(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 105357769 A
(43)申请公布日 2016.02.24

(21)申请号 201510808210.8

(22)申请日 2015.11.23

(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.
H04W 74/00(2009.01)
H04W 12/00(2009.01)

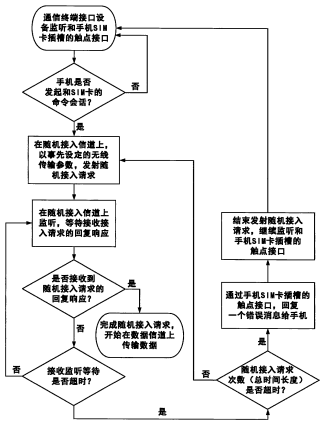
权利要求书4页 说明书10页 附图10页

(54)发明名称

一种无线 SIM 卡传输协议的随机接入及安全控制

(57)摘要

本发明属于移动通信终端领域。本发明公开了一种适用于在移动通信终端和 SIM 卡之间无线数据传输的随机接入及安全控制的流程和方法，使得移动通信终端和 SIM 卡之间通过无线传输接口能够透明而安全地传输数据。通过通信终端接口设备和智能型 SIM 卡卡座设备之间的随机接入信道，使得它们之间的无线数据数据信道能够及时有效地建立的同时，也节省了智能型 SIM 卡卡座设备的功率消耗。本发明还通过只共享于通信终端接口设备和智能型 SIM 卡卡座设备两端的鉴权密钥和鉴权算法，使得它们之间能够建立起安全的无线通信链路，保障了他们之间数据传输的安全。



CN 105357769 A

1.一种用于通信终端接口设备接入其和智能型SIM卡卡座设备之间的无线通信链路的随机接入方法,其特征在于,所述随机接入方法包括,

1)所述通信终端接口设备发起接入的时间是随机的,是被其它事件触发而无法事先确定的,任何时间都可以开始发起随机接入,

2)随机接入的无线传输参数,包括传输信道的频率,调制编码方式,数据帧结构信息等在收发两端是事先设定的,不需要在它们之间传输其它额外的数据信息,所述智能型SIM卡卡座设备在接收到随机接入请求的无线信号后,就能够正确的解调其中的数据,

3)所述随机接入主要用于通信终端接口设备和智能型SIM卡卡座设备之间的无线数据传输信道的建立和维护,也包括它们之间的身份认证鉴权。

2.根据如权利要求1所述的随机接入方法,其特征在于,通信终端接口设备发射随机接入请求的无线信号是通过如下步骤进行的,

1)通信终端接口设备和手机SIM卡插槽的触点接口处于监听状态,监听手机是否发起和SIM卡的命令会话,

2)通信终端接口设备监听检测到手机发起和SIM卡的命令会话,就读取命令并存储该命令,手机SM卡接口处于接收状态,等待SIM卡的回复响应数据,

3)通信终端接口设备在随机接入信道上,以预先设定的无线传输参数,发射随机接入请求,

4)通信终端接口设备在随机接入信道上,监听等待接收随机接入请求的回复响应,

5)通信终端接口设备如果接收到回复响应,就结束随机接入请求,开始在数据信道上传输和智能型SIM卡卡座设备的交换数据(包括身份鉴权数据和命令会话数据),

6)如果通信终端接口设备直到监听接收的等待时间结束,都没有接收到回复响应,就检测随机接入请求的总时间是否超时,

7)如果随机接入请求的总时间没有超时,通信终端接口设备就从第3)步骤开始,重新发射随机接入请求,

8)如果随机接入请求的总时间超时,通信终端接口设备就通过和手机SIM卡插槽的触点接口,回复一个错误消息给手机,

9)通信终端接口设备结束发射随机接入请求,从第1)步骤开始,继续监听和手机SIM卡插槽的触点接口。

3.根据如权利要求2所述的通信终端接口设备重复发射随机接入请求的总时间,其特征在于,所述总时间长度小于手机发起和SIM卡之间的命令会话后等到SIM卡回复响应的最大等待时间。

4.根据如权利要求2所述的通信终端接口设备等待接收随机接入请求的回复响应时间,其特征在于,所述等待时间大于无线通信接口信号的往返时间和智能型SIM卡卡座设备的接收,处理,发射回复响应的时间之和。

5.根据如权利要求1所述的随机接入方法,其特征在于,智能型SIM卡卡座设备是通过如下步骤进行监听接收通信终端接口设备的随机接入请求的,

1)智能型SIM卡卡座设备处于空闲等待状态,打开计数器,计时等待空闲等待状态的结束,

2)空闲状态结束,打开无线接收接口,监听随机接入信道,

3) 如果智能型 SIM 卡座设备监听一段时间后，没有接收到随机接入请求信号，就结束随机接入信道的监听，关闭无线信道，进入空闲等待状态，从第 1) 步骤开始，重新启动新的空闲等待计数器，

4) 如果智能型 SIM 卡卡座设备接收到随机接入请求，就在随机接入信道上回复该随机接入请求，包含有数据信道的无线传输参数，

5) 智能型 SIM 卡卡座设备进入数据传输信道接收等待状态，等待接收通信终端接口设备通过数据信道传输过来的数据，

6) 智能型 SIM 卡卡座设备接收并转发手机通过通信终端接口设备转发的命令会话数据，

7) 智能型 SIM 卡卡座设备接收 SIM 卡对会话命令的回复数据，并转发给通信终端接口设备，直到整个命令会话周期的结束，

8) 智能型 SIM 卡卡座设备从 1) 步骤开始，进入空闲状态，重新启动新的空闲等待计数器。

6. 根据如权利要求 5 所述的智能型 SIM 卡卡座设备监听随机接入信道的等待接收时间，其特征在于，所述的等待接收时间大于 2 倍的如权利要求 2 所述的通信终端接口发射随机接入请求的发射时间和 2 倍的如权利要求 2 所述的通信终端接口等待回复响应的等待时间之和。

7. 根据如权利要求 5 所述的智能型 SIM 卡卡座设备的空闲等待 - 监听接收时间周期，其特征在于，所述空闲等待时间和所述监听接收时间之和小于手机发起和 SIM 卡之间的命令会话后等到 SIM 卡回复响应的最大等待时间。

8. 根据如权利要求 1 所述的随机接入方法，其特征在于，所述的随机接入方是通过如下流程和步骤进行的，

1) 通信终端接口设备通过和手机 SIM 卡槽的触点电路连接，检测到手机发起和 SIM 卡的会话命令，就开始发起和建立和智能型 SIM 卡卡座的无线通信链路，

2) 通信终端接口设备扫描预先设定的固定频率的随机接入信道，检测其信道质量，根据该信道是否被其它的无线信号使用而判断是否适宜传输随机接入请求，或者根据信道的背景噪音的大小来判断信道质量的好坏，

3) 如果信道质量好且适宜传输随机接入请求，通信终端接口设备就在该信道上传输随机接入请求，随机接入请求的传输参数包括传输信道频率，数字信号调制方式，无线信道编码方式等都是设置固定的，

4) 如果所有的随机接入信道质量都差而不适宜传输随机接入请求，通信终端接口设备就等待一段时间后继续扫描，直到扫描到信道质量好的随机接入信道就使用该信道传输随机接入请求，

5) 如果扫描等待时间超过了手机和 SIM 卡之间会话周期的最大等待时间，通信终端接口设备就结束传输随机接入请求，通过和手机 SIM 卡插槽的触点连接接口，回复一个错误信息给手机，从而手机结束该会话周期，

6) 通信终端接口设备发送传输随机接入请求后，等待智能型 SIM 卡卡座的回复响应数据，

7) 如果等待一段时间后，还没有收到智能型 SIM 卡卡座的回复响应数据，通信终端接

口设备就从如上所述的第 2 步骤开始，重新扫描随机接入信道，为下一次新的随机接入请求传输寻找质量好的随机接入信道，直到发射出随机接入请求，或者传输时间超时，

8) 如果在一段时间范围内，通信终端接口设备接收到回复响应数据，则随机接入请求成功，

9) 通信终端接口设备接收到智能型 SIM 卡卡座的回复响应数据后，通过读取回复响应数据，获得所分配的数据信道传输参数，利用这些传输参数，建立起他们之间的无线数据传输信道，

10) 通信终端接口设备结束随机接入请求，通过和智能型 SIM 卡卡座建立起的无线通信链路，以及相应的数据转发，手机和 SIM 卡就建立起了连接，手机继续进行已经发起的和 SIM 卡的命令会话周期，直到 SIM 卡回复响应该命令，以结束命令会话周期。

