



[12] 发明专利说明书

[21] ZL 专利号 93106099.0

[51]Int.Cl⁶

H04B 7/26

[45]授权公告日 1996年1月31日

[24]颁证日 95.10.15

[21]申请号 93106099.0

[22]申请日 93.5.22

[30]优先权

[32]92.5.22 [33]US[31]07/888,685

[73]专利权人 摩托罗拉公司

地址 美国伊利诺斯

[72]发明人 查尔斯·约翰·马利克

格雷格·吉尔伯特·格雷昂德

H04L 7/02

[74]专利代理机构 中国国际贸易促进委员会专利商

标事务所

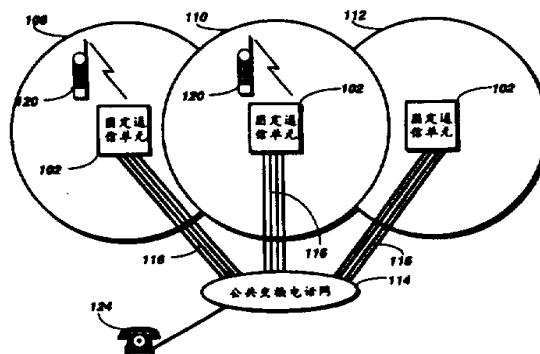
代理人 杨国旭

权利要求书 4 页 说明书 15 页 附图页数 5 页

[54]发明名称 在无线通信系统中越区切换时保持连续同步加密和解密的方法和设备

[57]摘要

在一个无线通信系统中包含有一组固定通信单元和便携式通信单元，其中每一个都包含有一个加密同步计数器，便携式通信单元和固定通信单元有一种数据发送格式，保持越区切换时间同步加解密的方法，包括以下步骤：(a)在越区切换初始化期间，装入持续值作为第二个固定通信单元加密同步计数器的内容；(b)在越区切换完成时刻从持续值开始同步增加第二个固定通信单元加密同步计数器和便携式通信单元加密同步计数器。



权 利 要 求 书

1. 在无线通信系统中保持信息的同步加解密在越区切换时不被中断的便携式通信单元(PCU)(120),该系统包括一组固定通信单元(FCUS)(102),每个固定通信单元(FCU)(102)包括一个FCU加密同步计数器(ESC)(314),和至少一个包括一个PCU加密同步计数器(ESC)(414)的便携式通信单元(PCU)(120)和固定通信单元(102)包括能发生和接收有一定数据格式(201)的信息发射的装置,这种数据格式包括至少一个发送通道和一个接收通道的时分多工,该至少一个发送通道和至少一个接收通道被搬移到单一的射频载波上,这种数据格式(201)还包括一种用来发射同步的周期性重复的同步标志(204),便携式通信单元(PCU)(120)其特征在于更进一步包括:

第一处理器装置(404),用来计算和转换一个持续值(419)和越区切换完成时间(420),并把它们转换到固定通信单元(102)中,这个持续值包括在越区切换完成时便携式通信单元的加密同步计数器中的期望值;

连接到便携式通信单元加密同步计数器(ESC)(414)用来增加便携式通信单元加密同步计数器(ESC)(414)值的增量装置;

用来响应从固定通信单元(102)接收的主同步信号(204),同

步便携式通信单元加密同步计数器 ESC(414) 的增量, 连接到递增设备(415)的同步设备(408)。

2. 根据权利要求 1 所述的便携式通信单元(PCU)(120), 其特征在于进一步包括连接到便携式通信单元加密同步计数器(414)上, 把预定义的起始值装入便携式通信单元加密同步计数器(414)的初始化设备(404, 418)。

3. 根据权利要求 2 所述的便携式通信单元(PCU), 其特征在于进一步包括:

连接到初始化装置(418, 404)的起始值加密装置(418, 404), 用予先定义的加密过程加密起始值; 和

连接到起始值加密装置(418, 404), 把加密后的起始值装入固定通信单元(102)的第二处理器装置(404)。

4. 在无线通信系统中, 用来保持信息的同步加解密在越区切换不受中断的固定通信单元(FCU)(102), 该系统包括: 一组固定通信单元(FCUS)(102)和至少一个便携式通信单元(PCU)(120), 每一个固定通信单元(102)包括一个 FCU 加密同步计数器(ESC)(314), 至少一个便携式通信单元(120)的每一个包括一个 PCU 加密同步计数器(ESC)(414), 便携式通信单元和固定通信单元包括发生和接收具有一种数据格式(201)的信息发射的装置, 这种数据格式包括至少一个发送通道和至少一个接收通道的时分多工, 该至少一个发送通道和至少一个接收通道被搬移到单

一的射频(RF)载波上,数据格式(201)还进一步包括用来同步发送的周期性重复的同步标志(204),固定通信单元(102)其特征在于还进一步包括:

用来存储便携式通信单元发送的持续值(320)和越区切换完成时间(318)的存储器装置(316);

连接到存储器装置(316),在越区切换完成时,把持续值(320)装入固定通信单元加密同步计数器(ESC)(314)的第一处理器装置(304);

连接到第一处理器装置(304)和固定通信单元加密同步计数器(ESC)(314)上,用来从越区切换完成时间起增加固定通信单元加密同步计数器(314)的增量装置;和

用来响应主同步信号的接收,同步固定通信单元的加密同步计数器(ESC)(314)的增量计数的同步装置(307)。

5. 根据权利要求4所述的固定通信单元(FCU)(102),其特征在于还进一步包括:连接到固定通信单元FCU加密同步计数器ESC(314)上的用来把起始值从便携式通信单元(120)装入固定通信单元加密同步计数器(ESC)(314)的初始化装置(302,308,304)。

6. 根据权利要求5所述的固定通信单元,其特征在于初始化装置(302,308,304)还包括:

连接到初始化装置(302,308,304),通过预先定义的解密过程,解密起始值的解密装置(304,316)。

连接到解密装置(304,316),用来把解密后的起始值装入固定通信单元加密同步计数器 *ESC*(102)的第二个处理器装置(304)。

说 明 书

在无线通信系统中越区切换时保持 连续同步加密和解密的方法和设备

本发明一般涉及一种无线电通讯系统，特别是涉及一种双通道无线电通讯系统，它包括进行同步加密和解密的方法与设备。

用于全双工数字无线通信系统的同步计数器驱动加密技术是已知的。这种系统在每个通信单元里，通常采用分离的加密和解密装置对发射和接收通道分别进行加密和解密。在每个通讯单元里，采用分离的加密和解密设备，使通讯单元成本昂贵，体积庞大，同时也使两种设备间的同步复杂化。

