PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : H04Q 7/02, H04M 1/66

A1

(11) International Publication Number: WO 91/14348

(43) International Publication Date: 19 September 1991 (19.09.91)

(21) International Application Number: PCT/SE91/00066

(22) International Filing Date: 29 January 1991 (29.01.91)

(30) Priority data:
9000856-6 9 March 1990 (09.03.90) SE

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON [SE/SE]; S-126 25 Stockholm (SE).

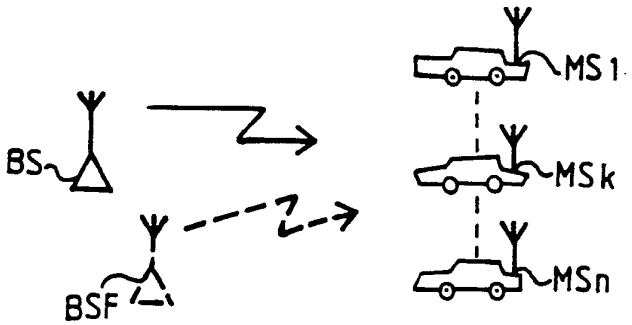
(72) Inventors: WILKINSON, Dent, Paul ; Stehags Prästgård, S-240 36 Stehag (SE). RAITH, Alex, Krister ; Sorögatan 19, S-164 41 Kista (SE). DAHLIN, Jan, Erik, Åke, Steinar ; Såningsvägen 152, S-175 45 Järfälla (SE).

(74) Agents: LÖVGREN, Tage et al.; Telefonaktiebolaget LM Ericsson, S-126 25 Stockholm (SE).

(81) Designated States: AU, BR, CA, FI, JP, KR, NO.

Published
With international search report.

(54) Title: A METHOD OF CARRYING OUT AN AUTHENTICATION CHECK BETWEEN A BASE STATION AND A MOBILE STATION IN A MOBILE RADIO SYSTEM



(57) Abstract

A method for carrying out an authentication check in a mobile telephone system in which an authentic base station (BS) serves a plurality of mobile stations (MS1-MSn). It is earlier known to carry out a unidirectional check from the base station (BS) to a calling mobile station (MSk). A false base station (BSf) is able, in this way, to carry out a false authentication check, by collecting a number of so-called RAND-Response pairs. In order to avoid this, there is introduced a further unidirectional authentication check, base station-mobile station, and also an authentication check from the mobile station to the base station. According to one embodiment of the method, the unidirectional check is excluded and only the bidirectional authentication check is carried out.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**ES**	Spain	**MG**	Madagascar
AU	Australia	**FI**	Finland	**ML**	Mali
BB	Barbados	**FR**	France	**MN**	Mongolia
BE	Belgium	**GA**	Gabon	**MR**	Mauritania
BF	Burkina Faso	**GB**	United Kingdom	**MW**	Malawi
BG	Bulgaria	**GN**	Guinea	**NL**	Netherlands
BJ	Benin	**GR**	Greece	**NO**	Norway
BR	Brazil	**HU**	Hungary	**PL**	Poland
CA	Canada	**IT**	Italy	**RO**	Romania
CF	Central African Republic	**JP**	Japan	**SD**	Sudan
CG	Congo	**KP**	Democratic People's Republic of Korea	**SE**	Sweden
CH	Switzerland			**SN**	Senegal
CI	Côte d'Ivoire	**KR**	Republic of Korea	**SU**	Soviet Union
CM	Cameroon	**LI**	Liechtenstein	**TD**	Chad
CS	Czechoslovakia	**LK**	Sri Lanka	**TG**	Togo
DE	Germany	**LU**	Luxembourg	**US**	United States of America
DK	Denmark	**MC**	Monaco		

A METHOD OF CARRYING OUT AN AUTHENTICATION CHECK BETWEEN A BASE STATION AND A MOBILE STATION IN A MOBILE RADIO SYSTEM

TECHNICAL FIELD

The present invention relates to a method of carrying out an authentication check between a base station and a mobile station in a mobile radio system, particularly in a cellular mobile telephone system. The proposed method can also be applied with other mobile radio systems, for instance paging systems.

BACKGROUND ART

In the case of a cellular mobile telephone system for instance, an authentication check is carried out before a call is set up between the mobile and the base station. The base station asks for information concerning the mobile, with respect to its identity, by ordering the mobile to send an identification number. The mobile is therewith forced to reveal its identity to the base station, so that the base station will know that the mobile is authorized to send a call over the system and so that the base station and also the exchange will know which mobile shall be charged for the call subsequently set up.

