(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104393948 A
(43)申请公布日 2015.03.04

(21)申请号 201410495484.1

(22)申请日 2014.09.25

(71)申请人 王家城
地址 100192 北京市朝阳区林萃西里 26 号楼 6 单元 602

(72)发明人 王家城

(51)Int.Cl.
H04L 1/00(2006.01)
H04W 28/18(2009.01)
H04W 92/08(2009.01)

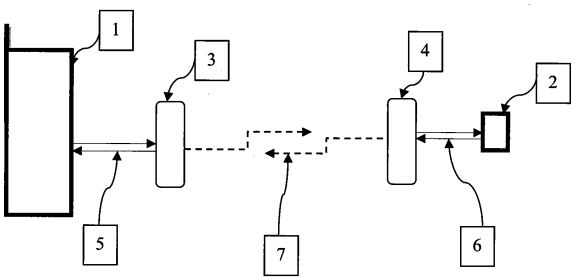
权利要求书2页 说明书10页 附图3页

(54)发明名称

一种通信终端设备和SIM卡之间的无线接口及功能实现

(57)摘要

本发明属于通信终端设备领域。本发明提供一种用于连接移动通信终端设备（简称手机）和用户身份模块卡（简称SIM卡）的无线传输协议，包括：1). 在手机端有一个手机接口设备，该设备通过ISO-7816协议和手机进行通信；在SIM卡端有一个SIM卡接口设备，该设备通过ISO-7816协议和SIM卡进行通信。手机接口设备和SIM卡接口设备通过无线传输协议进行通信。2). 提供了无线传输协议的差错控制(FEC)和传输协议数据单元(TPDU)，使得这种无线传输接口对于现有的手机和SIM卡之间的触点通信来说是透明的，即无论对于手机还是SIM卡来说，都不会觉察到它们中间的无线传输接口的存在。



CN 104393948 A

1. 一种用于连接通信终端设备和用户身份模块卡的无线传输通信协议及设备，其特征在于：

1) 在所述通信终端设备端有一个接口设备，称为通信终端接口设备，

2) 所述通信终端设备和所述通信终端接口设备通过 ISO-7816 智能卡传输协议进行连接通信，

3) 在所述用户身份模块卡端有一个接口设备，称为用户身份模块卡接口设备，

4) 所述用户身份模块卡和所述用户身份模块卡接口设备通过 ISO-7816 智能卡传输协议进行连接通信，

5) 所述通信终端接口设备和所述用户身份模块卡接口设备通过无线传输通信协议进行连接通信，

6) 所述通信终端设备和所述用户身份模块卡之间的数据通信是通过所述通信终端接口设备，所述用户身份模块卡接口设备以及它们之间的无线传输接口进行转发而建立的连接进行通信。

2. 根据权利要求 1 所述的无线传输通信协议，其特征在于：

1) 所述通信终端设备和在所述用户身份模块卡在建立通信会话的开始时的冷复位 ATR（复位应答）消息和其后的热复位 ATR 消息以及协议参数选择 PPS（如有）过程都是在手机端和用户身份模块卡端分别进行的，即通信终端接口设备对通信终端进行复位应答，用户身份模块卡对用户身份模块卡接口设备进行复位应答，分别建立起通信终端设备端和户身份模块卡端的 ISO-7816 通信协议参数，它们之间不通过无线传输协议来交换彼此的 ISO-7816 通信协议参数，也就是说，在通信终端设备端和户身份模块卡端两边的 ISO-7816 通信协议参数是不一致，

2) 或者，所述通信终端设备和在所述用户身份模块卡通过无线传输接口协议交换双方的 ISO-7816 通信协议参数，建立起户身份模块卡到通信终端设备的端到端的一致 ISO-7816 通信协议参数。

3. 根据权利要求 1 所述的无线传输通信协议，其特征在于：接通信终端设备和用户身份模块卡的数据交换对于无线转发通信来说是透明的，也就是说，通过无线传输接口的转发通信和他们之间的直接通信（ISO-7816 协议）是完全一样的，其传输时间延迟和传输差错都和 ISO-7816 协议以及 GSM 规范的 SIM 卡应用协议是一致的。

4. 根据权利要求 3 所述的无线传输通信协议的传输差错，其特征在于：所述传输差错包括如下部分：

1) 在每个传输的字节后面，附加有额外的奇偶检验比特位，

2) 多个传输字节组成一个传输字节块，他们一起进行循环冗余校验和前向纠错编码，

3) 纠错编码后的传输字节块和无线传输协议的控制信息组成无线传输的数据帧，在其后面有校验域，用于检验无线传输数据的可靠性，

4) 当接收端检测到错误的字节块，并且不能通过纠错编码进行错误纠正的时候，通过自动重传请求，要求发送端重新发送字节块。这种重传请求可以多次进行，直到收到正确的字节块，或者重传时间超过允许的最大时间延迟。

5. 根据权利要求 3 所述的无线传输通信协议的传输时间延迟，其特征在于：所述传输时间延迟是指手机传输的最后一个字节的起始时间到手机收到 SIM 卡的响应回复的第一

个字节的起始时间，所述传输时间延迟根据不同的应用场景，小于如下时间：

1) 所述传输时间延迟小于 500 毫秒，

2) 如果手机和 SIM 卡之间是应用 T = 0 协议，所述传输时间延迟小于 WT = 960*Wi，时间单位是工作 ETU，

a) 参数 Wi 是在复位应答消息 ATR 的 TC2 字节规定，

b) 如果复位应答消息 ATR 没有 TC2 字节，则 Wi = 10，

c)ETU 是工作基本时间单位，ETU = F/D*(1/f)，即传输一个比特位的持续时间，参数 F 和 D 在复位应答消息 ATR 的 TA1 字节规定，而 f 是 SIM 卡的时钟频率，

d) 如果复位应答消息 ATR 没有 TA1 字节，则 F = 372，D = 1，

3) 如果手机和 SIM 卡之间是应用 T = 1 协议，所述传输时间延迟小于 BWT = (11+2^BWI*960)，时间单位是工作 ETU，

a) 参数 BWI 是在复位应答消息 ATR 的 TB3 字节规定，

b) 如果复位应答消息 ATR 没有 TB3 字节，则 BWI = 4，

c)ETU 是工作基本时间单位，ETU = F/D*(1/f)，即传输一个比特位的持续时间，参数 F 和 D 在复位应答消息 ATR 的 TA1 字节规定，而 f 是 SIM 卡的时钟频率，

d) 如果复位应答消息 ATR 没有 TA1 字节，则 F = 372，D = 1，

4) 如果手机和 SIM 卡之间是应用 T = 0 协议，并且手机和 SIM 卡之间的复位应答消息 ATR 是通过无线传输接口协议传输的，所述传输时间延迟小于 9600ETU，ETU 是初始基本时间单位，ETU = 372*(1/f)，其中 f 是 SIM 卡的时钟频率。

6. 根据权利要求 1 所述的无线传输通信协议，其特征在于：所述通信终端接口设备和所述用户身份模块卡接口设备之间的无线传输通信协议是蓝牙通信 (Bluetooth)。

7. 根据权利要求 1 所述的无线传输通信协议，其特征在于：所述通信终端接口设备和所述用户身份模块卡接口设备之间的无线传输通信协议是无线局域网通信 (WLAN，WiFi)。

