[19]中华人民共和国专利局

[11] 授权公告号 CN 1024241C

[12]发明专利说明书

[21] ZL 专利号 91101527.2

[51]Int.Cl[5]

[45]授权公告日 1994 年 4 月 13 日

H04B 7/26

[24]颁证日 94.1.16

[21]申请号 91101527.2

[22]申请日 91.3.9

[30]优先权

[32]90.3.9 [33]SE[31]9000856

[73]专利权人 艾利森电话股份有限公司 地址 瑞典斯德哥尔摩

[72]发明人 保罗·W·登特

亚历克斯·K·赖特 扬·E·奥克 H04Q 7/04

[74]专利代理机构 中国专利代理(香港)有限公司

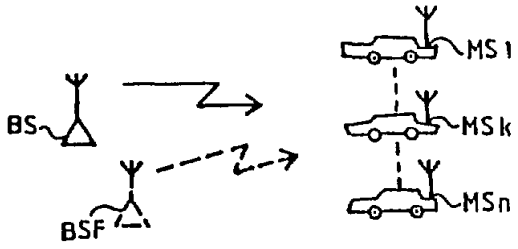
代理人 程天正 王忠忠

说明书页数: 附图页数:

[54]发明名称 在移动式无线电系统的基地台与移动台之间进行鉴别校验的方法

[57]摘要

一个可确信的基地台（BS）管理多个移动台（MSI-MSn）的移动式电话系统的鉴别校验方法。先有技术是从基地台（BS）对呼叫的移动台（MSK）鉴别校验。假基地台（BSF）通过收集若干所谓的RAND响应对，会执行假鉴别校验。为避免此情况，引入另一种单向鉴别校验，基地台—移动台，以及移动中向基地台的鉴别校验。在一个实施例中，排除单向校验，只进行双向鉴别校验。



1. 一种用于移动式无线电系统的基地台(BS)与移动台(MSK) 之间进行鉴别校验的方法，其中在建立连接前，该基地台发送有关于对该移动台鉴别的询问，并命令该流动台发送第一响应信号(Resp 1)，所述第一响应信号(Resp 1)被该基地台用于去确认该移动台的鉴别，其特征在于，在该基地台中确认了该移动台的鉴别(2,3,4) 之后，从该基地台向移动台发送第二响应信号(Resp 2)，该移动台于是形成相应的第二响应信号(resp 2) (8)，以确认该基地台的鉴别(9)，当确认了这种鉴别时，该移动台发送第三响应信号(Resp 3)，以及在建立连接前确认移动台的鉴别。

2. 根据权利要求1 的方法，其特征在于，所述第二响应售信号(Resp 2)是由该基地台内所产生的随机数(RAND 2)和该移动台的识别号(PIN) 所形成的，该基地台的鉴别是通过把所述第二响应信号与所述移动台内所产生的独立于所接收到的随机数(RAND 2)和在所述移动台内所得到的识别号(PIN) 的信号进行比较(9) 而确认的。

3. 根据权利要求2 的方法，其特征在于，发送到该基地台的所述第三响应信号(Resp 3)是由所述移动台的识别号(PIN) 和所述随机数(RAND 2)所形成的，所述信号被发送到该基地台去；所述基地台以相似的方式由在其内所获得的该移动台的识别号(PIN) 和所述随机数(RAND2) 形成相应的信号；在该基地台内对该形成的信号与该发送的信号作比较(12)，从而当发现所述各信号一致时，就能建立通话连接。

4. 一种用于移动式无线电系统的基地台(BS)与移动台(MSK) 之间进行鉴别校验的方法，在该移动台已经请求及被分配一个给定的信道

进行连接，其特征在于，在该基地台(BS)内形成第一响应信号(Resp 2)，把所述第一响应信号发送到该移动台(MSK)，该移动台为了检验该基地台的鉴别的目的于是形成相应的响应信号(Resp 2)，在确认这种鉴别后，该移动台向该基地台发送第二响应信号(Resp 3)，该基地台形成相应的响应信号，以及在建立连接前确认该移动台的鉴别。

