Title: A HIGH SECURITY SYSTEM AND METHOD USED IN RADIO SYSTEMS

(57) Abstract: The present invention relates to a high security system (1) and method (100) which prevents unauthorized (foreign) radios (R) that are not defined in the system from being served by the main communication system (MCS) in professional radio systems and which thus secures the communication of the radios (R) that are registered in the system.

Published:

— with international search report (Art. 21(3))
— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))
DESCRIPTION

A HIGH SECURITY SYSTEM AND METHOD USED IN RADIO SYSTEMS

Field of the Invention

The present invention relates to a high security system and method which prevents unauthorized (foreign) radios that are not defined in the system from being served by the system in professional radio systems and which thus secures the communication of the radios that are registered in the system.

Background of the Invention

In the state of the art applications, registration of unauthorized radios to the system is prevented by means of authentication methods. With this method, resource allocation is not made for the requests made by a radio that is not registered in the system.

In the state of the art applications, in a conventional system, the voice packets transmitted by a valid and authenticated radio in uplink can be listened to and the related parameters (LC, ES) in this valid packet can be obtained. These parameters can be programmed to a radio that is not registered in the system. When the foreign radio is enabled to start transmitting voice in the system frequency, the foreign radio both occupies the system and can engage in unauthorized communication via the system.

The International patent application document no. WO0124560, an application in the state of the art, discloses an encryption technique applied in the communication of the mobile device with the base station. This encryption
process is performed by an encryption key and it is stated that the parameters compared in the encryption process are changed periodically.

The United States Patent document no. US201 1314287, an application known in the state of the art, discloses a method which enables authentication between devices. It is disclosed that in this method, authentication is performed by matching the information of the device defined as the subscriber with the network information.

The United States Patent document no. US20120159588, an application known in the state of the art, discloses an authentication system which can also be applied in radio systems and allows access to a plurality of services through a single device. It is also disclosed that this system is periodically updated.

The United States Patent document no. US201 1029770, an application known in the state of the art, discloses a radio communication system which enables to select the suitable process for authentication for the same user.

**Summary of the Invention**

The objective of the present invention is to provide a high security system and method which, in professional radio systems, prevents unauthorized radios that are not defined in the system from being served by the system and which thus secures the communication of the radios that are registered in the system.
Detailed Description of the Invention

A high security system and method developed to fulfill the objective of the present invention are illustrated in the accompanying figures, in which:

Figure 1 is a schematic view of the high security system.
Figure 2 is a schematic view of the high security method.

The components in the figures are given reference numbers as follows:

1. High security system
2. Main control unit
3. Main receiver unit
4. Main transmitter unit
5. Main memory unit
6. Radio control unit
7. Radio receiver unit
8. Radio transmitter unit
9. Radio memory unit

MCS. Main communication system

R. Radio

The high security system (IT) which, in professional radio systems, prevents unauthorized radios that are not defined in the system from being served by the main communication system (MCS), and which thus secures the communication of the radios (R) that are registered in the system, basically comprises
- at least main control unit (2) which is adapted to perform main controls and generate the parameters,
- at least one main receiver unit (3) which is adapted to receive the signals coming from air interface and transmit them to the main control unit (2),
- at least one main transmitter unit (4) which is adapted to send out the signals coming from the main control unit (2) to air interface,
- at least one main memory unit (5) which is adapted to store the data and is preferably located on the main control unit (2),
- at least one radio control unit (6) which is adapted to perform parameter controls and to save the parameters when necessary,
- at least one radio receiver unit (7) which is adapted to receive the signals coming from air interface and transmit them to the radio control unit (6),
- at least one radio transmitter unit (8) which is adapted to send out the signals coming from the radio control unit (6) to air interface,
- at least one radio memory unit (9) which is adapted to store the data and parameters and is preferably located on the radio control unit (6).

In one embodiment of the invention, the high security system (1) includes thereon a main control unit (2) which is adapted to perform main controls and generate the parameters, a main receiver unit (3) which is adapted to receive the signals coming from air interface and transmit them to the main control unit (2), a main transmitter unit (4) which is adapted to send out the signals coming from the main control unit (2), and a main memory unit (5) which is adapted to store the data. The high security system (1) also includes a radio control unit (6) which is adapted to perform parameter controls and to save the parameters when necessary, a radio receiver unit (7) which is adapted to receive the signals coming from air interface and transmit them to the radio control unit (6), a radio transmitter unit (8) which is adapted to send out the signals coming from the radio control unit (6), and a radio memory unit (9) which is adapted to store the data and parameters.

In a preferred embodiment of the invention, the main memory unit (5) provided on the high security system (1) of the present invention can be used externally. Furthermore, the main memory unit (5) and the main control unit (2) can be used separately (not embedded), and the connection between the main memory unit (5) and the main control unit (2) can be provided by wired/wireless means.
In a preferred embodiment of the invention, the radio memory unit (9) provided on the high security system (1) of the present invention can be used externally. Furthermore, the radio memory unit (9) and the radio control unit (6) can be used separately (not embedded) and the connection between the radio memory unit (9) and the radio control unit (6) can be provided by wired/wireless means.

