[19]中华人民共和国专利局

[51]Int.Cl[6]
H04L 9/14

[12] 发明专利申请公开说明书

[21] 申请号 98108859.7

[43]公开日 1998 年 12 月 16 日

[11] 公开号 CN 1202060A

[22]申请日 98.5.20

[30]优先权

[32]97.5.21 [33]FR[31]9706180

[71]申请人 阿尔卡塔尔-阿尔斯托姆通用电气公司

地址 法国巴黎

[72]发明人 安特因·托塔罗 埃里克·福劳勒斯

[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

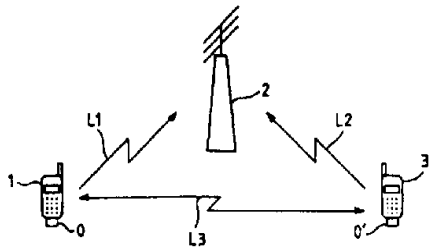
代理人 罗亚川

权利要求书 1 页 说明书 7 页 附图页数 2 页

[54]发明名称 移动无线网络终端间进行直接加密通信的方法及相应设施

[57]摘要

用于允许无线移动网络的两终端间直接加密通讯的方法及对应的站和终端的配置。允许在卫星和/或 GSM/DCS 类无线移动网络中两终端间，在借助于网络无线移动固定站（2）两终端中的一个呼叫后，以一次电波反射或直接的方式加密通讯的方法。在用常规方法实现的加密第一阶段之后，加密密钥由与主叫终端（1）相连的识别卡（0）和网络命令结构同时产生，以对该主叫终端和站之间无线电链路所发送的数据进行加密/解密。



权 利 要 求 书

1.一种加密通讯方法，它用于允许两终端间通过卫星和/或 GSM/DCS 无线移动网，在它们中的一个通过网络中一无线移动固定站建立起通话后，在一次电波反射中或简单地在网络中建立直接的加密通讯，其特征在于，在使用惯常的方法的加密第一阶段，在主叫用户被网络由该用户的个体识别卡通过卡所相关的主叫终端提供的标记应答（ SRES ）确认后，在接收到站发送向该主叫用户的随机数(RAND)时，由与主叫用户相关的卡和网络命令结构同时产生一加密密钥(K_{c1})，用于对该主叫用户和站间无线电链路所发送的数据进行加密/解密，所述的加密密钥也被存储在站的存储器中，然后该加密密钥在该站与被叫终端间建立无线电链路时被从站发送到被叫终端，以对与该主叫终端交换的数据进行加密/解密。

2.根据权利要求 1 所述的方法，其特征在于，当与被叫终端建立无线电链路时，加密密钥(K_{c1})被包括在站发送到被叫终端目的地的通话建立消息中。

3.根据权利要求 1 所述的方法，其特征在于，当与被叫终端建立无线电链路时，加密密钥(K_{cl})被站在与站向被叫终端目的地发送的通话建立消息相分开的专门消息中发送。

4.一种卫星和/或 GSM/DCS 类网络的固定无线站的设施，以使得依据权利要求 1， 2， 3 中的任一权利要求的方法能够应用，其特征在于它包括临时存储由网络命令结构发送的加密密钥的装置，通过它使得站和主叫终端间进行数据交换，及一能够通过所述站由主叫终端向被叫终端发送该加密密钥的装置，使得主叫终端和被叫终端之间直接通讯和在此通讯其间，每一终端加密/解密另一终端发送的数据时能够使用唯一的加密密钥。

5.一种卫星和/或 GSM/DCS 类网络移动无线终端的设施，以使得依据权利要求 1， 2， 3 中的任一权利要求的方法能够应用，其特征在于它包括在被叫时能够存贮每次呼叫的来自移动无线网络站的加密密钥的装置，及在与通过该站呼叫的终端直接通讯时能够使用密钥加密/解密所交换的数据的装置。

说　明　书

移动无线网络终端间进行直接加密通信的方法及相应设施

本发明的目的在于提供一种方法，该方法允许在由卫星和/或GSM/DCS 构成的无线移动通讯网的两终端间进行直接加密通讯，本发明还涉及到对应的无线移动通讯终端和站点的配置。

