, a wiretap channel is introduced and its secrecy capacity is analyzed, which is achievable even without a secret key. A more general (non-degraded) model of Wyner's wiretap channel was extended in Csiszár, I.; Körner, J.; "Broadcast Channel with Confidential Messages," IEEE Trans. Inf. Theory, Vol. 24, No. 3, pp. 339-348, May 1978.

[0005] In Foschini, G.J. and Gans, M.J.; "On limits of wireless communications in a fading environment when using multiple antennas," Wireless Personal Commun., Vol. 6, No. 3, pp. 311-335, Mar. 1998, and in Alamouti, S.M.; "A simple transmit diversity technique for wireless communications," IEEE J. Select. Areas Commun., Vol. 16, No. 8, pp. 1451-1458, Oct. 1998, Multiple-Input Multiple-Output (MIMO) technique is adopted as another key technology in current and future wireless standards, which allows a trade-off between high data throughput and high detection robustness. Hence, secure MIMO communications is another important issue. Further, many efforts were made to analytically investigate the secrecy capacity region of the MIMO wiretap channel. Also some practical solutions such as artificial noise, beamforming technique, precoding technique and secure downlink joint detection are investigated.

[0006] Other systems for securely transmitting messages through public channels are user-specific scrambling, user-specific precoding and generating artificial noise. However, the existing solutions generally require the channel information of the eavesdropper(s), which is not straightforwardly applicable in practice.

[0007] As a consequence, it is an object of the present invention to provide a method and a system for conveying secret messages without necessitating encryption.

[0008] This aim is achieved by the communications system according to claim 1, the communications method according to claim 8 and the computer program product according to claim 13. Preferred embodiments of the invention are subject of the respective dependent claims.

[0009] A secure communications scheme is provided with superimposed pilots. Embodiments of the invention are based on introduction of superimposed pilots on the communications channel that is used by transmitter and intended recipient, i.e. the user of interest, so as to create artificial noise on the channel. The pilots are known to the transmitter as well as to the intended recipient of the message. Consequently, the intended recipient is enabled to entirely filter out the known artificial noise on the channel and extract the disguised message as clear data. For an eavesdropper not being aware of the used pilot pattern that disguises the actual message, the superimposed pilot is a kind of noise that has to be eliminated. For this purpose the eavesdropper will have to employ standard noise filtering methods. Standard noise filtering methods however are limited in their ability to remove spurious signals and extract the clear message. If the channel becomes too noisy it is no longer possible to extract the message with standard noise filters.

[0010] Embodiments of the invention relate to a system concept enabling secure communications by introducing superimposed pilots. The superimposed pilots can be exploited in a trellis-based joint channel tracker and data detector by the intended recipient. Further, the intended recipient can adjust the power ratio between the user data and the superimposed pilot, which yields the secure capacity region. It allows the intended recipient to appropriately select the Forward Error Correction (FEC) code rate, so that the eavesdropper will not be able to decode the corresponding data any more.

[0011] Embodiments of the invention are susceptible for application not only in a Single-Input Single-Output (SISO) system, but also Multiple-Input Single-Output (MISO) with Space-Time Coding (STC), and Multiple-Input Multiple-Output (MIMO) with Spatial Multiplexing (SMX). The respective achievable secure capacity region is preferably determined in a Monte Carlo simulation.

[0012] Some embodiments of the system and/or method in accordance with embodiments of the present invention are now described, by way of example only, and with reference to the accompanying drawings, in which:

Fig. 1 schematically illustrates a model for secure communications with superimposed pilots according to the invention;

Fig. 2 shows in a schematic plot the secure capacity for SISO system for an i.i.d. Rayleigh channel according to the invention;

Fig. 3 is a flow diagram of a preferred embodiment of the method for securely transmitting an electronic message including security control mechanism according to the invention;

Fig. 4 schematically shows the achievable secure rate for SISO system for BPSK and QPSK modulation according to the invention; and

Fig. 5 schematically shows the achievable secure rate for MISO-STC and MIMO-SMX system for BPSK modulation according to the invention.

[0013] A secure communications scheme is provided with superimposed pilots. This scheme can be exploited not only by Single-Input Single-Output (SISO), but also by Multiple-Input Single-Output (MISO), Multiple-Input Multiple-Output (MIMO) systems with Space-Time Coding (STC) and Spatial Multplexing (SMX), respectively. The superimposed pilots serve as artificial noise and are known to an intended recipient but unknown to potential eavesdroppers.

[0014] In Fig. 1 a basic model of a communications environment is represented for explaining the invention. Part of the environment is a transmitter 1, an intended recipient 2 and a non-intended recipient 3, i.e. eavesdropper. As an example it is assumed that the transmitter 1 is a base station BS or relay station and the intended recipient 2 is a mobile terminal. In the rest of the description the conventional terminology is generally used with the transmitter 1 and the intended recipient 2 (user of interest) named Alice and Bob, respectively, and the potential eavesdropper 3 Eve.

