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

(11) EP 2 347 540 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
05.12.2012 Bulletin 2012/49

(21) Application number: **09821005.7**

(22) Date of filing: **05.10.2009**

(51) Int Cl.:
H04L 9/14 *(2006.01)* ***H04L 29/06*** *(2006.01)*

(86) International application number:
PCT/US2009/059503

(87) International publication number:
WO 2010/045044 (22.04.2010 Gazette 2010/16)

(54) METHOD AND DEVICE FOR SENDING ENCRYPTION PARAMETERS

VERFAHREN UND VORRICHTUNG ZUR SENDUNG VON VERSCHLÜSSELUNGSPARAMETERN

PROCÉDÉ ET DISPOSITIF POUR ENVOYER DES PARAMÈTRES DE CRYPTAGE

(84) Designated Contracting States:
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 SE SI SK SM TR

(30) Priority: **17.10.2008 US 253411**

(43) Date of publication of application:
27.07.2011 Bulletin 2011/30

(73) Proprietor: **Motorola Solutions, Inc.**
Schaumburg IL 60196 (US)

(72) Inventors:
- **CHOWDHARY, Dipendra, M.**
  Hoffman Estates, Illinois 60192 (US)
- **BELMONTE, John, P.**
  Schaumburg, Illinois 60194 (US)
- **WIATROWSKI, David, G.**
  Woodstock, Illinois 60098 (US)

(74) Representative: **Treleven, Colin**
Optimus Patents Limited
Grove House
Lutyens Close
Basingstoke
Hampshire, RG24 8AG (GB)

(56) References cited:
KR-A- 20040 059 146 **KR-A- 20040 059 146**
US-A1- 2007 053 512 **US-A1- 2007 053 512**
US-A1- 2008 232 589 **US-A1- 2008 232 589**

- **"Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems; Part 1: DMR Air Interface (AI) protocol; ETSI TS 102 361-1", IEEE, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, vol. ERM-TG-DMR, no. V1.4.5, 1 December 2007 (2007-12-01), XP014040497, ISSN: 0000-0001**

EP 2 347 540 B1

Description

TECHNICAL FIELD

[0001] The technical field relates generally to wireless communication systems and in particular to sending encryption parameters in an ETSI DMR voice superframe.

BACKGROUND

[0002] Over the last few decades, digital two-way radio networks have become widespread. Typically, two-way radios allow users to receive as well as transmit voice or data. To provide interoperability between various digital two-way radio systems and vendors, European Telecommunication Standards Institute (ETSI) has introduced a Digital Mobile Radio (DMR) air interface standard, which specifies various protocols used by the two-way radios at the data link layer (i.e., layer 2) of the well known seven-layer Open Systems Interconnection computer networking model, and which is described in ETSI TS (Technical Specification) 102 361-1 v1.4.5 (2007-12). Reference herein to the ETSI DMR standard includes the current version of the technical specification and all subsequent and future versions.

[0003] The ETSI DMR standard specifies a two-slot Time Division Multiple Access (TDMA) structure that transmitting and receiving devices can utilize to send voice and/or data signals. The voice and data signals are transmitted in the TDMA slots in accordance with a general burst format specified in the standard. In addition, the bursts comprising voice signals are transmitted in superframes that are 360 ms long and have six bursts that are designated with the letters "A" through "F".

[0004] Moreover, the voice and data messages can be sent in the clear as plain information or can be encrypted and made private so that the data cannot be read or the voice cannot be heard on any device other than one that has the proper parameters needed to decrypt the messages. Accordingly, encryption and decryption (or privacy) is a way to protect communications and keep them private when sending the messages between two devices. However, in the context of this disclosure, privacy does not provide any mechanism to authenticate the devices or users or to protect the integrity of the messages, for instance, to ensure that the messages are decoded in the proper order or that all of the messages were actually received at the receiving device.

[0005] The encryption process generally comprises a transmitting device combining certain cryptographic parameters with the plain information to generate protected information that is sent to a receiving device. For encryption processes that use a cryptographic algorithm, such as ARC4, the cryptographic parameters typically include a key, the cryptographic algorithm, and an initialization vector (IV) for the algorithm. Accordingly, in order to properly decrypt the protected information, the receiving device has to know and use the same key, cryptographic algorithm, and IV that were used by the transmitting device.

[0006] To make the cryptographic parameters known to the receiving device, the transmitting device can send to the receiving device the cryptographic parameters themselves and/or encryption identifiers (IDs) that identify one or more of the cryptographic parameters. The cryptographic parameters and encryption identifiers are collectively referred to herein as encryption parameters. Thus, when referring to a set of encryption parameters, the set could include one or more cryptographic parameters only, one or more encryption identifiers only, or a combination of both cryptographic parameters and encryption identifiers. Currently, there is no method defined in the DMR standard for transporting encryption parameters.

[0007] Thus, there exists a need for a method and device for transmitting encryption parameters that can be implemented in a DMR system.

BRIEF DESCRIPTION OF THE FIGURES

[0008] The accompanying figures, where like reference numerals refer to identical or functionally similar elements throughout the separate views, which together with the detailed description below are incorporated in and form part of the specification and serve to further illustrate various embodiments of concepts that include the claimed invention, and to explain various principles and advantages of those embodiments.

FIG. 1 shows a block diagram of a communication system in accordance with an illustrative embodiment.

FIG. 2 illustrates embodiments implemented within the framework of a DMR voice superframe, a voice burst within the superframe, and vocoder frames within the voice burst.

FIG. 3 shows a flow diagram of a method for transmitting encryption parameters in a DMR voice superframe in accordance with an illustrative embodiment.

FIG. 4 shows a flow diagram of a method of placing an IV within a DMR voice superframe in accordance with an illustrative embodiment.

FIG. 5 shows selecting bits from vocoder frames in a DMR voice superframe and replacing them with modified IV bits in accordance with an illustrative embodiment.

FIG. 6 shows a flow diagram of a method for placing encryption identifiers in a DMR voice superframe in accordance with an illustrative embodiment.

FIG. 7 shows placement of the encryption identifiers in an embedded signaling field of a DMR voice burst in accordance with an illustrative embodiment.

FIG. 8 shows a flow diagram of a method for receiving encryption parameters in a DMR voice superframe in accordance with an illustrative embodiment.

[0009] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions of some of the elements in the figures may be exaggerated relative to other elements to help improve understanding of various embodiments. In addition, the description and drawings do not necessarily require the order illustrated. Device and method components have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the various embodiments so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein. Thus, it will be appreciated that for simplicity and clarity of illustration, common and well-understood elements that are useful or necessary in a commercially feasible embodiment may not be depicted in order to facilitate a less obstructed view of these various embodiments.

DETAILED DESCRIPTION

[0010] Generally speaking, pursuant to the various embodiments, a transmitting device encrypts DMR voice superframes using cryptographic parameters that, in one embodiment, include a key, an encryption algorithm, and an IV and sends the encrypted DMR voice superframes to a receiving device. To assist the receiving device in decrypting the DMR voice superframes, the transmitting device: identifies a selected number of bits from a plurality of vocoder frames of a DMR voice superframe; replaces each of the identified bits with a corresponding bit of an encryption parameter (e.g., an IV or modified IV); places at least one encryption parameter (e.g., a key ID and an algorithm ID) in an embedded signalling field of the DMR voice superframe; and transmits the DMR voice superframe with the encryption parameters to the receiving device. The receiving device: extracts the encryption identifiers; extracts a selected number of bits from a plurality of vocoder frames of the DMR voice superframe; arranges the extracted bits to obtain the IV; and uses the extracted IV and encryption identifiers to decrypt the DMR voice superframes.

[0011] In one embodiment, the key ID and algorithm ID are sent in the embedded signaling field of the DMR voice superframe F burst and, therefore, does not interfere with the transmission of any other information. In a further embodiment, the bits from the vocoder frames that are replaced with the IV (or modified IV bits) are least significant bits to facilitate minimum distortion of the voice signal. Moreover in another embodiment, the IV, key ID and algorithm ID are sent in every DMR voice superframe to facilitate late entry of a subscriber unit to a voice call with minimum delay. Those skilled in the art will realize that the above-recognized advantages and other advantages described herein are merely illustrative and are not meant to be a complete rendering of all of the advantages of the various embodiments.

[0012] Referring now to the drawings, FIG. 1 shows a block diagram of a communication system 100 in accordance with an illustrative embodiment. Communication system 100 is depicted in a very generalized manner. For example, system 100 is illustrated as comprising a single infrastructure device 106 and three wireless communication devices 102, 104, 108, for ease of illustration. However, the teachings herein can be implemented in a system having additional infrastructure devices and wireless communication devices.

[0013] Each infrastructure device and wireless communication device is at least equipped with a transceiver (i.e., transmitter and receiver apparatus) 110, a memory 112 and a processing device 114 and is further equipped with any additional components as needed for a commercial embodiment. The transceiver 110, memory 112 and processing device 114 can have any suitable physical implementation and are topologically coupled depending on the particular device implementation. These components are further operatively coupled and can be adapted, arranged, configured, and designed to perform methods in accordance with the teachings herein, for example, as illustratively described by reference to the remaining figures 2 through 8.

[0014] As referred to herein, a wireless communication device includes, but is not limited to, devices commonly referred to as access terminals, mobile radios, mobile stations, subscriber units, user equipment, mobile devices, or any other device capable of operating in a wireless environment. Examples of wireless communication devices include, but are not limited to, two-way radios, mobile phones, cellular phones, Personal Digital Assistants (PDAs), laptops and two-way pagers. As used herein, an infrastructure device is a device that is a part of a fixed network infrastructure and can receive information (either control or media, e.g., data, voice (audio), video, etc.) in a signal from a wireless communication device and transmit information in signals to one or more wireless communication devices via a communication link. An infrastructure device includes, but is not limited to, equipment commonly referred to as repeaters, base radios, base stations, base transceiver stations, access points, routers or any other type of infrastructure equipment interfacing a wireless communication device in a wireless environment.