众所周知，在两无线移动通讯终端间，特别是在 GSM 类网络终端间建立通讯，一般要借助至少一个起网关作用的无线移动通讯固定站，如果两终端在站合适的无线电范围内，那么站对于两终端来说可以是同样的。在这种情况下，无线电资源管理及加密和解密处理都要通过连接两终端的站来执行。主叫终端和公共站间及该站和被叫终端间建立起无线电链路，加密在所述诸链路的首先提到的链路中通过加密密钥 K_{c1} 进行，在第二链路中通过加密密钥 K_{c2} 进行。

对于通过站进行通讯的两终端的任何一个，都要进行确认程序。因此，该站要发送一对于每一终端是不同的随机数 RAND。插入到终端的用户识别卡，例如一 SIM 卡，利用该终端接收到的随机数 RAND，借助于个体确认密钥 K_i 及与密钥 K_i 储存在一起的共享确认算法 A_3，以计算对应于标记应答的 SRES 数。卡所提供的标记应答 SRES 由带有该卡的终端发送出去，形成由移动无线网络的终端和卡所构成的整体识别。如果发送的标记应答 SRES 与从无线移动网络中同一数 RAND 同时计算所得的标记应答 SRES 相对应的话，就实现了确认。插入到终端的卡也利用终端接收到的数 RAND 及卡所存储的密钥 Ki，通过同样存储在卡中的密钥确定共享算法 A8，计算加密密钥 K_c，或是 K_{C1} 或 K_{C2}。每一由卡所产生的加密密钥被用于与加密共享算法 A5 相联系，以对带有该卡的终端所发送的数据进行加密，以及用于对终端接收的来自与其进行通讯的站的数据的解密。

然而，GSM/DCT 无线移动网中两终端处于合适的无线电范围内，它们之间如果不通过站目前也不能直接进行加密通信，因为该两终端使用不

同的加密密钥 K_{C1} 和 K_{C2}，所以任何一个都不能对另一个发送的数据解密。

同样，当无线移动网中两无线移动终端间通讯在地面控制站监管下建立，并经由一个或多个卫星中继的情况下，实际上由于上述原因，目前终端间在一次电波反射中通过一个或多个卫星不可能进行直接的加密通讯。

因此本发明提供了一种方法，用于允许两终端间通过卫星和/或 GSM/DCS 无线移动网，在两终端中的一个通过网络中无线移动固定站建立起通话后，为直接或在一次电波反射中与另一终端通讯，在一次电波反射中或简单地在网络中建立直接的加密通讯。

根据本发明的特点，在使用惯常的方法的加密第一阶段，通过来自用户个体识别卡提供的标记应答经有该卡的主叫用户通过网络确认后，在接收到站发送给该主叫终端的随机数时，由与主叫终端相关联的卡和网络控制结构同时产生一加密密钥，用于对该主叫终端和站间无线电链路所发送的数据进行加密/解密，所述的加密密钥也被存储在站的存储器中，然后该加密密钥在该站与被叫终端间应主叫终端的请求建立无线电链路时被发送到被叫终端，以对与该主叫终端交换的数据进行加密/解密。

本发明还提供了一种卫星和/或 GSM/DCS 类网络无线移动通讯固定站的配置，以使得依据本发明的方法能够应用。

根据本发明的特征，该配置包括临时存储发送自由网络命令结构发送的加密密钥的装置，通过所述站使得该站和主叫终端间进行数据交换，及一能够通过所述站由主叫终端向被叫终端发送该加密密钥的装置，使得它们之间直接通讯和在此通讯其间，每一终端加密/解密另一终端发送的数据时能够使用唯一的加密密钥。

本发明最后还提供了一种卫星和/或 GSM/DCS 类网络无线移动终端的配置，以使得依据本发明的方法能够应用。

根据本发明的特征，该配置包括在被叫时能够存贮通话对通话的，来自无线移动网络站的加密密钥的装置，及在与通过该站呼叫的终端间直接通讯时能够使用密钥加密/解密所交换的数据的装置。