为了在两个链接的通信单元之间保持同步，常规的系统必需在发射加密信息的同时，发送一个加密同步信号($E\text{-sync}$)，当被发送信息为可被任意中断的存贮数据时，发送加密同步信号($E\text{-sync}$)是不成问题的。另一方面，在话音通信系统中发送 $E\text{-sync}$ 在某种程度上就变得困难了，因为声音信息是连续的，不可能被 $E\text{-sync}$ 发送周期性地中断而在接收音频信号中不产生引人注意的间断或噪声脉冲。

一些常规的声音加密系统周期性地从声音信息里“挪用”比特，

使用挪用的比特发送 $E\text{-sync}$, 这种理论是: 如果仅是不经常地比特挪用, 这些比特的缺少将不会严重影响话音。但是, 丢失的比特仍会在某种程度上降低话音质量, 引起根据使用挪用的话音比特的加密系统在话音质量的主观测试方式方面, 加密模式看作未加密模式即“透明”(Clear)模式。

在无线通讯系统中, 由常规加密技术在将一个便携式通信单元(PCU)从一个固定通信单元越区切换到另一个固定通信单元(FCU)遇到的问题与越区切换工作过程有关。当连接两个通讯单元时, 其中每一个通讯单元的发送路径的加密装置在其它通讯单元的相应接收路径的加密装置提供加密同步信号($E\text{-sync}$)。因此, 当越区切换到一个新的 FCU 后, 加密同步将消失一段时间, 在这期间, PCU 中的加密装置和来自新的 FCU 中的新的 $E\text{-sync}$ 重新同步, 并使新的 FCU 中的加密装置和来自 PCU 的 $E\text{-sync}$ 重新同步。

由于越区切换重建同步的时间里, 加密同步信号的丢失将引起所有通讯信息的丢失, 用来发送连续信息例如声音的常规加密系统在每次越区切换前先回复到清零模式, 在重建加密同步所需充足时间完全过去以后, 重新转换到加密模式。这自然造成了在每次越区切换时伴随有短暂的发射信息可靠性受损害的时间。

因此, 就需要有一种加密技术克服前述的常规加密技术上的问题。这也就是说, 需要有一种在越区切换时能在加密模式连续工作的无信息丢失的加密技术。需要有一种不降低声音质量的加密

技术,而且,需要有一种比常规加密技术所需的成本和体积都小的技术。

在无线通信系统中,保持信息的同步加密和解密在完成越区切换时不受中断的方法包括一组固定通信单元(*FCUS*)和至少一个便携式通信单元(*PCU*),固定通信单元(*FCUS*)包括一个固定通信单元(*FCU*)加密同步计数器(*ESC*),便携式通信单元包括(*PCU*)一个便携式通信单元加密同步计数器(*PCU ESC*),*PCU*和*FCU*用于产生和接收具有数字结构并包括一个周期性重复的同步标志的用于同步发射的信号。此方法包括下列几步:

a)为接收从和第一个*FCU*的第一无线连接到与第二个*FCU*的第二天线连接的*PCU*的越区切换,在一个*PCU*和第二个*FCU*之间的无线联系建立后,向第二个*FCU*中的第二个*FCU ESC*的内容装入一个连续的值,此连续值中包括越区切换后在*PCU ESC*中希望得到的值。

b)在越区切换完成后*PCU ESC*和*FCU ESC*以步骤(a)中加装的连续值为起点开始同步增加。

图1是根据本发明的最佳实施例的一种无线电通信系统框图。

图2是根据本发明的最佳实施例遵守数字欧洲无绳电信 *Digital European Cordless Telecommunications (DECT)* 标准构成时分多路复用和时分双工的帧内容。

图3是根据本发明的最佳实施例的固定通信单元(*FCU*)的框

图。

图 4 是根据本发明的最佳实施例的一个便携式通信单元(PCU)的框图。

图 5 是根据本发明的最佳实施例的加密同步计数器(ESC)的框图。

图 6 是根据本发明最佳实施例所述的产生单个加密序列的影响信息的同步加解密方法的流程图。

图 7 是根据本发明最佳实施例所述的实现的在越区切换时保持信息的同步加密和解密不被中断的方法的流程图。

参看图 1, 根据本发明的最佳实例的一种无线电通信系统包含有一组固定通信单元(FCUS)102, 为一组射频覆盖区域 108, 110, 112 提供射频覆盖。FCU 通过一组电话线 116 连接到公共电话交换网(PSTN)114。本领域的技术人员知道: 根据本发明的无线通信系统不仅仅用于公共电话交换网(PSTN), 也用于象和用分支电话局这样的电话系统。而且, 该系统包括至少一个有越区切换能力, 能以时分多路复用和时分双工(TDMA/TDD)数字格式发送和接收的便携式通信单元(PCU) 120, 该系统还至少包含有一个有线电话机 124, 用于向便携式通信单元(PCU)120 发送呼叫和从便携式通信单元 120 接收呼叫。一个便携式通信单元 120 可以通过一个或多个固定通信单元(FCIS)102 中的其它便携式通信单元通信。

根据本发明, 进一步实现无线通信系统在多个 FCU 和至少一

个 *PCU* 之间通信标准协议的使用。该标准协议定义了用于请求和重建无线电通信链路的消息和规程,用于发送和接收信号数据,用来发送和接收用户通信信息,用来定义这里使用的时分多路复用和时分双工的格式。象这样的一个标准协议的例子是数字欧洲无绳电信 (*PECT*) 标准。该 *DECT* 标准是在欧洲电信标准文件 *prETS-300175* 题为“数字欧洲无绳电信公共接口”中定义的,是在 1991 年 8 月,由欧洲电信标准协会制定,文件中应用部分 2,3,5,7 合并为参考文件。

参看图 2,根据本发明的最佳实施例,并根据 *DECT* 标准构成的一个时分多路复用/时分双工帧结构 201 包含十二个时隙 202 用于固定通信单元 (*FCU*) 发射和十二个时隙 203 用于移动通信单元发射。时隙 202,203 以发射和接收信息的位置为基准组织在一起。例如,一个固定通信单元 102 (图 1) 在标号为“0”的时隙 202 发射信息,在标号为“0”的时隙 203 接收信息,每个时隙 202,203 都包含有一个同步部分 204 和一个数据部分 205。其中间同步部分包含了用于一条便携式通信单元 (图 1) 120 和固定通信单元 102 之间链路同步的同步标志。数据部分 205 包含有一个控制部分 206 和一个用户数据部分 208,其中控制部分 206 用于传送控制信息,也就是便携式通信单元 120 固定通信单元 102 之间链接的帧标志,时隙鉴别和其它控制信息,用户数据部分用于携带用户数据,例如演讲。