[0015] In this illustrative embodiment, system 100 is a DMR system, and the infrastructure device 106 and the wireless communication devices 102, 104, and 108 communicate using the air interface as specified in the DMR standard (as such, device 106 is hereinafter referred to as a base station (or BS), and devices 102, 104, and 108 are hereinafter referred to as mobile stations or (MSs)). In accordance with the DMR standard, the MSs can communicate in "direct mode" or "talkaround mode", wherein the MSs communicate directly with each other outside the control of a BS. MSs 102 and 104 are illustrated in FIG. 1 as communicating in direct mode. MSs can also

communicate in "repeater mode", wherein the MSs communicate through a BS. MSs 102 and 108 are illustrated in FIG. 1 as communicating in repeater mode using the BS 106. Transmissions from a BS to a MS in repeater mode are called outbound transmissions, and transmissions from a MS to a BS in repeater mode are called inbound transmissions.

[0016] As mentioned earlier, the devices in system 100 communicate using communication links (also referred to herein as channels). The channels comprise physical channels and logical channels. The physical channels are the physical communication resources over which information is sent between the elements within system 100. The physical channels can comprise wired links or wireless links. If the physical channels comprise wireless links, the corresponding physical resource is an allocation of radio spectrum that is partitioned into radio frequency (RF) carriers with each RF carrier partitioned in time into frames and timeslots. The slots for the two TDMA physical channels are labeled channel "1" and channel "2". A DMR burst is a period of RF carrier that is modulated by a media stream and represents the physical channel of a single timeslot. The burst is the smallest standalone unit of TDMA transmission defined in the DMR standard.

[0017] A physical channel is required to support a logical channel, which is a logical communication pathway between two or more parties. Logical channels are separated into two categories: traffic channels carrying speech or data information; and control channels carrying signaling, which is specifically concerned with the establishment and control of connections, and with management in the system 100. Signaling from a target to a source is referred to herein as Reverse Channel (RC) signaling. Details of illustrative embodiments will next be described by reference to figures 2 through 8.

[0018] FIG.2 illustrates embodiments implemented within the framework of a DMR voice superframe, a voice burst within the DMR voice superframe, and vocoder frames within the voice burst. A timing diagram for a DMR voice superframe is illustrated at 200. The DMR voice superframe is sent by a transmitting MS to a receiving MS and can be sent in either direct mode or repeater mode. The DMR voice superframe is sent on one of the two channels and comprises six bursts 204, labeled "A" through "F", i.e., 204-A, 204-B, 204-C, 204-D, 204-E, and 204-F. The other channel comprising blocks 206 may be unused or may be in use by other devices in system 100.

[0019] Illustrated by reference to 210 is one of the bursts 204 of the DMR voice superframe. The generic burst structure includes two 108 voice bit payload fields 212 and 214 and a 48-bit field 208 in the center of the burst referred to herein as the "embedded signaling" field. The embedded signaling field 208 carries either synchronization or embedded signaling depending on the particular burst within the DMR voice superframe. The defined burst takes 27.5 ms to transmit and may be followed by 2.5 ms of guard time or a Common Announcement Channel (CACH). Thus, one burst is 30 ms; one frame of two contiguous timeslots, referred to as 1 and 2, is 60 ms; and one DMR voice superframe is 360 ms (due to the timing for the other channel).

[0020] In one embodiment, Burst A, which marks the beginning of the DMR voice superframe, contains synchronization (for example in the form of known synchronization patterns) in field 208. Bursts B through F may contain embedded signaling such as Link Control (including, but not limited to, source and destination addresses, message type, length), RC signaling, etc., in field 208, and in some implementation scenarios field 208 in at least one of the bursts B through F can be empty (null) or have some unused bits.

[0021] As is well known in voice processing, a vocoder is used by a transmitting device to encode digitized speech for purposes of applying forward error correction (FEC), compression, encryption, interleaving, etc. In an embodiment, the transmitting device comprises a 3600 bps vocoder that produces 72-bit frames (including FEC) every 20 ms. Thus, the voice burst 204 carries three 72-bit vocoder frames (including FEC) 222, 224, and 226 plus the 48-bit embedded signaling field as illustrated at 220. Figures 3-8 illustrate embodiments, wherein a transmitting device sends encryption parameters (in this case the IV, key ID, and algorithm ID) in the embedded signaling field and in the vocoder frames, which contain encrypted voice bits. However, before describing embodiments of transporting the encryption parameters, a brief discussion is given below of how the encryption parameters are obtained and, in general, used in an illustrative encryption and decryption process.

[0022] In an embodiment, the transmitting device uses the cryptographic parameters of a key, a cryptographic algorithm, and an IV to initialize the cryptographic algorithm. The key and cryptographic algorithm may be selected from one of several keys and algorithms stored in and commonly used by both the transmitting and receiving devices. In an illustrative example, the selected key is 40 bits long and is uniquely identified by a key ID, and the algorithm (e.g., ARC4 as is well known in the art) is one that requires an IV and is identified by a unique algorithm ID. Moreover, different keys and algorithms can be used to encrypt voice message versus data messages.

[0023] The IV is a block of bits that is used as a seed to the algorithm to produce a unique key stream independent from other key streams produced by the same key. In this illustrative example, the transmitting device generates a 32 bit long IV, which is initialized by a random number that is different for each initialization and for each MS. The initialization can be done either upon power-on or at the beginning of a voice or data call. Moreover, to provide robust cryptographic protection, a different key stream is generated for each DMR packet data unit (PDU) and for each DMR voice superframe. For example, the IV can be updated by applying a Linear Feedback Shift Register (LFSR) on the previous IV. However, in other

embodiments, the same IV can be used to generate the key stream for a number of DMR voice superframes (or PDUs) or once for every call, but these methods provide less cryptographic protection. It should also be noted that, the key and IV bitwise lengths and the particular algorithm provided for herein are given merely as examples and are not meant to limit the scope of the teachings herein. Accordingly, any suitable key, algorithm, IV, or other relevant encryption parameter may be used depending on the particular encryption methodology implemented.

[0024] Returning to the description on the illustrative encryption process, to protect the plain information, the transmitting device selects a key and concatenates the key with the IV to use in initializing the cryptographic algorithm, which is used to generate a key stream byte by byte at the output of the algorithm. The key stream is combined with the plain information using a logical exclusive OR operator (i.e., XOR) to generate protected information, which is sent to a receiving device. To decrypt the protected information, the receiving device has to generate the same key stream as was generated in the transmitting device, and XOR the key stream with the protected information to obtain the plain information that can be read or heard by a user of the receiving device. However, in order to generate the same key stream, the receiving device has to use the same key, cryptographic algorithm, and IV as was used in the transmitting device. The remaining figures 3-8 provide for an illustrative embodiment for a transmitting device to transport encryption parameters to a receiving device in a DMR voice superframe and for the receiving device to extract those encryption parameters to use in the decryption process.

[0025] Turning now to FIG. 3 in which is shown a flow diagram of a method 300 for transmitting encryption parameters in a DMR voice superframe in accordance with an illustrative embodiment. In general, the encryption parameters are transported in a DMR voice superframe within an embedded signaling field and by replacing vocoder frame bits with bits of one or more of the encryption parameters.

[0026] More particularly, at 302, the transmitting device identifies a selected number of bits from a plurality of vocoder frames. Any bits may be identified and replaced. However, identifying and replacing only least significant bits are advantageous in that this has the least effect on, or in other words causes minimum distortion of, the audio heard at the receiving device. As used herein, the phrase "least significant bits" are those vocoder bits that have the least noticeable impact on audio quality regardless of bit order. Thus, as used in this sense, least significant bits do not just simply refer to the bits having the lowest bit numbering according to how all of the vocoder bits are numbered.

[0027] The transmitting device replaces (304) at least some of the identified bits with corresponding bits of at least one encryption parameter. In the embodiments described below by reference to figures 4 and 5, the identified bits are replaced with corresponding bits of the IV and, more particularly, each of the identified bits are replaced with corresponding bits of a modified IV, which are combined with error control bits (i.e., error detection parity bits and/or forward error detection parity bits). However, in another embodiment, the identified bits could be replaced with corresponding bits of a truncated or shortened IV. In yet another embodiment, the identified vocoder frame bits can be replaced with bits of other encryption parameters such as the key, key ID, algorithm ID, etc, in addition to or alternatively to the IV or modified IV.

[0028] The transmitting device, at 306, also places one or more encryption parameters in an embedded signaling field in the DMR voice superframe. Any encryption parameters (or portion thereof) can be placed in one or more embedded signaling fields of any voice burst. However, so as not to interfere with the transmission of other information and signaling in the DMR voice superframe, smaller sized encryption parameters such as encryption identifiers (e.g., the key ID and the algorithm ID) are placed into an embedded signaling field in a burst having bits that are not otherwise being used with other information or signaling, such as in the F burst. An illustrative embodiment of placing encryption parameters within an embedded signaling field is described by reference to figures 6 and 7. The transmitting device then transmits (308) the DMR voice superframe with the encryption parameters to one or more receiving devices.

