AUSTRALIA
Patents Act 1990

PATENT REQUEST: STANDARD PATENT/PATENT OF ADDITION

We, being the person identified below as the Applicant, request the grant of a patent to the person identified below as the Nominated Person, for an invention described in the accompanying standard complete specification.

Full application details follow.

[71] Applicant: TELEFONAKTIEBOLAGET L M ERICSSON
Address: S-126 25 STOCKHOLM, SWEDEN

[70] Nominated Person: TELEFONAKTIEBOLAGET L M ERICSSON
Address: S-126 25 STOCKHOLM, SWEDEN

[54] Invention Title: A METHOD OF TRANSMITTING SYNCHRONIZING INFORMATION IN THE CIPHERED TRANSMISSION OF DATA IN A MOBILE RADIO SYSTEM

[72] Name(s) of actual inventor(s): PAUL WILKINSON DENT

[74] Address for service in Australia: c/o WATERMARK PATENT & TRADEMARK ATTORNEYS, of The Atrium, 290 Burwood Road, Hawthorn, Victoria 3122, Australia
Attorney Code: WM

DIVISIONAL APPLICATION DETAILS

[62] Original application number: 74947/91

Drawing number recommended to accompany the abstract

By our Patent Attorneys,
WATERMARK PATENT & TRADEMARK ATTORNEYS

DATED this 14th day of January 1993.

for L. J. Dyson

F040480 15/01/93
1. A method of transmitting synchronizing information in the ciphered transmission of signals between a base station and a mobile station in a mobile radio system which operates in accordance with the TDMA-principle with transmission in frames and time slots, wherein control information is transmitted over a ciphered associated control channel (FACCH) and a non-ciphered associated control channel (SACCH), and wherein the base station and the mobile station each include a frame counter which counts transmitted and received frames (R1-R11, ...) and which controls the formulation of a cipher sequence which is superimposed in the base station on the non-ciphered signals transmitted to the mobile station, characterized by transmitting over the non-ciphered associated control channel (SACCH) from the base station during a given number of frames (R1-R11) an information word (W3) which denotes the sequence number (35, 46, ...) for that frame for which the frame counter of the mobile shall be set at the time (t1) at which said information word (W3) was received and which is related to the sequence number for the base-station frame counter at the time (t0) at which the information word (W3) was transmitted.
Application Number: 
Lodged:

Invention Title: A METHOD OF TRANSMITTING SYNCHRONIZING INFORMATION IN THE CIPHERED TRANSMISSION OF DATA IN A MOBILE RADIO SYSTEM

The following statement is a full description of this invention, including the best method of performing it known to -US
A METHOD OF TRANSMITTING SYNCHRONIZING INFORMATION IN THE CIPHERED TRANSMISSION OF DATA IN A MOBILE RADIO SYSTEM

TECHNICAL FIELD

The present invention relates to a method of transmitting synchronizing information in the ciphered transmission of speech/data in a mobile radio system. More specifically, the invention relates to the transmission of synchronizing information between a transmitting station (base station) and a receiving station (mobile) on those occasions when even the synchronization necessary for the ciphering is ciphered and has been lost.

BACKGROUND ART

In a mobile radio system which lacks a global time reference, i.e. a time reference which is common to all mobiles and base stations in the system, it is not possible to synchronize the mobiles and base stations to a common clock when the synchronization of a transmitting base station/mobile (or vice versa) is lost or drops-off for some reason or other, for instance during hand-over. When the conversation taking place between the two stations is also ciphered, further problems can occur due to a drop-off in the synchronism for the actual ciphering code, thereby making deciphering impossible.

A solution to this problem has been proposed in Swedish Patent Application No. 8902994-6, which describes a mobile radio system in which both speech/data and signalling information are ciphered. When both the crypted speech/data information and the signalling information drop-off, a ciphered (or non-ciphered) signal information is sent to the mobile, which discloses the number of frame intervals after which ciphering shall be re-commenced subsequent to said drop-off, for instance during hand-over. This earlier proposed method, however, uses solely the associated control channel (FACCH) which transmits ciphered signalling for the synchronization. If the ciphered signalling transmitted in accordance with this method should fail, there is no other pos-
sibility of resynchronizing the ciphering of speech/data and signalling information.

DISCLOSURE OF THE INVENTION

Thus, the drawback with the earlier proposed method of maintaining synchronization for ciphering purposes is that there is only one possibility of reestablishing synchronization, namely over the associated control channel FACCH, which normally transmits the synchronizing information contained by the random bit flow superimposed on the speech/data flow and the signalling flow. There is, however, a further associated control channel, the so-called slow associated control channel SACCH which could be used for transmitting synchronizing information. The present method can be applied to a mobile radio system which, in addition to the aforesaid fast associated control channel FACCH, also includes a slow associated control channel SACCH.