5.根据权利要求4 的方法，其特征在于，所述第一响应信号(Resp 2)是由该基地台内所产生的随机数(RAND 2)和该移动台的识别号(PIN) 所形成的，该基地台的鉴别是通过把所述第一响应信号与所述移动台内所产生的、随所接收到的随机数(RAND 2)和在该移动台内所获得的识别号(PIN) 而定的信号进行比较而确认的。

6.根据权利要求4 的方法，其特征在于，发送到该基地台的所述第二响应信号(Resp 3)是由所述移动台的识别号(PIN) 以及所述随机数(RAND 2)所形成的，所述信号被发送到该基地台去，所述基地台以相似的方式由在其内所获得的该移动台的识别号(PIN) 以及所述随机数(RAND 2)形成相应的信号；在该基地台内对由其所形成的信号与由其所接收到的信号作比较(12)，当这两种信号相符时，就建立通话连接。

在移动式无线电系统的基地台与移动台之间进行鉴别校验的方法

本发明涉及在移动式无线电系统、尤其是蜂窝式移动电话系统(Cellular mabile telephone system)的基地台与移动台之间进行鉴别校验的方法，本发明所提出的方法也可以用于其它的移动式无线电系统，例如寻呼系统。

就蜂窝式移动式电话系统来说，例如在移动台和基地台之间建立呼叫之前要进行鉴别校验。基地台通过命令移动台发送识别号而索求有关移动台身份的信息。于是使得移动台向基地台展示其身份，以便使基地台知道该移动台就是被认可通过本系统发出呼叫的移动台，因此基地台以及电话交换局就知道这个移动台因随后建立的呼叫而需向其收费。

另一方面，移动台必须肯定它是在与这个可确信的基地台通讯，亦即是，当移动台是呼叫方时（该移动台是一个A-用户），它是与一个真正被认可接通呼叫的基地台通讯；以及肯定该移动台会被正确地收呼叫费。

为了执行鉴别校验的目的，早先所公知的是在基地台和移动台内产生鉴别信号（即Resp信号）。从基地台向由其所覆盖的区域内的各移动台发送一个随机数(RAND)，呼叫的移动台用给定的信号(Resp 1)回答。基地台以相似的方式，根据呼叫移动台的身份和该随机数而形成同一种信号Resp 1。这些信号在正常情况下是相符合的，基地台就给移动台指定一条通话信道。

因此，在上述进行鉴别校验的公知方法中，对于某一个移动台形

成一对RAND响应，亦即是在该移动台内为给定的接收到的随机数RAND形成给定的响应信号，因而，基地台可以接收到用于若干个不同的随机数的若干个这样的响应信号。这意味着有可能产生一个能传送若干个互不相同的随机数及接收相应数量（不同）的响应信号的“假”基地台。这种假基地台于是能造成一种未经认可就在整个系统上发送呼叫的移动台预约。公知的鉴别校验的这种缺陷和不足是由于这种校验是单向的所以才引起的，即：仅仅是基地台需要响应信号以证实对移动台的鉴别。

根据本方法，鉴别校验是双向的，亦即是不仅基地台需要验证移动台的身份，而且移动台也需要验证基地台的身份。

因此，本发明的目的是提供一种经过改进的鉴别校验的方法，这种方法使假基地台企图获得利用移动式电话系统的鉴别码的操作成为不可能。

本发明作为一种用于移动式无线电系统的基地台(BS)和移动台(MSK)之间进行鉴别校验的方法，其中在建立连接前，该基地台发送有关于对该移动台鉴别的询问，并命令该移动台发送第一响应信号(Resp1)，所述第一响应信号(Resp 1)被该基地台用于去确认该移动台的鉴别；本发明的方法的特征在于：在该基地台中确认了该移动台的鉴别之后，从该基地台向移动台发送第二响应信号(Resp 2)，该移动台于是形成相应的第二响应信号(Resp 2)，以确认该基地台的鉴别(9)，当确认了这种鉴别时，该移动台发送第三响应信号(Resp 3)，以及在建立连接前确认移动台的鉴别。

本发明所提出的方法的进一步发展在于，所述第二响应信号(Resp2)是由该基地台内所产生的随机数(RAND 2)和该移动台的识别号(PIN)所形成的，该基地台的鉴别是通过把所述第二响应信号与所述移动台内所产生的独立于所接收到的随机数(RAND 2)和在所述移动