9. 一种用于通信终端接口设备接入其和智能型 SIM 卡卡座设备之间的无线通信链路的安全数据传输，其特征在于，所述安全数据传输包含有如下功能模块，

1) 在通信终端接口设备中，有一个随机接入请求鉴权算法和一个随机接入响应鉴权算法，

2) 在智能型 SIM 卡卡座设备中，有一个和通信终端接口设备中相同的随机接入请求鉴权算法，还有一个和通信终端接口设备中相同的随机接入响应鉴权算法，

3) 在通信终端接口设备中，有一个接入鉴权系统密钥和和一个接入鉴权用户密钥，

4) 在智能型 SIM 卡卡座设备中，有一个和通信终端接口设备相同的接入鉴权系统密钥和和一个和通信终端接口设备相同的接入鉴权用户密钥，

5) 通信终端接口设备运行随机接入请求鉴权算法，以接入鉴权系统密钥和接入鉴权用户密钥为输入，能够得到一个唯一确定的随机接入请求数据，

6) 智能型 SIM 卡卡座设备运行随机接入请求鉴权算法，以接入鉴权系统密钥和随机接入请求数据为输入，能够得到一个唯一确定接入鉴权用户密钥，

7) 智能型 SIM 卡卡座设备能够产生一个随机数序列，这个随机数产生过程能够多次重复的进行，每次产生一个不同的随机数序列，

8) 智能型 SIM 卡卡座设备运行随机接入响应鉴权算法，以接入鉴权系统密钥和随机数序列为输入，能够得到一个唯一确定的随机接入响应数据，

9) 通信终端接口设备运行随机接入响应鉴权算法，以接入鉴权系统密钥和随机数序列为输入，能够得到一个唯一确定的随机接入响应数据。

10. 一种用于通信终端接口设备接入其和智能型 SIM 卡卡座设备之间的无线通信链路的随机接入的安全控制流程，其特征在于，所述安全控制流程包含有步骤，

1) 在通信终端接口设备和智能型 SIM 卡卡座设备中，分别写入相同的随机接入请求鉴权算法和相同的随机接入响应鉴权算法，

2) 在使用之前，用户在通信终端接口设备和智能型 SIM 卡卡座设备中分别设定相同的接入鉴权系统密钥和相同的接入鉴权用户密钥，

3) 通信终端接口设备在传输随机接入请求时，运行随机接入请求鉴权算法，以接入鉴权系统密钥和接入鉴权用户密钥为输入数据，得到一个唯一确定的随机接入请求数据，

4) 通信终端接口设备以随机接入请求数据为传输信息的一部分，在随机接入信道发射随机接入请求，

5) 智能型 SIM 卡卡座设备接收到随机接入请求信号，运行随机接入请求鉴权算法，以接收到的随机接入请求数据和接入鉴权系统密钥为输入数据，得到一个运行结果的接入鉴权用户密钥，

6) 智能型 SIM 卡卡座设备比较运行结果的接入鉴权用户密钥和存储的接入鉴权用户密钥，如果是一致的，就判断其随机接入请求是有效的，需要对该接入请求进行回复响应，如果不一致，则该接入请求是无效的，就直接忽略而不予响应，

7) 对于有效的随机接入请求，智能型 SIM 卡卡座设备就产生一个随机数序列，作为回复响应数据的一部分，

8) 智能型 SIM 卡卡座设备在随机接入信道上，发射回复响应随机接入请求，除了数据信道的无线传输参数外，产生的随机数序列也包含在回复响应中，

9) 智能型 SIM 卡卡座设备在本地保存有随机数序列的一个备份拷贝，以备接下来的对通信终端接口设备的身份鉴权使用，

10) 通信终端接口设备在随机接入信道上接收到接入请求的回复响应，获得数据信道的无线传输参数和随机数序列，

11) 通信终端接口设备运行随机接入响应鉴权算法，以接收到的随机数序列和接入鉴权系统密钥为输入，得到随机接入响应数据，

12) 通信终端接口设备以接收到的无线数据信道传输参数，在数据信道上传输其运算结果随机接入响应数据，

13) 智能型 SIM 卡卡座设备在数据信道上接收到随机接入响应数据，

14) 智能型 SIM 卡卡座设备运行随机接入响应鉴权算法，以先前存储的备份拷贝随机数序列和接入鉴权系统密钥为输入，得到运算结果随机接入响应数据，

15) 智能型 SIM 卡卡座设备比较运算结果的随机接入响应数据和接收到的随机接入响应数据，如果一致，则完成对通信终端接口设备的身份鉴权，认为其是合法有效的，如果两个数据不一致，则判断通信终端接口设备不是合法的，立即中断随机接入请求过程，

16) 对于通过身份认证鉴权的通信终端接口设备的接入请求，智能型 SIM 卡卡座设备在数据信道回复一个确认消息，通知其鉴权认证鉴权完成，可以继续传输手机的命令会话数据，

17) 通信终端接口设备结束随机接入请求，在无线数信道上转发手机命令会话，并接收智能型 SIM 卡卡座设备转发过来的 SIM 卡的回复响应数据，直到整个命令会话周期的结束。

一种无线 SIM 卡传输协议的随机接入及安全控制

技术领域

[0001] 本发明属于移动通信终端领域。具体地说，本发明涉及一种适用于在移动通信终端和 SIM 卡之间无线数据传输的的随机接入及安全控制的流程和方法，使得移动通信终端和 SIM 卡之间通过无线传输接口能够透明而安全地传输数据。

背景技术

[0002] 目前，移动通信用户设备主要由移动通信终端设备（包括日常生活中通常使用的手机以及其它一些能够接入蜂窝移动通信网络的用户终端设备如移动固话，平板电脑，笔记本电脑等，以下都简称手机）和用户身份模块卡（包括 GSM 系统的 SIM 卡，CDMA 系统的 UIM 卡，以及 2G，3G 和 4G 移动通信系统都可以使用的 USIM 卡，以下都简称 SIM 卡）两个部分组成。其中手机的主要功能是连接蜂窝式移动通信网络，为用户提供移动通信的应用服务，而 SIM 卡主要用于移动通信用户身份标识和认证，以及移动通信业务使用的鉴权和授权，还包括对移动通信网络的鉴权。在现有的技术实现中，手机内部有一个 SIM 卡卡座，使得 SIM 卡插入卡座后通过引脚接触和手机进行通信。具体的通信协议在有关的智能卡传输标准中定义（如 ISO-7816 定义传输协议，ETSI TS 102211，3GPP TS 11.11 等定义电信应用协议）。这种通信是一种有线通信形式，通过 SIM 卡的触点和手机内部的卡座引脚接触，建立起有线的通信链路。也就是说，移动通信用户设备的这两个部分之间的数据通信是通过直接的电路连接通信完成的。

[0003] 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，公开了一种在手机和 SIM 卡之间的中间设备，智能型 SIM 卡卡座设备。通过智能型 SIM 卡卡座，手机和 SIM 卡之间的通信可以通过转发通信而间接地完成。也就是说，智能型 SIM 卡卡座可以是手机和 SIM 卡之间的数据交换的传输中继，并且这个数据的转发传输中继可以是无线通信。

[0004] 在中国发明申请 201410495484.1“一种通信终端设备和 SIM 卡之间的无线接口及功能实现”中，更进一步公开了一种无线传输协议，使得这种数据转发的传输差错和传输时间延迟都在现有标准的容许范围之内。这样，在 SIM 卡和网络双方看来，这个中间的数据转发通信过程就是透明的，它们都不会觉察到其存在。对现有的移动用户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以及手机和 SIM 卡之间无线传输接口的方便性。

[0005] 在中国发明申请 201410735422.3“一种通信终端和 SIM 卡无线数据传输的终端接口设备”中，公开了一种通信终端接口设备，该接口设备具有标准的 SIM 的形状和大小，可以直接插入现有的手机的 SIM 卡卡槽。一方面，通信终端接口设备和手机之间具有触点连接的直接电路连接通信，而另一方面，它也具有无线通信接口，能够和智能型 SIM 卡卡座建立无线通信链路。这样，手机和 SIM 卡之间就可以通过通信终端接口设备，智能型 SIM 卡卡座以及它们之间的无线通信链路连接起来，进行数据通信。

[0006] 本发明的主要目的是公开了一种无线数据传输的的随机接入及安全控制的流程

和方法，用于手机和SIM卡之间的无线数据传输协议，使得手机和SIM卡之间的无线传输接口可以透明并安全地传输数据，就好像手机和SIM卡是直接的电路连接通信一样。

发明内容

[0007] 现有的手机和SIM卡之间的传输接口是标准的智能卡－终端设备接口，即满足ISO-7816智能卡传输协议的接口，它们之间的传输性能如传输数据差错，传输时间延迟需要满足其规范要求。因此，手机和SIM卡的无线数据传输，包括手机和通信终端接口设备之间的数据转发，通信终端接口设备和智能型SIM卡卡座之间的无线数据转发，智能型SIM卡卡座和SIM卡之间的数据转发的总体性能，都要满足其规范要求。这样，对于通信终端接口设备和智能型SIM卡卡座之间无线通信链路的建立，连接，维护，释放等过程，对于手机和SIM卡来说，都需要是透明，以至不会影响到其数据传输。本发明的无线数据传输信道的随机接入方法，就是为了实现这种数据的透明传输而提出的技术实施方案。

[0008] 图1是无线信道的划分示意图，在整个通信终端接口设备和智能型SIM卡卡座之间的无线信道上，按照它们的使用功能的不同，主要划分为两种不同的无线信道，用于它们之间不同的数据类型的传输。其中数据信道是用于传输标准的智能卡－终端设备接口数据，而随机接入信道主要用于数据传输信道的建立和维护，控制数据信道的使用。随机接入信道在无线频率上是固定的，无线传输和接收双方是预先约定的。在整个无线信道的频段上，有一个或者多个频率固定的信道作为随机接入信道，而其余的所有信道都是数据信道。

[0009] 由于智能卡－终端设备接口的数据交换（一个完整的数据交换过程称为一个命令会话周期）总是由终端设备向智能卡发起命令为开始，而由智能卡对该命令的回复响应为结束。所以，随机接入信道总是由手机端的通信终端接口设备作为发射端而发起接入请求，智能型SIM卡卡座通过判断接收到的接入请求数据信息，进而回复响应接入请求，或者如果不是该接入请求的目标接收端，对接入请求不予响应。而数据信道则是由对接入请求的回复响应进行分配的，用于紧接着的手机-SIM卡命令会话周期的数据传输。