本发明的特点和优点将结合下面的附图在说明书中详细描述。

图 1 描述了无线移动网络两终端间通讯过程的原理图。

图 2 描述了在 GSM 类网络中对于主叫终端加密过程的简图。

图 3 描述了加密密钥在被叫终端的作用。

卫星和/或 GSM/DCS 类型网构成的无线移动网中的两终端要建立直接加密无线电话联系，就要包括图 1 所示的双重操作。

在通常 GSM/DCS 网的情况下，假设主叫终端 1 在通话时位于至少一个发送-接收无线移动站 2 合适的无线电范围内，以便能够在需要的情况下通过第一无线电链路 L1 与该站建立双向通信。

在通过卫星网络的情况下，假设主叫终端 1 处于卫星系统的覆盖下，该卫星系统使其能够与地面控制站类型的无线移动发送-接收站 2 通过第一无线电链路 L1 建立双向通信。

实际上，站 2 可以是卫星无线移动网络地面控制站类型，此类站可用英文缩略语 GSC 表示，或是 GSM/DCS 无线移动网络的发送-接收子系统。该子系统为通常用英文缩略语 BSS 表示的类型，并且它包括至少一个与通常的有线通讯网络相连接的无线发送接收部件及一控制器部件。

网络中直接的或如前所考虑的一次电波反射直接的加密无线电话联接的建立，假设呼叫时被叫终端 3 或位于站 2 的无线电范围内或在卫星的覆盖下，以便同样能够在站与被叫终端间建立通过直接或一次反射第二无线电链路 L2 的双向通信。最后假设两终端都在无线电范围内或在卫星系统覆盖下，尤其当两者之间建立一直接的第三无线电链路 L3，而不是两者分别与站建立起来的两个链路时。

如前面所述，主叫终端 1 只能通过无线移动网络进入到它所通话的终端的无线通路通讯中。终端在被提供通话号码后，比如用户使用该终端的按键键入，在信号信道中向该网络发送一请求消息。该消息被终端的无线电所覆盖的无线移动网络中的一个站 2 所接收。

主叫终端确认程序因而就由网络通过站 2 进行，如前所述。

如果这能无障碍地进行，该程序能够获得一加密密钥 K_{c1}，该密钥使得能够对主叫终端 1 发送的数据加密，及对由站 2 发往目的地的数据解密，并且这是借助于加密算法 A5 实现的。该算法只要对于提供给对于所有无线移动网络终端用户的一个同样算法是常规的，就被称为共享的，使用该算法主叫终端力图进行通讯。如前面已经描述过的，此加密算法储存

在用户个体识别卡中，这里表示为 0 和 0'。

确认之后，主叫终端 1 发送所呼叫终端的号码，执行无线移动网络级的通话建立阶段。

站 2 执行朝向主叫终端 1 所提供的通话号码的终端的通话程序。

为使在主叫终端和被叫终端间建立直接加密通讯，加密密钥 K_c 必需对于此两终端而言是同样的，另外还要设定两终端要有同样的可用加密算法 A5。

根据本发明，要为处于第一建立阶段的被叫终端分配一加密密钥 K_{c1}，该密钥要给主叫终端，然而这意味着主叫终端对其它终端的建立直接加密通讯的建立请求由无线移动网络一级所知悉，并且至少在站 2 一级上借助于此，主叫终端的请求被收到了。

主叫终端在网络中，这里假设是 GSM/DCS 类型，的呼叫建立请求通常导致所述终端发射接入请求的无线电脉冲序列，该序列尤其是包括了一服务请求代码，目前情况下是呼出请求。该脉冲序列在公共接入请求信道上被发送。负责处理该通话的无线移动网络的站 2 给主叫终端分配一无线电信号信道，以建立所请求的通讯，终端位于该信道上并通过“移动管理” 3 级消息建立 2 级连接，通常被表示为英文缩略语 MM，在目前情况下它包含一服务请求，该请求中通常以 IMSI 或 TMSI 的形式表明了主叫终端的身份及所请求服务的类型，这时所请求的服务的类型是呼出。在接到该请求后，站 2 通过保留的保留的信令信道建立起与通常以英文缩略语 MSC 表示的固定网络交换机 4 的链路，在该网中是有线连接的，并且向网络命令结构 5 发送尤其是包含有上述 MM 消息的连接请求消息 SCCPCR，网络命令结构 5 也称为发送子系统 NSS，它构成交换中心 4 的一部分。如公知的那样，此命令结构尤其是包括了一更高的级，该级包括涉及用户的一般位置和特征的特征中央数据库 6，该数据库通常以英文缩略语 HLR 和 AUC 表示并在物理上位于确认中心 7（AUC）。