[0029] Turning now to FIG. 4, shown therein is a flow diagram of a method of placing a modified IV within a DMR voice superframe in accordance with an illustrative embodiment. FIG. 4 will be described in conjunction with FIG. 5 to show a specific example of each of selected vocoder frame bits being replaced by corresponding bits of the modified IV. Upon generating an IV (502), the transmitting device calculates (402) error detection parity bits over the IV, which are concatenated (404) with the IV to generate a concatenated IV. Any error detecting techniques can be used to generate the error detection parity bits including, but not limited to, hash functions, simple parity, Checksum, etc. However, in the embodiment illustrated by reference to FIG. 5, the transmitting device calculates a cyclic redundancy check (CRC) check over the IV to generate the error detection parity bits 504 that are appended to the IV 502. In one illustrative example, the CRC is calculated using polynomial arithmetic using a CRC generator polynomial, such as $x^4 + x + 1$, to generate a 4-bit CRC, but any other suitable method to calculate the CRC can be used.

[0030] At 406, the transmitting device appends error correction parity bits to the concatenated IV to generate the modified IV using any suitable error correction technique including, but not limited to, use of Automatic repeat-request (ARQ) techniques, a Hamming code, a Golay code, a Reed-Solomon code, to name a few. In the embodiment illustrated by reference to FIG. 5, the transmitting device splits the 36 bit concatenated IV into three segments and applies an extended (24, 12, 8)

Golay code to the concatenated IV, to append 36 forward error correction (FEC) parity bits and, thereby, generate 72 bits of modified IV 506. More or fewer than 72 bits could be generated if using a different error correcting technique. The transmitting device divides the modified IV into three equal segments 508, 510, and 512 of 24 bits to be transported in the vocoder frames of the DMR voice superframe. As shown in FIG. 5, segment 508 comprises bits 0 to 23; segment 510 comprises bits 24 to 47; segment 512 comprises bits 48 to 71. Dividing the modified IV into equal segments of 24-bits is not required to implement the teachings herein. The modified IV need not be divided at all or could be divided into a different number of segments having an equal or unequal number of bits.

[0031] The transmitting device identifies (408) a selected number of bits from the vocoder frames and replaces these bits with the 72 bits of modified IV. In an illustrative embodiment, the transmitting device identifies four least significant bits from each of the three vocoder frames (VF1, VF2, VF3) in each of the six bursts (204-A to 204-F) of the DMR superframe shown in FIG. 2 and interleaves (410) the modified IV bits into the positions of the identified vocoder frame bits. In case the modified IV is longer or shorter than 72 bits, more or fewer bits can be identified from the vocoder frames to transport the IV. Using certain 3600 bps vocoders, up to six bits can be selected from the vocoder frames with minimum distortion to the transmitted voice signal.

[0032] The bits from each of the modified IV segments 508, 510, 512 could be sequentially placed into the positions of the identified vocoder bits. However, in this illustrative example, the modified IV are interleaved into the vocoder frame bit positions in order to arrange the IV bits in a non-contiguous way to protect the IV against burst errors during transmission. The modified IV bits can be interleaved bit by bit, but in this example, small blocks of bits (e.g., four bit blocks in this case) are interleaved in the positions of equal sized blocks of identified vocoder frame bits. For example, block 514 of the segment 508 is placed in vocoder frame (VF3) of the burst 204-F. Block 516 of the segment 510 is placed in the vocoder frame (VF2) of burst 204-F; and block 518 of the segment 512 is placed in the vocoder (VF1) of the burst 204-F. Similarly, the next four-bit block from each segment 508, 510, 512 is placed in the vocoder frames VF3, VF2 and VF1 of burst 204-E, and so on.

[0033] As mentioned above figures 6 and 7 provide for an illustrative example of placing encryption parameters (in this case a key ID 702 and an algorithm ID 704) in the DMR voice superframe. In one embodiment, the key ID is 8-bits long, and the algorithm ID is 3-bits long, although the length of the encryption identifiers can vary. More particularly, in accordance with a method 600, the transmitting device generates (602) error correction parity bits over one or more of the encryption identifiers and concatenates (604) the error correction parity bits with the encryption identifiers. As illustrated in FIG. 7, 21 FEC parity bits 706 are generated over the key ID 702 and algorithm ID 704 and then appended to the key and algorithm IDs. The error correction parity bits can be generated using any suitable error correction techniques including any one of those mentioned above to thereby generate the same number, more, or fewer error correction parity bits, or the error correction parity bits could be calculated over only the key ID or the algorithm ID. Moreover in another embodiment, the transmitting device could calculate error detection parity bits (e.g., using CRC, Checksum, simple parity, etc.) over one or more of the encryption identifiers before generating the error correction parity bits or instead of generating the error correction parity bits.

[0034] In this illustrative implementation, the transmitting device places (606) the key ID 702, algorithm ID 704 and concatenated FEC parity bits 706 into the embedded signaling field 208-F of the F burst 204-F of the DMR voice superframe shown in FIG. 2. As mentioned above, placing encryption parameters in the F burst is advantageous because, at present, the embedded signaling field is null. However, the encryption parameters could be placed in the embedded signaling field of any one or more of the bursts in the DMR voice superframe. Moreover, the transmitting device could place the encryption parameters in a single embedded signaling field throughout the entire voice call (comprising a plurality of DMR voice superframes) or periodically place the encryption parameters in several embedded signaling fields during the call. However, to best facilitate late entry by a receiving device to a voice call after initial headers having the encryption parameters have been sent, it is further advantageous for the transmitting device to place the encryption parameters in every DMR voice superframe of the call.

[0035] FIG. 8 shows a flow diagram of a method 800 for receiving encryption parameters in a DMR voice superframe in accordance with an illustrative embodiment. Upon receiving (802) voice transmissions from a transmitting device, a receiving device detects that the transmissions are encrypted. For instance, in one embodiment the receiving device detects that a privacy bit is set in a Voice Link Control (LC) header, which indicates that the receiving device needs to extract the encryption parameters in order to decrypt the voice transmissions. In addition, or in the alternative, a bit could be set in embedded LC signaling during the voice transmission and/or in a Terminator with LC at the end of the voice transmission to indicate to the receiving device to extract the encryption parameters from the DMR voice superframes. Other methods of indicating to the receiving device to extract the encryption parameters could also be implemented without detracting from the scope of the teachings herein.

[0036] Accordingly, the receiving device extracts (804) at least one encryption parameter from an embedded signaling field of the DMR voice superframe 200. In this case, the receiving device extracts the key ID 702 and algorithm ID 704 from the embedded signaling field of the F burst and applies the FEC bits 706 to these encryp-

tion identifiers to correct any errors, if present. The receiving device also extracts and de-interleaves (806) bits from the vocoder frames of the DMR voice superframe to obtain the IV.

[0037] More particularly, the receiving device removes the four least significant bits (four-bit blocks) from each of the eighteen vocoder frames in the DMR voice superframes and de-interleaves the four bit blocks to obtain the 72 bit modified IV, which includes the FEC parity bits. In a different implementation, a subset of the four-bit blocks could be removed from the vocoder frames to obtain the IV. FEC is applied over the error-protected IV to obtain the 32 bit IV and four bit CRC. Upon verifying the 4 bit CRC, the receiving device selects the appropriate key as identified by the key ID and the appropriate algorithm as identified by the algorithm ID.

[0038] In this case, the algorithm is ARC4, which uses the key concatenated with the IV to generate the same key stream as was generated in the transmitting device. To obtain the plain voice payload of the DMR voice superframe, the receiving device XORs the encrypted part of the payload with the key stream. Method 800 can be performed for each DMR voice superframe, or once the encryption parameters are obtained in a particular DMR voice superframe, they can be used to decrypt that DMR superframe. For each subsequent DMR voice superframe, the receiving device can simply update the IV using the LFSR of the previous IV to decrypt the subsequent DMR voice superframe.

[0039] In the foregoing specification, specific embodiments have been described. However, one of ordinary skill in the art appreciates that various modifications and changes can be made without departing from the scope of the invention as set forth in the claims below. Accordingly, the specification and figures are to be regarded in an illustrative rather than a restrictive sense, and all such modifications are intended to be included within the scope of present teachings. The benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential features or elements of any or all the claims. The invention is defined solely by the appended claims including any amendments made during the pendency of this application and all equivalents of those claims as issued.

[0040] Moreover in this document, relational terms such as first and second, top and bottom, and the like may be used solely to distinguish one entity or action from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions. The terms "comprises," "comprising," "has", "having," "includes", "including," "contains", "containing" or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises, has, includes, contains a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. An element proceeded by "comprises ...a", "has ...a", "includes ...a", "contains ...a" does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or apparatus that comprises, has, includes, contains the element. The terms "a" and "an" are defined as one or more unless explicitly stated otherwise herein. The terms "substantially", "essentially", "approximately", "about" or any other version thereof, are defined as being close to as understood by one of ordinary skill in the art, and in one non-limiting embodiment the term is defined to be within 10%, in another embodiment within 5%, in another embodiment within 1% and in another embodiment within 0.5%. The term "coupled" as used herein is defined as connected, although not necessarily directly and not necessarily mechanically. A device or structure that is "configured" in a certain way is configured in at least that way, but may also be configured in ways that are not listed.

[0041] It will be appreciated that some embodiments may be comprised of one or more generic or specialized processors (or "processing devices") such as microprocessors, digital signal processors, customized processors and field programmable gate arrays (FPGAs) and unique stored program instructions (including both software and firmware) that control the one or more processors to implement, in conjunction with certain non-processor circuits, some, most, or all of the functions of the method and apparatus for sending encryption parameters described herein. The non-processor circuits may include, but are not limited to, a radio receiver, a radio transmitter, signal drivers, clock circuits, power source circuits, and user input devices. As such, these functions may be interpreted as steps of a method to perform the sending of encryption parameters described herein. Alternatively, some or all functions could be implemented by a state machine that has no stored program instructions, or in one or more application specific integrated circuits (ASICs), in which each function or some combinations of certain of the functions are implemented as custom logic. Of course, a combination of the two approaches could be used. Both the state machine and ASIC are considered herein as a "processing device" for purposes of the foregoing discussion and claim language.