On the other hand, the mobile station must be certain that it communicates with the authentic base station, i.e. with a base station which is truly authorized to put connect a call when the mobile is the calling party (the mobile is an A-subscriber), and that the mobile station will be charged correctly for the call.

For the purpose of performing an authentication check, it is earlier known to form authentication signals, "Resp"-signals, in the base station and the mobile station. A random number (RAND) is sent from the base to mobiles within the area covered by the base station. The calling mobile answers with a given signal (Resp 1). In a similar manner, the base station forms the same signal Resp 1 from the random number and the identity of the calling mobile.

These signals normally coincide and the base station orders the mobile to a speech channel.

DISCLOSURE OF THE INVENTION

Thus, in the aforesaid known method of carrying out authentication checks, there is formed a RAND-Response pair for a given mobile station, i.e. a given Response signal is formed in the mobile for a given received random number RAND, and a base station can thus receive a number of such response signals for a number of different random numbers. This means that it is possible to establish a "false" base station which is able to transmit a number of mutually different random numbers and receives a corresponding (different) number of Response signals. The false base station is therewith able to create a mobile subscription which is not authorized to send calls over the system. This drawback or deficiency of the known authentication check is due to the fact that the check is uni-directional, namely it is only the base station which requires the response signal in proof of the authentication of the mobile.

According to the present method, the authentication check is bi-directional, i.e. it is not only the base station which requires the identity of the mobile, but that the mobile also requires the identity of the base station.

The object of the present invention is thus to provide an improved authentication check method which renders impossible manipulation by a false base station with the intention of obtaining access to the authentication code of the mobile telephone system.

The inventive method is characterized by the steps set forth in the characterizing clause of Claim 1. Further developments of the proposed method are set forth in depending Claims 2-3.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will now be described in more detail with reference to the accompanying drawings, in which

Figure 1 illustrates schematically communication between two base stations and a plurality of mobile stations;

Figure 2 is a flow sheet which illustrates one embodiment of the proposed method;

Figure 3 is a block schematic of the input and output magnitudes of an authenticity algorithm incorporated in a mobile station; and

Figure 4 is a flow sheet which illustrates another embodiment of the proposed method.

BEST MODE OF CARRYING OUT THE INVENTION

Figure 1 illustrates an authentic base station BS which listens by transmitting random numbers to a plurality of mobiles MS1-MSn over a given control channel. Of these mobiles, a response is received from a mobile MSk which indicates that it wishes to establish a call over a given speech channel. As described above, a uni-directional authentication check is carried out, where the base station requires a response Resp 1 from the mobile MSk. This will be described below in more detail with reference to Figure 2. Since the connection is unidirectional during this stage, a false base station BSF is able to obtain a response from a number of mobiles when transmitting the aforesaid random number RAND, in the aforesaid manner. The base station BSF is therewith able to create a bank of RAND-Response replies, which can then be utilized in an unauthorized manner by a mobile station.

In order to make this impossible, there is proposed in accordance with the invention an authentication method disclosed in the flow chart of Figure 2.

An authentic base station BS listens to a number of mobiles MS1-MSn within the area covered by said base station, by transmitting a random number RAND, block 1.

A given mobile station MSk wishing to establish a call, answers with a signal Resp 1, block 2. This signal is formed in the microprocessor of the mobile from a number of input data PIN, ESN and DN, in addition to the random number RAND received, see Figure 3, where PIN represents the personal identification number of the mobile, ESN represents the electronic serial number of the mobile, and DN represents the number dialled. The mobile station MSk is therewith an A-subscriber. The microprocessor 13 then delivers the Resp 1 signal, which consists of an 18-bit AUTH-signal and an 8-bit RANDC-signal, which is sent to the base station.

The base station calculates Resp 1 in a corresponding manner, block 3, from the incoming signals AUTH and RANDC and makes a comparison with the value of the Resp-signal calculated and transmitted by the mobile, block 4. When these coincide, the base station orders the mobile to a given, allocated speech channel, block 5, and the connection is established in a known manner, block 6. The aforedescribed method is previously known.