每一交换机 4 包括有一未表示的命令子结构，通过它可与前述的命令结构的较高级通讯，并且它还结合一用户精确定位数据库 8，通常被称为访问者位置寄存器，用英文缩略语 VLR 表示，在其命令子结构上提供。

主叫用户确认过程由网络 5 的命令结构在接到 MM 型连接请求命令

消息时起动，并且根据一程序(这里未展示出)使该用户所使用的终端 1 发送确认应答，通常这是常规的，相对于本发明而言这只是间接的，故不在此描述。确认程序成功后，由网络命令结构 5 进行加密判定，通常在由交换机 4 与定位数据库 8 构成的子设备级上进行。因而一加密形式的用于交换的命令消息被发送到站 2，站 2 在该时间内以无线电的形式连接主叫终端，该命令消息通常是根据被表示为英文缩略语 BSSMAP 的特殊交换协议而在交换机和站间传输的。由主叫终端所使用的加密密钥 K_{cl} 在网络确认中心 7 级上借助于所建立的用户确认密钥 K_i 和由站 2 传送到该主叫终端提供给通话用的随机数 RAND 被建立起来后，被发送到站 2，密钥 K_i 被存储到用于主叫用户的库 6 中并被确定。加密密钥 K_{c1}，随机数 RAND 及通过来自上述二者的算法 A3 所计算的数 SRES 以加密命令的形式，向由交换机 4 和定位数据库 8 构成的子部件级上定位的命令子结构发送。再向站 2 传送一加密命令，该命令包括加密密钥 K_{c1} 和所要使用的识别算法 A5 的标识符。站 2 存储这些信息并以加密的形式通过无线电信道向主叫终端 1 发送通过指令，以便以后在二者之间建立加密通讯。

这里所描述的确认过程只是指示性的，然而所展示的程序也适合于通常的 GSM。

一作为站 2 的命令子结构存储器中的专门表 T 能够存储建立与主叫终端通讯所提供的加密密钥 K_{c1}。

主叫终端使用在确认过程中自站 2 接收的数 RAND 来获得数 SRES，并借助于当时其所配备的卡 0 来获得加密密钥 K_{c1}。如前所述，数 SRES 借助于确认算法 A3 和卡中的用户确认密钥 K_i 来获得，而加密密钥也借助于同样存于卡 0 中的密钥确定算法 A8 来确定。

主叫终端 1 向站 2 发送一应答，以指出它已到加密模式，并且站通过保留的信令信道通知网络 5 的命令结构。该主叫终端的应答后接着一通话建立请求，借助于此，所述终端与其想要直接通讯的无线移动终端 3 进行数字通话。另外，站 2 在位于与其相连的交换机 4 一级的命令结构的较高级进行它所发送的通话建立请求识别。被叫用户的号码，例如这里用英文缩略语 MSISDN 表示，一方面被发送向通用定位和用户特征中央数据库 6，以在该级别上实现通常的有效性验证，另一方面被存储在站 2 存储

器的表 T 中，以在直接通讯建立时使用。

在中央数据库 6 一级上的被叫用户的定位可以确定通过网络所要建立的通路，以在连接主叫无线移动终端 1 的站 2 和被叫用户所使用的无线移动终端 3 相连接的站间通讯，后一站在现在的假设里就是站 2 本身。