According to the present invention, information concerning frame synchronization is transmitted continuously between the two stations, in the form of a sequence or order number for the frames of the master station, i.e. even when the ciphered transmission between a master station (base station) and a slave station (mobile station) functions normally. This information is transmitted continuously over the slow associated control channel SACCH. If synchronization over the fast associated control channel FACCH drops-off, for instance during hand-over, there is provided a further possibility of synchronizing the frame generator of the slave station to the frame generator of the master station, and therewith ciphering between the stations.

The object of the present invention is therefore to provide a reserve possibility for synchronizing ciphered transmission of speech/data signals between a stationary and a mobile station in a mobile radio system which includes a fast and a slow associated control channel.
The method according to the invention is characterized by the features set forth in the characterizing clause of the following Claim 1.

BRIEF DESCRIPTION OF THE DRAWINGS

The proposed method will now be described in more detail with reference to the accompanying drawings, in which Figure 1 is a block diagram illustrating that part of a base station in which the proposed method is applied; and Figure 2 is a time diagram which illustrates the proposed method.

BEST MODES OF CARRYING OUT THE INVENTION

Figure 1 is a block schematic which illustrates that part of a base station in which the inventive method is applied.

A speech coder 1 generates coded speech/data signals received from an analog/digital converter (not shown) and the speech-coded signals are passed to a channel coder 2, which introduces a given redundancy for the purpose of discovering and correcting bit errors in the speech/data block.

A FAACH-generator FA generates control and monitoring signals for transmission between the base station and a mobile station. These signals are generated in blocks and one such block can replace a speech/data block in a TDMA-frame in a known manner at any time whatsoever when the system finds it suitable. A FACCH-block includes a flag, a message and a check field so-called CRC, in total 65 bits. The FACCH-block is coded in the channel coder 3 so as to render the block more tolerable to bit errors than the speech/data block.

A SACCH-generator SA generates the control and monitoring messages between the base station and the mobile with a duration of 12 bits and occupies only a small part of a time slot in a TDMA-frame, although each time slot includes these SACCH-bits. The SACCH-generator SA is connected to a channel coder 4 and to an in-
The channel coders 2 and 3 have outputs connected to a selector 5. In one position of the selector (upper position), the channel coded speech/data signals from the channel coder 2 are delivered to an adder 8, whereas in the other position of the coder (bottom position), the associated control channel signals from the channel coder 3 are applied to the adder 8.

The various signals from the selector 5 and the interleaver 6, and a sync.-message SY and a verification code DVCC are combined in a burst generator 9 to form a single burst of signals which occupy a given time slot. All of these signals form a channel to a given receiving mobile and are thereafter modulated with a given carrier frequency.

Prior to transmission, the signals from the speech/data generator 1 and from the FACCH-generator FA shall be ciphered with a given ciphering code, whereas the SACCH-signals shall be transmitted unciphered. To this end, there is provided a cipher-generator 11 which generates a pseudo random sequence to the modulo-2 adder 8. In this way, the random sequence is added (mod 2) to the interfoliated speech/data signals and the FACCH-signals in the selector 5 and the signals are thus ciphered.

The cipher-generator is controlled by a cipher code from the unit 12 and by a frame counter 10, in a manner to generate the pseudo random sequence. In this case, the cipher code comprises the given configuration of a whole bit pattern of a pulse sequence and also the start of the pulse sequence. The starting time point of the pulse sequence within a frame is determined by the frame counter 10.

A microprocessor 13 is connected between the frame counter 10 and to a control input of the SACCH-generator SA for the purpose of
carrying out the inventive method, which will now be described in more detail with reference to Figure 2.

The SACCH-generator SA in Figure 1 generates SACCH-words in sequence, each word containing 66 bits. Subsequent to passing through the channel coder 4, there is obtained a 132-bit word which contains parity bits, etc. The interleaver unit 6 groups these 132 bits in each word into groups of 12-bits, so that the burst generator 9 is able to transmit 12 bits from each SACCH-word in the duration of one time slot. Each SACCH-word is thus divided into $132/12 = 11$ time slots during sequential frames, i.e. 11 frames are required for transmitting one SACCH word.