[0010] 对于手机端的通信终端接口设备来说，由于手机发起和SIM卡的命令会话周期的时间是不确定的，因此，在什么时候发起建立和智能型SIM卡卡座的无线通信链路也是不确定的。当手机发起和SIM卡的命令会话时，需要立即建立起无线通信链路以交换该会话周期的数据，否则，如果手机和SIM卡之间的连接建立超时，手机就判断SIM卡数据读取错误而结束该命令会话周期。所以，通信终端接口设备发起无线通信链路的建立时间是随机的，不确定的，是有手机发起和SIM卡的命令会话时间决定的。通信终端接口设备需要随时做好准备，等待手机发起命令会话。本发明公开的随机接入的方法和流程，就是用于通信终端接口设备随时建立和智能型SIM卡卡座之间的无线通信链路。如图2所示，本发明的随机接入流程包含有如下步骤：

[0011] 1. 手机发起和SIM卡之间的命令会话周期，通信终端接口设备通过手机SIM卡槽的触点接触电路连接，检测到手机发起的该会话命令，就开始发起建立和智能型SIM卡卡座设备的无线通信链路。

[0012] 2. 通信终端接口设备扫描预先设定的固定频率的随机接入信道，检测其信道质量，根据该信道是否被其它的无线信号使用而判断是否适宜传输随机接入请求，或者根据信道的背景噪音的大小来判断信道质量的好坏。

[0013] 3. 如果信道质量好且适宜传输随机接入请求，通信终端接口设备就在该信道上传输随机接入请求。随机接入请求的传输参数包括传输信道频率，数字信号调制方式，无线信道编码方式等都是设置固定的，使得接收端使用相同固定的接收参数，能够接收到随机接入请求。如果所有的随机接入信道质量都差而不适宜传输随机接入请求，通信终端接口设备就等待一段时间后继续扫描，直到扫描到信道质量好的随机接入信道就使用该信道传输随机接入请求。当扫描等待时间超过了手机和 SIM 卡之间会话周期的最大等待时间，通信终端接口设备就结束发射随机接入请求，通过和手机的 SIM 卡插槽的触点连接电路接口，回复一个错误信息给手机，从而手机结束该命令会话周期。

[0014] 4. 通信终端接口设备发射随机接入请求后，就等待智能型 SIM 卡卡座设备的回复响应数据。如果等待一段时间后，还没有收到智能型 SIM 卡卡座设备的回复响应数据，通信终端接口设备就从如上所述的第 2 步骤开始，重新扫描随机接入信道，为下一次新的随机接入请求传输寻找质量好的随机接入信道，直到发射出随机接入请求，或者传输时间超时。如果在一段时间范围内，通信终端接口设备接收到回复响应数据，则随机接入请求成功。

[0015] 5. 通信终端接口设备接收到智能型 SIM 卡卡座的回复响应数据后，通过读取回复响应数据，获得所分配的数据信道传输参数，例如数据传输信道的频道，调制编码方式等，开始利用这些传输参数，建立起他们之间的无线数据传输信道。

[0016] 6. 通信终端接口设备结束随机接入请求，通过和智能型 SIM 卡卡座建立起的无线通信链路，以及相应的数据转发，手机和 SIM 卡就建立起了连接，手机得以继续进行已经发起的和 SIM 卡的命令会话周期，直到 SIM 卡回复响应该命令，以结束命令会话周期。

[0017] 对于插入手机 SIM 卡插槽的 SIM 卡来说，由于和手机插槽的触点有直接的电路连接，并且 SIM 卡的数据传输接口一直处于命令接收等待状态，当手机发起命令会话时，SIM 卡就会立即接收到命令并在很短的时间内对该命令进行回复响应。但是对于手机和 SIM 卡之间的无线连接来说，除了两端的数据转发通信会带来额外的时间延迟，无线信道的空中传输，无线信号的调制解调也会引入时间延迟，这些时间延迟需要小于手机发起发起命令会话后等待 SIM 卡回复响应的最大等待时间。而另一方面，智能型 SIM 卡卡座设备通常是由电池供电的用户移动设备，虽然插入其中的 SIM 卡是可以一直处于命令接收等待状态，但其无线通信接口就很难一直处于无线信号接收状态，因为电池的续航时间对于移动设备来说非常重要。所以，智能型 SIM 卡卡座设备的无线接口通常情况下都是处于关闭状态，只是在需要的时候，才打开其无线通信接口，接收从通信终端接口设备传输的信号。而同时，通信终端接口设备传输随机接入请求的时间是随机的，无法事先确定，智能型 SIM 卡卡座设备只能周期性地打开无线通信接口，接收并解调无线信号，以检测判断是否有随机接入请求。

[0018] 图 3 是智能型 SIM 卡卡座设备在时间上无线数据传输帧结构。在固定的时间周期，智能型 SIM 卡卡座设备打开其无线通信接口，监测随机接入信道。经过一段时间，如果没有接收到随机接入请求，智能型 SIM 卡卡座设备就关闭其无线通信接口，进入低功耗的空闲模式（或睡眠模式）。再经过一个固定的时间周期后，智能型 SIM 卡卡座设备继续监测随机接入信道，如果接收到随机接入请求，就回复数据传输信道的无线传输参数，进入无线信号接收等待状态，等待接收通信终端接口设备通过数据信道传输过来的数据，并在手机和 SIM 卡的整个会话周期中透明转发它们之间的数据交换，直到命令会话周期结束。

[0019] 图 4 是本发明的智能型 SIM 卡卡座设备的工作状态流程图，包含有步骤：

[0020] 1. 智能型 SIM 卡卡座设备处于空闲状态，打开计数器，计时等待空闲状态的结束时间。

[0021] 2. 空闲状态结束，打开无线接口，监听随机接入信道。

[0022] 3. 如果智能型 SIM 卡卡座设备监听一段时间后，没有接收到随机接入请求信号，就结束随机接入信道的监听，关闭无线信道，进入空闲状态，从步骤 1 开始，重新启动新的空闲等待计数器。

[0023] 4. 如果智能型 SIM 卡卡座设备接收到随机接入请求，就在随机接入信道上回复该随机接入请求，包含有数据信道的无线传输参数。

[0024] 5. 进入数据传输信道接收等待状态，等待接收通信终端接口设备通过数据信道传输过来的数据。

[0025] 6. 接收手机通过通信终端接口设备转发过来的会话命令，并转发给 SIM 卡。

[0026] 7. 接收 SIM 卡对会话命令的回复数据，并转发给通信终端接口设备，直到整个命令会话周期的结束。

[0027] 8. 进入空闲状态，从步骤 1 开始，重新启动新的空闲等待计数器。

[0028] 由于手机发起命令会话周期后，有一个等待 SIM 卡回复响应的最大等待时间，并且手机发起命令会话的时间是随机的，所以智能型 SIM 卡卡座设备的随机信道监听时间间隔必须小于这个最大等待时间，以保证数据传输信道能够及时地建立。

[0029] 图 5 是本发明的智能型 SIM 卡卡座设备的用于随机接入请求信道的时间关系图：

[0030] 1. 在时间上，按功能划分，主要分为低功耗的空闲时间，处于无线接收状态的随机接入信道监听时间。如果收到随机接入请求的话，还包括回复响应时间，命令会话周期时间。

[0031] 2. 一个命令数据从手机到 SIM 卡（一个回复响应数据从 SIM 卡到手机也类似），其时间包括通信终端接口设备的信号转发时间，无线信道的传输时间（包括空中传输时间以及传输和接收端对信号的处理时间等），智能型 SIM 卡卡座设备的转发时间。

[0032] 3. 为了保证智能型 SIM 卡卡座设备在随机接入监听的时间窗口内能够接收到随机接入请求，其监听的时间必须大于通信终端接口设备的信号转发时间和无线信道的传输时间的总和。

[0033] 4. 为了保证手机发起命令会话后能够在有效的时间范围内收到 SIM 卡的回复响应，智能型 SIM 卡卡座设备的空闲时间，随机接入的监听时间，回复响应时间的总和必须小于手机等待 SIM 卡响应回复的最大等待时间。

[0034] 这样，通过智能型 SIM 卡卡座设备在时间上的空闲－监听方式，并控制它们相应的持续时间长度，一方面节省了功率消耗，延长了电池的续航时间。另一方面，也使得手机的等待时间在其最大等待时间范围内，手机和 SIM 卡之间可以透明的传输数据。

[0035] 图 6 是本发明的通信终端接口设备的工作状态流程图，为了及时有效地响应手机发起的命令会话，通信终端接口设备与手机 SIM 卡插槽的触点接口一直处于监听状态，监听是否有手机发起的与 SIM 卡的命令会话，包含有步骤：

[0036] 1. 通信终端接口设备和手机 SIM 卡插槽的触点接口处于监听状态，监听手机是否发起和 SIM 卡的命令会话。

[0037] 2. 通信终端接口设备监听检测到手机发起和 SIM 卡的命令会话，就读取命令并存储该命令，手机 SM 卡接口处于接收状态，等待 SIM 卡的回复响应数据。