通过被叫用户无线电信道要达到的寻找过程在连接站 2 的交换机 4 的命令子结构级上进行管理。包含该被叫用户识别码的消息由站 2 在广播无线电信道上，例如被表示为英文缩略语 PCH 的信道和/或无线电信标信道上发送。该识别码在站 2 级上是，例如，用户国际标识符 TMSI 或用户临时标识符 TMSI 。预期有来自终端 3 的应答通过无线电信道经过公共信道到达，终端 3 上插有分配给该用户的卡 0'，该应答为该用户起动了站 2 的信号无线电信道的分配，并且以与前述的处于同样通信阶段的主叫终端 1 类似的方式由移动管理消息建立连接。然后，处于类似上面对于主叫终端所描述的确认阶段。在终端 3 和站 2 之间建立的通讯加密判定在网络的命令结构 5 的较高级执行，该较高级借助于位于交换机 4 和定位数据库 8 构成的部件一级的命令子结构向该站 2 发送加密形式的通讯通行命令。在这里依然描述的是一种指示性的程序，它也适于一般的 GSM 。

加密密钥 K_{c2},随机数 RAND'及由加密算法 A3 计算的数 SRES'以三位组的形式被传送到与站 2 相关的交换机 4 的命令子结构。站 2 接收到含有密钥 K_{c2} 和数 RAND'的加密命令，并将数 RAND'传送被叫终端 3 ，终端 3 推算出加密密钥 K_{c2} 。然后被叫终端 3 向站 2 发送应答，以表明它进入到加密模式，并且该站通知网络 5 的命令结构。该加密密钥 K_{c2} 的使用，对于通常的 GSM ，使能够对被叫终端和站 2 建立阶段的后续信息，尤其是向被叫终端传送的加密密钥 K_{c1} 的消息进行加密。

站 2 因而接收到与被叫终端的通讯建立请求消息，它是被经由位于交换机 4 一级的子结构的命令结构所发送的。

站 2 探测到通过无线通讯信道相连的主叫终端 1 和被叫终端 3 之间直接通讯的建立命令，并确保存储在表 T 中的分配给主叫终端 1 的加密密钥 K_{c1} 被传送到被叫终端。该加密密钥 K_{c1} 在例如通话建立消息中被传送，通常站 2 向被叫终端发送该消息，以维持建立过程的持续直到其结束，也就是说直到接到对应于通常电话振铃的通话信号之后，该被叫终端进行接