[0015] An electronic message is to be conveyed from the transmitter 1 to the intended recipient 2 in a secure way, that is, no other party shall be able to intercept the transmitted signal and extract the actual message therefrom. The mobile terminal 2 of Bob has several superimposed pilot patterns 4 and is registered in the system, i.e. a priori known to the transmitter 1. The pilot patterns 4 may be implemented e.g. in hardware or stored in a memory as software code with Bob's mobile terminal 2. In a secure communication mode the superimposed pilots are transmitted along with the actual message that is to be conveyed from the transmitter 1 to the intended recipient 2. The message to be conveyed consists of information symbols 5. These information symbols 5 and the pilot symbols 4 are transmitted each with power Ed and power Ep for data symbols 5 and pilot symbols 4, respectively. Hence, the total energy per transmitted symbol Es is $Es = Ed + Ep$.

[0016] As an example Fig. 2 represents the channel capacity over the ratio of Es/N0, where Es is the power of the overall transmitted signal and N0 is the power of noise on the channel. In Fig. 2 the channel capacity is illustrated for BPSK, QPSK and 16QAM modulation schemes for an independent identically distributed (i.i.d.) Rayleigh fading channel.

[0017] It is assumed that the intended recipient 2 Bob is fully aware of the Channel State Information (CSI). On the other side an eavesdropper 3 Eve does not a priori know the superimposed pilot pattern and thus suffers from an artificial noise which may be quantified by the SNR value $10\log(Ed / Ep)$. As an example it is assumed that $Ep = 0.25$ and $Ed = 0.75$. Hence, Eve suffers from an artificial noise $10\log(Ed / Ep) \approx 4.77$ dB. Even if the eavesdropper 3 had the perfect Channel State Information (CSI) like the intended recipient 2, which although not a very strong prerequisite is almost inapplicable in practice, the eavesdropper 3 is only able to decode the intended recipient's 2 information that is encoded with a Forward Error Correction (FEC) code rate corresponding to the area below a horizontal line through the intersection points A, B, C, for 16QAM, QPSK and BPSK, respectively.

[0018] Hence, the intended recipient 2 is able to extract messages that are conveyed with an forward error correction rate below the respective BPSK bound, QPSK bound, 16 QAM bound limit yet still above the horizontal line through the intersection points A, B, and C. These allowed and secure regions are marked in Fig. 2 as an upper obliquely hatched area 6 for 16 QAM modulation, a vertically hatched area 7 for QPSK modulation and a lower obliquely hatched area 8 for BPSK modulation. This shows from the view point of secure communications that an eavesdropper 3 Eve will not be able to decode information, if an FEC code is used with a sufficiently high code rate to encode the information.

[0019] Fig. 3 shows a flow diagram as an embodiment of a method for securely transmitting electronic messages. The flow diagram is based on the above analysis in Fig. 2.

[0020] In step 10 the intended recipient 2 Bob communicates with the transmitter 1 BS in a normal mode using a predetermined Modulation and Coding Scheme (MCS) in accordance with the current Signal to Interference plus Noise Ratio (SINR) on the channel and the respective Channel State Information (CSI).

[0021] In step 11 it is queried whether or not a secure communication mode is intended. In the negative the method branches back to step 10. In the affirmative the method continues at step 12.

[0022] In step 12 it is queried whether the request for secure communication comes from the intended recipient 2 himself. In the negative, it is assumed that the request originated from the transmitter 1 (branch labelled "No (DL aspect)"). Otherwise it is recognized that the request originates from the intended recipient 2 (branch labelled "Yes (UL aspect)").

[0023] If the request originated from the transmitter 1 (label "No (DL aspect)"), the method continues at step 13.

[0024] In step 13 the transmitter determines the superimposed pilot pattern in accordance with the security level.

[0025] Subsequently, in step 14 the transmitter selects the power ratio between data and pilot, namely Ed / Ep, and adjusts the MCS according to current SINR, CSI and security level.

[0026] The transmitter then sends the command in step 15 via Downlink (DL) and keeps the intended receiver informed of steps 13 and 14 above.

[0027] After receiving the acknowledgement from the intended recipient the transmitter starts the secure communication in step 16.

[0028] On the other side, if in step 12 it has been recognized that the request for secure communication originated from the intended recipient himself, the method branches to step 17, labelled "Yes (UL aspect)", and the intended recipient determines the superimposed pilot pattern according to the security level in step 17.

[0029] In step 18 the intended recipient selects the power ratio between data and pilot, namely Ed / Ep, and adjusts the MCS in accordance with the current SINR, CSI and security level.

[0030] The intended recipient then sends the request via Uplink (UL) to the transmitter in step 19 and keeps the transmitter informed of steps 17 and 18 above.

[0031] After receiving the acknowledgement from the transmitter the intended recipient starts the secure communication in step 20.

[0032] After steps 16 and 20, respectively, the method terminates, and in another query (not shown) it may be determined that the method leaves the secure communications mode and returns to the normal communications mode again.