根据本发明,同步部分 204 和控制部分 206 用来同步携带在用

户数据部分 208 之中的信息的加解密,还用来同步携带在控制部分 206 中的用户信号。通过使用 *DECT* 时隙 202,203 的现存部分 204, 206 来同步加密和解密过程,没有必要从用户数据部分 208 中挪用比特。因此根据本发明,这种加密和解密技术不会象常规的采用比特挪用来同步的加解密技术、那样降低话音质量。通过在固定通信单元 102 和便携式通信单元 120(图 1)获得同步信号来同步加解密电路,较少的部分需要用来同步,从而减小了便携式通信单元 (*PCU*)120 和固定通讯单元 102 的成本和体积。

在操作上,在固定通信单元 (*FCU*)102 和便携式通信单元 (*PCU*)120 内的时分多址/时分双工 (*TDMA/TDD*)电路(这里顺序描述)的帧同步部分,使得当控制部分 206 包含用户信号信息时,在控制部分 206 发射和用户数据部分 208 发送期间,信息的加解密成为可能时分多址/时分双工 (*TDMA//TDD*)电路使得在发送所有其它部分期间加解密不可能实现。

参看图 3,根据本发明,固定通信单元 102(图 1)的一个最佳实施所述包含一个射频(*RF*)收发信机 302,用于发射和接收包含有以时分多址/时分复用 (*TDMA/TDD*)格式发射和接收的数字信息的射频信号。射频收发信机通过总线 306 连接到微处理器 304 上,微处理器 304 用来控制收发信机 302。微处理器 304 通过总线 306 连接到系统的帧同步电路 307,帧同步电路 307 用来保持系统内所有固定通信单元 (*FCUS*)之间的帧同步,帧同步电路 307 终端 305 接收

主系统同步信号。如果同公共电话交换网 114 和一组固定通信单元 102(图 1)之间的不同延迟得到调整以后,主同步信号可以从例如其中的同步标志中获得。

射频(RF)收发信机 302 也被连接到时分多地/时分双工(TDMA/TDD)电路 308, TDMA/TDD 电路 308 通过模二累加器 309 把射频收发信机 302 和用于完成由固定通信单元(FCU)102 发送和接收信号的音频到数字和数字到音频的转换的编译码器(CODECS)310 连接起来。这一组编译码器(CDDECS)310 被连接到一组电话接口 312 上,该电话接口 312 用于把一组电话线 116 连接到编译码器 310 上。模二累加器 309 被连接到加密同步计数器(ESC)314 上,加密同步计数器(ESC)314,由工作在速率为编译码器 310 和时分多址/时分复用(TDMA/TDD)电路 308 的串行比特率的增时钟发生器 315 驱动,模二累加器 309 也通过时分多址/时分复用(TDMA/TDD)电路 308 与主系统同步信号同步,为本发明所述为通过编译码器 310 与 TDMA/TDD 电路 308 之间的信息提供加解密。

时分多址/时分双工电路(TDMA/TDD)308,编译码器(CODECS)310,增时钟发生器 315,加密同步计数器(ESC)314 和电话接口 312 都连接到通过微处理器 304 提供控制的总线 306 上。存储器 316 也连接到微处理器上,用来存储程序控制软件和两组数值,一组存贮位置 320 为加密同步计数器(ESC)内容保留,另一组

存贮位置 318 为越区切换完成时间保留, 两组相应的存贮位置 320、318 中的每一组都与相应的固定通信单元 102 使用的成对接收和发射的时分多地/时分双工(TDMA/TDD)时隙 202, 203(图 2)有关。

当成对接收和发送 TDMA/TDD 时隙 202, 203(图 2)中的一个携带用户信息时, 在每个 TDMA/TDD 时隙 202、203 末端的加密同步计数器(ESC)的内容值被存贮在相应的成对接收和发送 TDMA—TDD 时隙 202、203 专为加密同步计数器 ESC 内容值保留的存贮位置 320 上, 然而专为越区切换完成时间保留的存贮位置 318 未被使用。存贮在专为加密同步计数器(ESC)内容保留的位置 320 上的值则用来在下一个相应的成对接收和发送时隙 202、203 的开始刷新加密同步计数器(ESC), 根据本发明, 如同以上描述那样, 通过使用存贮器 316, 单个加密同步计数器(ESC)提供了在整个固定通信单元使用的全部 TDMA/TDD 时隙 202, 203 上信息的加解密, 因此降低了固定通信单元(FCU)的成本和体积。

当一个发送/接收时隙对没有携带用户信息仅仅等待一个链接的开始或者正在进行中的越区切换的完成时, 对应于等待时隙对专为加密同步计数器 ESC 内容保留的存贮器位置 320 用来贮存一个 PCU 发送影响链接开始的开始值或者影响正在进行的越区切换的连续值。根据本发明, 只要有一个正在进行的越区切换指向 TDMA—TDD 时隙对时, 对应于 TDMA—TDD 时隙对用于越区切换完成

时间的存储器位置 318 就用来控制越区切换的时间。

参看图 4, 根据本发明的最佳实施例, 便携式通信单元 (PCU) 120 包括一个射频 (RF) 收发信机 402, 用来发射和接收包含有以时分多址/时分双工 (TDMA/TDD) 格式发射或接收的数据信息的射频信号。射频收发信机连接到微处理器 404 上, 微处理器 404 通过总线 406 控制收发信机 402。射频收发信机 402 也连接到时分多址/时分双工 (TDMA/TDD) 电路 408 上, TDMA/TDD 电路 408 通过模二累加器 409 将射频收发信机 402 编码器 (CODEC) 410 连在一起。CODEC 用于将便携式通信单元 120 发送和接收信号分别进行音频到数字和数字到音频的转换。模二累加器也被连接到由发生器 415 驱动的加密同步计数器 (ESC) 414 上, 增时钟计数器 (ESC) 414 以编码器 (CODEC) 410 和时分多址/时分双工 (TDMA/TDD) 电路的串行数据速率工作, CODEC 410 用来提供在 CODEC 410 和 TDMA-TDD 电路 408 之间传递信息的加解密。通过使用单个加密同步计数器 (ESC) 414 进行 TDMA/TDD 信息的加解密, 同常规的使用分离发送和接收设备的加解密技术相比, 便携式通信单元的成本和体积都降低了。