In a preferred embodiment of the invention, the high security system (1) of the present invention is used in APCO P25 professional radio systems.

The high security method (100), which, in professional radio systems, prevents unauthorized radios that are not defined in the system from being served by the main communication system (MCS) and which thus secures the communication of the radios (R) that are registered in the system, basically comprises the steps of

- the main control unit (2) starting the high security system (1) (101),
- controlling the ALGID values in the uplink voice packet (102),
- controlling the Authentication Response (RES1) values in LSD (Low Speed Data) included in the uplink voice packet (103),
- controlling the Source ID in the downlink voice packet (104),
- terminating the high security system (1) (105).

The step of "controlling the ALGID values in the uplink voice packet (102)" of the high security method (100) comprises the sub-steps of

- the radio transmitter unit (8) transmitting the ALGID values in the radio memory unit (9) by means of the radio control unit (6) (201),
- the main receiver unit (3) receiving the ALGID values and sending them to the main control unit (2) (202),
- comparing the ALGID values with the values in the main memory unit (5) (203),
if there is a discrepancy between the ALGID values and the values in the main memory unit (5), the main control unit (2) stopping broadcasting the voice packets; if the values match, passing to step 103 (204).

5 The step of "controlling the Authentication Response (RES1) values in LSD (Low-Speed Data) included in the uplink voice packet (103)" of the high security method (100) comprises the sub-steps of
- transmitting the RES1 (response) value, which is recorded in the radio memory unit (9) and is used by the radio (R) for authentication, to the radio control unit (6) (301),
- entering the RES1 value coming from the radio control unit (6) into the LSD (Low Speed Data) field in the uplink voice packet, and the radio transmitter unit (8) sending the voice packet (302),
- the main receiver unit (3) receiving the voice packet and sending it to the main control unit (2) (303),
- comparing the RES1 value in the LSD field within the uplink voice packet with the values in the main memory unit (5) (304),
- if there is a discrepancy between the RES1 value and the values in the main memory unit (5), the main control unit (2) stopping broadcasting the voice packets, renewing registration and authentication of the concerned radio (R) by sending registration command (U_REG_CMD) to the radio and updating RES1 value; if the values match, passing to step 104 (305).

The step of "controlling the Source ID in the downlink voice packet (104)" of the high security method (100) comprises the sub-steps of
- the radio receiver unit (7) receiving the downlink voice packet and transmitting it to the radio control unit (6) (401),
- the radio control unit (6) carrying out the control of the Source ID in the downlink voice packet (402),
- if, as a result of the control, the radio (R) sees its own ID as the Source ID, upon figuring out that a foreign radio has copied its parameters and is
sending voice packets with these parameters, the radio (R) renewing registration and authentication and updating RES1 value; if the radio (R) does not see its ID as the Source ID, going to step 105 (403).
CLAIMS

1. A high security system (1), which, in professional radio systems, prevents unauthorized radios that are not defined in the system from being served by the main communication system (MCS), and which thus securing the communication of the radios (R) that are registered in the system, basically characterized by:
   - at least main control unit (2) which is adapted to perform main controls and generate the parameters,
   - at least one main receiver unit (3) which is adapted to receive the signals coming from air interface and transmit them to the main control unit (2),
   - at least one main transmitter unit (4) which is adapted to send out the signals coming from the main control unit (2) to air interface,
   - at least one main memory unit (5) which is adapted to store the data and is preferably located on the main control unit (2),
   - at least one radio control unit (6) which is adapted to perform parameter controls and to save the parameters when necessary,
   - at least one radio receiver unit (7) which is adapted to receive the signals coming from air interface and transmit them to the radio control unit (6),
   - at least one radio transmitter unit (8) which is adapted to send out the signals coming from the radio control unit (6) to air interface,
   - at least one radio memory unit (9) which is adapted to store the data and parameters and is preferably located on the radio control unit (6).

2. A high security system (1) according to Claim 1, characterized by the main memory unit (5) which can be used externally.

3. A high security system (1) according to Claim 1, characterized by the main memory unit (5) which can be used separately from (not embedded in) the main control unit (2).
4. A high security system (1) according to Claim 1, characterized by the main memory unit (5) whose connection with the main control unit (2) can be provided by wire.

5. A high security system (1) according to Claim 1, characterized by the main memory unit (5) whose connection with the main control unit (2) can be provided by wireless means.

6. A high security system (1) according to Claim 1, characterized by the radio memory unit (9) which can be used externally.

7. A high security system (1) according to Claim 1, characterized by the radio memory unit (9) which can be used separately from (not embedded in) the radio control unit (6).

8. A high security system (1) according to Claim 1, characterized by the radio memory unit (9) whose connection with the radio control unit (6) can be provided by wire.

9. A high security system (1) according to Claim 1, characterized by the radio memory unit (9) whose connection with the radio control unit (6) can be provided by wireless means.