According to the proposed method, SACCH-words are used in sequence for transmitting continuously information concerning the frame count status (sequence number) of the base station to the frame counter of the mobile, for the purpose of synchronizing the two frame counters. Since the frame counters control the ciphering in the base station and in the mobile respectively, the ciphering can therefore also be synchronized. The base station transmits a given frame counter number via the SACCH-channel (non-ciphered), and the frame counter number of the mobile shall therewith coincide with the transmitted base station number while taking into account known delays and group transit times between base station and mobile.

At a given arbitrary time point $t_0$, according to Figure 2, there is transmitted a burst $S_1$ belonging to the SACCH-word $W_3$, which contains information concerning the value to which the frame counter of the base station is set when receiving the SACCH-word $W_3$ in the mobile. As an example, it is assumed that at the time $t_0$ of transmitting the SACCH-word, the base-station frame counter is set to the numerical value 24. It is also assumed in the Figure 2 example that the SACCH-word $W_3$ is transmitted during the aforesaid 11 bursts, $S_1-S_{11}$, i.e. during the duration $R_1-R_{11}$ of the frame.

When the last burst $S_{11}$ has been received in the mobile at $t_1$, the mobile will know the value transmitted from the base station. The
frame counter of the base station has then reached the value 24 + 11 = 35. Thus, the value 35 in the SACCH-word W3 is transmitted to the mobile during the time interval \( t_0 - t_1 \). The frame counter value 35 obtained is compared in the mobile with its frame counter setting and a correction is made if the values do not coincide. Ciphering continues over the whole period and remains unchanged.

During the next SACCH-word W4, a new frame counter number, namely 46, is transmitted in a similar manner by means of the bursts S12-S22, since when this new number is received by the mobile at the time \( t_2 \), the frame counter of the base station is set to 35 + 11 = 46. The transmission of frame counter numbers from the base station to the mobile is continued continuously in the same manner, thereby enabling continuous monitoring of the frame counter of the mobile to be carried out and optional adjustments to be made to said counter. This enables ciphering to be constantly synchronized between base station and mobile, since ciphering is dependent on which frame counter number is sent to the ciphering generator 11 in Figure 1.

The aforesaid adjustment of the frame counter number of the base station with respect to the number of transmitted bursts S1-S11, S12-S22, ... is carried out by the microprocessor 13 between the frame counter 10 and the SACCH-generator SA. The microprocessor 13 also corrects the value obtained from the frame counter 10 with respect to the time delay in the transmission circuits. The time delay constitutes a known parameter. The propagation time of the radio signal between base station and mobile is in the order of some microseconds, whereas the distance between two mutually sequential frames is 20 ms and is compensated for by means of the synchronizing word in a burst. The time delay parameter is thus not influenced by the propagation time over the radio medium. Thus, the proposed method makes possible non-ciphered signalling of synchronizing information for ciphering/deciphering between a base station and a mobile. This signalling is additional to the normal synchronization between the ciphered fast associated control channel FACCH and replaces this normal synchronization in the event of a drop-off.
THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method of transmitting synchronizing information in the ciphered transmission of signals between a base station and a mobile station in a mobile radio system which operates in accordance with the TDMA-principle with transmission in frames and time slots, wherein control information is transmitted over a ciphered associated control channel (FACCH) and a non-ciphered associated control channel (SACCH), and wherein the base station and the mobile station each include a frame counter which counts transmitted and received frames (R1-R11, ...) and which controls the formulation of a cipher sequence which is superimposed in the base station on the non-ciphered signals transmitted to the mobile station, characterized by transmitting over the non-ciphered associated control channel (SACCH) from the base station during a given number of frames (R1-R11) an information word (W3) which denotes the sequence number (35, 46, ...) for that frame for which the frame counter of the mobile shall be set at the time (t_1) at which said information word (W3) was received and which is related to the sequence number for the base-station frame counter at the time (t_o) at which the information word (W3) was transmitted.

2. A method according to Claim 1, characterized by transmitting said information word (W3) relating to the sequence number of the mobile-station frame counter in the form of a plurality of bursts (S1-S11) during a corresponding number of frames (R1-R11), wherein the sequence number is the same as the sequence number of the base-station frame counter at the transmission time (t_o) increased with the number of bursts required for transmission of the information word.

3. A method according to Claims 1-2, characterized by following said information word (W3) with a further information word (W4, W5, ...) which is transmitted to the mobile station for continuously monitoring of the counter setting of the frame counter in the mobile station.

DATED this 14th day of January 1993.

TELEFONAKTIEBOLAGET L M ERICSSON

WATERMARK PATENT & TRADEMARK ATTORNEYS
"THE ATRIUM"
290 BURWOOD ROAD, HAWTHORN, VIC. 3122.
Fig. 2