增时钟发生器 415 通过时分多址/时分双工 (TDMA/TDD) 电路 408 与从固定通信单元 (FCU) 102 的无线链路接收来的帧同步信号标志同步, 而该帧同步信号标志在固定通信单元 (FCU) 区内通过终端 305 (图 3) 的主系统同步信号同步。编码器 CODEC 410 被连

接到用于向便携式通信单元 120 的一个用户发送信息和从便携式通信单元 (PCU) 120 的一个用户接收信号的音频接口上。时分多址/时分双工 (TDMA/TDD) 电路 408, 编译码器 (CODEC) 410, 增同步时钟发生器 415, 加密同步计数器 (ESC) 414 和话音接口 412 也被连接到微处理器 404 提供控制的总线 406 上, 存贮器 418 也连接到微处理器 404 上, 用来存贮程序控制软件, 还分别存贮加密同步计数器内容 419 和越区切换完成时间 420 的值, 存贮器 419, 420 上的值由微处理器决定, 从一个便携式通信单元发送到一个固定通信单元, 根据本发明, 这两个值用于链接起点值和链路越区切换。用来显示从微处理器 404 发送信息的显示器 417 也连接到微处理器 404 上, 用来接收用户输入的控制信号的键盘也连接到微处理器 404 上。

参看图 5, 根据本发明, 加密同步计数器 (ESC) 314, 414 的最佳实施例包括有一个并行数据输入口 504 的一个移位寄存器 502, 移位寄存器 502 的并行口使能端 (PE) 506, 允许并行数据输入口 504 把来自微处理器 304, 404 (图 3, 图 4) 的起始值和持续值装入移位寄存器 502。根据本发明, 移位寄存器 502 有一个由增时钟发生器 315, 415 (图 3, 图 4) 驱动的时钟输入端 508, 微处理器 304, 404 使能时钟使能端 510, 允许或禁止在编译码器 (CODECS) 310, 410 和时分多址/时分双工 (TDMA/TDD) 电路 308, 408 (图 3, 图 4) 传递信息两加密和解密。移位寄存器被用作线性反馈移位寄存器, 把它的最后一级输出 512 和中间输出 518、514 通过模二累加器 516, 520 反馈

到它的串行数据输入端 522,这样连接,该移位寄存器在最后一级输出 512 产生一个预先定义的中行比特序列,用来同步信息的编解码。

更为可取的是,为了获得更大的可靠性,在最后一级输出口 512 输出的串行比特序列被送往一个密钥流产生算法装置 524,此送密钥流产生算法装置由微处理器 304,404(图 3,图 4)从一个 KV 口提供的密钥变量初始化,在最后输出端 526 产生一个可靠加密序列。象这样的装置有位于伊利诺沙,绍姆堡的莫托罗拉公司(Inc. of Schaumburg, Illinois、)生产 TRN4836A 装置。在最后输出端 526 输出的串行信号在模二累加器 309,409(图 3,图 4)被累加,用来完成固定通信单元 102 和便携式通信单元 120 发送接收信息的加解密。

更为可取的是,在固定通信单元 102 里,一个分离唯一的密钥变量是用于每个时分多址/时分双工(TDMA/TDD)时隙对 202、203(图 2),每个 TDMA/TDD 时隙对 202, 203 的分离的且唯一的密钥变量被存储在存储器 316(图 3)中,在每个相关联的时分多址/时分双工(TDMA/TDD)开始由微处理器 304(图 3)转移到 KV 口 528,象刚才描述的那样,在固定通信单元 102 里,每个时隙对的分离唯一的密钥变量的使用提供了更大程度的加密可靠性,同时仍然允许使用包含单个密钥流产生算法装置的单个加密计数器 ESC,产生所有的时分多址/时分双工 202,203。

参看图 6,根据本发明的一种最佳实施例,通过产生单个的加密

序列影响信息的同步加解密的方法包括在固定通信单元(FCU)102(图1)中接收在便携式通信单元120(图1)和固定通信单元(FCU)102之间建立链路时来自便携式通信单元120(图1)的登记信息,该登记信息包含一个加密的用户识别码(CPIN),作为接收登记信息后的响应,固定通信单元102用预先定义的算法解密604一个相应的用户识别码(PIN),并把用户识别码储存在专为与固定通信单元102链路时隙相应的加密同步计数器(ESC)(3)内容保留的存储位置320中,因为用户识别码也被存储便携式通信单元(PCU)120中,在固定通信单元102和便携式通信单元120中的微处理器304,404(图3,4)将在下面描述的适当时刻把用户识别码的值装入606步他们各自的加密加同步计数器(ESC)(图3,4)中。

当链路建立到准备进行用户通信时,在固定通信单元102中的微处理器304和便携式通信单元中的微处理器404把用户识别码分别装进608步加密同步计数器314,414中,同时固定发送单元102在发送时隙202(图2)发送的信号同步部分204(图2)中的下一个同步标志的开始时刻允许各自的加密同步计数器314,414的时钟使能端510。本领域的技术人员认为:只要同一信号在固定通信单元102和便携式通信单元中使用,同时启动加密同步计数314,414的时钟使能端510,便携式通信单元120在PCU发送时隙203发送信号的同步部分204也能用来启动各自的增时钟发生器315,415。

在重建链路期间,加密同步计数器(ESC)314,414的增时钟发

生器 315,415 通过时分多址/时分双工电路 308,408(图 3,4)分别同步 609,来作为对固定通信单元 102(图 1)发送信号的同步部分的同步标志重现的响应。

如本领域的技术人员熟知的那样,如果第一个串行比特流和另一个与比特串行码流速率相同并且同步的第二个伪随机串行比特流在模二累加器(异或逻辑门)中累加,就会在模二累加器的输出端产生一个新的加密串行比特流,如果这个新的(已加密)的串行比特流与和第二个伪随机)序列同步并且相同的第三个伪随机串行比特流在模二累加器二中累加,则在模二累加器二的输出端就会产生和第一个串行比特流完全一样的串行比特流。因此,本发明提供了一个通过产生单个加密序列实现信息的同步加解密的方法和设备,用于控制发生在固定通信单元 102 和移动通讯单元 120 中的加解密。