8. 根据权利要求 6 所述的蓝牙通信技术，其特征在于：所述蓝牙通信协议是应用 RFCOMM(串行线仿真协议) 来建立起链路连接，数据发送，数据接收，链路断开的无线通信过程，所述蓝牙通信协议是应用蓝牙通信物理层技术的 CRC 循环冗余校验位，编码率为 1/3 和 2/3 的 FEC 前向纠错编码，以及 ARQ 自动重传机制来实现如根据权利要求 4 所述的传输差错控制。

一种通信终端设备和SIM卡之间的无线接口及功能实现

技术领域

[0001] 本发明属于通信终端设备领域。具体地说，本发明涉及一种适用于通信终端设备和用户身份模块卡之间的无线传输接口协议，同时，也涉及具体实现这种无线通信传输接口协议的设备和方法。

背景技术

[0002] 目前，移动通信用户设备主要由通信终端设备（包括手机，移动固话，平板电脑，笔记本电脑，台式电脑，智能家居设备如智能电视，家庭媒体中心如机顶盒，家庭网络中心如路由器。为简便，以下都一律简称手机）和用户身份模块卡（包括GSM系统的SIM卡，CDMA系统的UIM卡，2G，3G和4G系统的USIM卡。为简便，以下都一律简称SIM卡）两个部分组成。其中通信终端设备具有连接蜂窝式移动通信网络的基本功能。而用户身份模块卡主要用于在安全的条件下完成用户身份认证鉴权和用户信息加密算法的全过程，并且还可以完成对网络的认证，以防止冒充的虚假网络，保护用户的通信安全。

[0003] 在现有的技术实现中，手机有一个固定在其内的SIM卡卡座，卡座上有六个引脚，使得SIM卡插入卡座后通过这些引脚（主要是数据IO引脚）和SIM卡进行接触式的通信。具体的通信协议在有关的标准中定义（如ISO-7816定义传输协议，3GPP TS 11.11等定义GSM应用协议）。这种通信是一种有线通信形式。然而，由于无线通信的固有方便性，人们做出大量的努力，希望能用一种方便的无线通信来连接手机和SIM卡。但另一方面，由于SIM卡存储有用户最为敏感的机密信息（如鉴权密钥Ki等）并承担着保护用户的通信安全的重任，这些努力而得到的方法都或多或少地以牺牲通信安全性为代价，在现有蜂窝式移动通信网络的身份认证鉴权和接入安全控制机制下，不能够被实现。

[0004] 在中国发明专利申请201080022761.7“便携式个人SIM卡”中（美国专利US 8244181B2“Portable personal SIM card”），就提出一种方法，通过近场通信(NFC)把SIM卡的数据下载到手机，进而手机应用下载的数据接入到移动通信网络。为了叙述方便起见，下面引用该专利申请的原文及附图进行说明：

[0005] 权力要求1. 一种用于对移动装置进行供应的方法，其包括：

[0006] 在所述移动装置与含有SIM卡的个人物品之间建立近程通信链路；以及

[0007] 经由所述所建立的近程通信链路接收存储在所述SIM卡中的供应数据。

[0008] 权力要求27. 一种个人物品，其包括：

[0009] 处理器；

[0010] SIM卡，其耦合到所述处理器，其中所述SIM卡在其中存储有用于蜂窝式通信网络的供应数据；以及

[0011] 近程通信收发器，其耦合到所述处理器，

[0012] 其中所述处理器以软件指令配置以执行包括以下操作的步骤：

[0013] 建立与移动装置的近程通信链路；以及

[0014] 经由所述所建立的近程通信链路将存储在所述SIM卡内的所述供应数据发射到

所述移动装置。

[0015] 发明内容[0004]揭示一种用于将存储在单个SIM卡中的供应数据提供给多个移动装置的方法和设备。供应数据存储在包含于例如一件珠宝或腕表等个人物品内的SIM卡中。所述个人物品建立与近程通信链路的有效范围内的移动装置的近程通信链路，且发射存储在所述SIM卡上的供应数据。移动装置使用不同于所述近程通信链路的第二通信链路来使用所发射和所接收的供应数据与蜂窝式或其它无线通信网络连接。一旦供应数据已交换，近程通信链路便可终止，且移动装置可使用第二通信链路来建立或接收无线数字通信呼叫。

[0016] 根据如上所述原文的权利要求1和27，发明内容和图6，7，8(原文的图4A，8，6)所示，可以得到发明申请201080022761.7的有关基本方法和步骤：

[0017] 1)手机通过和SIM卡之间的无线通信链路，下载存储在SIM卡上的供应数据(provisioning data)。

[0018] 2)手机在下载完SIM卡上的供应数据后，断开和SIM卡的通信链路。

[0019] 3)手机通过下载而得到的供应数据，接入到蜂窝式通信网络，进而建立起和网络的通信链路。

[0020] 实际上，根据发明申请201080022761.7所述的方法，按照现有技术对手机接入移动通信网络的安全控制的要求，手机是不可能接入到网络并为用户提供无线通信服务的。蜂窝式移动通信网络（如GSM系统以及新一代的3G，4G通信系统）有完备的身份认证鉴权过程和网络接入安全控制机制，对于那些用户安全敏感的数据，是不允许在空中传输的，也是不能被用户获取的。

[0021] 根据发明申请201080022761.7所述的方法，手机需要首先下载SIM卡的供应数据，再用所下载的供应数据接入到移动通信网。诚然，手机可以下载存储在SIM卡上的部分数据（如存储在SIM卡上的短消息内容，电话号码等），但是，那些用于手机接入到移动通信网络的安全控制数据（如鉴权密钥Ki和鉴权密码算法A38(A3算法和A8算法的合体，又称COMP128算法）的具体实现）是不能被下载的。实际上，根据SIM卡的功能性标准ETSI GSM 02.17，根本就没有用于读取这些数据的接口。这些与用户安全有关的数据只能存储在于SIM卡内部，只在SIM卡内部被使用，并受到访问控制。这是因为：

[0022] 1)SIM卡作为移动通信用户的唯一身份标识，是智能卡的一种，除了中央处理器CPU和串行通信接口外，其存储区域有三个即工作存储器RAM，程序存储器ROM和数据存储器EEPROM，存储在其上的数据具有不同的访问权限。特别，作为网络接入控制的安全数据甚至不是由SIM卡生产商在生产阶段写入的，而是由网络服务提供商在供给用户使用时才写入的，并只能被网络服务提供商访问，以保证安全数据被充分保密。因此，即使用户拥有了SIM卡，并不是存储在SIM卡上的所有数据都能被用户访问。

[0023] 2)SIM卡作为智能卡的一种，遵循ISO-7816标准。ISO-7816就是为了提供一种智能的，不能被复制的身份卡而制作的标准。如果SIM卡的所有数据能被手机下载，那么这个SIM卡就可以很容易地被复制，甚至不需要具有一个实体的SIM卡而在手机中存储全部数据而作为一个“虚拟”的SIM卡，进一步还可以使同一个“虚拟”SIM卡具有多个拷贝。这样一来，ISO-7816标准就失去了作为身份卡标准而存在的意义。每一个智能卡都需要一个唯一的身份号码（如ICCID，集成电路卡识别码）来彼此区分，它们不能彼此互相代替，更不能