According to the proposed method, the base station now forms a response signal Resp 2 from a further random number RAND 2 and from the personal identification number PIN of the mobile, this number being known in the base station (blocks 2, 3). Both Resp 2 and RAND 2 are sent to the mobile, block 7. The mobile station forms a value of Resp 2 from its PIN and the received random number RAND 2, block 8. A comparison is now made in the mobile, block 9, between the received Resp 2 and the formed value of Resp 2. If these two values coincide, the mobile forms a value Resp 3 and sends this value to the base station, block 10. Resp 3 is formed from RAND 2 and PIN in the mobile. The base station forms Resp 3 in a similar manner from RAND 2 and PIN, which are known in the base station, block 11. A comparison is then made, block 12, between the received and formed values of Resp 3. If the values coincide, connection of the call continues to establish a speech connection.

The method steps according to block 7, 8 and 9 provide an authentication check in which the mobile decides whether or not the base station is authentic, since verification of the signal Resp 2 sent

from the base station takes place in the mobile, and against a value Resp 2 calculated in said mobile. The signal Resp 2 from the base station can therefore be taken as a response signal from said station. The aforedescribed method constitutes the main difference between the proposed method and the known method according to blocks 2, 3 and 4.

The check carried out in accordance with blocks 10, 11 and 12 constitutes substantially a repetition of the method according to blocks 2, 3 and 4, i.e. a check from the base station that the mobile is authentic.

An essential difference in relation to the known authenticity method (blocks 1-4) is that the mobile also requires a response Resp 2 from the base station and verifies this response in accordance with blocks 7-9. A false base station must therefore know exactly how this response signal shall be calculated. The check is therewith bidirectional.

The authentication check according to blocks 2, 3 and 4 can be carried out on a general control channel in the mobile radio system, and the authentication check according to blocks 7-12 can be carried out on the speech channel established between the base station BS and the mobile MSk (blocks 5 and 6).

Figure 4 is a block diagram illustrating the first method steps in the case when solely a bidirectional authentication check is carried out. In this case, the steps according to blocks 1-3 replace the steps according to blocks 1-6 in Figure 2. In this case, no unidirectional (and known) authentication check is carried out prior to the bidirectional check. A calling mobile, for instance MSk, asks for a connection from the base station BS. When receiving this call request, the base station BS looks for a free speech channel and orders the mobile MSk to this free channel. In this way, a free connection is established over the speech channel without carrying out an authentication check. The actual authentication check is then carried out in the manner

aforedescribed with reference to blocks 7-12 of Figure 2, i.e. only a bidirectional authentication check is carried out.

C L A I M S

1. A method for carrying out an authentication check between a base station (BS) and a mobile station (MSk) in a mobile radio system, in which prior to establishing a connection, the base station sends a question concerning the authentication of the mobile and orders the mobile to send a first response signal (Resp 1) which is used in the base station to establish the authentication of the mobile, c h a r a c t e r i z e d in that subsequent to establishing the authentication of the mobile (2, 3, 4) in the base station, there is sent from the base station a second response signal (Resp 2) to the mobile, which therewith forms (8) a corresponding second response signal (Resp 2) in order to establish (9) the authentication of the base station and, when this authentication is established, the mobile sends a third response signal (Resp 3) and establishes the authentication of the mobile prior to the connection being established.

2. A method according to Claim 1, c h a r a c t e r i z e d in that said second response signal (Resp 2) is formed from a random number (RAND 2) produced in the base station and from the identification number (PIN) of the mobile, and in that the authentication of the base station is established by comparing (9) said second response signal with a signal produced in the mobile in dependence on the received random number (RAND 2) and the identification number (PIN) available in the mobile.

3. A method according to Claim 2, c h a r a c t e r i z e d in that said third response signal (Resp 3) sent to the base station is formed from said random number (RAND 2) and from the identification number (PIN) of said mobile, in that said signal is sent to the base station; and in that said base station forms a corresponding signal in a similar manner from said random number (RAND 2) and the identification number (PIN) of the mobile available in said base station; and in that a comparison (12) is made in the base station between the formed signal and the sent signal such that when agreement is found between said signals, a speech connection can be established.

4. A method of carrying out an authentication check between a base station (BS) and a mobile station (MSk) in a mobile radio system subsequent to the mobile station having asked for and being assigned a connection over a given channel, c h a r a c t e r i - z e d by forming in the base station (BS) a first response signal (Resp 2), sending said first response signal to the mobile (MSk) which therewith forms a corresponding response signal (Resp 2) for the purpose of verifying the authentication of the base station and, subsequent to establishing such authentication, the mobile sends a second response signal (Resp 3) to the base station, which forms a corresponding response signal and establishes the authentication of the mobile prior to establishing a connection.