参看图 7,根据本发明的最佳实施例,保持信息的加解密在越区切换不被中断的方法包括:和第一个固定通信单元 120(图 1)链接的便携式通信单元 102 决定 701 是否有必要越区切换到中另一固定通信单元 120,然后选择过越区换完成时间,选中的越区切换完成时间与后来的由第一个固定通信单元 102 在用来链接的 FCU 发送时隙 202 发送信号的同步部分 204(图 2)中同步标志同时发生。在同一步骤 710 中紧接着是便携式通信单元 120 计算越区切换持续值,也就是在所选择的越区切换完成时刻在便携式通信单元 120 的加密同步计数器(图 4)的希望值。

下一步 702, 便携式通信单元 120 和第二个固定通信单元 102 建立第二条无线链路, 发送持续值和比选择的越区切换完成时间。因为越区切换完成时间与后来的由第一个固定通信单元在 *FCU* 发送时隙 202 发送信号的同步部分 204(图 2)中的同步标志同时发生, 还因为系统中所有的固定通信单元必须和在固定通信单元 102 中的端口 305(图 3)的主系统同步, 第二个固定通信单元 102 能够相当精确地决定越区切换的时间。

第二个固定通信单元 102(图 1)在 706 步中存贮持续值和越区切换完成时间, 在存储器位置 320 存储加密同步计数器(图 3)的内容, 而且在存储器位置 318 存贮越区切换完成时间(图 3)。存储器位置 320, 318 分别与固定通信单元 102 使用的第二条无线链路的时分多址/时分双工(*TDMA/TDD*)时隙有关。

当选定的越区切换完成时间到后, 微处理器 304(图 3)访问它的存储器 316 恢复持续值, 持续值装入 708 步中的加密同步计数器 314(图 3), 接着启动加密同步计数器(*ESC*)314 的增时钟, 启动第二个固定通信单元 102 的加密同步计数器 *ESC*, 以便便携式通信单元 120 的加密同步计数器 414(图 4)同时到达的值开始计数。

在第二条无线链路的持续期间, 第二个固定通信单元 102 的加密同步计数器 314 的增时钟发生器 315, 便携式通信单元的加密同步计数器 414 的增时钟发生器 415 分别被时分多址/时分以工(*TDMA/TDD*)电路 308, 408 彼此同步, 709 步, 响应第二个固定通信

单元 102(图 1)发送信号的同步部分 204(图 2)的周期性的同步标志。

因此,本发明包括一种实现信息的同步加解密的方法和设备,它通过产生 单个加密序列控制发生在固定通信单元 102 和便携式通信单元 120 的加解密。而且本发明包括保持信息的同步加解密在越区切换不被中断的方法与设备。因此,本发明提供了克服常规加密技术中上述问题的一种加密技术。它提供了:(a)在越区切换时能连续工作在加密模式而没有信息丢失的加密技术,(b)不进行比特挪用因此不降低语音质量的技术,(c)建立比常规加密技术成本更低,体积更小的加密系统的加密技术。