被修改。所以这种能够被任意复制的“虚拟”SIM 卡从本质上讲就不是一个 SIM 卡（由于技术缺陷等原因如果 SIM 卡确实能够被复制，只能说明需要升级技术，加强 SIM 卡的安全性），因为它不能被唯一地区分。

[0024] 综上所述，发明申请 201080022761.7 所述的从 SIM 卡下载的供应数据，是不能用于移动通信网络的网络接入，至少是不能接入按照现有技术实现的网络接入安全控制机制的蜂窝式移动通信网络。

[0025] 同样，根据发明申请 201080022761.7 的方法，手机在下载完 SIM 卡上的供应数据后，断开和 SIM 卡的通信链路。这是把手机接入移动通信网络的过程看成是一个静止的，从手机到网络的单向过程（如发明申请 201080022761.7 的图 6 所示）。然而实际上，SIM 卡和网络之间的身份认证鉴权是一个动态的交互过程，涉及到手机和网络连接的整个持续期间。

[0026] 1) 手机接入到移动通信网络的过程涉及到身份认证鉴权，网络和 SIM 卡之间（而不是网络和手机之间，手机只能作为一个消息的传递者）有一个消息信令交互过程。手机向网络发出入网请求后，网络生成一个随机数序列 RAND，发送给手机，手机收到 RAND 后，需要把 RAND 发给 SIM 卡，SIM 卡以 RAND 和鉴权密钥 Ki 为参数，在 SIM 卡内部运行鉴权密码算法 A38，生成鉴权码 SRES，然后 SIM 卡把 SERS 码传给手机，手机再传送给网络，供网络验证用户的合法性。在这个过程中，必须有 SIM 卡的参与，这正是 SIM 卡作为智能卡而具有中央处理器 CPU 的意义，否则它只需要存储数据而把计算工作转交的手机就可以了。而如果手机在发起网络接入请求之前就断开了和 SIM 卡的连接，就无法完成这个入网身份认证鉴权过程。

[0027] 2) 为了进一步加强安全性，有时需要双向的身份认证鉴权。也就是说，SIM 也需要验证网络的合法性，防止接入到一个虚假的冒充网络。这个时候，由于 SIM 卡已经断开了和手机的通信链路，就无法和网络进行消息信令交互，完成对网络的身份认证鉴权。

[0028] 3) 实际上，在整个手机与移动通信网络维持连接的过程中，SIM 卡与网络之间的身份认证鉴权需要持续的进行。例如在在每次发起网络呼叫请求，或者手机收到网络的寻呼的时候，都需要 SIM 卡的身份认证鉴权的过程，甚至在没有呼叫请求和被呼叫的时候，只要用户的位置发生变化而需要改变其 VLR（访问位置寄存器）时，也需要进行身份认证鉴权的过程。而如果手机和 SIM 卡的 连接是断开的，就无法完成这些身份认证鉴权过程。

[0029] 综上所述，发明申请 201080022761.7 所述的从 SIM 卡下载的供应数据后，就断开和 SIM 卡的通信链路的方式，也是不能完成移动通信网络的网络接入，至少是不能接入按照现有技术实现的网络接入安全控制机制的蜂窝式通信网络，也不能维持和网络的持续连接。

[0030] 退一步讲，如果网络服务提供商愿意和用户分享用于网络接入安全控制的数据（如鉴权密钥 Ki 等），也愿意冒着敞开网络安全的大门，迎接假冒各种身份的网络入侵者的风险，那么实际上，就没有必要需要一个 SIM 卡。用户只需要把那些用于网络接入安全控制的数据存储在手机上就足够了，当然，也就不需要根据发明申请 201080022761.7 所述的方法来下载 SIM 卡的供应数据，然后再接入到蜂窝式无线通信网络。

[0031] 所以，要使用发明申请 201080022761.7 所述的方法来完成手机接入到移动通信网络，需要改变现有的蜂窝式移动通信网络接入的安全控制机制，在不需要用户鉴权密钥

Ki 的情况下，也能够完成身份认证鉴权。这样的安全控制机制类似互联网的用户名 - 密码登陆方式，大大降低了移动通信网络的安全性。

[0032] 在中国发明申请 201210266545.8“使用单个无线用户身份模块在无线链路上同时验证多个设备”中，提出了在多个设备之间通过无线连接的方式分享同一个 SIM 卡的方法：

[0033] 权力要求 1. 一种用于建立从用户身份模块 (SIM) 到第一设备的无线通信路径的方法，所述方法包括：

[0034] 在 SIM 处接收来自所述第一设备的访问请求；

[0035] 从 SIM 向第二设备发送报警；以及

[0036] 在 SIM 处接收来自所述第二设备的消息，

[0037] 其中，所述第一设备和所述第二设备是物理地独立的，

[0038] 其中，当所述消息允许所述第一设备访问 SIM 时，SIM 对于所述第一设备准许访问，以及

[0039] 其中，当所述消息不允许所述第一设备访问 SIM 时，SIM 对于所述第一设备拒绝访问。

[0040] 发明内容 [0007] 本发明通过提供一种能够与移动设备进行无线通信的 SIM，以使至少一个设备能够远程地使用一个 SIM 连接到无线网络来解决现有技术的至少一些缺陷。SIM 可以出现在移动电话中，或可以是独立 (stand-alone) 设备。因为 SIM 无需物理地在这些设备中重新定位，所以在膝上型设备或手持设备访问 SIM 时，移动电话仍可使用。

[0041] 根据权利要求 1 和发明内容，可以得到有关发明申请 201210266545.8 的关键点：

[0042] 1) 另外的一个或多个设备访问手机的 SIM 卡。

[0043] 2) 同时，手机连接于网络中，为用户提供服务。

[0044] 3) 另外的一个或多个设备通过从 SIM 卡获得的信息连接到无线网络

[0045] 这种多个设备同时通过同一 SIM 卡的（通过访问与网络接入有关的信息）接入到无线通信网络的方法，本质上是违背现有无线通信网络的网络接入安全控制机制的，同时，网络和手机之间的通信会引起通信的混乱和安全隐患。因为：

[0046] 1) 根据 3GPPTS 11.11 标准，当手机和网络处于连接中时，手机和 SIM 的通信接口 SIM-ME 接口是处于持续的连接中，甚至在通话过程中，如果 SIM 卡从手机中移出而断开 SIM-ME 接口，通话连接就会立即中断。

[0047] 2) 与此同时，另外的设备如果要通过同一个 SIM 的鉴权信息接入到无线通信网络，在网络看来，已经有用户在网络中，并得到有关的唯一的账单信息和业务授权，但此时有新的用户请求使用同一账单信息和业务授权，网络端就会引起混乱，无所适从。例如，当两个设备同时使用网络时，如何去处理账单。

[0048] 3) 由于多个设备同时接入无线通信网络，当网络端有消息或者数据（例如，电话呼入或者数据下载）需要传输给用户时，数据被传输给哪一个设备是无法确定的。因为 SIM 卡是被网络作为唯一的身份标识，多个设备在网络端看来就是一个用户，无法彼此区分。而如果同时传给所有设备又违背了无线通信网络最基本的保密通信原则，即用户数据不能被中途窃听。即使是用户同意分享的信息，也是在接收到后再分享给多个设备，而不能在网络不知道的情况下，在无线通信链路的中途分发给多个设备。