[0033] The method as represented in Fig. 3 and other embodiments on the same principle may be summarized as follows. Any communications method of this kind that is employed for securely transmitting an electronic message from at least one transmitter to at least one intended receiver over at least one public communications channel essentially comprises the following steps. A predetermined pilot pattern is selected by a selecting means. The selecting means may be located at the transmitter or at the intended recipient. After the pilot pattern has been determined said selecting means advises the remote party, i.e. the transmitter or the intended receiver of said selected pilot pattern. Once the pilot pattern has been acknowledged by all involved (intended) parties a superimposed signal comprising of said electronic message and said selected pilot pattern is transmitted over said public communications channel by the transmitter. The superimposed signal is received by the intended recipient, and potentially by an eavesdropper. Yet, only the intended recipient is able to extract the electronic message from the superimposed signal due to his knowledge of the selected pilot pattern. The eavesdropper, on the other hand, faces huge difficulties in his endeavours to extract the actual data from the "noisy" channel.

[0034] The communications method is applicable to a single transmitter and a single intended receiver (SISO) which both communicate over a public communications channel. Alternatively, instead of one transmitter only the communications system may also comprise multiple transmitters and a single intended receiver (MISO) which communicate over a public communications channel using Space-Time Coding (STC). And consequently, also multiple intended receivers (MIMO) may be involved which communicate with multiple transmitters over a public communications channel using Spatial Multiplexing (SMX).

[0035] As mentioned above, the embodiments of the invention are not limited to a particular input-output-system or type of modulation. In the following further examples will be given of input-output-system and modulation types to which the invention is applicable.

[0036] In Fig. 4 a SISO system using BPSK and QPSK modulation is considered. The secure region that is achievable with superimposed pilots is illustrated by oblique hatchings for BPSK modulation in an area 21 and by vertical hatchings for QPSK modulation in an area 22. Furthermore, the Low-Density Parity-Check (LDPC) code - as a linear error correcting code - is deployed to verify the achievable secure capacity region. Both of them coincide to each other very well.

[0037] Similarly, in Fig. 5 a MISO-STC system and a MIMO-SMX system, respectively, is considered. The achievable secure region is illustrated by oblique hatchings for STC modulation in an area 23 and by vertical hatchings for SMX modulation in an area 24. It becomes clear that an eavesdropper Eve manages to intercept and decode the information, as soon as the FEC code rate is selected slightly outside of the achievable secure capacity region. This is indicated by stars in the plot labelled as "successful eavesdropping".

[0038] A person of skill in the art would readily recognize that steps of various above described methods can be performed by programmed computers. Herein, some embodiments are also intended to cover program storage devices, e.g., digital data storage media, which are machine or computer readable and encode machine executable or computer-executable programs of instructions, wherein said instructions perform some or all of the steps of said above-described methods. The program storage devices may be, e.g., digital memories, magnetic storage media such as a magnetic disks and magnetic tapes, hard drives, or optically readable digital data storage media. The embodiments are also intended to cover computers programmed to perform said steps of the above-described methods.

[0039] The description and drawings merely illustrate the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements that, although not explicitly described or shown herein, embody the principles of the invention and are included within its spirit and scope. Furthermore, all examples recited herein are principally intended expressly to be only for pedagogical purposes to aid the reader in understanding the principles of the invention and the concepts contributed by the inventor(s) to furthering the art, and are to be construed as being without limitation to such specifically recited examples and conditions. Moreover, all statements herein reciting principles, aspects, and embodiments of the invention, as well as specific examples thereof, are intended to encompass equivalents thereof.

[0040] The functions of the various elements shown in

the FIGs., including any functional blocks labeled as "processors", may be provided through the use of dedicated hardware as well as hardware capable of executing software in association with appropriate software. When provided by a processor, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared. Moreover, explicit use of the term "processor" or "controller" should not be construed to refer exclusively to hardware capable of executing software, and may implicitly include, without limitation, digital signal processor (DSP) hardware, network processor, application specific integrated circuit (ASIC), field programmable gate array (FPGA), read only memory (ROM) for storing software, random access memory (RAM), and non volatile storage. Other hardware, conventional and/or custom, may also be included. Similarly, any switches shown in the FIGS. are conceptual only. Their function may be carried out through the operation of program logic, through dedicated logic, through the interaction of program control and dedicated logic, or even manually, the particular technique being selectable by the implementer as more specifically understood from the context.

[0041] It should be appreciated by those skilled in the art that any block diagrams herein represent conceptual views of illustrative circuitry embodying the principles of the invention. Similarly, it will be appreciated that any flow charts, flow diagrams, state transition diagrams, pseudo code, and the like represent various processes which may be substantially represented in computer readable medium and so executed by a computer or processor, whether or not such computer or processor is explicitly shown.

[0042] The present inventions may be embodied in other specific apparatus and/or methods. The described embodiments are to be considered in all respects as only illustrative and not restrictive. In particular, the scope of the invention is indicated by the appended claims rather than by the description and figures herein. All changes that come within the meaning and range of equivalency of the claims are to be embraced within their scope.