[0042] Moreover, an embodiment can be implemented as a computer-readable storage element or medium having computer readable code stored thereon for programming a computer (e.g., comprising a processing device) to perform a method as described and claimed herein. Examples of such computer-readable storage elements include, but are not limited to, a hard disk, a CD-ROM, an optical storage device, a magnetic storage device, a ROM (Read Only Memory), a PROM (Programmable Read Only Memory), an EPROM (Erasable Programmable Read Only Memory), an EEPROM (Electrically Erasable Programmable Read Only Memory) and a Flash memory. Further, it is expected that one of ordinary skill,

notwithstanding possibly significant effort and many design choices motivated by, for example, available time, current technology, and economic considerations, when guided by the concepts and principles disclosed herein will be readily capable of generating such software instructions and programs and ICs with minimal experimentation.

[0043] The Abstract of the Disclosure is provided to allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in various embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separately claimed subject matter.

Claims

1. A method (300) for sending encryption parameters in a European Telecommunications Standards Institute Digital Mobile Radio (DMR) voice superframe, the method comprising:

   identifying (302) a selected number of bits from a plurality of vocoder frames of the DMR voice superframe;
   replacing (304) at least some of the identified bits with a corresponding bit of a first encryption parameter;
   placing (306) at least a second encryption parameter in an embedded signaling field of the DMR voice superframe; and
   transmitting (308) the DMR voice superframe, which includes the encryption parameters.

2. The method of claim 1, wherein:

   the first encryption parameter comprises an initialization vector (IV).

3. The method of claim 2, wherein replacing (304) at least some of the identified bits with a corresponding bit of initialization vector comprises:

   generating (406) a modified initialization vector by combining the initialization vector with at least one of error detection parity bits or forward error correction parity bits;
   and
   replacing (410) each of the identified bits with a corresponding bit of the modified initialization vector.

4. The method of claim 3, wherein generating the modified initialization vector comprises:

   calculating (504) a Cyclic Redundancy Check (CRC) for the initialization vector;
   concatenating (404) the Cyclic Redundancy Check with the initialization vector to generate a concatenated initialization vector;
   adding (406) forward error correction (FEC) parity bits to the concatenated initialization vector to generate the modified initialization vector.

5. The method of claims 2 to 4, wherein:

   replacing (304) each of the identified bits comprises interleaving the bits of the initialization vector in positions of the identified bits.

6. The method of any previous claim, wherein:

   placing (306) the at least a second encryption parameter in the embedded signaling field comprises positioning at least one encryption identifier in the embedded signaling field of Burst F of the DMR voice superframe.

7. The method of any previous claim, wherein the at least a second encryption parameter comprises at least one of:

   an encryption key identifier;
   an encryption algorithm identifier;
   the encryption key identifier combined with error control bits;
   the encryption algorithm identifier combined with error control bits; or
   the encryption key identifier and the encryption algorithm identifier combined with error control bits.

8. A method (800) for receiving encryption parameters in a European Telecommunication Standards Institute Digital Mobile Radio (DMR) voice superframe, the method comprising:

   receiving (802) the DMR voice superframe;
   extracting (804) a first encryption parameter from an embedded signaling field of the received DMR voice superframe;
   extracting (806) a selected number of bits from a plurality of vocoder frames of the DMR voice superframe; and
   arranging the extracted bits to obtain a second encryption parameter.

9. The method of claim 8, wherein:

the first encryption parameter is extracted from the embedded signaling field of Burst F of the DMR voice superframe.

10. The method of claim 8 or claim 9, wherein the first encryption parameter comprises at least one of:

an encryption key identifier;
an encryption algorithm identifier;
the encryption key identifier combined with error control bits;
the encryption algorithm identifier combined with error control bits; or
the encryption key identifier and the encryption algorithm identifier combined with error control bits.

11. The method of claim 10, further comprising:

decrypting the received DMR superframe using a key selected based on the key ID and an encryption algorithm selected based on the algorithm ID.

12. The method of claims 1 or 8, wherein:

the selected number of bits from the plurality of vocoder frames comprises a selected number of least significant bits.

13. The method of claim 12, wherein:

the selected number of least significant bits comprises four least significant bits extracted from each of the plurality of vocoder frames of the DMR voice superframe.

14. The method of any of claims 8-11, wherein:

the second encryption parameter comprises an initialization vector, and wherein the method further comprises decrypting the received DMR superframe using the initialization vector.

15. A device for sending encryption parameters in a European Telecommunications Standards Institute Digital Mobile Radio (DMR) voice superframe, the device comprising:

a processing device (114) for:

identifying a selected number of bits from a plurality of vocoder frames of the DMR voice superframe;
replacing at least some of the identified bits with a corresponding bit of an initialization vector (IV); and
placing at least one encryption identifier in an embedded signaling field of the DMR voice superframe;

a transceiver (110) coupled to the processing device (114) for transmitting the DMR voice superframe, which includes the initialization vector and encryption identifiers.

Patentansprüche

1. Verfahren (300) zum Senden von Verschlüsselungsparametern in einem DMR-Sprachsuperrahmen für Digital Mobile Radio (DMR) des Europäischen Instituts für Telekommunikationsnormen, wobei das Verfahren aufweist:

Identifizieren (302) einer ausgewählten Anzahl von Bits aus mehreren Vocoderrahmen des DMR-Sprachsuperrahmens;
Ersetzen (304) wenigstens einiger der identifizierten Bits durch ein entsprechendes Bit eines ersten Verschlüsselungsparameters;
Einsetzen (306) wenigstens eines zweiten Verschlüsselungsparameters in ein eingebettetes Signalgabefeld des DMR-Sprachsuperrahmens; und
Übertragen (308) des DMR-Sprachsuperrahmens, welcher die Verschlüsselungsparameter enthält.

2. Verfahren nach Anspruch 1, wobei:

der erste Verschlüsselungsparameter einen Initialisierungsvektor (IV) enthält.

3. Verfahren nach Anspruch 2, wobei das Ersetzen (304) wenigstens einiger der identifizierten Bits durch ein entsprechendes Bit eines Initialisierungsvektors aufweist:

Erzeugen (406) eines modifizierten Initialisierungsvektors durch Kombinieren des Initialisierungsvektors mit wenigstens einem aus dem Folgenden:

Fehlererkennungsparitätsbits oder Vorwärtsfehlerkorrekturparitätsbits; und
Ersetzen (410) eines jeden der identifizierten Bits durch ein entsprechendes Bit des modifizierten Initialisierungsvektors.

4. Verfahren nach Anspruch 3, wobei das Erzeugen des modifizierten Initialisierungsvektors aufweist:

Berechnen (504) einer zyklischen Redundanz-

prüfung (CRC) für den Initialisierungsvektor;
Verketten (404) der zyklischen Redundanzprüfung mit dem Initialisierungsvektor, um einen verketteten Initialisierungsvektor zu erzeugen;
Hinzufügen (406) von Vorwärtsfehlerkorrekturparitätsbits zu dem verketteten Initialisierungsvektor, um den modifizierten Initialisierungsvektor zu erzeugen.

5. Verfahren nach einem der Ansprüche 2 bis 4, wobei:

das Ersetzen (304) eines jeden der identifizierten Bits ein Einflechten der Bits des Initialisierungsvektors in Positionen der identifizierten Bits umfasst.

6. Verfahren nach einem der vorangehenden Ansprüche, wobei:

in dem Einsetzen (306) des wenigstens einen zweiten Verschlüsselungsparameters in das eingebettete Signalgabefeld wenigstens ein Verschlüsselungsidentifikator in dem eingebetteten Signalgabefeld von Burst F des DMR-Sprachsuperrahmens positioniert wird.

7. Verfahren nach einem der vorangehenden Ansprüche, wobei der wenigstens eine zweite Verschlüsselungsparameter wenigstens eines aus dem Folgenden aufweist:

einen Verschlüsselungsschlüsselidentifikator;
einen Verschlüsselungsalgorithmusidentifikator;
den Verschlüsselungsschlüsselidentifikator in Verbindung mit Fehlersteuerbits;
den Verschlüsselungsalgorithmusidentifikator in Verbindung mit Fehlersteuerbits; oder
den Verschlüsselungsschlüsselidentifikator und den Verschlüsselungsalgorithmusidentifikator in Verbindung mit Fehlersteuerbits.

8. Verfahren (800) zum Empfangen von Verschlüsselungsparametern in einem DMR-Sprachsuperrahmen für Digital Mobile Radio (DMR) des Europäischen Instituts für Telekommunikationsnormen, wobei das Verfahren aufweist:

Empfangen (802) des DMR-Sprachsuperrahmens;
Extrahieren (804) eines ersten Verschlüsselungsparameters aus einem eingebetteten Signalgabefeld des empfangenen DMR-Sprachsuperrahmens;
Extrahieren (806) einer ausgewählten Anzahl von Bits aus mehreren Vocoderrahmen des DMR-Sprachsuperrahmens; und
Anordnen der extrahierten Bits, um einen zweiten Verschlüsselungsparameter zu erhalten.

9. Verfahren nach Anspruch 8, wobei:

der erste Verschlüsselungsparameter aus dem eingebetteten Signalgabefeld von Burst F des DMR-Sprachsuperrahmens extrahiert wird.

10. Verfahren nach Anspruch 8 oder Anspruch 9, wobei der erste Verschlüsselungsparameter wenigstens eines aus dem Folgenden aufweist:

einen Verschlüsselungsschlüsselidentifikator;
einen Verschlüsselungsalgorithmusidentifikator;
den Verschlüsselungsschlüsselidentifikator in Verbindung mit Fehlersteuerbits;
den Verschlüsselungsalgorithmusidentifikator in Verbindung mit Fehlersteuerbits; oder
den Verschlüsselungsschlüsselidentifikator und den Verschlüsselungsalgorithmusidentifikator in Verbindung mit Fehlersteuerbits.