[0049] 4) 实际上，通过鉴权加密算法 A38 的“碰撞”攻击，早期的 SIM 卡有可能被猜测到

用户鉴权密钥Ki而复制（目前的SIM卡由于安全性的加强，已经不能被复制），同一SIM卡就有可能被复制成 多个完全相同的SIM卡而被多个设备同时使用，接入到无线通信网络。实际的试验表明，通过这种方式接到无线网络的多个设备，当网络呼叫用户时，要么是随机地呼叫多个设备中的某一个设备，要么是呼叫最后一个接入无线通信网络的设备。同样，发明申请201210266545.8通过共享SIM而接入无线网络的多个设备，即使可以接入，但是当网络呼叫用户时，也只能是一个设备被呼叫。

[0050] 5）更进一步地，在手机通话过程中，如果有呼入，现有的网络会提示“..... 请稍后再拨”。而如果是两个手机通过同一个SIM卡接入到网络，一个在通话过程中，另一个被呼叫，如何处理这种情况，根据现有的技术，还不清楚。因为在网络端看来，只有一个用户接入到网络，而在用户端看来，有两个设备接入到网络。

[0051] 所以，通过发明申请201210266545.8的方法接入到无线通信网络的多个设备在现有的网络中是无法支持的，也是不被网络服务提供商所允许的。

[0052] 在中国发明申请201410452312.6“一种智能的分离式SIM卡卡座设备及通信方法”中，提出一种在手机和SIM卡之间的中间设备，智能型SIM卡卡座，来取代现有的固定在手机内部的SIM卡卡座。智能型SIM卡卡座和SIM卡的接口是现有的接触式引脚，而和手机的接口可以是无线接口。这样，智能型SIM卡卡座只有一个单单的连接作用，只是转发手机和SIM卡之间的数据交换。并且在任一时刻，只有一个用户设备连接于蜂窝式的无线通信网络。在SIM卡和网络双方看来，这个智能型SIM卡卡座是透明的，不会觉察到其存在。对现有的身份认证鉴权过程和网络接入安全控制机制没有任何的影响，很好地兼顾了现有无线通信网络的安全性和手机-SIM卡之间无线传输接口的方便性。

[0053] 本发明的目的就是公开了一种手机和SIM卡之间无线传输接口的通信协议。通过这个无线传输接口的通信协议，把现有在手机中通过SIM卡座的六个引脚的直接电路信号连接（实际上，只有两个引脚，串口数据IO口和重置RST口，涉及到信息交换），转化成无线通信连接，并对现有的蜂窝式移动通信网络的网络接入安全控制机制和身份认证鉴权过程没有任何影响，极大地方便了用户的使用。

发明内容

[0054] 本发明的关键之处在于对现有的手机和SIM卡之间的带触点的接触式引脚的数据通信来说，本发明公开的手机和SIM卡之间无线传输接口协议的转接通信是透明的。也就是说，这种无线传输接口的通信协议无论是对手机还是对SIM卡来说，都不会觉察到这个中间转发通信的存在。其具体的技术方案是控制中间无线转发通信的传输时间延迟和传输差错，使得传输时间延迟和传输差错都在原来的手机和SIM卡之间通过接触引脚直接通信的传输时间延迟和传输差错的允许范围之内。

[0055] 本发明的目的是通过以下的技术方案实现的。图1是本发明的各个功能模块示意图和它们之间的通信连接图。模块1是手机，模块2是SIM卡，模块3是手机接口设备，模块4是SIM卡接口设备。其中手机（模块1）和手机接口设备（模块3）通过现有的智能卡传输协议ISO-7816连接（模块5）而进行通信，SIM卡（模块2）和SIM卡接口设备（模块4）也是通过智能卡传输协议ISO-7816连接（模块6）进行通信。手机接口设备（模块3）和SIM卡接口设备（模块4）进一步通过无线传输通信协议（模块7）进行通信，这样，手机

和 SIM 卡之间通过各自的接口设备和接口设备之间的无线传输转发，建立起了它们之间的通信连接。

[0056] 在手机和 SIM 卡建立起通信会话的开始阶段，或者在通信会话过程中由于传输错误需要重启通信会话，有一个通信协议参数协商过程。SIM 卡向手机传输 ATR（冷复位应答或者热复位应答）消息，传输协议参数包括在 ATR 消息中，或者包括在紧接着 ATR 消息后得 PPS（协议参数选择）会话中。在本发明中，其 ATR 消息（或者 PPS 消息）就不需要通过无线传输接口从 SIM 卡传输给手机，而是在手机端，由手机接口设备（模块 3）对手机（模块 1）进行复位应答，在它们之间商议 ISO-7816 协议参数（模块 5 的协议参数）；而同时在 SIM 端，由 SIM 卡（模块 2）对 SIM 卡接口设备（模块 4）进行复位应答 ATR（或者 PPS，协议参数选择），在它们之间商议 ISO-7816 协议参数（模块 6 的协议参数）。其中模块 5 的协议参数和模块 6 的协议参数可以不一致。当然，它们之间也可以通过无线传输接口彼此交换复位应答消息或者 PPS 消息，使得两端的 ISO-7816 传输协议参数是一致的。

[0057] 在现有的技术实现中，SIM 卡和手机之间大多是应用 ISO-7816 的 T ＝ 0 协议（字节传输协议），也就是说 T ＝ 0 协议所处理的最小单位是单个字节，包含 8 个比特位。在 8 个比特位之前有 1 个起始位，在 8 个比特位之后有 1 个传输错误检测的校验位，总共有十个比特位传输一个字节。在 SIM 卡和手机之间是一个字节接着一个字节的传输，字节之间通过其起始位（一个比特位（工作 ETU，工作基本时间单位）的低电平信号）来区分，并且在字节之间有一个传输错误反馈机制，对于错误的传输字节，需要紧接着立即重传该错误的字节。在本发明中，模块 5 和模块 6 遵循现有的智能卡传输协议 ISO-7816（即现有的 SIM 卡和手机之间的传输协议）。在无线传输接口协议模块 7 中，由于有无线传输协议数据单元的封装，每 8 个比特可以表示一个字节，它们之间不需要一个比特位来区分。为了提供更强的无线传输差错控制，在 8 个比之特后有一个额外的校验位。也就是说，加上原来的校验位，总共有 10 个传输比特位中，其中前面的 8 个是一个字节的信息比特位，后面的 2 个是错误检测的校验比特位。

[0058] 图 2 是本发明的字节传输协议单元的一个例子，包括 2 个单元模块，即模块 8 和模块 9。其中模块 8 是传输字节的 8 个信息比特位，比特 0 至比特 7。而模块 9 是传输字节的 2 个校验比特位，比特 8 至比特 9。校验比特位 8 和 9 可以是相同的奇偶校验位的重复，也可以是其它形式。通过比 ISO-7816 协议多 1 个比特的校验位，提供更强的字节差错控制，使得无限传输接口协议更为可靠。