收通讯的应答，或“摘机”。

在其它的实施例中，站 2 在常规的通话建立消息之后，并为了分开程序，向被叫终端发送一特殊的消息，以向被叫终端传输加密密钥 K_{c1}。

在这两种情况下，被叫终端表明它注意到它所接收到的特殊消息，因此对于它们的通讯时所有的加密和解密操作，站 2 及两终端的每一个都使用唯一的加密密钥 Kc_1。

图1

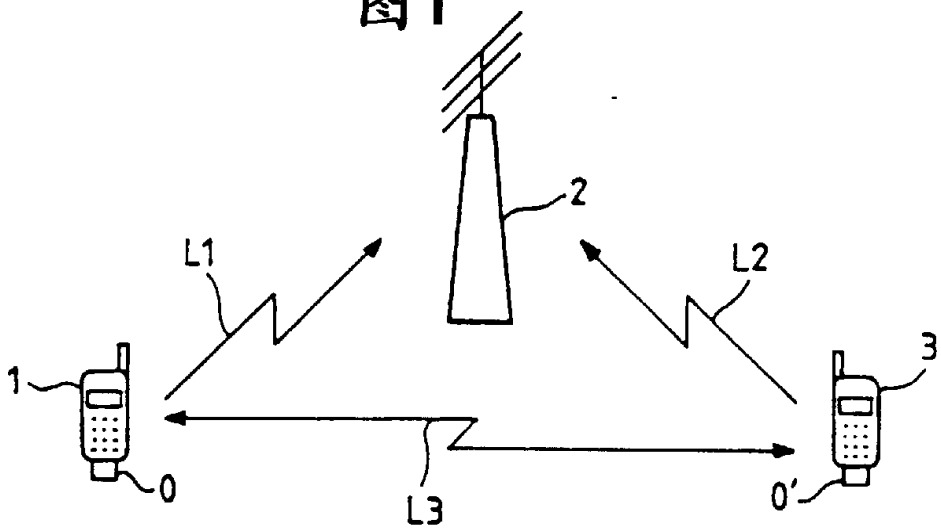

2
L1
L2
1
3
0
L3
0'

图2