11. Verfahren nach Anspruch 10, das darüber hinaus aufweist:

Entschlüsseln des empfangenen DMR-Superrahmens unter Verwendung eines auf der Grundlage des Schlüsselidentifikators ausgewählten Schlüssels und eines auf der Grundlage des Algorithmusidentifikators ausgewählten Verschlüsselungsalgorithmus.

12. Verfahren nach Anspruch 1 oder 8, wobei:

die ausgewählte Anzahl von Bits aus den mehreren Vocoderrahmen eine ausgewählte Anzahl niedrigstwertiger Bits enthält.

13. Verfahren nach Anspruch 12, wobei:

die ausgewählte Anzahl niedrigstwertiger Bits vier niedrigstwertige Bits enthält, die aus jedem der mehreren Vocoderrahmen des DMR-Sprachsuperrahmens extrahiert wurden.

14. Verfahren nach einem der Ansprüche 8 bis 11, wobei:

der zweite Verschlüsselungsparameter einen Initialisierungsvektor enthält und wobei das Verfahren darüber hinaus ein Entschlüsseln des empfangenen DMR-Superrahmens unter Verwendung des Initialisierungsvektors enthält.

15. Vorrichtung zum Senden von Verschlüsselungsparametern in einem DMR-Sprachsuperrahmens für Digital Mobile Radio (DMR) des Europäischen Insti-

tuts für Telekommunikationsnormen, wobei die Vorrichtung aufweist:

eine Verarbeitungsvorrichtung (114) zum:

Identifizieren einer ausgewählten Anzahl von Bits aus mehreren Vocoderrahmen des DMR-Sprachsuperrahmens;
Ersetzen wenigstens einiger der identifizierten Bits durch ein entsprechendes Bit eines Initialisierungsvektors (IV); und
Einsetzen des wenigstens einen Verschlüsselungsidentifikators in ein eingebettetes Signalgabefeld des DMR-Sprachsuperrahmens;

einen an die Verarbeitungsvorrichtung (114) gekoppelten Sendeempfänger (110) zum Übertragen des DMR-Sprachsuperrahmens, der den Initialisierungsvektor und Verschlüsselungsidentifikatoren enthält.

Revendications

1. Procédé (300) pour l'envoi de paramètres de cryptage dans une super-trame de parole conforme à la norme des Radiocommunications Mobiles Numériques (DMR) de l'Institut Européen des Normes de Télécommunication (ETSI), le procédé comprenant les étapes suivantes :

identification (302) d'un nombre sélectionné de bits parmi une pluralité de trames de vocodeur de la super-trame de parole DMR ;
remplacement (304) d'au moins certains des bits identifiés par un bit correspondant d'un premier paramètre de cryptage ;
placement (306) d'au moins un deuxième paramètre de cryptage dans un champ de signalisation intégré de la super-trame de parole DMR ; et
transmission (308) de la super-trame de parole DMR, qui comprend les paramètres de cryptage.

2. Procédé selon la revendication 1, dans lequel le premier paramètre de cryptage comprend un vecteur d'initialisation (IV).

3. Procédé selon la revendication 2, dans lequel le remplacement (304) d'au moins certains des bits identifiés par un bit correspondant d'un vecteur d'initialisation comprend les étapes suivantes :

génération (406) d'un vecteur d'initialisation modifié par combinaison du vecteur d'initialisation avec au moins l'un des bits de parité de détection d'erreur ou des bits de parité de correction d'erreur directe ; et
remplacement (410) de chacun des bits identifiés par un bit correspondant du vecteur d'initialisation modifié.

4. Procédé selon la revendication 3, dans lequel la génération du vecteur d'initialisation modifié comprend les étapes suivantes :

calcul (504) d'un Contrôle de Redondance Cyclique (CRC) pour le vecteur d'initialisation ;
concaténation (404) du Contrôle de Redondance Cyclique (CRC) avec le vecteur d'initialisation pour générer un vecteur d'initialisation concaténé ;
ajout (406) de bits de parité de Correction d'Erreur Directe (FEC) au vecteur d'initialisation concaténé pour générer le vecteur d'initialisation modifié.

5. Procédé selon les revendications 2 à 4, dans lequel le remplacement (304) de chacun des bits identifiés comprend l'entrelacement des bits du vecteur d'initialisation aux positions des bits identifiés.

6. Procédé selon l'une quelconque des revendications précédentes, dans lequel le placement (306) de l'au moins un deuxième paramètre de cryptage dans le champ de signalisation intégré comprend le positionnement d'au moins un identifiant de cryptage dans le champ de signalisation intégré de la Salve F de la super-trame de parole DMR.

7. Procédé selon l'une quelconque des revendications précédentes, dans lequel l'au moins un deuxième paramètre de cryptage comprend au moins l'un des éléments suivants :

un identifiant de clé de cryptage ;
un identifiant d'algorithme de cryptage ;
l'identifiant de clé de cryptage combiné à des bits de contrôle d'erreur ;
l'identifiant d'algorithme de cryptage combiné à des bits de contrôle d'erreur ; ou
l'identifiant de clé de cryptage et l'identifiant d'algorithme de cryptage combinés à des bits de contrôle d'erreur.

8. Procédé (800) pour la réception de paramètres de cryptage dans une super-trame de parole conforme à la norme des Radiocommunications Mobiles Numériques (DMR) de l'Institut Européen des Normes de Télécommunication (ETSI), le procédé comprenant les étapes suivantes :

réception (802) de la super-trame de parole DMR ;

extraction (804) d'un premier paramètre de cryptage d'un champ de signalisation intégré de la super-trame de parole DMR reçue ;
extraction (806) d'un nombre sélectionné de bits à partir d'une pluralité de trames de vocodeur de la super-trame de parole DMR ; et
agencement des bits extraits de façon à obtenir un deuxième paramètre de cryptage.

9. Procédé selon la revendication 8, dans lequel le premier paramètre de cryptage est extrait du champ de signalisation intégré de la Salve F de la super-trame de parole DMR.

10. Procédé selon la revendication 8 ou la revendication 9, dans lequel le premier paramètre de cryptage comprend au moins l'un des éléments suivants :

un identifiant de clé de cryptage ;
un identifiant d'algorithme de cryptage ;
l'identifiant de clé de cryptage combiné à des bits de contrôle d'erreur ;
l'identifiant d'algorithme de cryptage combiné à des bits de contrôle d'erreur ; ou
l'identifiant de clé de cryptage et l'identifiant d'algorithme de cryptage combinés à des bits de contrôle d'erreur.

11. Procédé selon la revendication 10, comprenant en outre l'étape de décryptage de la super-trame DMR reçue à l'aide d'une clé sélectionnée selon l'ID de clé et d'un algorithme de cryptage sélectionné selon l'ID de l'algorithme.

12. Procédé selon la revendication 1 ou 8, dans lequel le nombre de bits sélectionné parmi la pluralité de trames de vocodeur comprend un nombre sélectionné de bits les moins significatifs.

13. Procédé selon la revendication 12, dans lequel le nombre sélectionné de bits les moins significatifs comprend quatre bits les moins significatifs extraits de chacune de la pluralité de trames de vocodeur de la super-trame de parole DMR.

14. Procédé selon l'une quelconque des revendications 8 à 11, dans lequel le deuxième paramètre de cryptage comprend un vecteur d'initialisation, et dans lequel le procédé comprend en outre le décryptage de la super-trame DMR reçue à l'aide du vecteur d'initialisation.

15. Dispositif pour l'envoi de paramètres de cryptage dans une super-trame de parole conforme à la norme des Radiocommunications Mobiles Numériques (DMR) de l'Institut Européen des Normes de Télécommunication (ETSI), le dispositif comprenant :

un dispositif de traitement (114) pour :

l'identification d'un nombre sélectionné de bits parmi une pluralité de trames de vocodeur de la super-trame de parole DMR ;
le remplacement d'au moins certains des bits identifiés par un bit correspondant d'un vecteur d'initialisation (IV) ; et
le placement d'au moins un identifiant de cryptage dans un champ de signalisation intégré de la super-trame de parole DMR ;
un émetteur-récepteur (110) couplé au dispositif de traitement (114) pour la transmission de la super-trame de parole DMR, qui comprend le vecteur d'initialisation et les identifiants de cryptage.