[0059] 在 ISO-7816 的 T ＝ 0 协议中，在同一个传输方向（手机向 SIM 卡传输，或者 SIM 卡向手机传输），字节是一个一个的传输，并且传输错误检测和重传也是基于字节的。在本发明中的无线传输接口协议中，为了更有效率的传输手机和 SIM 卡之间的数据交换，在同一个方向上连续传输的若干字节就可以连接起来，组成一个传输字节块。这样的一个字节块可以进行联合纠错编码，例如传输字节块的 CRC 校验（循环冗余校验）和 FEC（前向纠错）纠错编码。并且连续传输的若干字节在一起传输，可以组成一个完整的命令或者对命令的响应，这样当手机或者 SIM 卡收到字节块后，就可处理命令，而不需要等待下一个字节在无线传输接口的传输延迟。

[0060] 图 3 是本发明的一个无线传输数据帧形成的例子。模块 10 是一个典型的 ISO-7816 命令传输协议数据单元 (C-TPDU)，它包含有 5 个字节的命令头。CLA 表示命令类别，INS 表

示指令代码，P1 和 P2 表示命令的两个附加参数，P3 指名了紧接着手机要传给 SIM 卡的数据的长度，或者期待 SIM 卡要回送的数据的最大长度。这 5 个字节的命令头就组成一个传输字节块，每个字节有 8 个信息比特位和 2 个校验比特位，总共 50 个信息比特位，再加上 CRC 循环冗余校验位和 FEC 前向纠错编码位，就组成了模块 11，即无线传输的信息比特域。最后，加上一些必要的传输控制信息如无线传输的目标地址，数据的长度指示就构成了无线传输接口的数据帧，即模块 12。这样的无线传输的数据帧在空中接口被一次性地传输，5 个字节的命令头就可以被 SIM 卡一次完整地接收，减少了命令传输协议数据单元在空中无线接口的传输延迟。

[0061] 当 SIM 卡接收到命令头以后，向手机回送一个过程字节。如果过程字节指明手机可以传输该命令头的后续数据，同样，这些数据字节就组成了一个传输字节块，加上 CRC 循环冗余校验位和 FEC 前向纠错编码位，并形成无线传输接口的数据帧，一次性的全部传送个 SIM 卡。SIM 卡需要回送给手机的数据也可以用同样的方式在无线空中接口一次传输，从而减少数据在空中无线接口的传输延迟。

[0062] 对于 ISO-7816 的 T ＝ 1 协议（字节组传输协议），由于一次传输的字节组是由多个字节组成，所以，在无线传输的数据帧形成过程中，传输字节组的多个字节就形成了一个自然的字节块，它们一起进行 CRC 校验和 FEC 纠错编码，并最终形成一个无线数据帧，一次性地在空中传输。

[0063] 图 4 是 T ＝ 1 字节组传输协议的无线传输的数据帧形成例子示意图。模块 13 是字节组传输协议的字组数据帧，包含 3 个部分，组头字段，信息字段和组尾字段。其中组头字段有 3 个字节，即节点字节 (NAD)，协议控制字节 (PCB) 和长度 (LEN)；信息字段是可选地，长度是 0-254 个字节，包含有应用协议数据单元 (APDU) 或者控制信息 (INF)；而组尾字段是 1 个字节的错误检测 (EDC)。这些字节就是本发明的无线传输接口协议的有效信息载荷，把它们一起进行 CRC 循环冗余校验位和 FEC 前向纠错编码位，就形成了无线传输的信息域，即模块 14。最后，再加上一些必要的无线传输的控制信息域，就组成了本发明的无线传输接口协议的空中接口数据帧，即模块 15，在无线传输接口协议的空中接口中一次性地被传输。

[0064] 当接收端检测到无线数据帧有传输错误，并且错误是无法通过纠错编码进行错误纠正的时候，就可以通过 ARQ（自动重传请求）机制，请求发射端重新传送字节块。并且这种字节块的重新传送可以重复多次， 直到接收到正确的字节块，或者同一字节块的传输时间大于最大等待时间 (WT)，手机发出热复位命令或者终止和 SIM 卡的会话。

[0065] 这样，通过多层次的传输错误控制机制，包括单个字节的奇偶检验，多个连续传输的字节快的 CRC 校验和纠错编码的错误比特保护，和自动重传请求机制，确保了本发明的无线传输协议的可靠性。使得和现有的手机和 SIM 卡之间的触点通信比较起来，具有相同的传输可靠性。

[0066] 手机和 SIM 卡的数据交换总是从手机发送命令，SIM 卡对命令进行回应的方式进行。根据本发明的传输方式，由于手机接口设备和 SIM 卡接口设备以及它们之间的无线传输接口的转发，这种命令和响应的交互方式就会有额外的延迟（相对于现有的带触点的接触式引脚通信来说）。为了使得本发明的无线传输接口对于手机和 SIM 卡的数据交换是透明的，这种数据传输的延迟就应当在现有的 ISO-7816 的最大传输延迟和 GSM 规定的最大处

理延迟的范围之内。

[0067] 图 5 是本发明的传输延迟的例子，模块 16 是总的传输时间延迟。即手机端在发送最后一个命令字节后，直到它接收到 SIM 卡的响应的第一个回应字节之间的总共时间延迟。包括手机接口设备的数据处理和无线转发延迟，从手机接口设备到 SIM 卡接口设备之间无线传输的空中传输延迟，SIM 卡接口设备接收处理及向 SIM 卡的转发延迟，SIM 卡的处理延迟，SIM 卡接口设备的数据发送处理及无线转发延迟，SIM 卡接口设备到手机接口设备之间无线传输的空中传输延迟，最后还有手机接口设备的接收处理及向手机的转发延迟。模块 16 的时间延迟是指手机传输的最后一个字节的起始时间到手机收到 SIM 卡的响应回复的第一个字节的起始时间。根据 ISO-7816 智能卡传输协议，在 T ＝ 0 和 T ＝ I 协议中都规定了这种在相反方向上的最大等待时间。为了使得本发明的无线传输接口协议对于手机和 SIM 卡之间的数据交换是透明的，传输时间总延迟模块 16 就必须小于这些协议规定的最大延迟，如下所述 ：

[0068] 1) 如果 SIM 卡的复位应答消息 ATR 是通过无线传输方式在手机和 SIM 卡之间交换的，对于 T ＝ 0 协议，有一个最大初始等待时间，也就是说，SIM 卡回复的连续两个数据的起始沿之间的时间间隔。ISO-7816 规定这个时间间隔不超过 9600 个初始 ETU，对于缺省的参数设置来说，这个时间就是 1 秒。在手机和 SIM 卡建立连接的开始，ATR 消息的第一个字符，初始字符 TS，可以直接由手机接口设备直接传给手机，而不需要经过无线传输接口协议由 SIM 卡传来。因为初始字符 TS 只是规定了后续字节的逻辑约定，只存在于手机接口设备和手机之间。对于后续的传输协议参数约定，其最大的时间延迟，模块 16，就必须小于 9600 个初始 ETU 的时间。当然，如果复位应答消息 ATR 不是通过无线传输接口协议由 SIM 卡传输给手机的，而是在手机和手机接口设备之间，SIM 卡接口设备和 SIM 卡之间分别建立的，那么，总计延迟时间模块 16 的时间就可以不受这个最大初始等待时间的限制。