[0038] 3. 通信终端接口设备在随机接入信道上，以预先设定的无线传输参数，发射随机接入请求。

[0039] 4. 通信终端接口设备在随机接入信道上，监听等待接收随机接入请求的回复响应。

[0040] 5. 通信终端接口设备如果接收到回复响应，就结束随机接入请求，开始在数据信道上传输和智能型 SIM 卡卡座设备的交换数据（包括身份鉴权数据和命令会话数据）。

[0041] 6. 如果通信终端接口设备直到监听接收的等待时间结束，都没有接收到回复响应，就检测随机接入请求的总时间是否超时。

[0042] 7. 如果随机接入请求的总时间没有超时，通信终端接口设备就从第 3 步骤开始，重新发射随机接入请求。

[0043] 8. 如果随机接入请求的总时间超时，通信终端接口设备就通过和手机 SIM 卡插槽的触点接口，回复一个错误消息给手机。

[0044] 9. 通信终端接口设备结束发射随机接入请求，从第 1 步骤开始，继续监听和手机 SIM 卡插槽的触点接口。

[0045] 当手机发起和 SIM 卡的命令会话后，就一直处于等待 SIM 卡回复响应状态，直到收到 SIM 卡的回复响应数据，或者等待超时而进入错误处理。所以，本发明的通信终端接口设备重复发射随机接入请求的总时间长度小于手机的最大等待时间，并且通信终端接口设备在每次发射随机接入请求后的等待时间大于两次无线信道的传输时间和智能型 SIM 卡卡座设备的转发时间之和。如图 7 所示，它们的时间关系如下：

[0046] 1. 通信终端接口设备一个完整的随机接入请求包括随机接入请求发射时间和随后的回复响应的等待时间。

[0047] 2. 通信终端接口设备的回复响应等待时间大于 2 次的无线信道的传输时间和智能型 SIM 卡卡座设备的转发时间之和，也就是说，通信终端接口设备发射随机接入请求后，要等待接入请求被智能型 SIM 卡卡座设备收到（1 次无线信道的传输时间），并处理收到的信号以及发射回复响应（智能型 SIM 卡卡座设备的转发时间），再等待回复响应数据被通信终端接口设备收到（1 次无线信道的传输时间）。

[0048] 3. 智能型 SIM 卡卡座设备的随机接入监听时间大于 2 次完整的随机接入请求时间，即 2 次的随机接入请求发射时间和 2 次的回复响应等待时间之和。由于智能型 SIM 卡卡座设备和通信终端接口设备之间的随机接入信道没有时间同步，这样的时间关系保证了智能型 SIM 卡卡座设备在任意时刻开始的随机接入监听都能够收到一个完整的随机接入请求信号。

[0049] 4. 通信终端接口设备重复发射随机接入请求总次数的时间之和小于手机等待 SIM 卡回复响应的最大等待时间，这样使得无线通信链路能够及时有效的建立，手机和 SIM 卡之间的命令会话得以继续进行而不至于中断。

[0050] 与移动通信业务有关的用户身份标识与认证的安全数据都存储在 SIM 卡中。其中用于身份鉴权的数据如鉴权密钥和鉴权算法等只能在 SIM 卡内部运行使用，是不能被读取出来而在无线信道中传输。其他一些与用户身份信息相关的敏感数据如 IMSI（国际移动用

户识别码）等需要在无线数据信道上传输，用于手机接入移动通信网络的身份标识。所以，对于通信终端接口设备于与智能型 SIM 卡卡座设备之间的无线通信链路来说，其数据传输的安全性非常重要。特别，在其随机接入信道上，智能型 SIM 卡卡座设备如何识别真实用户的通信终端接口设备，进行回复响应以建立起无线数据信道的同时，有对那些不是真实用户的随机接入请求不予响应，使得非真实用户无法获得 SIM 卡的数据。本发明在随机接入信道还具有额外的安全控制技术实施方案，使得保障真实用户的随机接入请求获得及时回复响应的同时，非真实用户的通信终端接口设备却不能通过随机接入信道和智能型 SIM 卡卡座设备建立连接，保证了其中 SIM 卡数据的安全性。

[0051] 图 8 是本发明的随机接入安全控制功能模块图，包含有如下的功能模块：

[0052] 1. 在通信终端接口设备和智能型 SIM 卡卡座设备两端，都具有两个相同的随机接入鉴权算法，一个称为随机接入请求鉴权算法，一个称为随机接入响应鉴权算法。它们对两个鉴权算法的使用方式是不同的。

[0053] 2. 在通信终端接口设备于和智能型 SIM 卡卡座设备两端，都具有相同的接入鉴权系统密钥和相同的接入鉴权用户密钥。

[0054] 3. 通信终端接口设备使用随机接入请求鉴权算法，以接入鉴权系统密钥和接入鉴权用户密钥为输入，得到随机接入请求数据。

[0055] 4. 智能型 SIM 卡卡座设备使用随机接入请求鉴权算法，以接入鉴权系统密钥和通过无线接口接收到的随机接入请求数据为输入，得到接入鉴权用户密钥。

[0056] 5. 智能型 SIM 卡卡座设备在回复响应随机接入请求的时候，能够产生一个随机数序列，并通过无线通信接口传输给通信终端接口设备。这个随机数序列是一次性使用的，在下一次回复响应时，重新产生一个新的随机数序列。

[0057] 6. 智能型 SIM 卡卡座设备使用随机接入响应鉴权算法，以接入鉴权系统密钥和一次性使用的随机数序列为输入，得到随机接入响应数据。

[0058] 7. 通信终端接口设备使用随机接入响应鉴权算法，以接入鉴权系统密钥和通过无线接口接收到的随机数序列为输入，得到随机接入响应数据。

[0059] 图 9 和图 10 是本发明的随机接入的安全控制流程图。一方面，当通信终端接口设备发射随机接入请求后，如果智能型 SIM 卡卡座设备是其目标接收者（被请求接入并读取其中的 SIM 卡数据），智能型 SIM 卡卡座设备就能够接收到接入请求。另一方面，如果智能型 SIM 卡卡座设备不是接入请求的目标接收者，就不能正确的就收到随机接入请求。这样一个过程相当于通信终端接口设备对智能型 SIM 卡卡座设备进行身份鉴权，避免接入到一个非目标的智能型 SIM 卡卡座而泄露了安全数据如接入鉴权用户密钥。当智能型 SIM 卡卡座接收到随机接入请求后，又通过随机数序列的质问－回答方式，对通信终端接口设备的身份进行了鉴权。这样，通过他们之间相互的双向鉴权，保障了随机接入信道的安全性。只有通信的双方都确认了对方是合法真实的有效终端后，它们之间的随机接入信道才能够建立起来，并进一步建立起无线数据传输信道。这样的安全控制流程包含有如下步骤：

[0060] 1. 在通信终端接口设备和智能型 SIM 卡卡座设备中，分别写入相同的随机接入请求鉴权算法和相同的随机接入响应鉴权算法。对于任何一个算法来说，其输出数据能够被输入数据唯一地确定，也就是说，算法的输出数据能够且只能够通过相同的输入数据被重现。

[0061] 2. 在使用之前，用户在通信终端接口设备和智能型 SIM 卡卡座设备中分别设定相同的接入鉴权系统密钥和相同的接入鉴权用户密钥。这些鉴权密钥被存储在它们的非易失性存储器中（例如闪存），只需要一次性的设定而可以一直使用。当需要使用的时候，就从其存储器中读取出来，用户不需要记住鉴权密钥。为了保障数据安全性，系统密钥和用户密钥不能被其它设备读取而只能在用户的通信终端接口设备或者智能型 SIM 卡卡座设备内部被使用。

[0062] 3. 当通信终端接口设备在传输随机接入请求时，就运行随机接入请求鉴权算法，以接入鉴权系统密钥和接入鉴权用户密钥为输入数据，得到一个唯一确定的随机接入请求数据序列。

[0063] 4. 通信终端接口设备以随机接入请求数据为传输信息的一部分，在随机接入信道发射随机接入请求。

[0064] 5. 智能型 SIM 卡卡座设备接收到随机接入请求信号，运行随机接入请求鉴权算法，以接收到的随机接入请求数据和接入鉴权系统密钥为输入数据，得到一个运行结果的接入鉴权用户密钥。由于使用了和通信终端接口设备相同的算法和相同的数据，并且算法的输出数据能够被输入数据唯一地确定，如果智能型 SIM 卡卡座设备是接入请求的目标，那么就能够得到正确的接入鉴权用户密钥，并且和其存储的接入鉴权用户密钥是一致的。对于存储有多个接入鉴权用户密钥的智能型 SIM 卡卡座设备，是和其中的某一个接入鉴权用户密钥一致的。如果智能型 SIM 卡卡座设备不是接入请求的目标接收者，由于其不具有接入鉴权系统密钥，就不能通过运行随机接入请求鉴权算法而得到正确的接入鉴权用户密钥，这样就避免了接入鉴权用户密钥被非接入请求目标的智能型 SIM 卡卡座设备获得。

[0065] 6. 智能型 SIM 卡卡座设备比较运行结果的接入鉴权用户密钥和存储的接入鉴权用户密钥，如果是一致的，就判断其随机接入请求是有效的，需要对该接入请求进行回复响应。如果不一致，则该接入请求是无效的，就直接忽略而不予回复响应。

[0066] 7. 对于有效的随机接入请求，智能型 SIM 卡卡座设备就产生一个随机数序列，作为回复响应数据的一部分。这个随机数序列是一次性使用的，每次进行随机接入请求的回复响应时，都要重新产生一个新的随机数序列。