Claims

1. Communications system for securely transmitting an electronic message from at least one transmitter (1) to at least one intended receiver (2) over at least one public communications channel, comprising:

   selecting means for selecting a predetermined pilot pattern (4) and advising said at least one transmitter (1) and said at least one intended receiver (2) of said selected pilot pattern;
   wherein at least one transmitter (1) is adapted to transmitting a superimposed signal comprising of said electronic message (5) and said selected pilot pattern (4) over said at least one public communications channel;
   at least one of said intended receivers (2) is adapted to receiving said superimposed signal and extracting said electronic message from said superimposed signal using said selected pilot pattern.

2. Communications system according to claim 1, wherein said selecting means is part of the transmitter (1).

3. Communications system according to claim 1, wherein said selecting means is part of the intended receiver (2).

4. Communications system according to any of the preceding claims, comprising a single transmitter and a single intended receiver (SISO) communicating over said at least one public communications channel.

5. Communications system according to any of claims 1 to 3, comprising multiple transmitters and a single intended receiver (MISO) communicating over said at least one public communications channel using Space-Time Coding (STC).

6. Communications system according to any of claims 1 to 3, comprising multiple transmitters and multiple intended receivers (MIMO) communicating over said at least one public communications channel using Spatial Multiplexing (SMX).

7. Communications system according to any of the preceding claims, wherein at least one parameter out of a power ratio of said pilot pattern versus electronic message and a modulation and coding scheme (MCS) is determined as a function of at least one out of a signal to interference plus noise ration (SINR) and a channel state information (CSI).

8. Communications method of securely transmitting an electronic message from at least one transmitter (1) to at least one intended receiver (2) over at least one public communications channel, comprising the steps of:

   selecting a predetermined pilot pattern (4) by a selecting means and advising said at least one transmitter (1) and said at least one intended receiver (2) of said selected pilot pattern;
   transmitting a superimposed signal comprising of said electronic message (5) and said selected pilot pattern (4) over said at least one public communications channel by said at least one transmitter;
   receiving said superimposed signal and extracting said electronic message by at least one of

said intended receivers (1) from said superimposed signal using said selected pilot pattern.

9. Communications method according to claim 8, wherein a single transmitter and a single intended receiver (SISO) communicate over said at least one public communications channel.

10. Communications method according to claim 8, wherein multiple transmitters and a single intended receiver (MISO) communicate over said at least one public communications channel using Space-Time Coding (STC).

11. Communications method according to claim 8, wherein multiple transmitters and multiple intended receivers (MIMO) communicate over said at least one public communications channel using Spatial Multiplexing (SMX).

12. Communications method according to any of claims 8 to 11, wherein at least one parameter out of a power ratio of said pilot pattern versus electronic message and a modulation and coding scheme (MCS) is determined as a function of at least one out of a signal to interference plus noise ration (SINR) and a channel state information (CSI).

13. A computer program product comprising computer executable instructions to perform any of the steps as claimed in any of the above method claims.

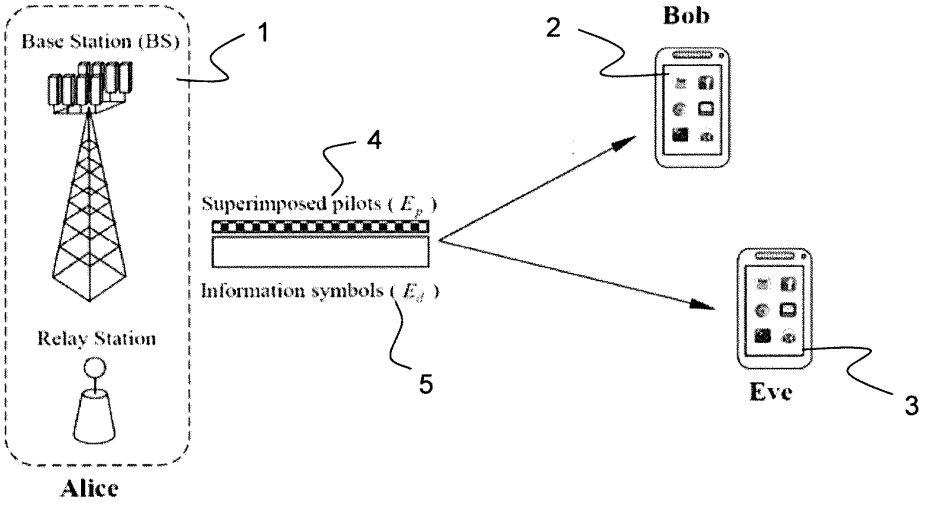
Base Station (BS)
1
Bob
2
4
Superimposed pilots (E_p)
Information symbols (E_d)
5
Relay Station
Alice
Eve
3