[0069] 2)T ＝ 0 协议规定了在字节传输过程中，有一个等待时间 WT，即两个连续字节之间（当前字节是由 SIM 卡传输，上一个字节是由手机或者 SIM 卡传输）的最大等待时间延迟为 WT。其具体的计算是 :WT ＝ 960*Wi，时间单位是工作 ETU。其中参数 Wi 是在复位应答消息 ATR 的 TC2 字节规定，如果 ATR 没有提供 TC2 字节，则 Wi 取缺省值 10，即 WT 等于 9600 个工作 ETU。这样，总延迟时间模块 16 的时间就小于 WT ＝ 9600 个工作 ETU 的传输时间。

[0070] 3)T ＝ I 协议规定了在字组传输过程中，有一个块等待时间 BWT，即相反方向上两个连续字节块的最大时间延迟。BWT ＝ (11+2^BWI*960)，时间单位是工作 ETU。参数 BWI 是在复位应答消息 ATR 的 TB3 字节规定，取值范围是 0-4 之间，缺省值是 4。即 BWT 的缺省时间是 15371 个工作 ETU。这样，总延迟时间模块 16 的时间就小于 BWT ＝ 15371 个工作 ETU 的传输时间（缺省）。

[0071] 4) 在 SIM 卡应用协议 3GPP TS 03.20 中，规定了用户身份认证鉴权算法 A3 的运行时间是小于 500ms（毫秒），即是说 SIM 卡的处理时间（运行 A3 算法时）小于 500 毫秒。在本发明中，再加上接口设备的转发和空中的无线传输延迟，也就小于 500 毫秒。这样，总延迟时间模块 16 的时间就小于 500 毫秒。

[0072] 根据以上的计算，现有的无线传输技术，如无线局域网 WiFi，无线蓝牙技术，其传输时间延迟都远远小于这些时间延迟要求，可以直接应用于本发明的无线传输接口协议。例如，对于蓝牙技术，从发射端到接收端的时间延迟可以短至 3 毫秒，在空中一个往返传输

就是 6 毫秒，远远小于 ISO-7816 的字节传输等 待时间，也远远小于 GSM 规范规定的 SIM 卡处理时间延迟要求。这样，在 SIM 卡接口设备和手机接口设备之间，可以多次重传同一个无线传输数据帧，而时间延迟也在要求的范围之内，从而提高本发明的无线传输接口协议的传输可靠性。

[0073] 综上所述，本发明的无线传输接口协议提供了完备的传输差错控制和传输延迟控制，使得无线传输接口协议的转接通信对于手机和 SIM 卡来说都是透明的，对它们之间的数据交换没有任何影响，它们之间的数据传输可以无缝地进行。

[0074] 发明的效果

[0075] 在本发明的技术实施方案中，无线传输接口协议提供了完备的传输差错控制和传输延迟控制，把现有在手机中通过 SIM 卡座的六个引脚的直接电路信号连接转化成无线传输通信连接，使得这种无线转发（包括手机和手机借口设备之间，SIM 卡和 SIM 卡接口设备之间的有线转发）通信对于手机和 SIM 卡来说都是透明的，对现有的蜂窝式移动通信网络的网络接入安全控制机制和身份认证鉴权过程没有任何影响，也对 SIM 卡对网络的通信鉴权没有任何影响。移动通信网络服务提供商无需也不能知道这个转发通信的存在，对用户身份的认证鉴权，网络接入安全控制，用户帐单的处理都可以按照现有的方式进行。对用户来说，可以通过本发明的无线传输接口协议，在不同的应用场景，把 SIM 卡连接于不同的通信终端设备而获取移动通信服务，极大地方便了用户的使用。

附图说明

[0076] 图 1 是本发明的各个功能模块示意图和它们之间的通信连接图。模块 1 是手机，模块 2 是 SIM 卡，模块 3 是手机接口设备，模块 4 是 SIM 卡接口设备。模块 1 和模块 3 通过模块 5 进行通信，模块 2 和模块 4 通过模块 6 进行通信。模块 3 和模块 4 进一步通过无线传输通信协议模块 7 进行通信。

[0077] 图 2 是本发明的字节传输协议单元的一个例子。其中模块 8 是传输字节的 8 个信息比特位，比特 0 至比特 7。而模块 9 是传输字节的 2 个校验比特位，比特 8 至比特 9。

[0078] 图 3 是本发明的一个无线传输数据帧形成的例子。模块 10 是传输字节信息块，模块 11 是加上错误检测和纠错编码后，组成无线传输的信息比特域，模块 12 是加上传输控制信息的无线传输接口数据帧。

[0079] 图 4 是本发明的另一个无线传输数据帧形成的例子。模块 13 是传输字组信息块，模块 14 是加上错误检测和纠错编码后，组成无线传输的信息比特域，模块 15 是加上传输控制信息的无线传输接口数据帧。

[0080] 图 5 是本发明的传输延迟示意图，传输时间延迟模块 16 是指手机传输的最后一个字节的起始时间到手机收到 SIM 卡的响应回复的第一个字节的起始时间。包括手机接口设备的数据处理和无线转发延迟，从手机接口设备到 SIM 卡接口设备之间无线传输的空中传输延迟，SIM 卡接口设备接收处理及向 SIM 卡的转发延迟，SIM 卡的处理延迟，SIM 卡接口设备的数据发送处理及无线转发延迟，SIM 卡接口设备到手机接口设备之间无线传输的空中传输延迟，以及手机接口设备的接收处理及向手机的转发延迟。

[0081] 图 6 是发明申请 201080022761.7 原文的图 4A，图 7 是发明申请 201080022761.7 原文的图 8，图 8 是发明申请 201080022761.7 原文的图 6。

具体实施方式

[0082] 根据不同的现有无线传输技术，本发明的通信终端设备和 SIM 卡之间的无线传输接口协议可以有不同的具体实施方式。下面就以蓝牙通信技术为例来进一步对本发明进行说明。

[0083] 如图 1 所示，在手机端，手机和手机接口设备之间的通信是现有的 ISO-7816 智能卡传输协议；而在 SIM 卡端，SIM 卡和 SIM 卡接口设备之间的通信也是现有的 ISO-7816 智能卡传输协议。所以，下面就具体说明在手机接口设备和 SIM 卡接口设备之间通过蓝牙通信技术来实现本发明的无线传输接口协议。

[0084] 从蓝牙通信技术的数据链路协议来看，有一个中间协议层，电缆替代协议 (RFCOMM)。RFCOMM 是基于 ETSI TS-07.10 规范的串行线仿真协议，RFCOMM 协议层位于 L2CAP 协议层和应用层协议之间，是 一个传输层协议，在蓝牙基带协议上仿真 RS-232 控制和数据信号，为使用串行线传送机制的上层协议提供服务。RFCOMM 是使一种简单的传输协议，其目的是针对如何在两个不同设备上的应用之间保证一条完整的通信路径，并在它们之间保持一个通信段。在 RFCOMM 的基础上，蓝牙串口协议 (SPP Profile) 提供了面向应用的 Profile，具有更好的设备之间传输兼容性。本发明的通信终端设备和 SIM 卡之间的无线传输接口协议就可以基于 RFCOMM 协议来实现。其具体的实施方案可以分为链路连接，数据发送，数据接收，链路断开的过程。