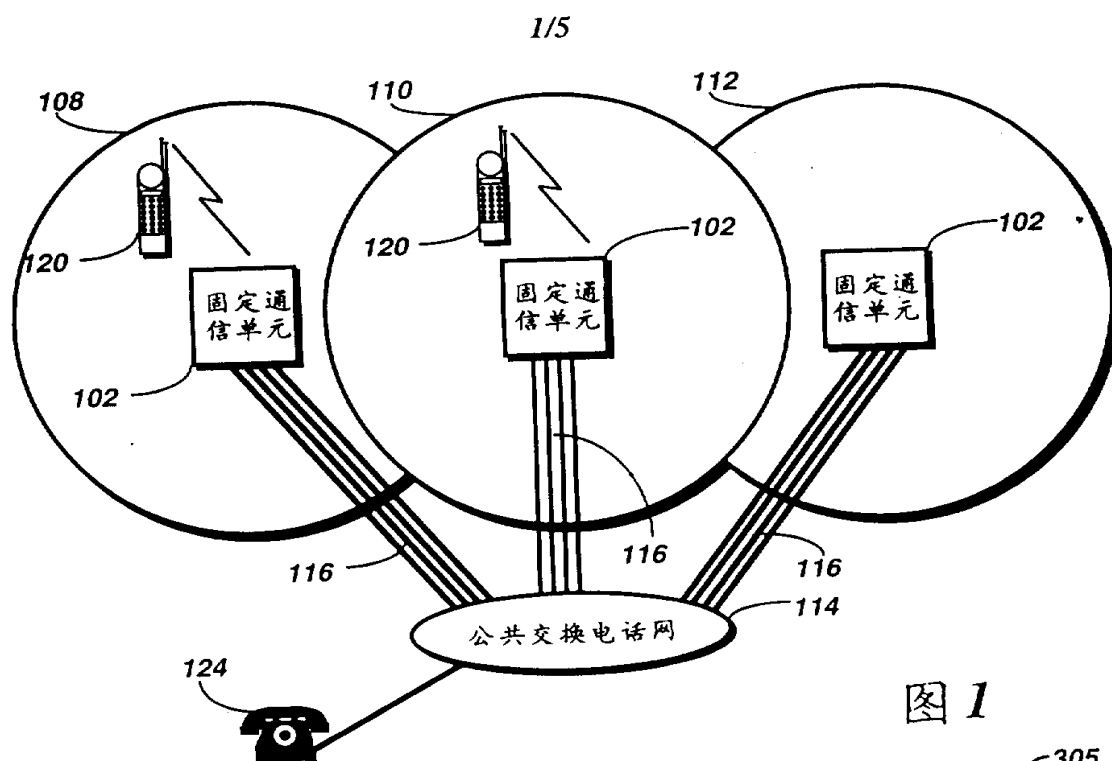


图 1

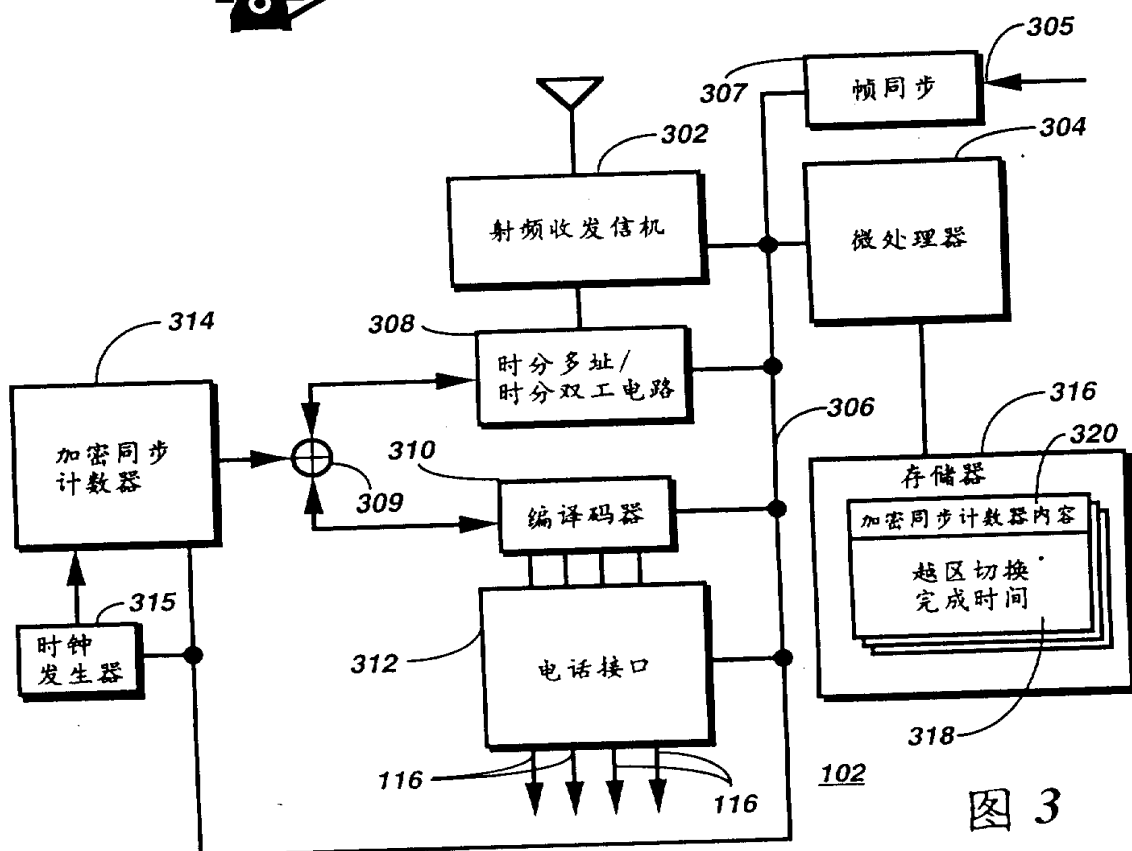


图 3