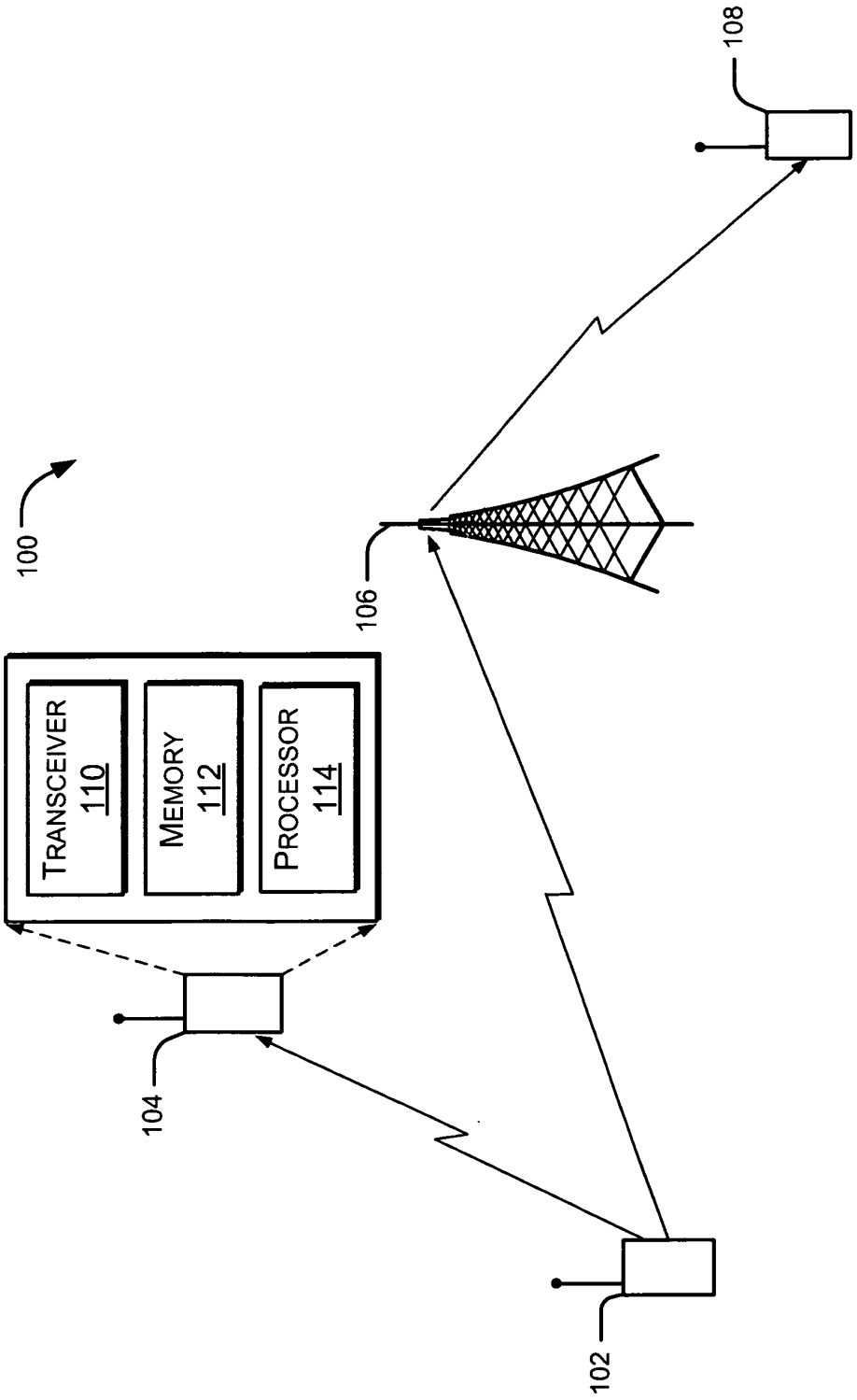
100
TRANSCEIVER 110
MEMORY 112
PROCESSOR 114
104
106
108
102

FIG. 1

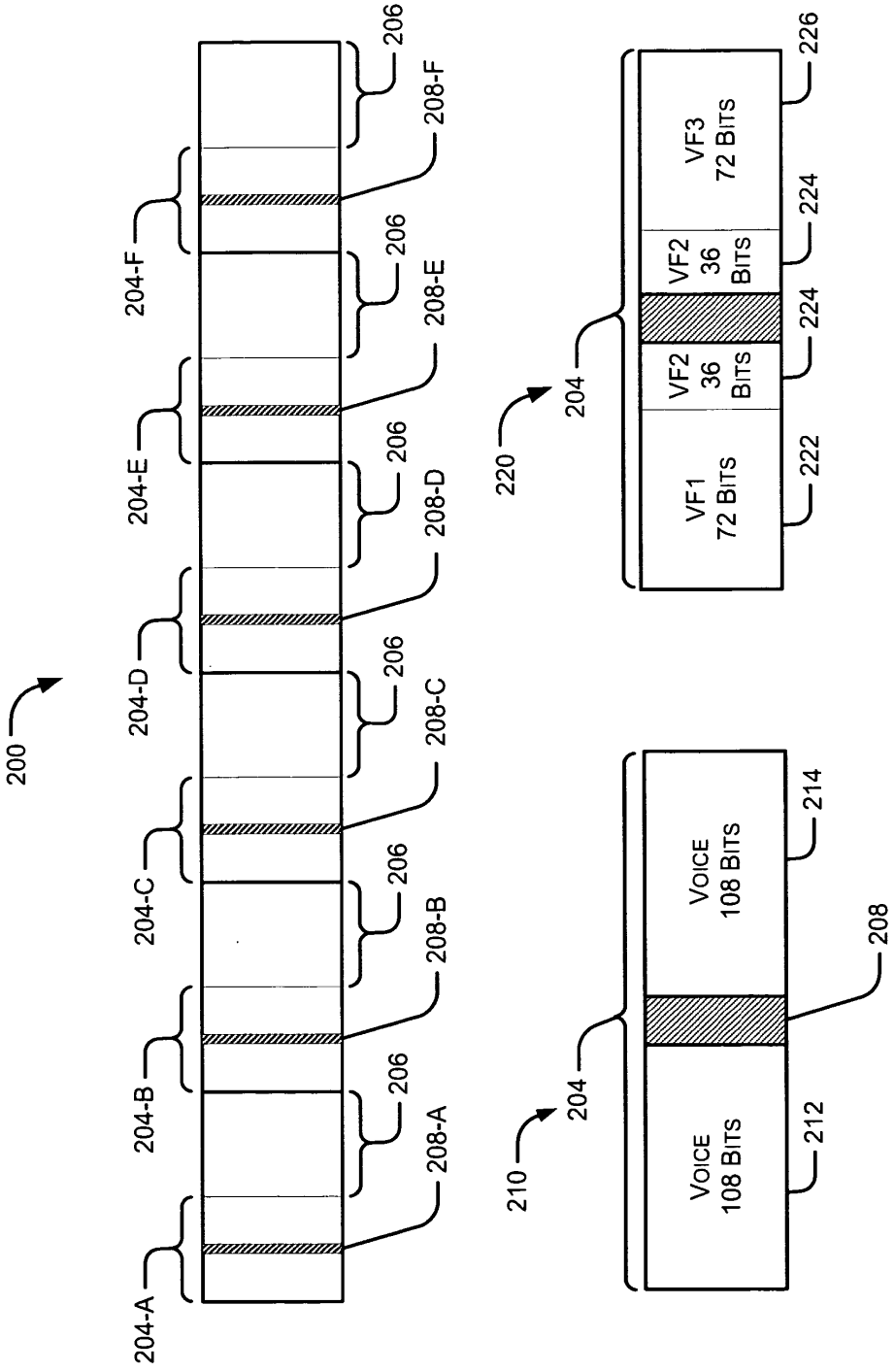
200
204-A
204-B
204-C
204-D
204-E
204-F
206
208-A
208-B
208-C
208-D
208-E
208-F
210
212
214
208
VOICE
108 BITS
VOICE
108 BITS
220
222
224
226
VF1
72 BITS
VF2
36
BITS
VF2
36
BITS
VF3
72 BITS

FIG. 2

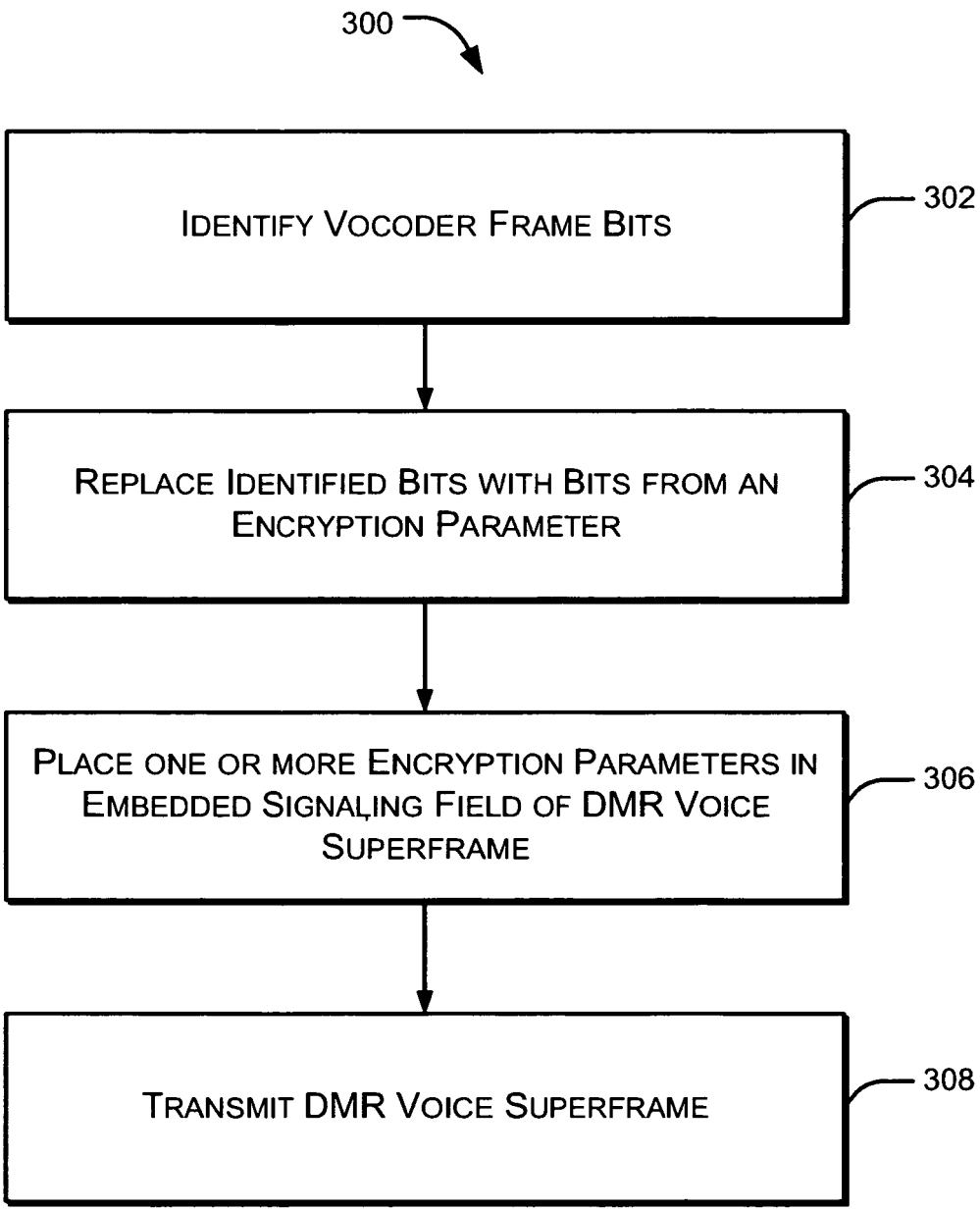
300
IDENTIFY VOCODER FRAME BITS
302
REPLACE IDENTIFIED BITS WITH BITS FROM AN ENCRYPTION PARAMETER
304
PLACE ONE OR MORE ENCRYPTION PARAMETERS IN EMBEDDED SIGNALING FIELD OF DMR VOICE SUPERFRAME
306
TRANSMIT DMR VOICE SUPERFRAME
308