[0085] 1) 链路连接，首先要建立 RFCOMM 会话，协商传输信道的传输参数，并建立起用户数据的传输链路，得到确认后就建立起了链路连接。

[0086] 2) 用户数据和控制命令的发送，在这个过程中有数据链路的传输流量控制。

[0087] 3) 用户数据和控制命令的接收。

[0088] 4) 链路断开，当接收端和发射端的两个应用要结束通信对话的时候，就断开他们之间的 RFCOMM 链接。

[0089] 在蓝牙通信技术的物理层，也提供了完备的传输差错控制机制，包括 CRC 循环冗余校验位，编码率为 1/3 和 2/3 的 FEC 前向纠错编码，以及 ARQ 自动重传机制。这些差错控制协议都可以直接应用于本发明的无线传输接口协议，而得到很好的传输差错控制。

[0090] 蓝牙通信技术也提供了很好的传输时间延迟控制。在两个蓝牙设备之间，通过蓝牙 4.0 协议，可以在 3 毫秒之内建立起通信链路并开始进行数据通信。应用于本发明的无线传输接口协议，完全满足传输时间延迟的需求。

[0091] 通过蓝牙通信技术来转发手机接口设备和 SIM 卡接口设备之间的数据交换，几乎可以不加以任何修改的具体实施。蓝牙通信技术为本发明的通信终端设备和 SIM 卡之间的无线传输接口协议提供了一个很好的具体实施例子。

[0092] 通过其它的一些现有无线传输技术，也可以具体实施本发明的通信终端设备和 SIM 卡之间的无线传输接口协议，只要其传输时间延迟和传输差错控制满足要求就可以了。例如 WiFi，无线 USB，Zigbee 等都可以应用于本发明的具体实施例子中。