台内所得到的识别号(PIN) 的信号进行比较而确认的。

发送到该基地台的所述第三响应信号(Resp 3)是由所述移动台的识别号(PIN) 和所述随机数(RAND 2)所形成的，所述信号被发送到该基地台去；所述基地台以相似的方式由在其内所获得的该移动台的识别号(PIN) 和所述随机数(RAND 2)形成相应的信号；在该基地台内对该形成的信号与该发送的信号作比较，从而当发现所述各信号一致时，就能建立通话连接。

现在参照附图对本发明进行更详细的描述，其中

图1 简略地例示两个基地台与多个移动台之间的通讯情况；

图2 是例示本发明所提出的方法的一个实施例的流程图；

图3 是移动台中含有的对于鉴别校验结果的真实性的一种算法的输入和输出量的方框图；以及

图4 是例示本发明所提出的方法的另一个实施例的流程图。

图1 例示了一个可确信的基地台BS通过发送随机数给多个移动台MS1-MSn 而经一个给定的控制信道进行侦听。在这些移动台中，其中一个表示希望通过给定的通话信道建立呼叫的移动台MSK 接收到响应。如上所述，在基地台需要来自移动台MSK 的响应Resp 1的情况下，进行了一种单向的鉴别校验。这种校验在下文会参照图2 进行更详细的描述。由于在这一阶段期间进行的是单向连接，因此当以上述方式发送上述随机数RAND时，一个假基地台BSF 能够获得来自若干移动台的响应。基地台BSF 于是能产生一组RAND响应的答复，这种答复则可能为一个移动台以未经认可的方式所采用。

为了使这种情况不可能发生，根据本发明提出了一种在图2 的流程图中所公开的鉴别方法。

可确信的基地台BS通过发送随机数RAND（方框1）而在其所覆盖的区域内侦听若干个移动台MS1-MSn 。

希望建立呼叫的给定的移动台MSK 用信号Resp 1回答（方框2)。这种信号除了所接收到的随机数外，是在移动台的微处理机内由若干种输入数据PIN，ESN和DN而形成的（见图3），其中PIN 表示移动台的专用识别号，ESN 表示移动台的电子系列号，以及DN表示拨号。移动台MSK 同时又是一个A-用户。微处理机13于是就输出发送到基地台去的Resp 1信号，后者由18比特的AUTH信号和 8比特的RANDC 信号所组成。

基地台以相应的方式根据输入信号AUTH和RANDC 计算Resp 1（方框3)，并且把算出的Resp信号值与由移动台所传送的Resp信号值进行比较（方框4)。当它们一致时，基地台就给移动台规定出一个给定的、分配好的通话信道（方框5)，以公知的方式建立连接（图6）。上述方法是原已公知的。

根据本发明所提出的方法，基地台现在根据另一个随机数RAND 2以及移动台的专用识别号PIN 形成响应信号Resp 2，这个专用识别号是基地台所知道的（方框2,3)。信号Resp 2和随机数RAND 2都被发送给移动台（方框7)。移动台根据其PIN 以及接收到的随机数RAND 2形成Resp 2的值（方框8)。此时在移动台内对接收到的Resp 2与所形成的Resp 2的值进行比较（方框9)。如果这两个值相符，移动台就产生值Resp 3，并将这个值发送给基地台（方框10）。值Resp 3是由随机数RAND 2和移动台的专用识别号PIN 所形成的。基地台以类似的方法由其已知的随机数RAND 2和专用号PIN 形成值Resp 3（方框11）。然后，将接收到的Resp3 值与所形成的Resp 3值作比较（方框12）。如果这两个值相符，呼叫连接就继续下去，从而建立通话连接。

在本方法，根据方框7,8 和9 的步骤提供了一种鉴别校验，即移动台判定基地台是不是可确信的，这是由于对从基地台所发出的信号Resp 2的检验是在移动台内对照所述移动台所算出的值Resp 2而进行