[0067] 8. 智能型 SIM 卡卡座设备在随机接入信道上，发射回复响应数据给随机接入请求，除了数据信道的无线传输参数外，产生的随机数序列也包含在回复响应中。随机数序列在智能型 SIM 卡卡座设备的本地还保存有一个备份拷贝，以备接下来的对通信终端接口设备的身份鉴权使用。

[0068] 9. 通信终端接口设备在随机接入信道上接收到接入请求的回复响应，获得数据信道的无线传输参数和随机数序列。

[0069] 10. 通信终端接口设备运行随机接入响应鉴权算法，以接收到的随机数序列和接入鉴权系统密钥为输入，得到随机接入响应数据。

[0070] 11. 通信终端接口设备以接收到的无线数据信道传输参数，在数据信道上传输其运算结果随机接入响应数据。

[0071] 12. 智能型 SIM 卡卡座设备在数据信道上接收到随机接入响应数据。

[0072] 13. 智能型 SIM 卡卡座设备运行随机接入响应鉴权算法，以先前存储的备份拷贝随机数序列和接入鉴权系统密钥为输入，得到运算结果随机接入响应数据。

[0073] 14. 智能型 SIM 卡卡座设备比较运算结果的随机接入响应数据和接收到的随机接入响应数据，如果是一致的，则完成对通信终端接口设备的身份认证鉴权，认为其是合法有效的。如果两个数据不一致，则判断通信终端接口设备不是合法的，立即中断随机接入请求过程。通过这样一个质问 - 回答的过程，一个非法的通信终端接口设备由于不具有有效的接入鉴权系统密钥，是不能通过这样一个身份认证过程。

[0074] 15. 对于通过身份认证鉴权的通信终端接口设备的接入请求，智能型 SIM 卡卡座设备在数据信道回复一个确认消息，通知其认证鉴权完成，可以继续进行命令会话。

[0075] 16. 通信终端接口设备结束随机接入请求，在无线数信道上转发手机命令会话，并接收智能型 SIM 卡卡座设备转发过来的 SIM 卡的回复响应数据，直到整个命令会话周期的结束。

[0076] 这样，通过只共享于通信终端接口设备和智能型 SIM 卡卡座设备两端的接入鉴权系统密钥（通过用户的设置），它们就完成了相互的认证鉴权，保证了它们之间的无线通信链路的安全性。当同一个用户的多个通信终端接口设备需要接入同一个智能型 SIM 卡卡座设备时，多个通信终端接口设备的接入鉴权系统密钥是相同的，但它们的接入鉴权用户密钥可以不一样。这样，通过各不相同的接入鉴权用户密钥，还可以在无线传输数据信道上进行多址接入区分。

[0077] 发明的效果

[0078] 本发明通过通信终端接口设备和智能型 SIM 卡卡座设备之间的随机接入信道，在时间上分片段地使用它们之间的无线信道，并控制每一个时间片段的长度，使得它们之间的数据信道能够及时有效地建立的同时，也节省了智能型 SIM 卡卡座设备的功率消耗，延长了电池的续航时间，在穿戴设备中提高了用户的使用体验。本发明还通过只共享于通信终端接口设备和智能型 SIM 卡卡座设备两端的鉴权密钥和鉴权算法，使得它们之间能够建立起安全的无线通信链路，保障了他们之间数据传输的安全。

附图说明

[0079] 图 1 是通信终端接口设备和智能型 SIM 卡卡座设备之间无线通信接口在频率上的划分，分为数据信道和随机接入信道，其中随机接入信道在频率上是固定的。

[0080] 图 2 是本发明的随机接入流程图，随机接入由通信终端接口设备发起，由智能型 SIM 卡卡座设备的回复响应结束。

[0081] 图 3 是本发明的通信终端接口设备和智能型 SIM 卡卡座设备之间无线通信接口在时间上的无线数据帧结构图，主要分为空闲等待时间和随机接入请求的监听时间，还包括手机和 SIM 卡之间命令会话周期的数据无线转发时间。

[0082] 图 4 是本发明的智能型 SIM 卡卡座设备在时间上的状态流程图。

[0083] 图 5 是本发明的智能型 SIM 卡卡座设备用于随机接入请求信道的时间关系图，以保证各个信道的时间在标准的范围内，使得手机和 SIM 卡之间的智能卡 - 终端设备接口的正常通信得以进行。

[0084] 图 6 是本发明的通信终端接口设备的工作状态流程图。

[0085] 图 7 是通信终端接口设备的随机接入请求的时间关系图，发射随机接入请求的总时间长度小于手机等待 SIM 卡回复响应的最大等待时间。

[0086] 图 8 是本发明的随机接入安全控制功能模块图。

[0087] 图 9 和图 10 是本发明的随机接入的安全控制流程图，通过随机接入的安全控制流程，通信终端接口设备和智能型 SIM 卡卡座设备都完成双向的身份认证，建立起它们之间安全的无线传输信道。

具体实施方式

[0088] 通信终端接口设备和智能型 SIM 卡卡座设备之间的无线接口可以使用不同的技术方案，如蓝牙，无线局域网等，并且不同设备提供商的具体无线传输方案也不相同，所以本发明的随机接入和安全控制的可以有不同的具体实施方式。下面以挪威 Nordic 公司的蓝牙片上系统 (SoC，System on chip) 芯片 nRF51822 为例，来具体说明本发明的技术实施方式。

[0089] 芯片 nRF51822 支持多协议的 2.4G 无线通信，包括专有的传输协议和标准的蓝牙 4.0 协议，用户也可以利用其应用编程接口实现自己的应用通信协议。这样的特点为实现本发明的随机接入和安全控制的具体实施方式提供了灵活性。

[0090] 在 nRF51822 的整个无线频率 2400MHz-2483.5MHz 上，在每 1MMHz 的频率带宽上，可以划分一个传输信道，共计 83 个传输信道。其中间频率的一个信道，如中心频率为 2440MHz 的信道设定为通信终端接口设备和智能型 SIM 卡卡座设备之间的随机接入信道，其余的 82 个信道为数据信道。

[0091] 芯片 nRF51822 提供的 RSSI(Received Signal Strength Indication，接收的信号强度指示）功能可以用于扫描随机接入信道的质量，以评估是否适宜于传输随机接入请求。由于 2.4G 的频段是公共频段，其它的设备也可能使用，所以根据随机接入信道的 RSSI，如果信道质量差，就等待一段时间，当其它设备释放该信道后，再利用其传输随机接入请求，可以大大地提高随机接入请求无线信号的接收质量。

[0092] 当手机发起命令会话后等待 SIM 卡回复响应的最大等待时间可以在它们之间的初始会话 (ATR，Answer To Reset) 时商议，下面以这个最大等待时间为 1 秒 (1000 毫秒）为例来说明。在智能型 SIM 卡卡座设备的 nRF51822 芯片程序中，启动一个实时时钟计数器 (RTC，Real Time Counter)，计数器每 500 毫秒产生一个时钟中断。在时钟中断的服务程序里，nRF51822 芯片就可以打开其无线接收模块，监听随机接入信道。如果在监听过程中接收到随机接入请求，就可以进行接收解调，解码等，根据结果而决定进一步的行动。如果一直没有接收到随机接入请求，中断的服务程序在运行 10 毫秒后，就结束中断的服务程序，等待下一个时钟中断（每 500 毫秒产生一个）。在等待时钟中断中间，nRF51822 芯片关闭无线接收模块，进入低功耗的睡眠模式。这样，在手机等待 SIM 卡回复响应的最大等待时间内，智能型 SIM 卡卡座设备就有 2 次机会监听随机接入信道。更进一步增加了它们之间无线通信链路建立的及时性。

[0093] nRF51822 芯片的无线传输时间可以小于 1 毫秒，通信终端接口设备在发射随机接入请求后，等待 3 毫秒，以等待接收智能型 SIM 卡卡座设备对接入请求的回复响应。这样，在智能型 SIM 卡卡座设备 10 毫秒的时钟中断服务程序里，通信终端接口设备可以有 2 次随机接入请求发射机会，无论智能型 SIM 卡卡座设备在什么时候开始监听随机接入信道，都有机会收到一个完整的随机接入请求无线信号。

[0094] nRF51822 芯片也提供随机数发生器的功能，其随机数的产生是根据背景热噪声信号，具有很好的随机性能。接入鉴权系统密钥和接入鉴权用户密钥由用户输入设定，为16 个字节，即 128 位，存储在 nRF51822 芯片的闪存上。nRF51822 的 ARM Cortex M0 32 位微控制器可以很容易地实现各种不同随机接入请求鉴权算法和随机接入请求响应算法，例如，可以是接入鉴权系统密钥和接入鉴权用户密钥的按位异或，得到相同长度的运行结果数据。在产生随机数序列是，也可以是相同的长度，即 128 位 (16 个字节)，就很容易地实现按位异或的鉴权算法。

[0095] 通过 nRF51822 芯片上的程序运行，可以实现本发明的随机接入安全控制流程，建立起通信终端接口设备和智能型 SIM 卡卡座设备之间安全的的无线通信链路，保障他们之间数据传输的安全。