Fig. 1

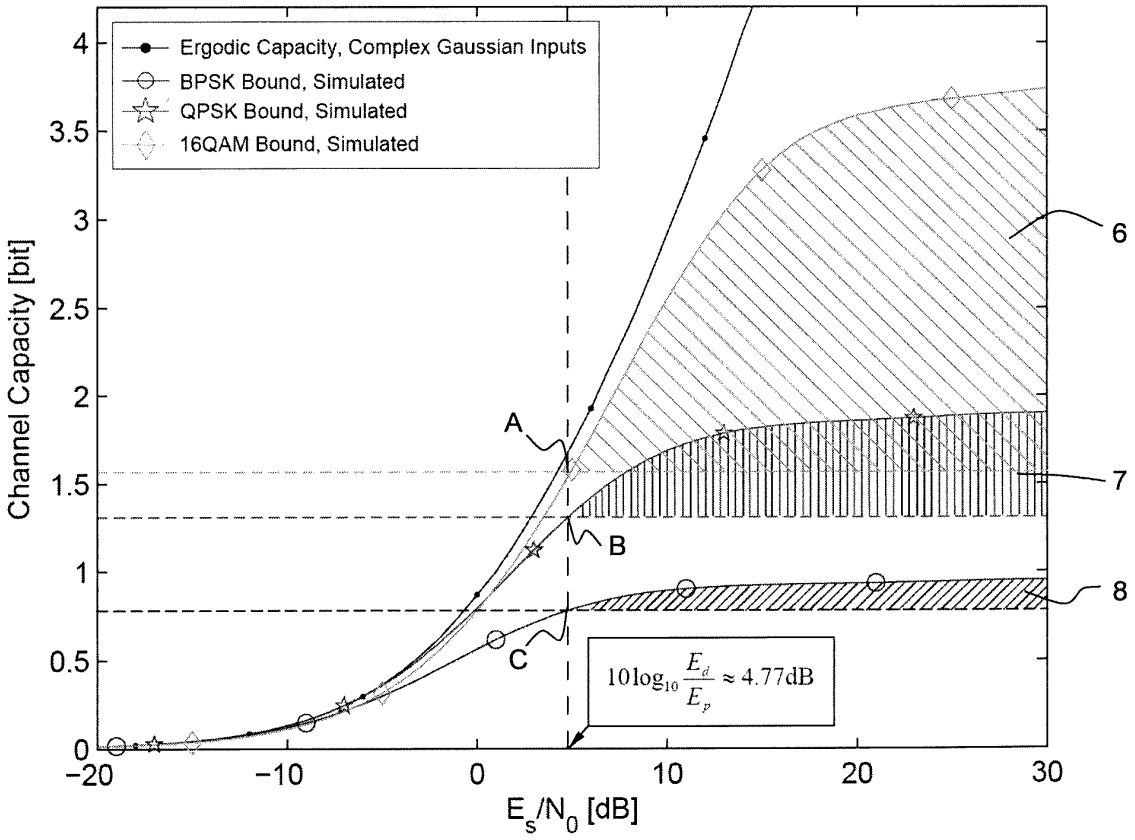
Ergodic Capacity, Complex Gaussian Inputs
BPSK Bound, Simulated
QPSK Bound, Simulated
16QAM Bound, Simulated
Channel Capacity [bit]
E_s/N_0 [dB]
A
B
C
6
7
8
$10\log_{10}\frac{E_d}{E_p} \approx 4.77\text{dB}$