的。因此来自基地台的信号Resp 2可以看作从所述台所发出的响应信号。上述方法的内容构成了本发明所提出的方法与根据方框2,3 和4的公知方法的主要差别。

根据方框10、11和12所进行的校验实质上构成了根据方框 2、 3和 4的方法的重复，亦即是从基地台校验移动台是否可确信。

本发明相对于公知的真实性鉴别方法（方框1-4)的基本区别在于，移动台还需要来自基地台的响应Resp 2，以及根据方框7-9 对这种响应进行检验。因此，假基地台就必须准确地了解这种响应信号应该怎样计算（才可避免假鉴别）。这种检验又是双向的。

根据方框2,3 和 4的鉴别检验可以在移动式无线电系统的一般控制信道上进行，而根据方框7-12的鉴别校验可以在基地台BS与移动台MSK（方框 5和6)之间所建立的通话信道上进行。

图4 是例示在只进行双向鉴别校验时的情况下的第一种方法的步骤。在这种情况下，根据方框1-3 的步骤代替了根据图2 中方框1-6的步骤。在这种情况下，在双向校验之前不进行单向（及公知）的鉴别校验。一个正在呼叫的移动台，例如MSK ，请求与基地台BS进行连接。当基地台BS接收到这个呼叫请求时，就找到一条空闲的通话信道，并且给移动台MSK 指定这条空闲信道。这样，通过这条通话信道就建立了自由连接(free connection)，而不用进行鉴别校验。实际的鉴别校验则是以上述方式参照图2 的步骤7-12进行的，亦即只进行双向鉴别校验。