FIG. 3

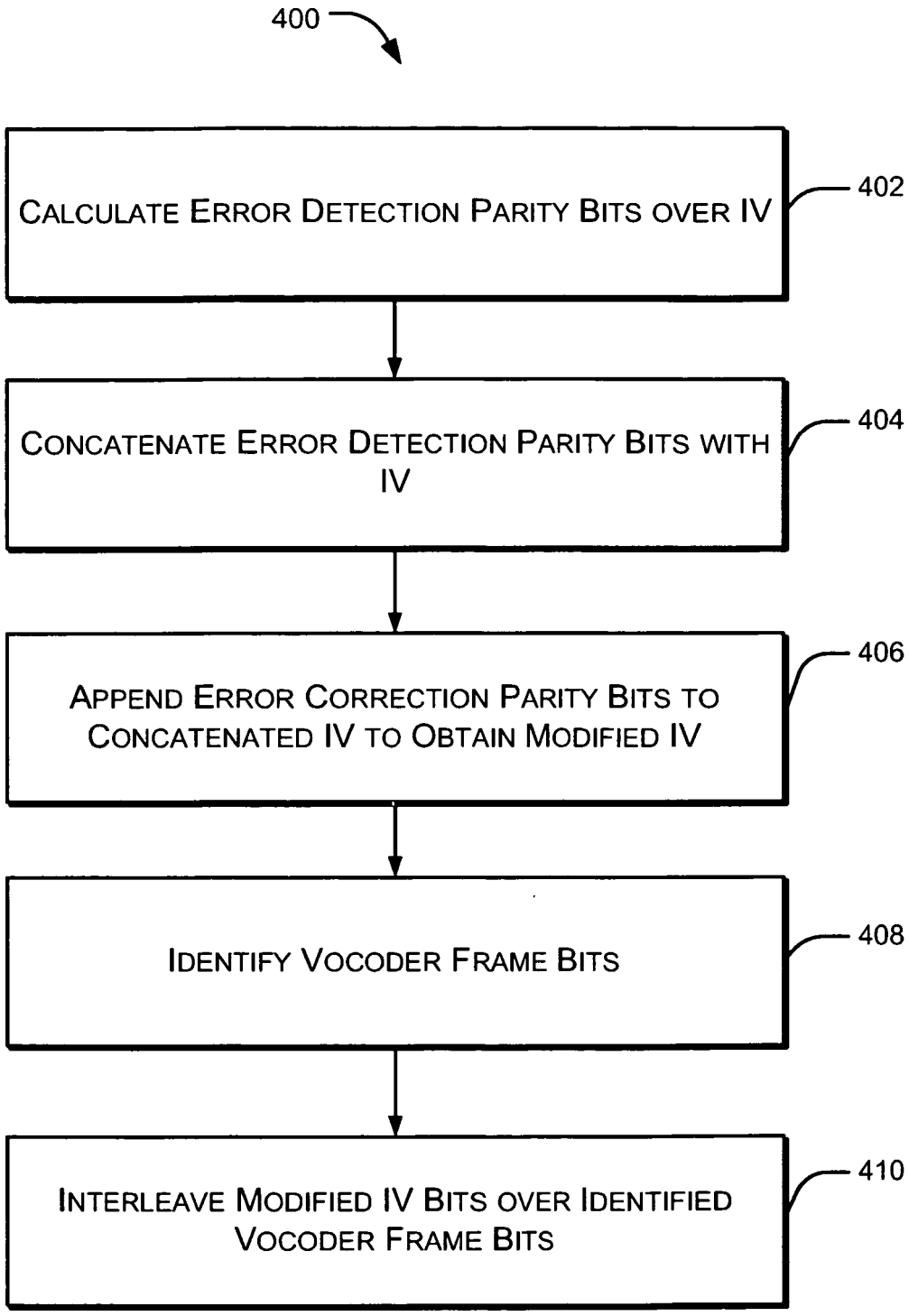
400
CALCULATE ERROR DETECTION PARITY BITS OVER IV
402
CONCATENATE ERROR DETECTION PARITY BITS WITH IV
404
APPEND ERROR CORRECTION PARITY BITS TO CONCATENATED IV TO OBTAIN MODIFIED IV
406
IDENTIFY VOCODER FRAME BITS
408
INTERLEAVE MODIFIED IV BITS OVER IDENTIFIED VOCODER FRAME BITS
410

FIG. 4

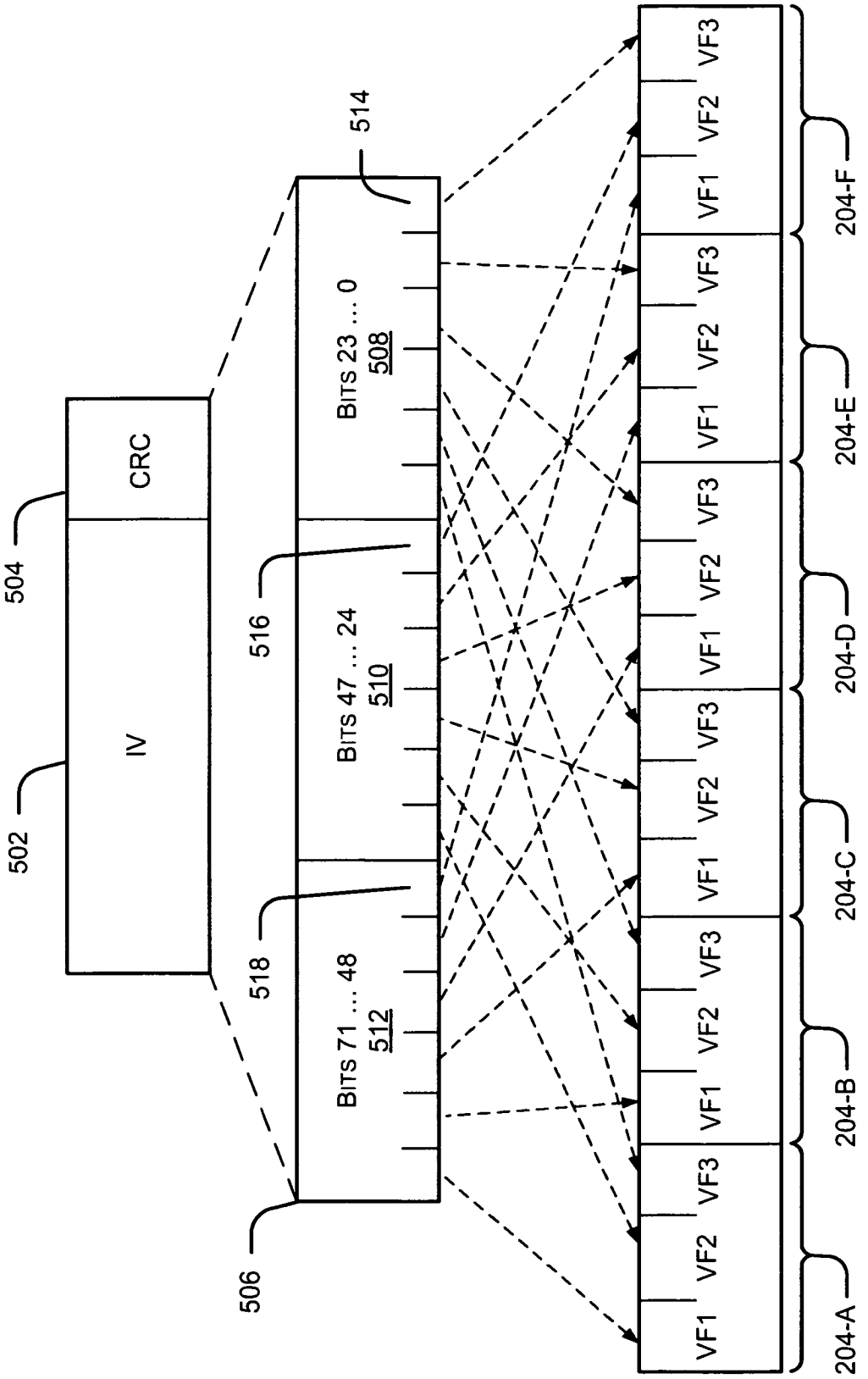
CRC
IV
504
502
506
516
518
514
BITS 23 ... 0
508
BITS 47 ... 24
510
BITS 71 ... 48
512
VF1
VF2
VF3
204-A
204-B
204-C
204-D
204-E
204-F