Fig. 2

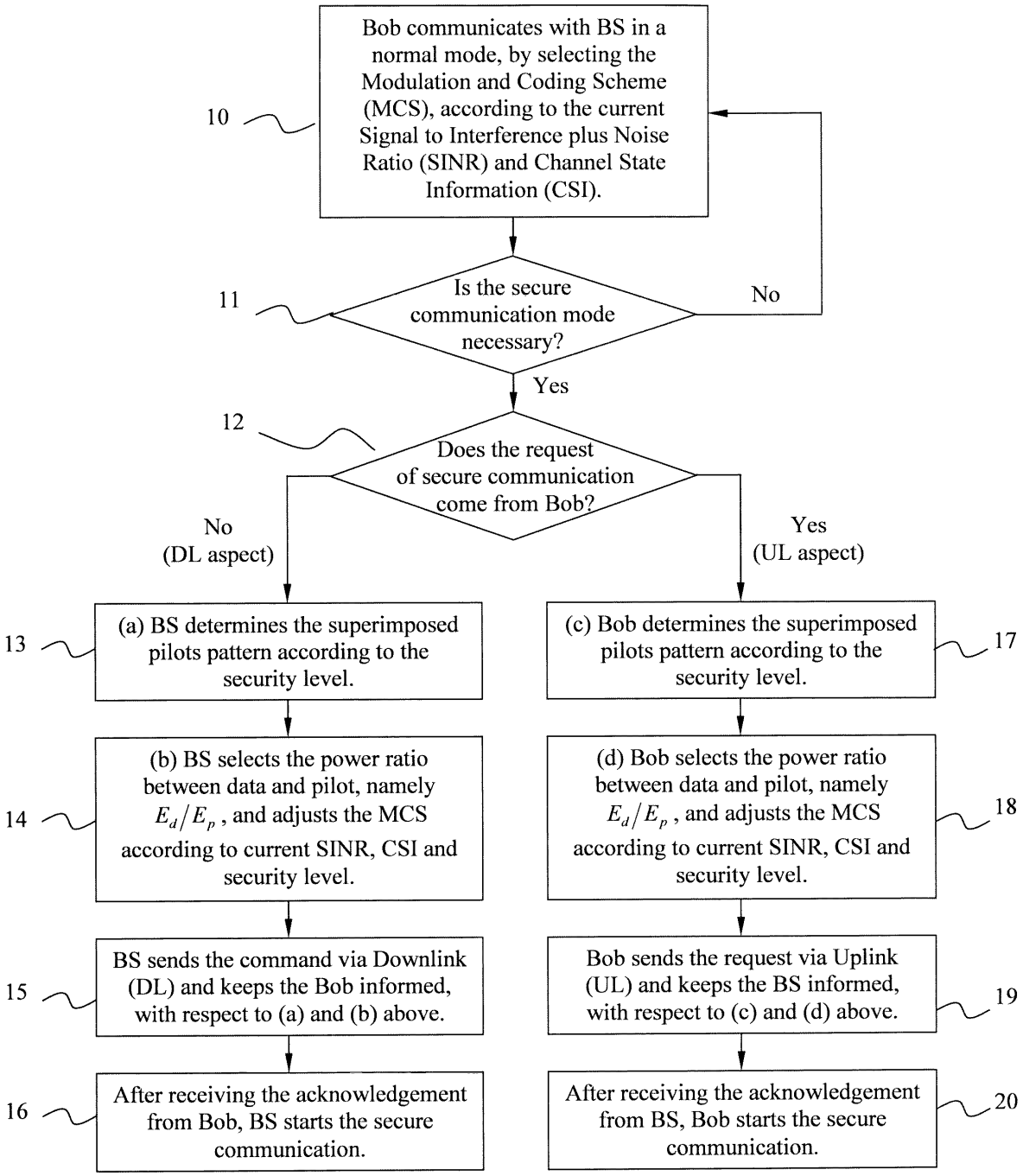
Bob communicates with BS in a normal mode, by selecting the Modulation and Coding Scheme (MCS), according to the current Signal to Interference plus Noise Ratio (SINR) and Channel State Information (CSI).
10
Is the secure communication mode necessary?
11
No
Yes
Does the request of secure communication come from Bob?
12
No (DL aspect)
Yes (UL aspect)
(a) BS determines the superimposed pilots pattern according to the security level.
13
(b) BS selects the power ratio between data and pilot, namely E_d/E_p, and adjusts the MCS according to current SINR, CSI and security level.
14
BS sends the command via Downlink (DL) and keeps the Bob informed, with respect to (a) and (b) above.
15
After receiving the acknowledgement from Bob, BS starts the secure communication.
16
(c) Bob determines the superimposed pilots pattern according to the security level.
17
(d) Bob selects the power ratio between data and pilot, namely E_d/E_p, and adjusts the MCS according to current SINR, CSI and security level.
18
Bob sends the request via Uplink (UL) and keeps the BS informed, with respect to (c) and (d) above.
19
After receiving the acknowledgement from BS, Bob starts the secure communication.
20