5. A method according to Claim 4, c h a r a c t e r i z e d in that said first response signal (Resp 2) is formed from a random number (RAND 2) produced in the base station and from the identification number (PIN) of the mobile, and in that the authentication of the base station is established by comparing (9) said first response signal with a signal produced in the mobile and contingent on the received random number (RAND 2) and the identification number (PIN) accessible in the mobile.

6. A method according to Claim 4, c h a r a c t e r i z e d in that said second response signal (Resp 3) sent to the base station is formed from said random number (RAND 2) and from the identification number (PIN) of the mobile, said signal being sent to the base station, and in that the base station forms a corresponding signal in a similar manner from said random number (RAND 2) and from the identification number (PIN) of the mobile available in the base station; and in that a comparison (12) is carried out in the base station between the signal formed by said base station and the signal received by said station and a speech connection is established when these signals coincide.

1/2

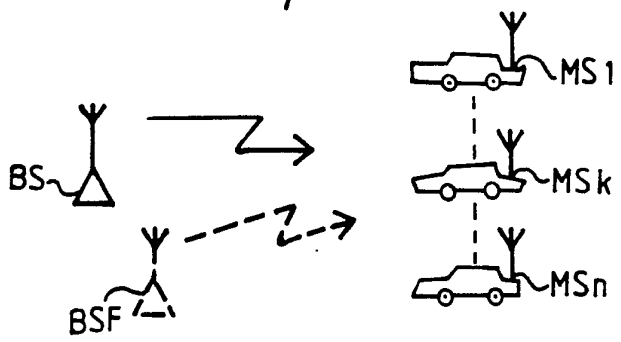


Fig.1

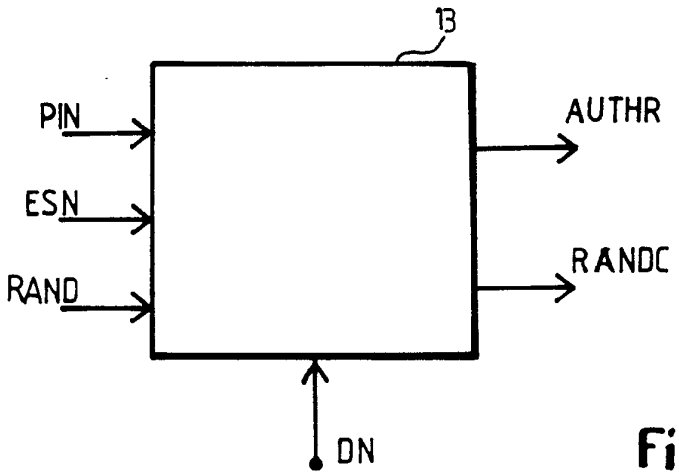


Fig 3

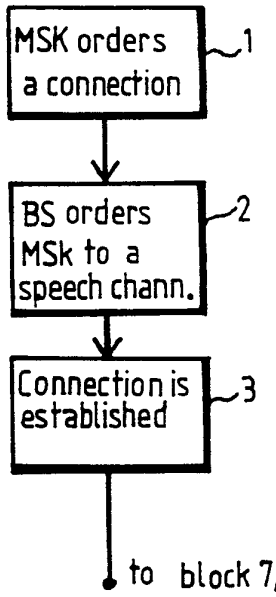


Fig.4

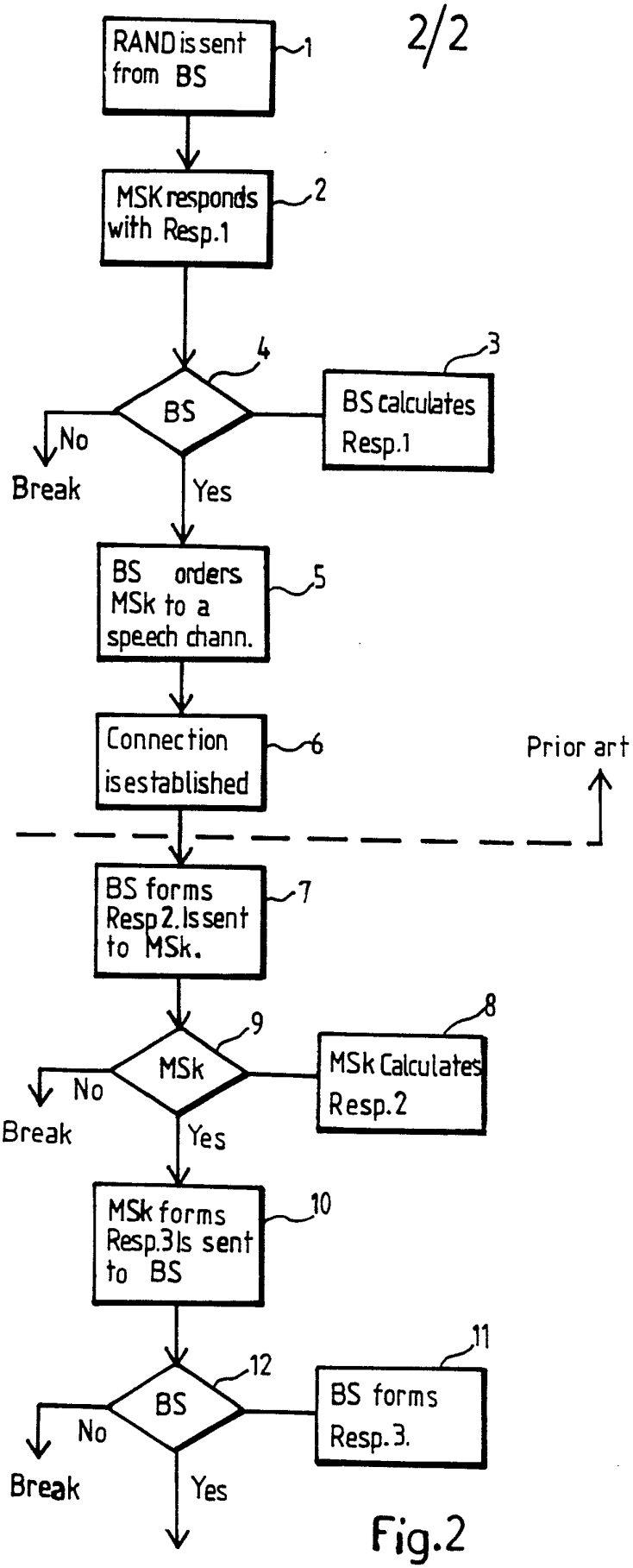

RAND is sent from BS
1
MSK responds with Resp.1
2
BS
4
BS calculates Resp.1
3
No
Break
Yes
BS orders MSk to a speech chann.
5
Connection is established
6
Prior art
BS forms Resp 2. Is sent to MSk.
7
MSk
9
MSk Calculates Resp.2
8
No
Break
Yes
MSk forms Resp.3 Is sent to BS
10
BS
12
BS forms Resp.3.
11
No
Break
Yes

Fig.2

INTERNATIONAL SEARCH REPORT

International Application No PCT/SE 91/00066