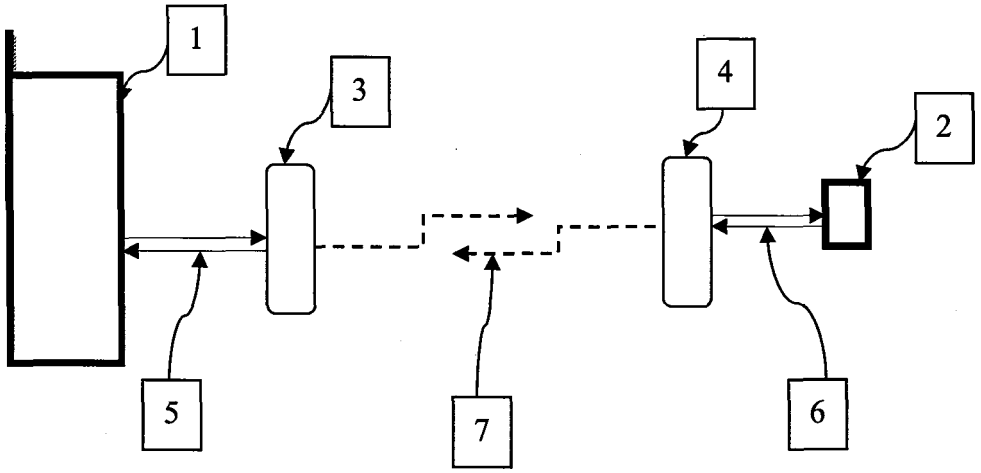

1
3
4
2
5
7
6

图 1

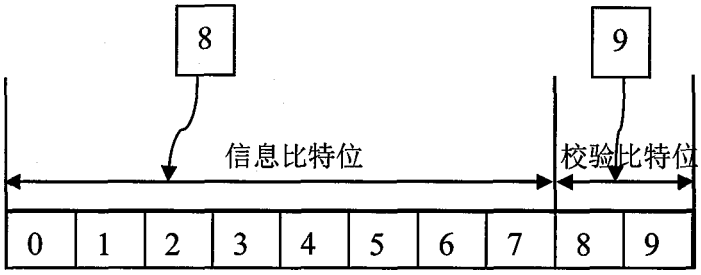

8
9
信息比特位
校验比特位
0 1 2 3 4 5 6 7 8 9

图 2

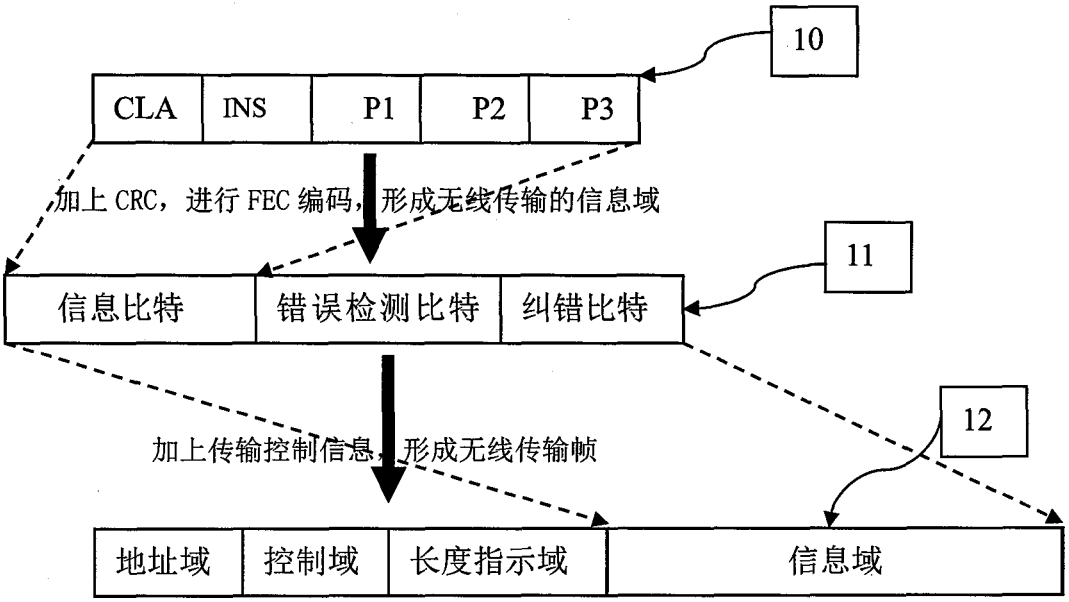

10
CLA INS P1 P2 P3
加上 CRC，进行 FEC 编码，形成无线传输的信息域
11
信息比特 错误检测比特 纠错比特
加上传输控制信息，形成无线传输帧
12
地址域 控制域 长度指示域 信息域

图 3

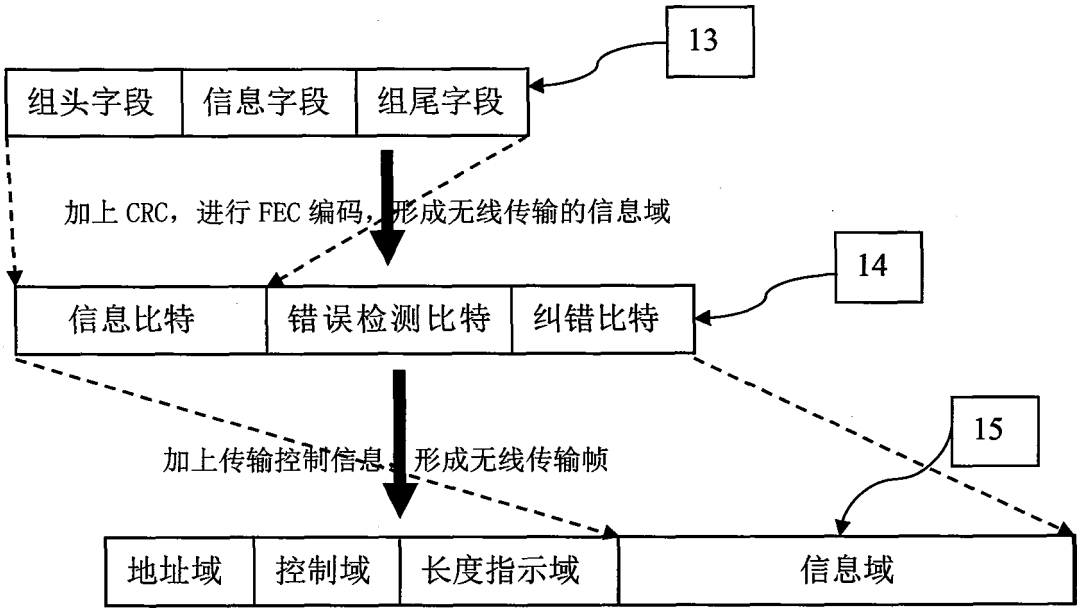

13
组头字段
信息字段
组尾字段
加上 CRC，进行 FEC 编码，形成无线传输的信息域
14
信息比特
错误检测比特
纠错比特
15
加上传输控制信息，形成无线传输帧
地址域
控制域
长度指示域
信息域

图 4

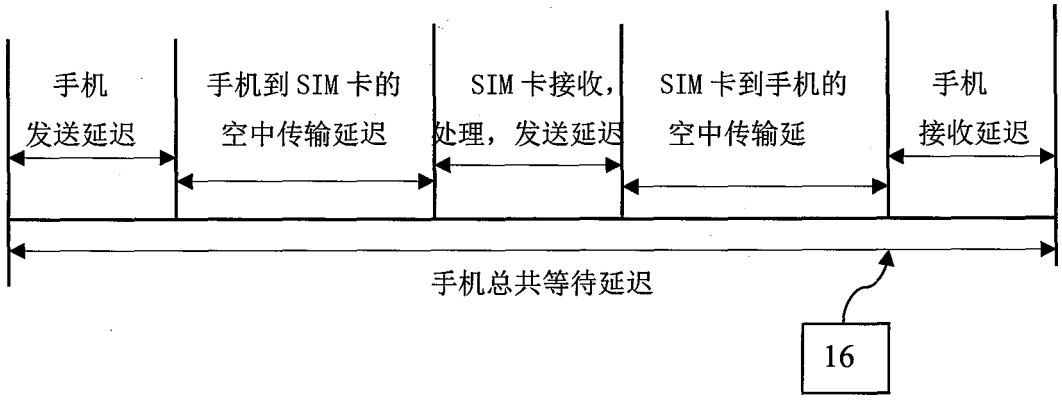

手机
发送延迟
手机到 SIM 卡的
空中传输延迟
SIM 卡接收，
处理，发送延迟
SIM 卡到手机的
空中传输延
手机
接收延迟
手机总共等待延迟
16

图 5

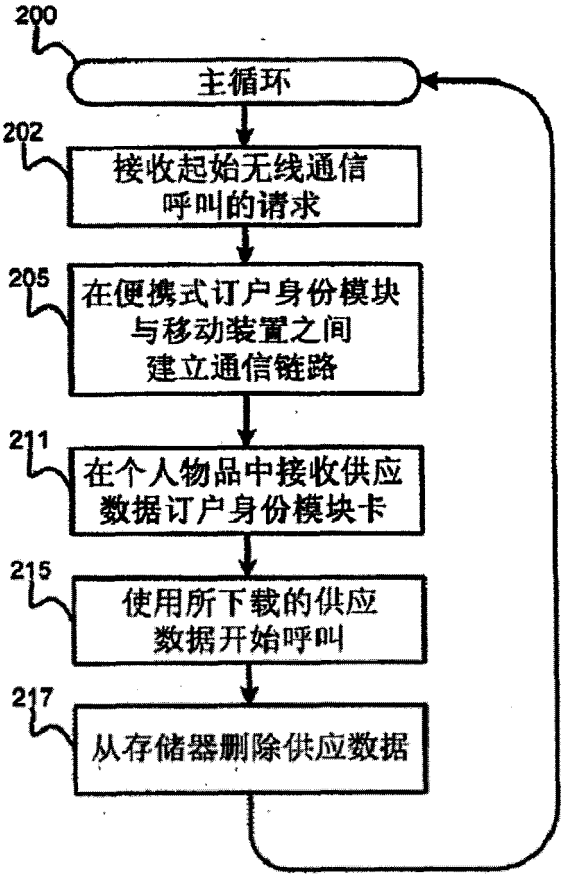

200
主循环
202
接收起始无线通信呼叫的请求
205
在便携式订户身份模块与移动装置之间建立通信链路
211
在个人物品中接收供应数据订户身份模块卡
215
使用所下载的供应数据开始呼叫
217
从存储器删除供应数据

图 6

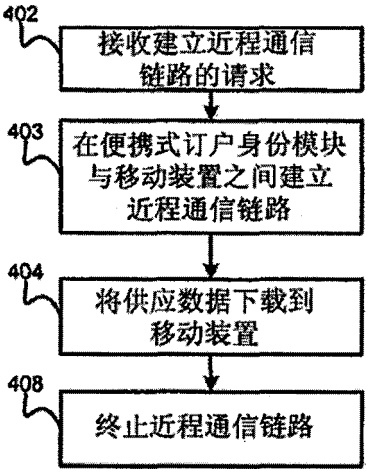

402
接收建立近程通信链路的请求
403
在便携式订户身份模块与移动装置之间建立近程通信链路
404
将供应数据下载到移动装置
408
终止近程通信链路

图 7

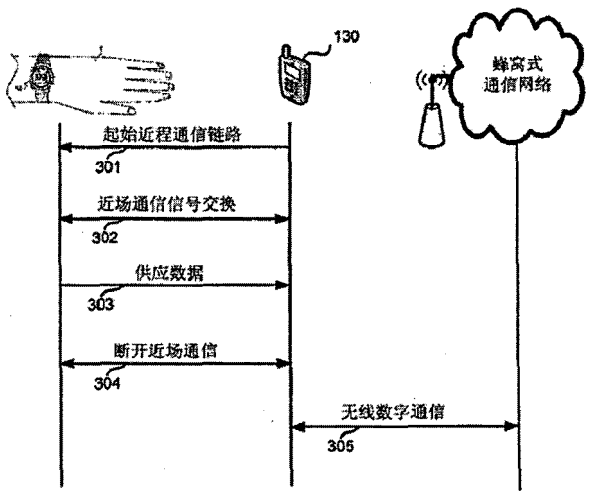

130
蜂窝式通信网络
起始近程通信链路
301
近场通信信号交换
302
供应数据
303
断开近场通信
304
无线数字通信
305

图 8