Fig. 3

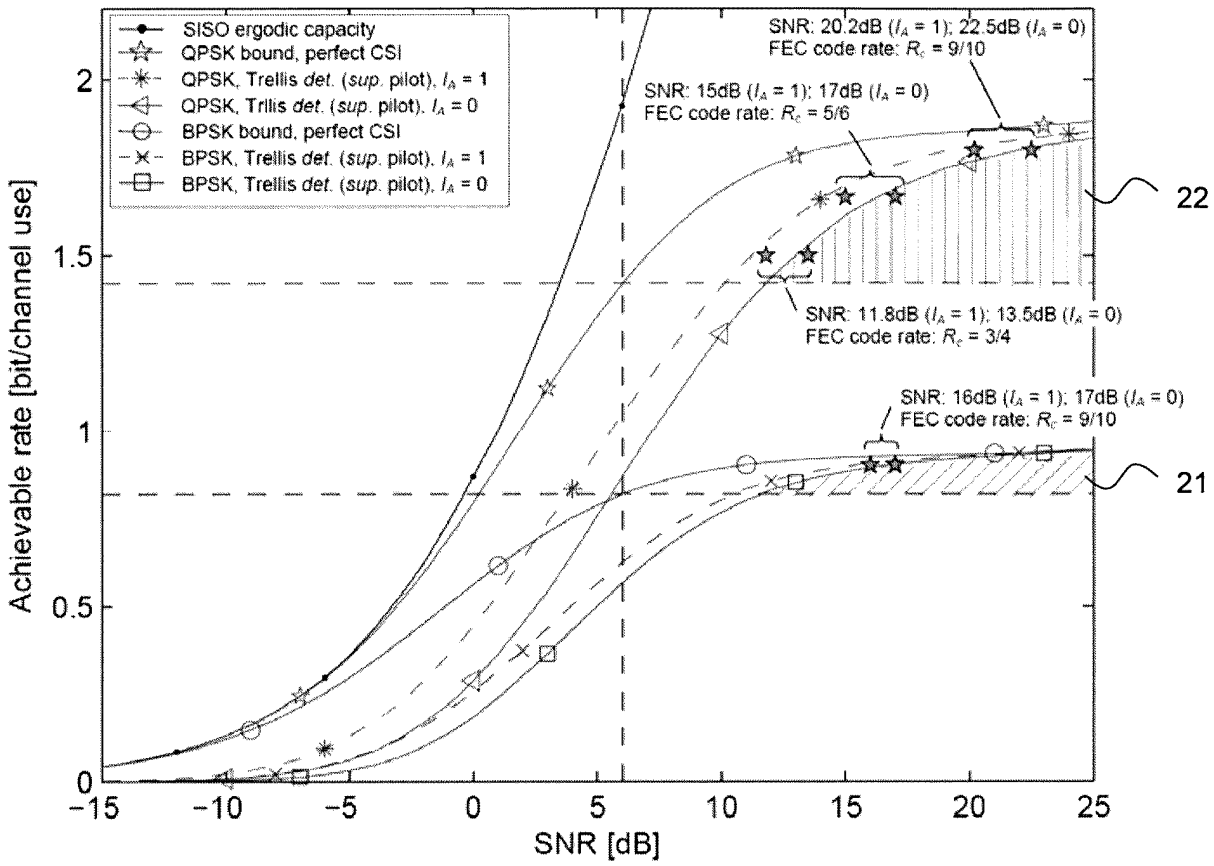
SISO ergodic capacity
QPSK bound, perfect CSI
QPSK, Trellis det. (sup. pilot), I_A = 1
QPSK, Trilis det. (sup. pilot), I_A = 0
BPSK bound, perfect CSI
BPSK, Trellis det. (sup. pilot), I_A = 1
BPSK, Trellis det. (sup. pilot), I_A = 0
SNR: 20.2dB (I_A = 1); 22.5dB (I_A = 0)
FEC code rate: R_c = 9/10
SNR: 15dB (I_A = 1); 17dB (I_A = 0)
FEC code rate: R_c = 5/6
SNR: 11.8dB (I_A = 1); 13.5dB (I_A = 0)
FEC code rate: R_c = 3/4
SNR: 16dB (I_A = 1); 17dB (I_A = 0)
FEC code rate: R_c = 9/10
22
21
Achievable rate [bit/channel use]
SNR [dB]
0
0.5
1
1.5
2
−15
−10
−5
0
5
10
15
20
25

Fig. 4

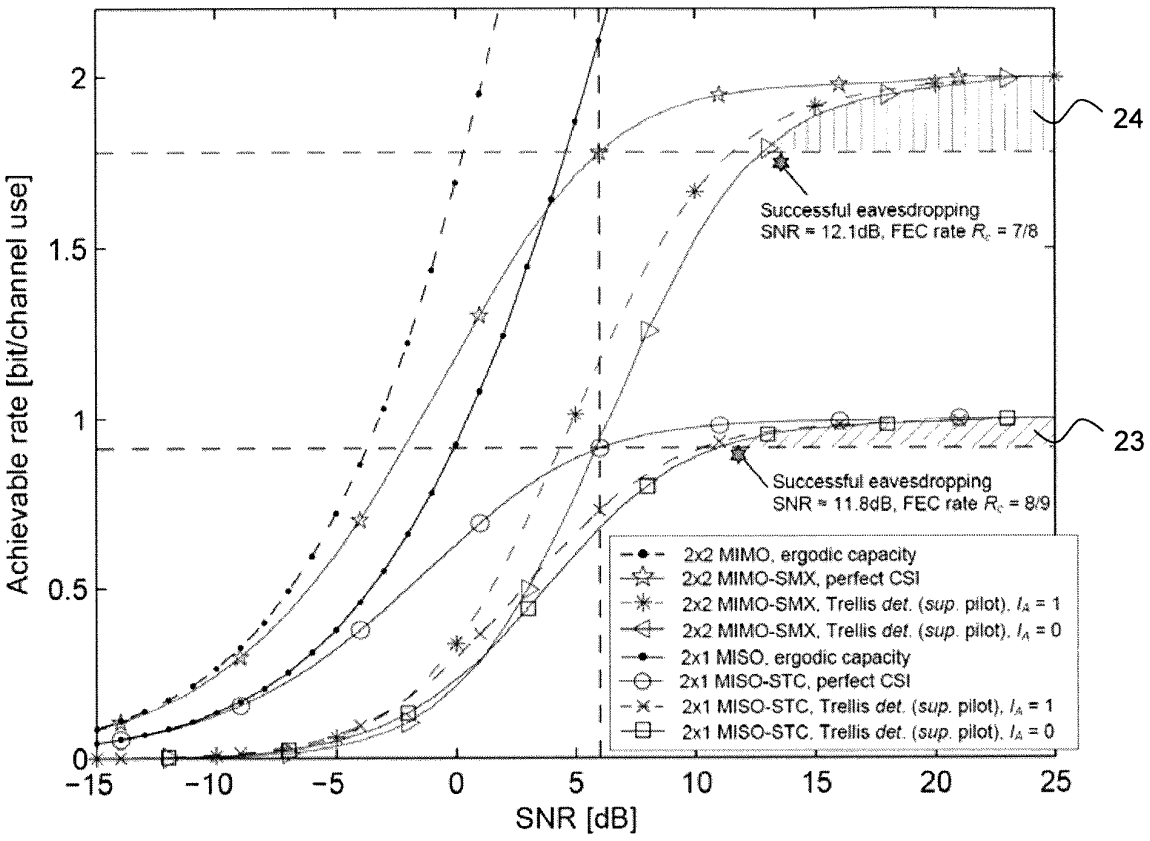
Achievable rate [bit/channel use]
SNR [dB]
2
1.5
1
0.5
0
−15
−10
−5
0
5
10
15
20
25
24
23
Successful eavesdropping
SNR = 12.1dB, FEC rate R_c = 7/8
Successful eavesdropping
SNR = 11.8dB, FEC rate R_c = 8/9
2x2 MIMO, ergodic capacity
2x2 MIMO-SMX, perfect CSI
2x2 MIMO-SMX, Trellis *det.* (*sup.* pilot), I_A = 1
2x2 MIMO-SMX, Trellis *det.* (*sup.* pilot), I_A = 0
2x1 MISO, ergodic capacity
2x1 MISO-STC, perfect CSI
2x1 MISO-STC, Trellis *det.* (*sup.* pilot), I_A = 1
2x1 MISO-STC, Trellis *det.* (*sup.* pilot), I_A = 0