10. A high security method (100), which, in professional radio systems, prevents unauthorized radios that are not defined in the system from being served by the main communication system (MCS), and which thus secures the communication of the radios (R) that are registered in the system, basically characterized by the steps of
   - the main control unit (2) starting the high security system (1) (101),
   - controlling the ALGID values in the uplink voice packet (102),
controlling the Authentication Response (RESl) values in LSD (Low Speed Data) included in the uplink voice packet (103),
- controlling the Source ID in the downlink voice packet (104),
- terminating the high security system (1) (105).

11. A high security method (100) according to Claim 10, characterized in that the step of "controlling the ALGID values in the uplink voice packet (102)" comprises the sub-steps of
- the radio transmitter unit (8) transmitting the ALGID values in the radio memory unit (9) by means of the radio control unit (6) (201),
- the main receiver unit (3) receiving the ALGID values and sending them to the main control unit (2) (202),
- comparing the ALGID values with the values in the main memory unit (5) (203),
- if there is a discrepancy between the ALGID values and the values in the main memory unit (5), the main control unit (2) stopping broadcasting the voice packets; if the values match, passing to step 103 (204).

12. A high security method (100) according to Claim 10, characterized in that the step of "controlling the Authentication Response (RES1) values in LSD (Low Speed Data) included in the uplink voice packet (103)" comprises the sub-steps of
- transmitting the RES 1 (response) value, which is recorded in the radio memory unit (9) and is used by the radio (R) for authentication, to the radio control unit (6) (301),
- entering the RESl value coming from the radio control unit (6) into the LSD (Low Speed Data) field in the uplink voice packet, and the radio transmitter unit (8) sending the voice packet (302),
- the main receiver unit (3) receiving the voice packet and sending it to the main control unit (2) (303),
comparing the RES1 value in the LSD field within the uplink voice packet with the values in the main memory unit (5) (304),

- if there is a discrepancy between the RES1 value and the values in the main memory unit (5), the main control unit (2) stopping broadcasting the voice packets, renewing registration and authentication of the concerned radio (R) by sending registration command (UJREG_CMD) to the radio and updating RES1 value; if the values match, passing to step 104 (305).

13. A high security method (100) according to Claim 10, characterized in that the step of "controlling the Source ID in the downlink voice packet (104)" comprises the sub-steps of

- the radio receiver unit (7) receiving the downlink voice packet and transmitting it to the radio control unit (6) (401),

- the radio control unit (6) carrying out the control of the Source ID in the downlink voice packet (402),

- if, as a result of the control, the radio (R) sees its own ID as the Source ID, upon figuring out that a foreign radio has copied its parameters and is sending voice packets with these parameters, the radio (R) renewing registration and authentication and updating RES1 value; if the radio (R) does not see its ID as the Source ID, going to step 105 (403).
A. CLASSIFICATION OF SUBJECT MATTER
H04L29/06  H04W12/06  H04W12/10
H04W84/08

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W  H04L

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

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

EPO-Internal  , WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>&quot;Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security&quot;, EUROPEAN STANDARD, EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI), 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS ; FRANCE, vol. TETRA 6, no. V3.3.1, July 2012 (2012-07), XP014070176, sections 4.1.1, 4.1.2, 4.2.1, 4.5.1, 4.5.1.1, 4.2.1, 4.5.1.3, 5.4.2.2, 5.4.6, 6.5, 6.6.2.1.2, 6.6.2.3 figures 4.20, 4.29, 4.30, 5.1</td>
<td>1-13</td>
</tr>
</tbody>
</table>

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

*"I" 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

*"Z" document member of the same patent family

Date of the actual completion of the international search: 2 July 2015

Date of mailing of the international search report: 09/07/2015

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

Authorized officer: Kufer, Lena
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>figure 7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraphs [0003] - [0007], [0028]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraphs [0029], [0033] - [0038]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraphs [0059], [0060], [0065]</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>figure 1</td>
<td>5,6,9-13</td>
</tr>
<tr>
<td></td>
<td>paragraphs [0002], [0005], [0019]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraphs [0026], [0027], [0031], [0033]</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>figure 1</td>
<td>2,3,5,6,</td>
</tr>
<tr>
<td></td>
<td>pages 1-4</td>
<td>9-13</td>
</tr>
<tr>
<td></td>
<td>paragraphs [0017] - [0019], [0022]</td>
<td></td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>US 2013243195 Al</td>
<td>19-09-2013</td>
<td>US 2013243195 Al</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2014198916 Al</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wo 2013142007 Al</td>
</tr>
<tr>
<td>US 2013227294 Al</td>
<td>29-08-2013</td>
<td>AU 2013226552 Al</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2865314 Al</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 112013001180 T5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB 2513764 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2013227294 Al</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wo 2013130218 Al</td>
</tr>
<tr>
<td>US 2013072155 Al</td>
<td>21-03-2013</td>
<td>NONE</td>
</tr>
</tbody>
</table>