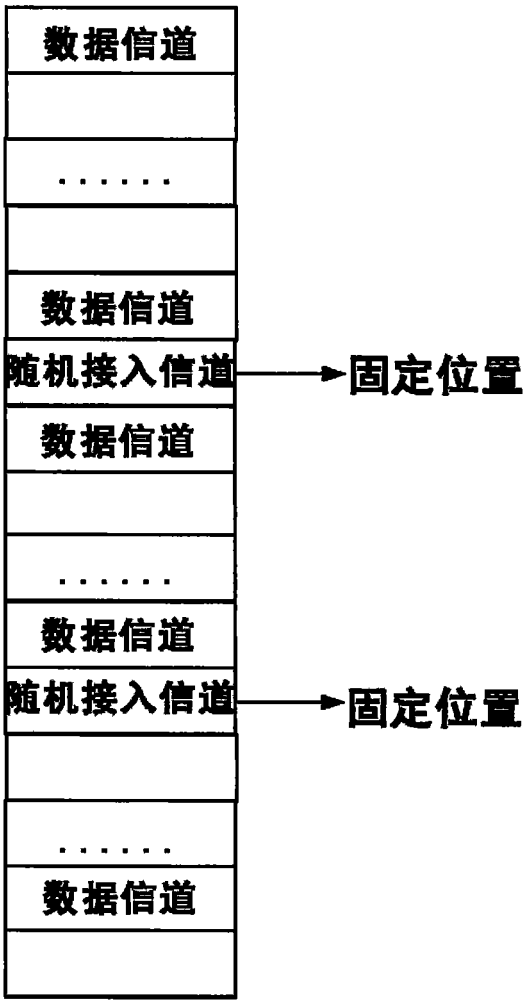


图 1

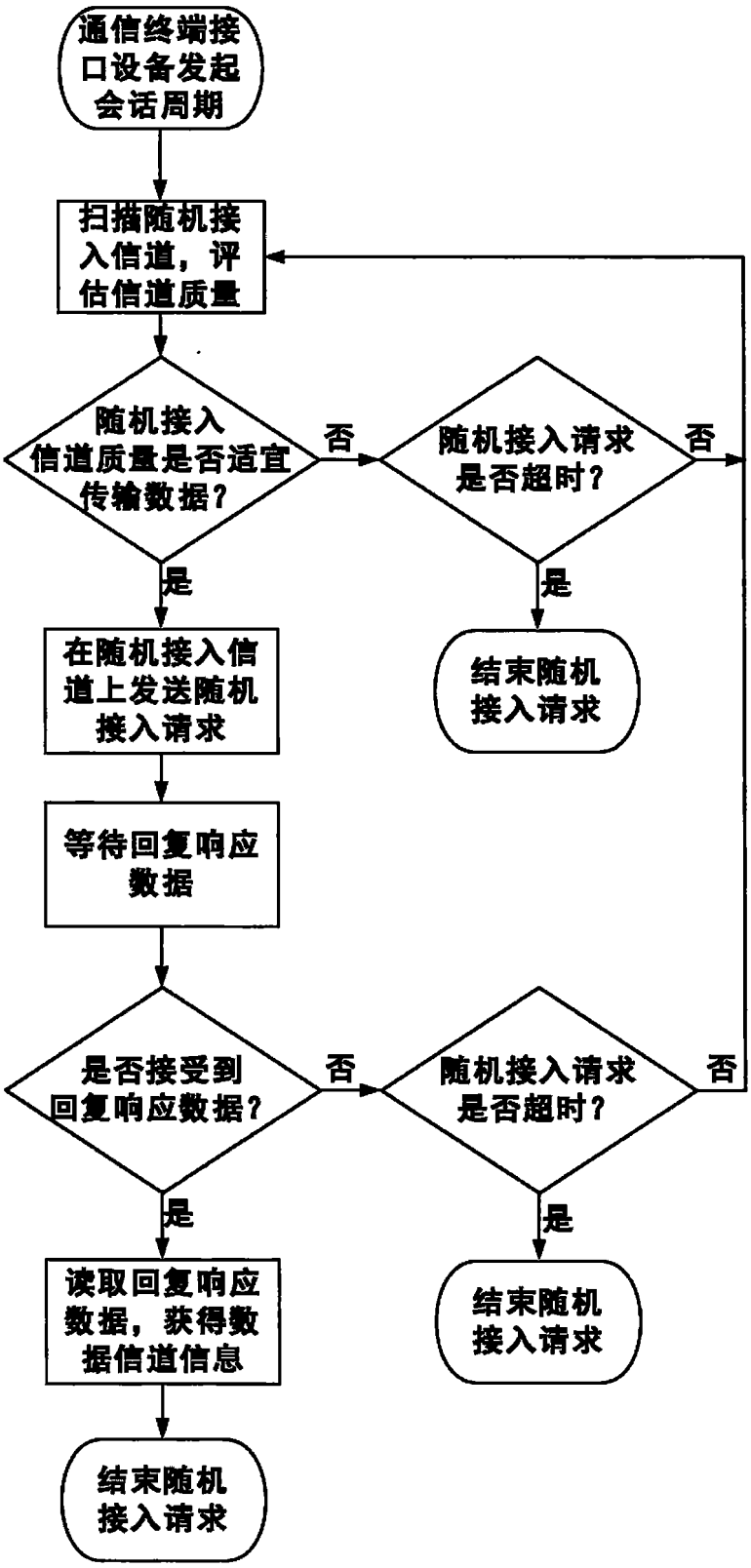

通信终端接口设备发起会话周期
扫描随机接入信道，评估信道质量
随机接入信道质量是否适宜传输数据？
否
随机接入请求是否超时？
否
是
是
在随机接入信道上发送随机接入请求
结束随机接入请求
等待回复响应数据
是否接受到回复响应数据？
否
随机接入请求是否超时？
否
是
是
读取回复响应数据，获得数据信道信息
结束随机接入请求

图 2

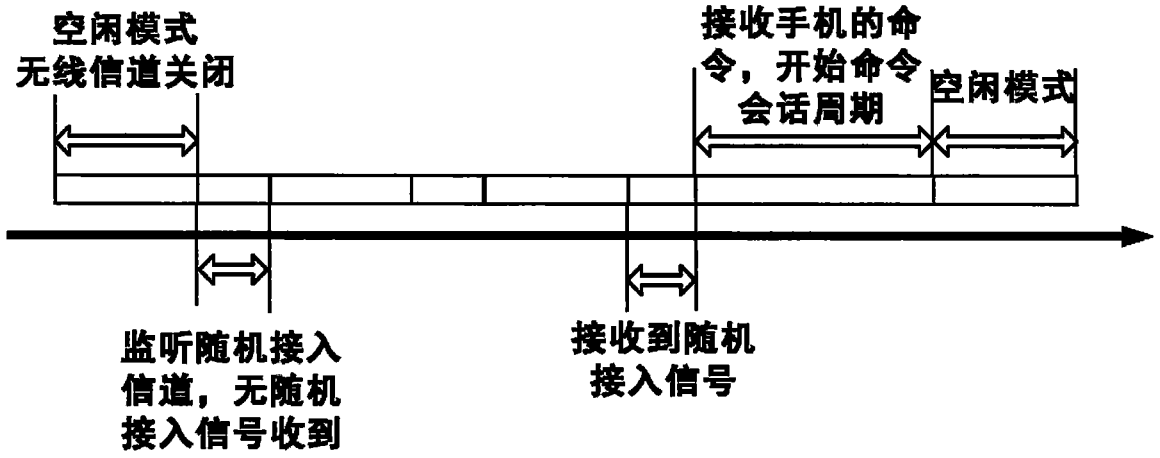

空闲模式
无线信道关闭
接收手机的命令，开始命令会话周期
空闲模式
监听随机接入信道，无随机接入信号收到
接收到随机接入信号

图 3

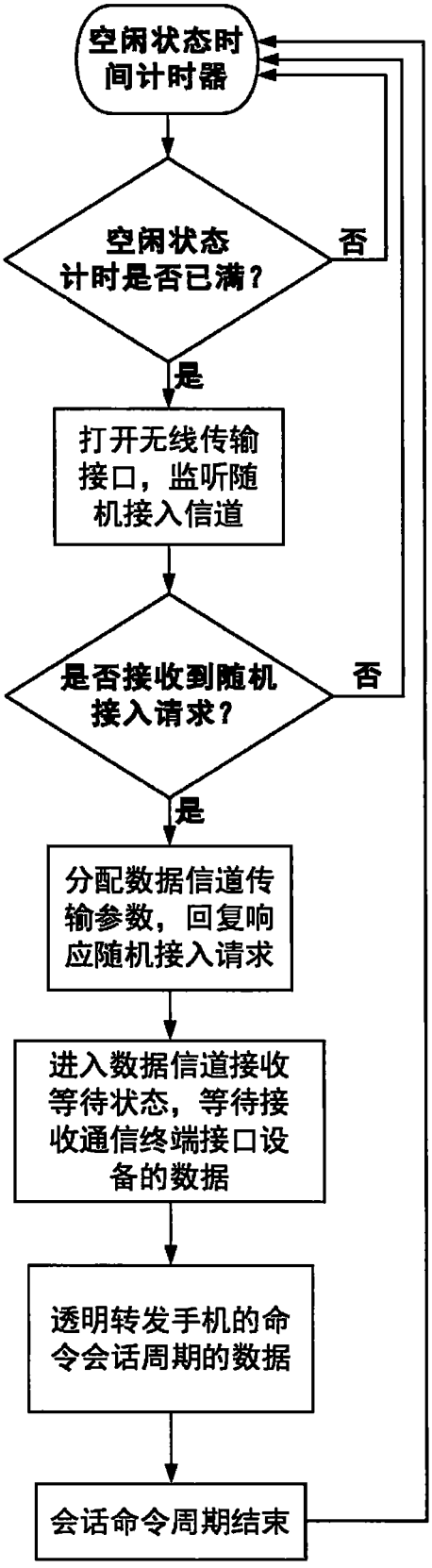

空闲状态时间计时器
空闲状态计时是否已满？
否
是
打开无线传输接口，监听随机接入信道
是否接收到随机接入请求？
否
是
分配数据信道传输参数，回复响应随机接入请求
进入数据信道接收等待状态，等待接收通信终端接口设备的数据
透明转发手机的命令会话周期的数据
会话命令周期结束