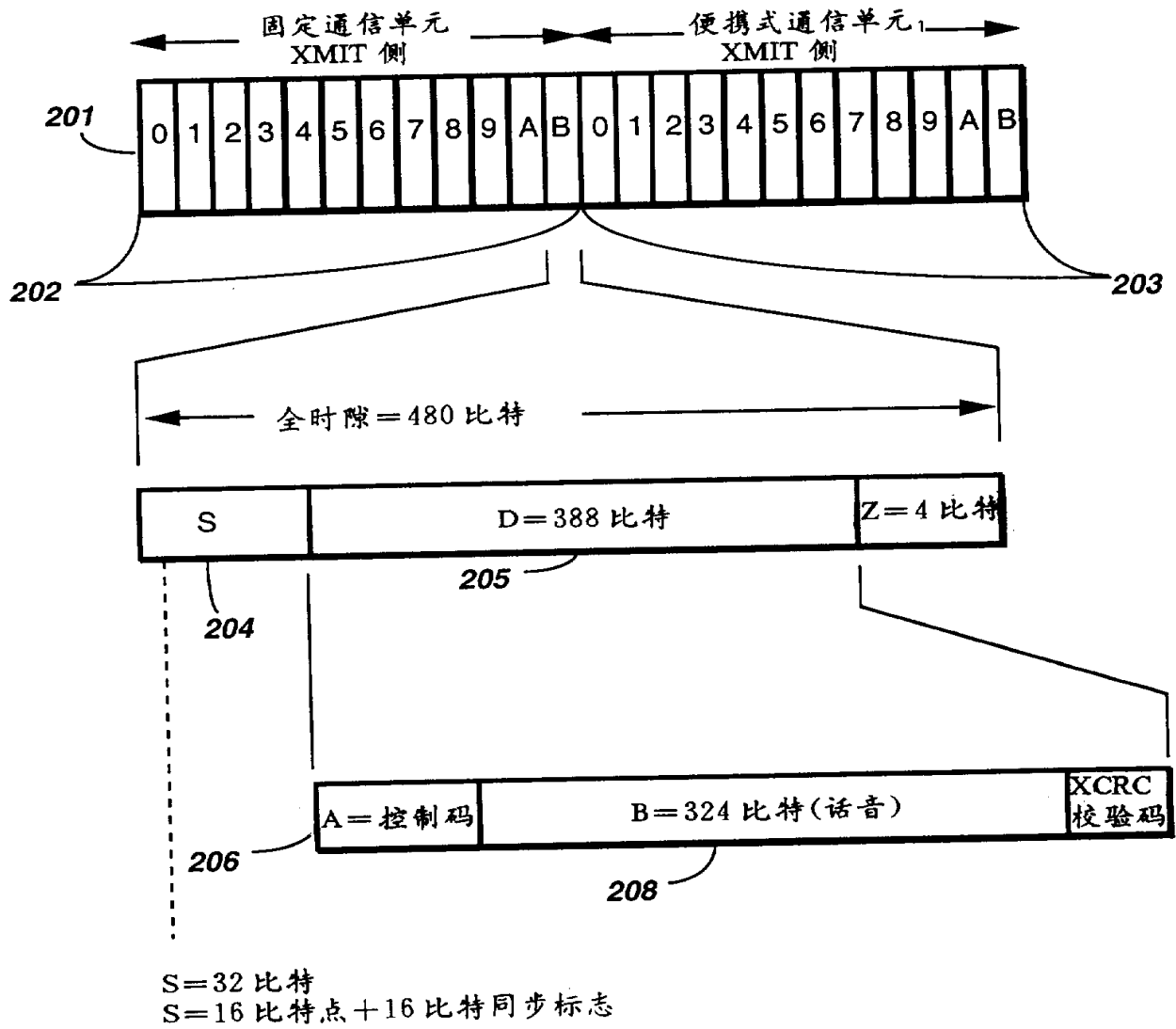


图 2

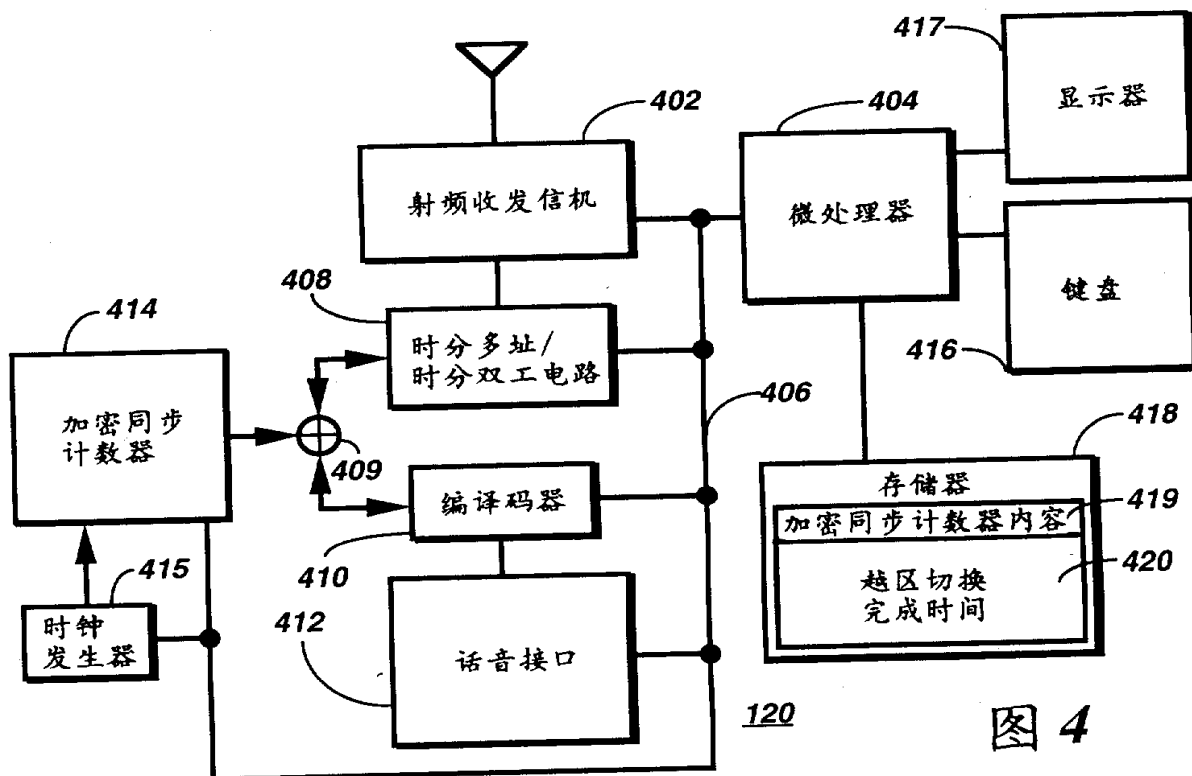


图 4

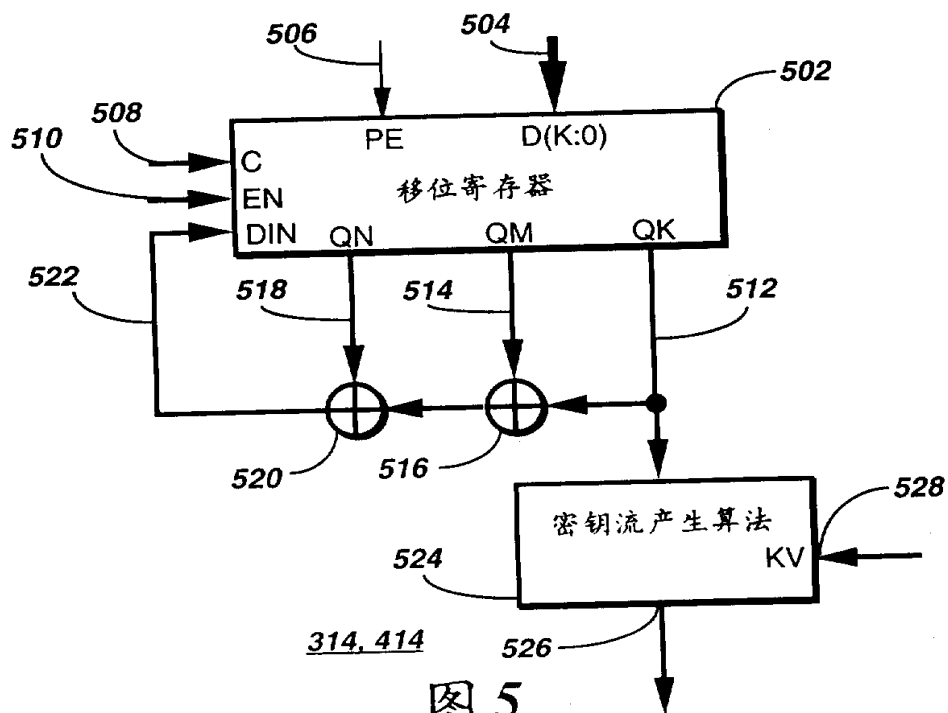