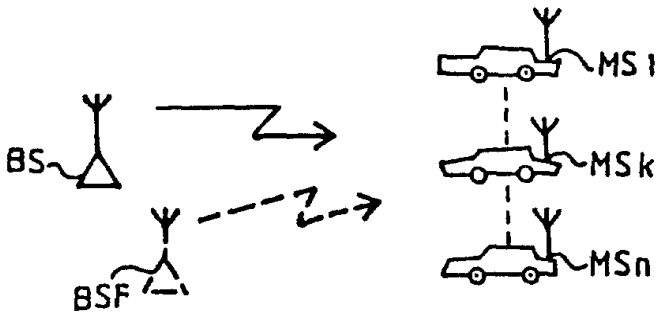


图　1

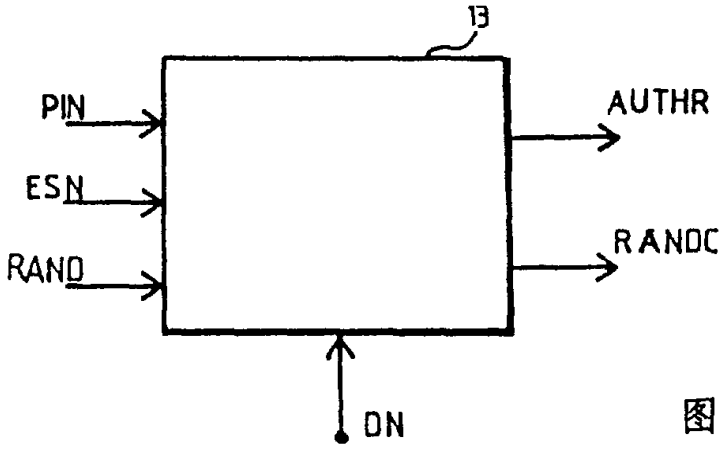


图　3

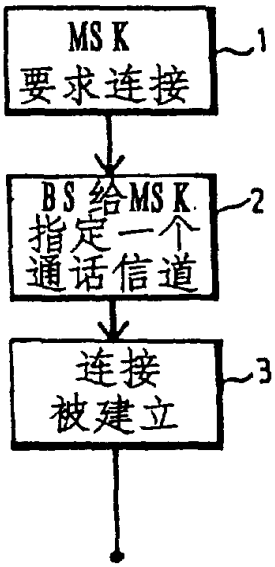


图　4

至图2 方框1

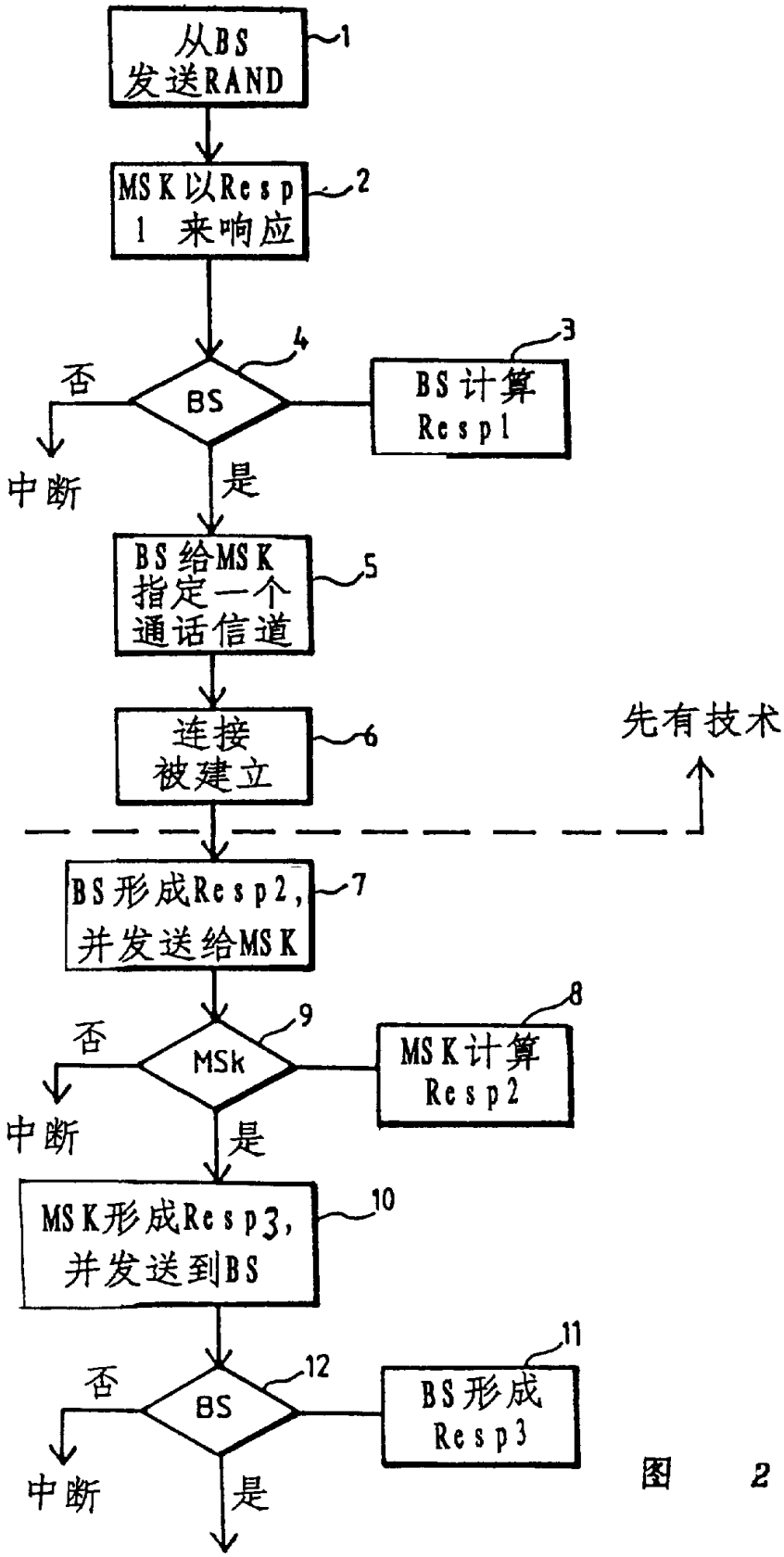

从BS
发送RAND
1
MSK以Resp
1 来响应
2
否
BS
4
BS计算
Resp1
3
中断
是
BS给MSK
指定一个
通话信道
5
连接
被建立
6
先有技术
BS形成Resp2,
并发送给MSK
7
否
MSk
9
MSK计算
Resp2
8
中断
是
MSK形成Resp3,
并发送到BS
10
否
BS
12
BS形成
Resp3
11
中断
是

图 2