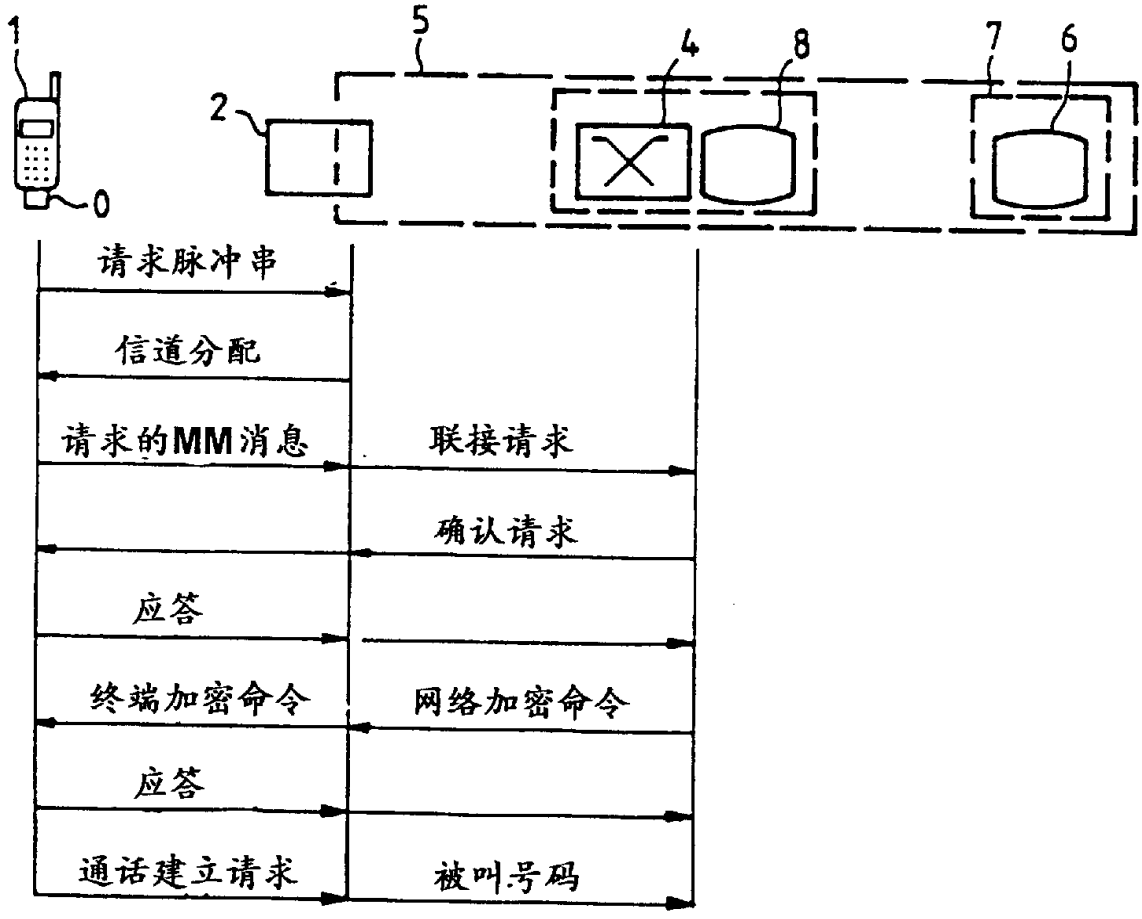
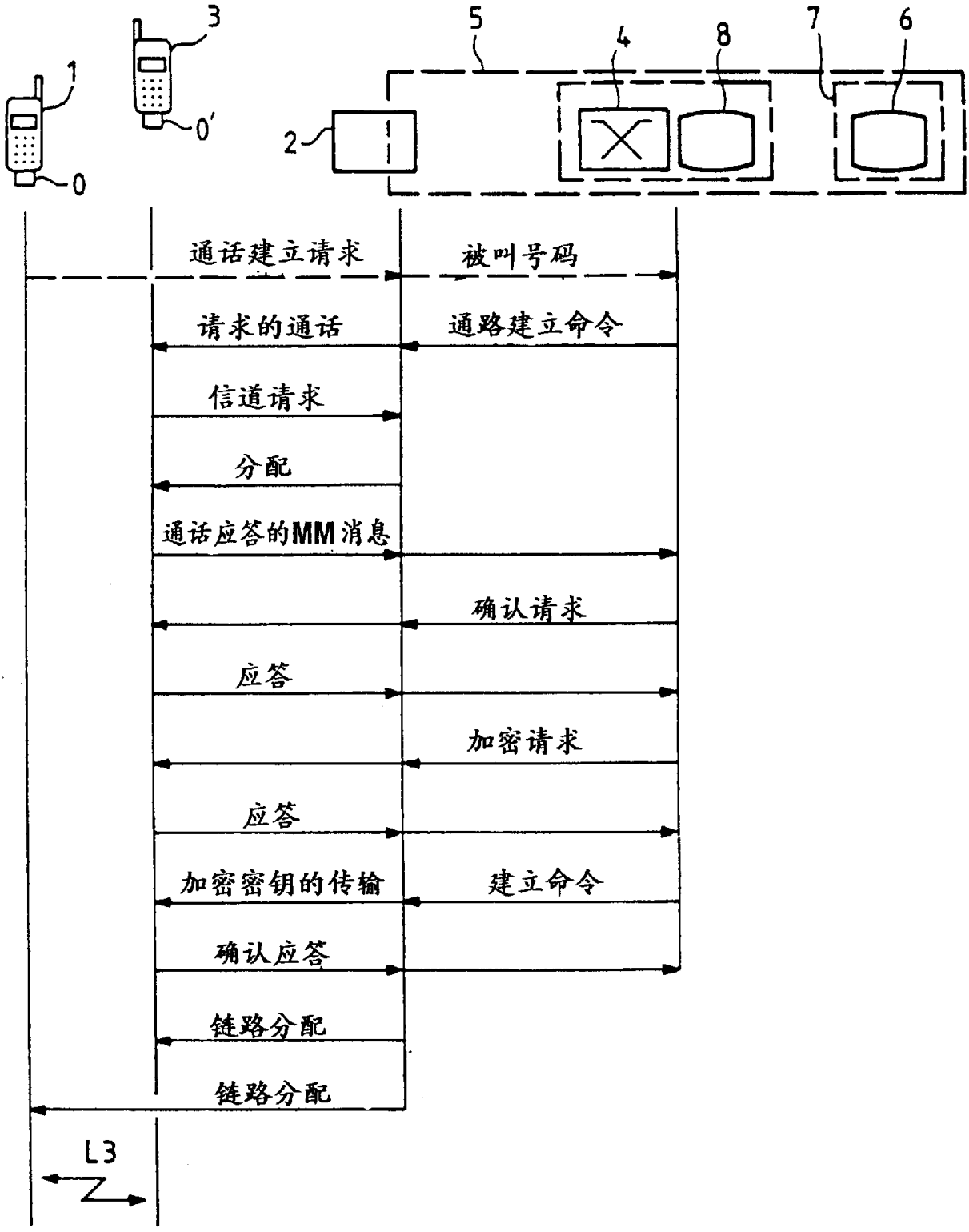

1
5
4
8
7
6
2
0
请求脉冲串
信道分配
请求的MM消息
联接请求
确认请求
应答
终端加密命令
网络加密命令
应答
通话建立请求
被叫号码

图3


3
5
4
8
7
6
1
0'
2
0
通话建立请求
被叫号码
请求的通话
通路建立命令
信道请求
分配
通话应答的MM消息
确认请求
应答
加密请求
应答
加密密钥的传输
建立命令
确认应答
链路分配
链路分配
L3