图 5

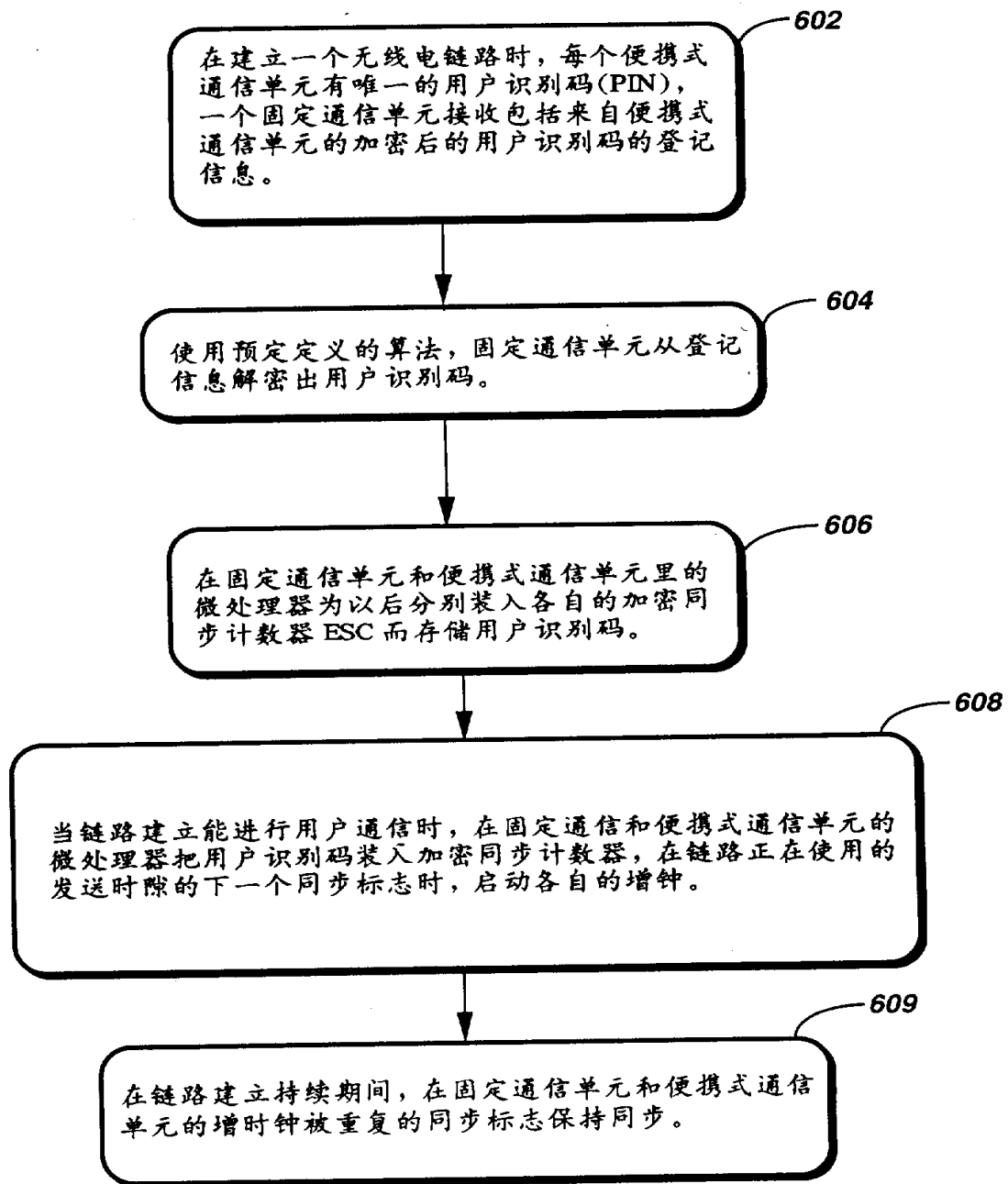


图 6

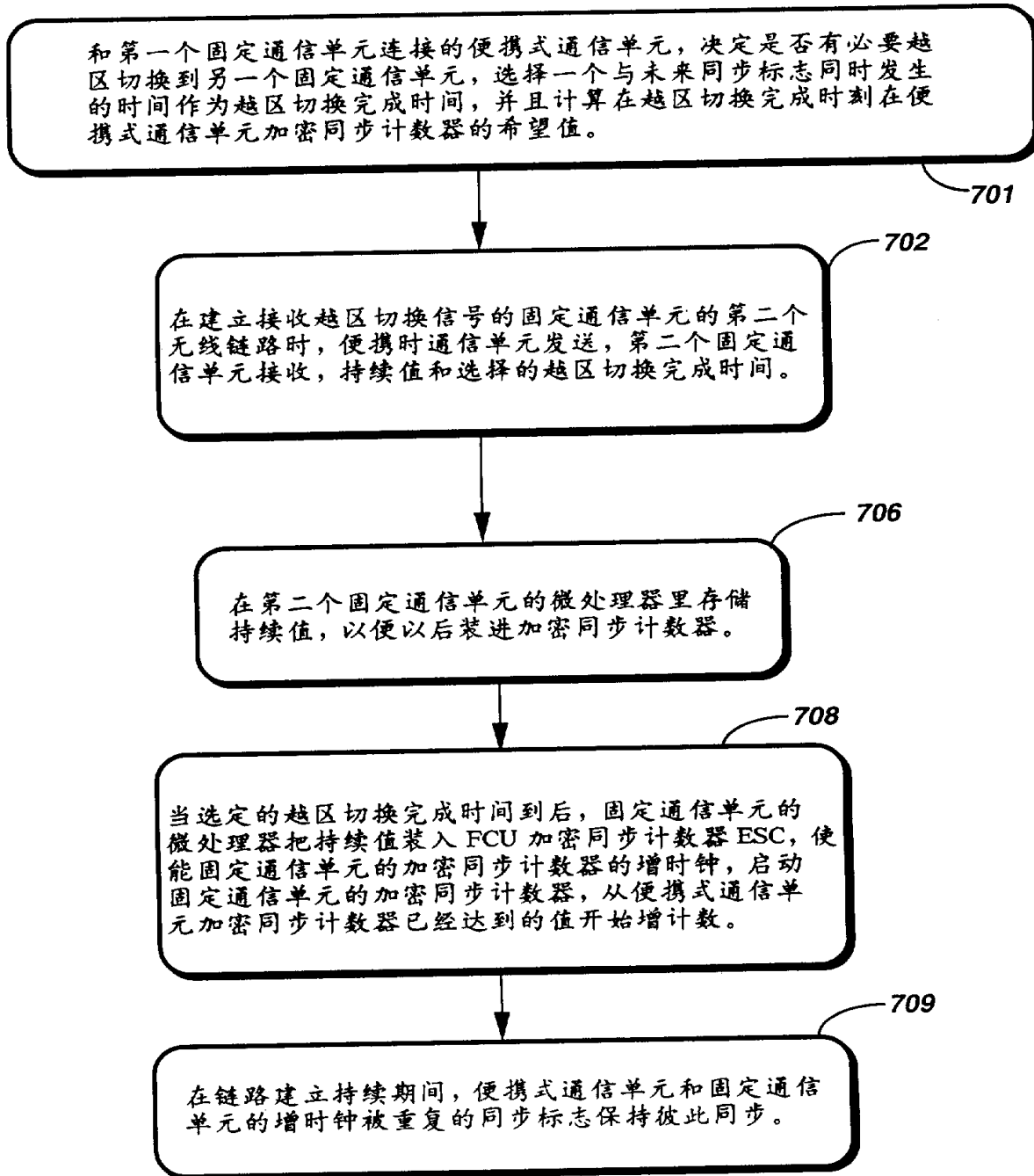


图 7