图 4

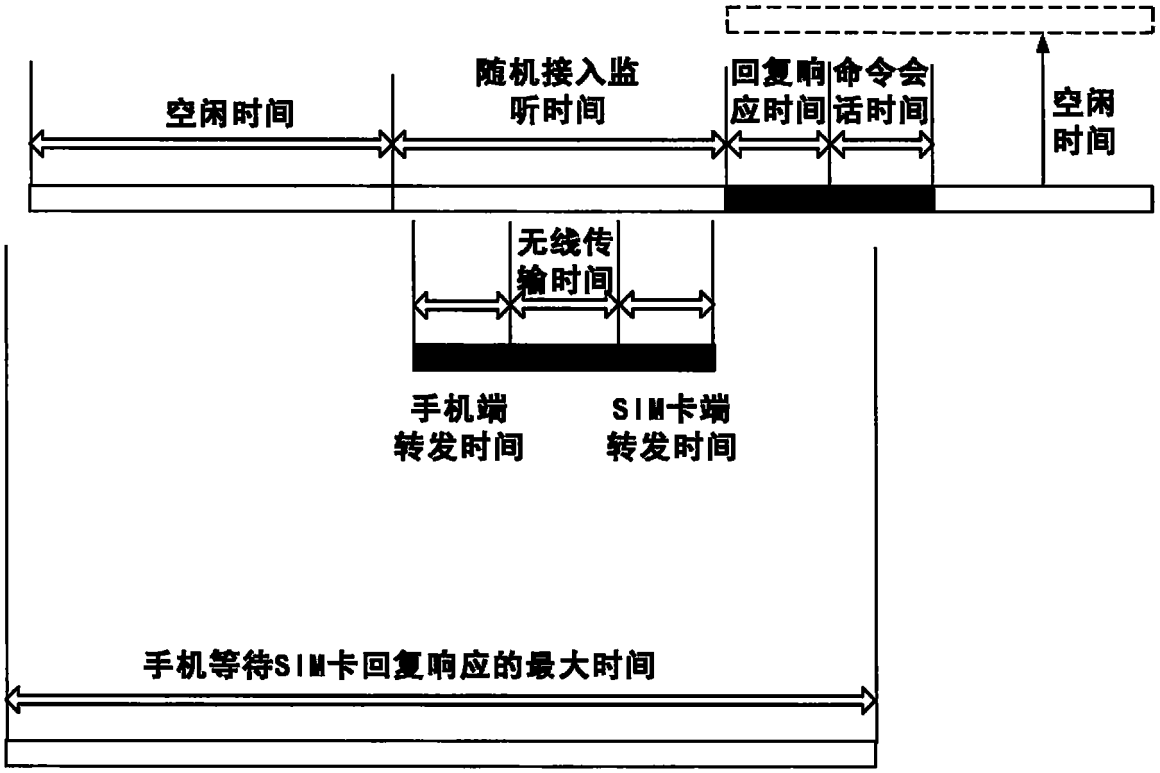

空闲时间
随机接入监听时间
回复响应时间
命令会话时间
空闲时间
无线传输时间
手机端转发时间
SIM卡端转发时间
手机等待SIM卡回复响应的最大时间

图 5

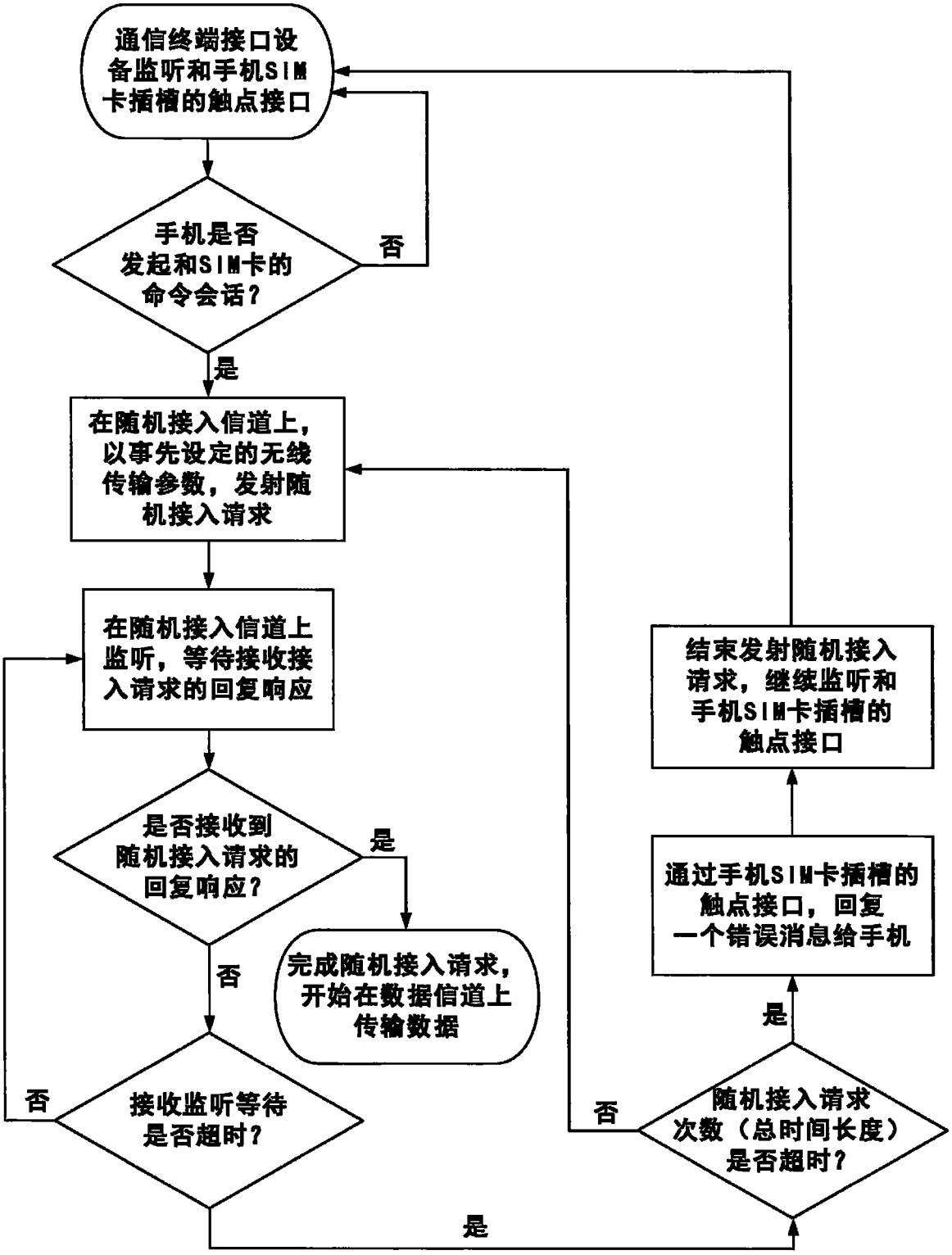

通信终端接口设备监听和手机SIM卡插槽的触点接口
手机是否发起和SIM卡的命令会话？
否
是
在随机接入信道上，以事先设定的无线传输参数，发射随机接入请求
在随机接入信道上监听，等待接收接入请求的回复响应
是否接收到随机接入请求的回复响应？
是
否
完成随机接入请求，开始在数据信道上传输数据
接收监听等待是否超时？
否
是
随机接入请求次数（总时间长度）是否超时？
否
是
通过手机SIM卡插槽的触点接口，回复一个错误消息给手机
结束发射随机接入请求，继续监听和手机SIM卡插槽的触点接口