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all)[6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC5: H 04 Q 7/02, H 04 M 1/66

II. FIELDS SEARCHED

Minimum Documentation Searched[7]

Classification System	Classification Symbols
IPC5	H 04 Q 7/02, /04, H 04 M 1/66

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in Fields Searched[8]

SE,DK,FI,NO classes as above

III. DOCUMENTS CONSIDERED TO BE RELEVANT[9]

Category *	Citation of Document,[11] with indication, where appropriate, of the relevant passages[12]	Relevant to Claim No.[13]
A	DE, A1, 3405381 (PHILIPS KOMMUNIKATIONS INDUSTRIE AG) 22 August 1985, see page 6, line 23 - page 7, line 32 --	1-6
A	DE, A1, 3420460 (PHILIPS PATENTVERWALTUNG GMBH) 5 December 1985, see the whole document --	1-6
A	US, A, 4436957 (F. MAZZA ET AL) 13 March 1984, see the whole document --	1-6

---

* Special categories of cited documents: [10]

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

"E" earlier document 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

"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

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
27th May 1991	1991 -06- 05
International Searching Authority	**Signature of Authorized Officer**
SWEDISH PATENT OFFICE	Lars Henriksson LARS HENRIKSSON

Form PCT/ISA/210 (second sheet) (January 1985)

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO.PCT/SE 91/00066

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report.
The members are as contained in the Swedish Patent Office EDP file on 91-04-30
The Swedish Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
DE-A1- 3405381	85-08-22	EP-A-	0152150	85-08-21
DE-A1- 3420460	85-12-05	CA-A-	1236532	88-05-10
		EP-A-	0163358	85-12-04
		JP-A-	61029294	86-02-10
US-A- 4436957	84-03-13	AU-D-	9157382	83-06-30
		JP-A-	58151137	83-09-08