Fig. 5

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 13 29 0221

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2 418 119 A (HANSEN WILLIAM W) 1 April 1947 (1947-04-01) * column 1, line 1 - line 44 * * column 2, line 1 - column 8, line 27 * * figures 1-2 * * claim 1 * -----	1-13	INV. H04K1/02
X	JP S59 70039 A (FUJITSU LTD) 20 April 1984 (1984-04-20) * abstract * -----	1-13	
X	US 2013/226586 A1 (JANG JOON YOUNG [KR] ET AL) 29 August 2013 (2013-08-29) * abstract * * paragraph [0009] - paragraph [0016] * * paragraph [0032] - paragraph [0125] * * figures 1-10 * -----	1-13	
X	US 2002/114492 A1 (RHOADS GEOFFREY B [US]) 22 August 2002 (2002-08-22) * abstract * * paragraph [0002] - paragraph [0003] * * paragraph [0025] - paragraph [0376] * * figures 1-27 * -----	1-13	TECHNICAL FIELDS SEARCHED (IPC) H04K H04L
X	US 2006/210080 A1 (TUYLS PIM T [NL] ET AL) 21 September 2006 (2006-09-21) * abstract * * paragraph [0001] - paragraph [0036] * * paragraph [0041] - paragraph [0055] * * figures 1-3 * -----	1-13	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	9 April 2014	Dujardin, Corinne

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 13 29 0221

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

09-04-2014

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2418119 A	01-04-1947	GB 586315 A	14-03-1947
		US 2418119 A	01-04-1947
JP S5970039 A	20-04-1984	NONE	
US 2013226586 A1	29-08-2013	KR 20130097445 A	03-09-2013
		US 2013226586 A1	29-08-2013
US 2002114492 A1	22-08-2002	US 6560349 B1	06-05-2003
		US 2002114492 A1	22-08-2002
		US 2003174860 A1	18-09-2003
		US 2007274386 A1	29-11-2007
		US 2007274523 A1	29-11-2007
		US 2008037824 A1	14-02-2008
		US 2008253740 A1	16-10-2008
		US 2009060265 A1	05-03-2009
		US 2010008534 A1	14-01-2010
		US 2010040255 A1	18-02-2010
		US 2011106539 A1	05-05-2011
US 2006210080 A1	21-09-2006	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- **WYNER, A.D.** The wire-tap channel. *Bell Syst. Tech. J.,* 1975, vol. 54, 1355-1387 **[0004]**
- **CSISZÁR, I. ; KÖRNER, J.** Broadcast Channel with Confidential Messages. *IEEE Trans. Inf. Theory,* May 1978, vol. 24 (3), 339-348 **[0004]**
- **FOSCHINI, G.J. ; GANS, M.J.** On limits of wireless communications in a fading environment when using multiple antennas. *Wireless Personal Commun.,* March 1998, vol. 6 (3), 311-335 **[0005]**
- **ALAMOUTI, S.M.** A simple transmit diversity technique for wireless communications. *IEEE J. Select. Areas Commun.,* October 1998, vol. 16 (8), 1451-1458 **[0005]**