FIG. 5

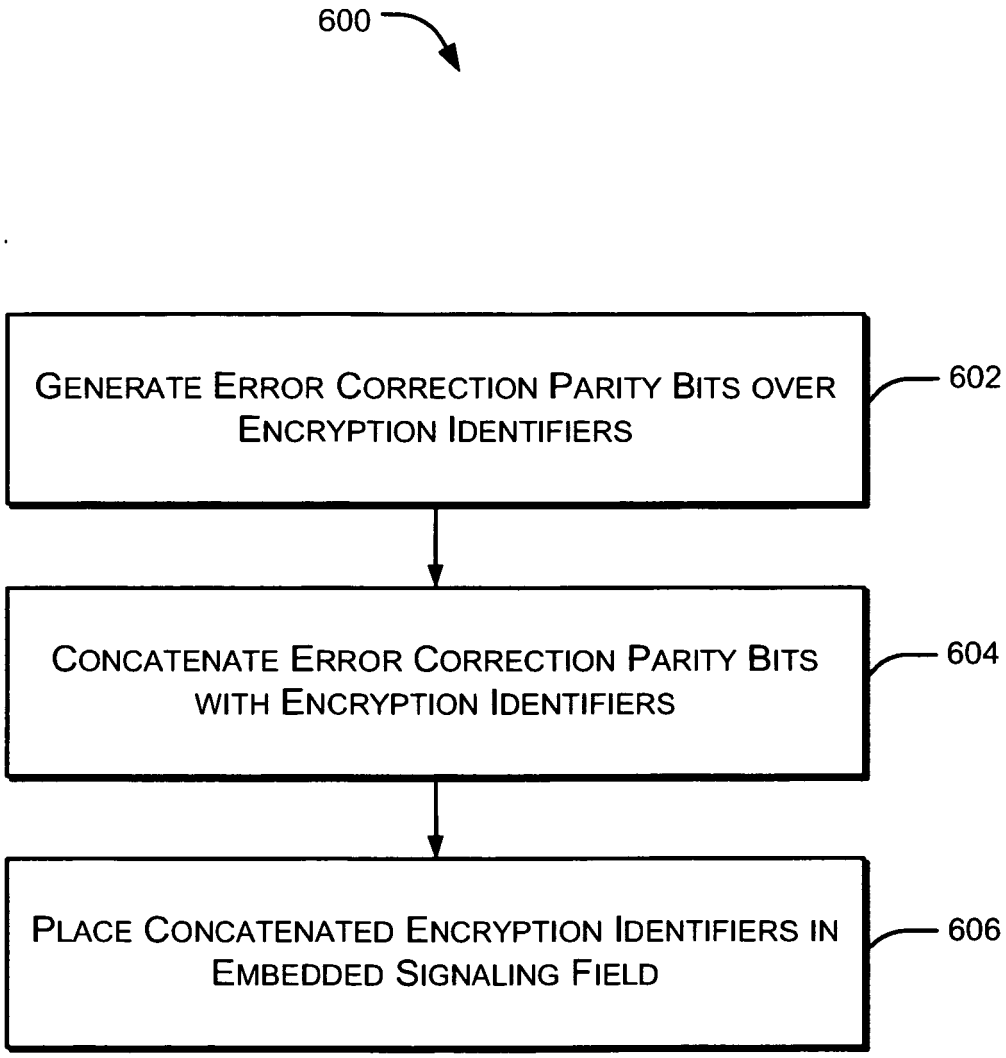
600
GENERATE ERROR CORRECTION PARITY BITS OVER ENCRYPTION IDENTIFIERS
602
CONCATENATE ERROR CORRECTION PARITY BITS WITH ENCRYPTION IDENTIFIERS
604
PLACE CONCATENATED ENCRYPTION IDENTIFIERS IN EMBEDDED SIGNALING FIELD
606

FIG. 6

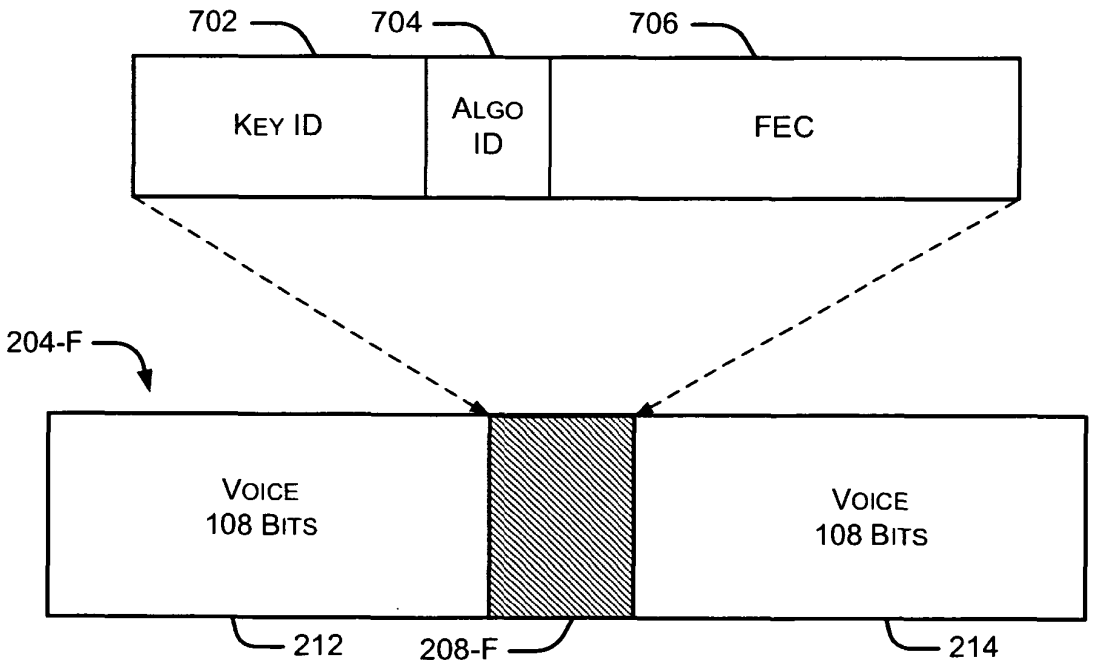
702
704
706
KEY ID
ALGO ID
FEC
204-F
VOICE 108 BITS
VOICE 108 BITS
212
208-F
214

FIG. 7

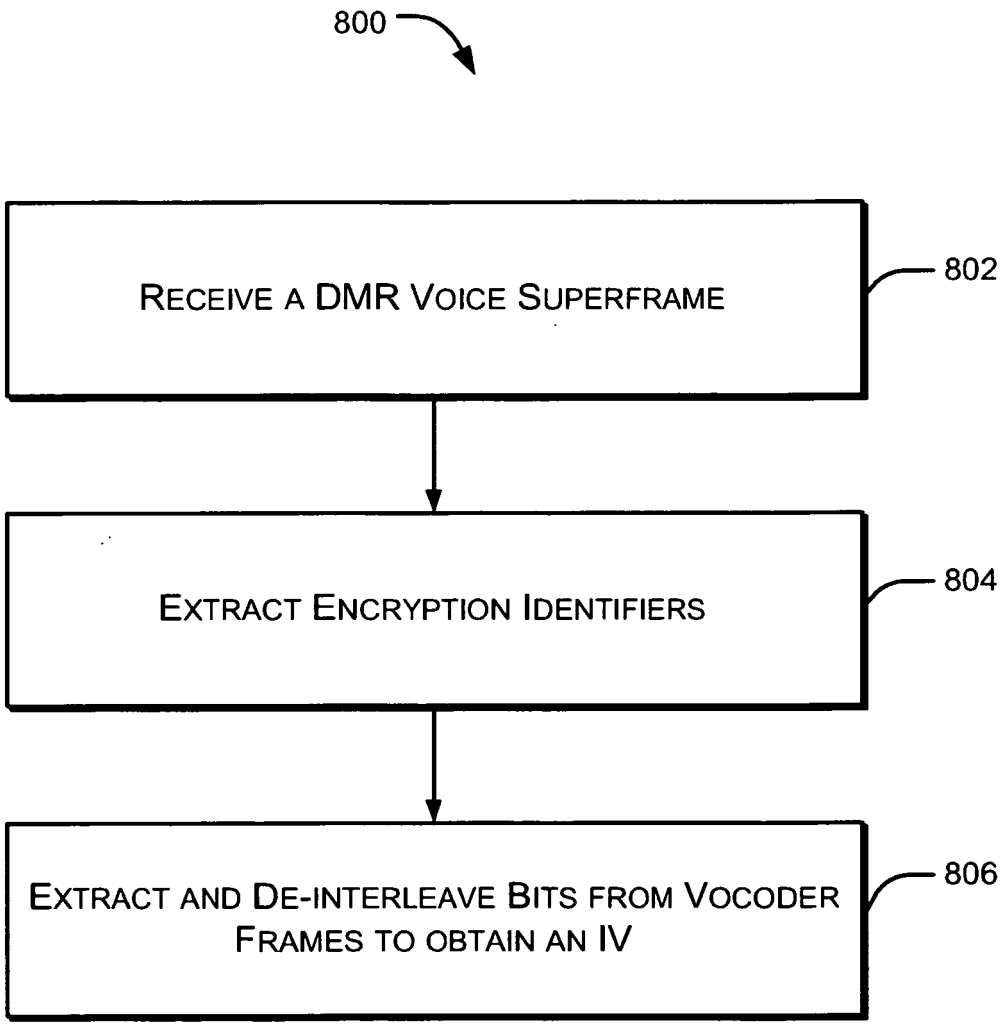
800
RECEIVE A DMR VOICE SUPERFRAME
802
EXTRACT ENCRYPTION IDENTIFIERS
804
EXTRACT AND DE-INTERLEAVE BITS FROM VOCODER FRAMES TO OBTAIN AN IV
806

FIG. 8