图 6

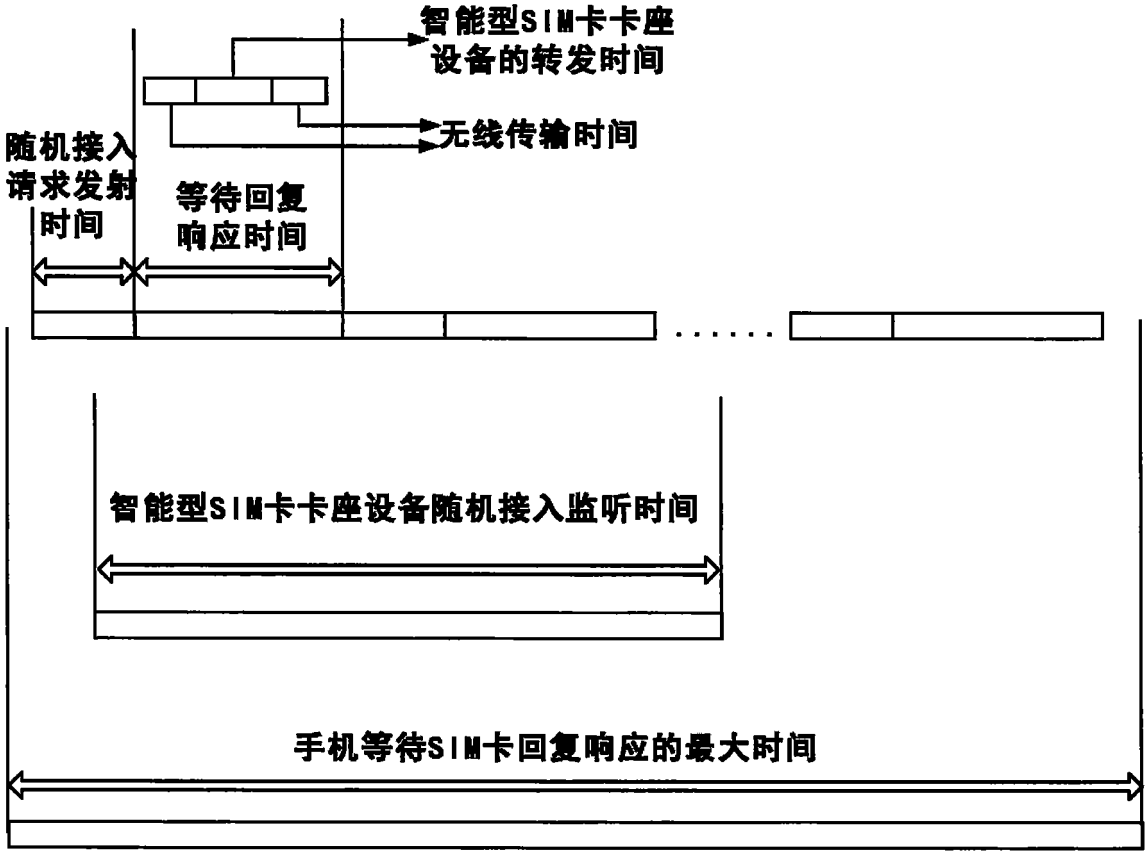

智能型SIM卡卡座
设备的转发时间
无线传输时间
随机接入
请求发射
时间
等待回复
响应时间
智能型SIM卡卡座设备随机接入监听时间
手机等待SIM卡回复响应的最大时间

图 7

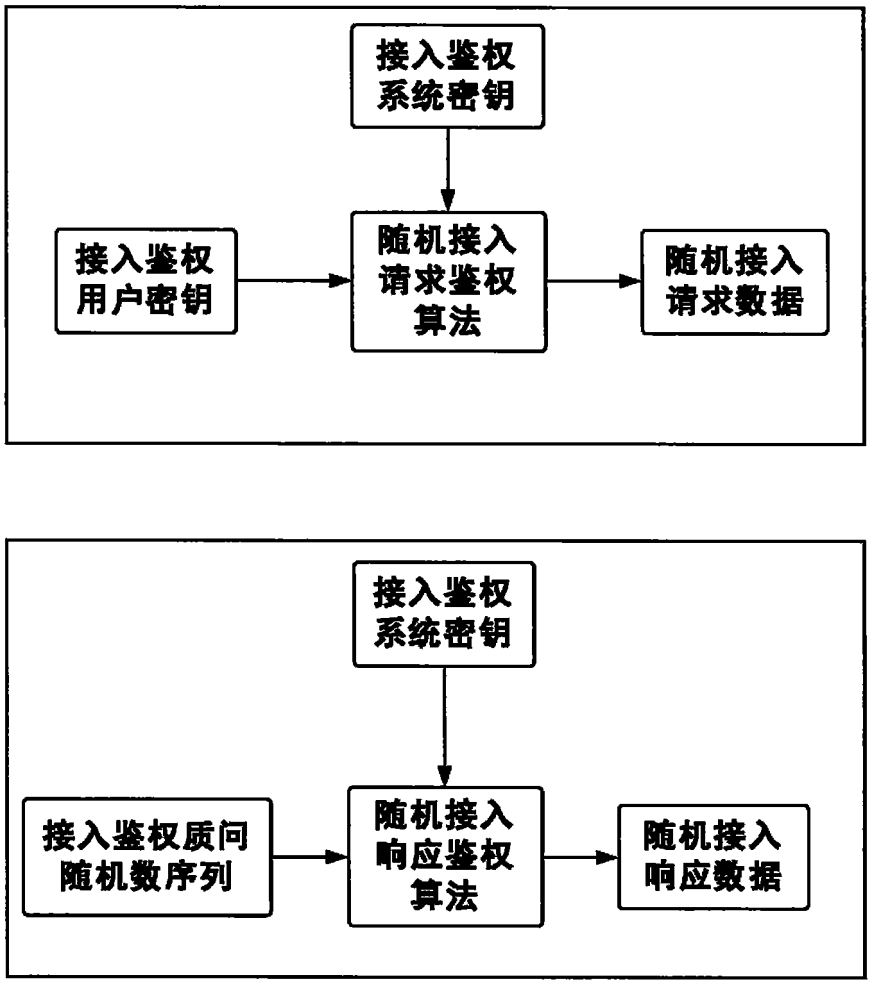

接入鉴权
系统密钥
接入鉴权
用户密钥
随机接入
请求鉴权
算法
随机接入
请求数据
接入鉴权
系统密钥
接入鉴权质问
随机数序列
随机接入
响应鉴权
算法
随机接入
响应数据

图 8

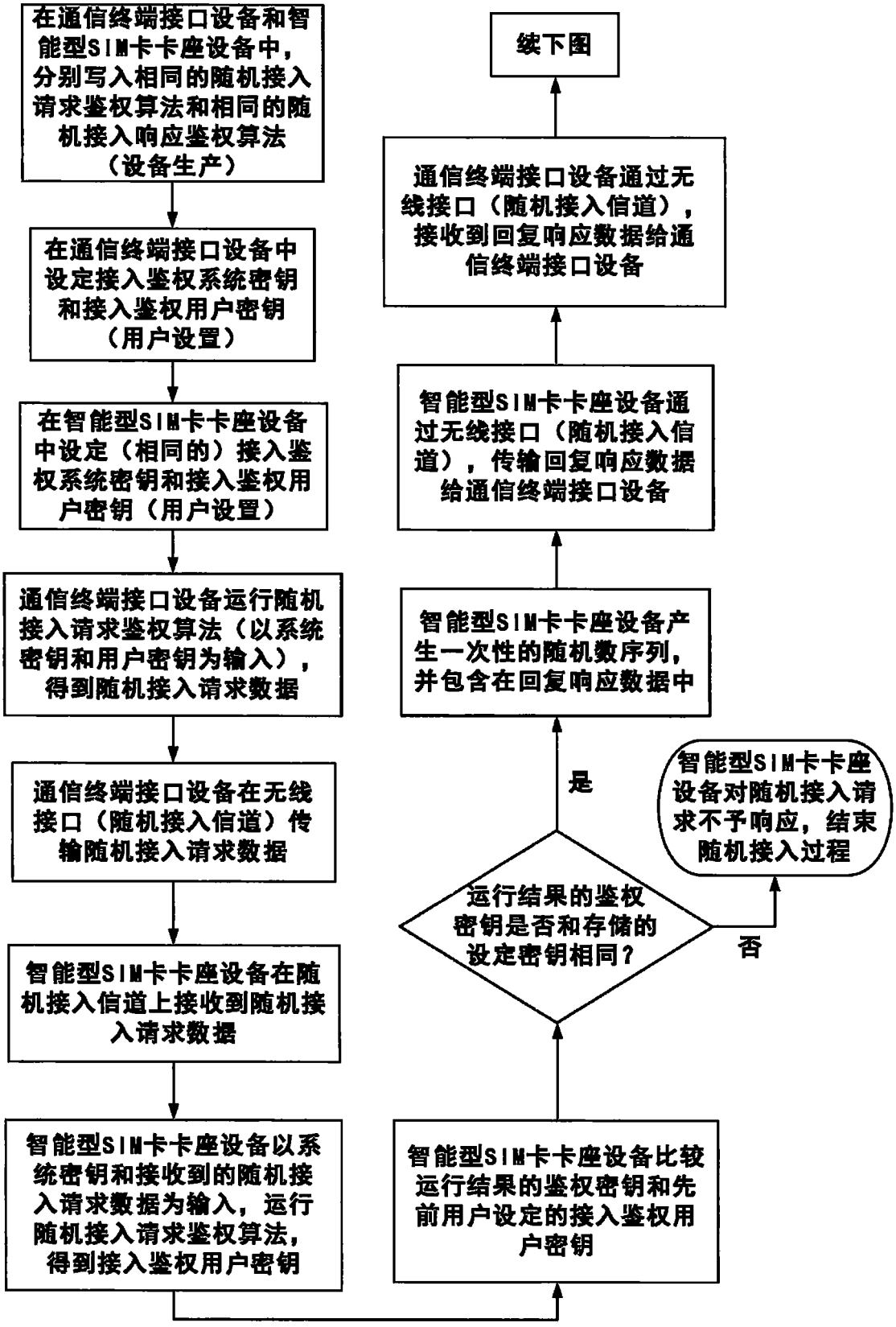

在通信终端接口设备和智能型SIM卡卡座设备中，分别写入相同的随机接入请求鉴权算法和相同的随机接入响应鉴权算法（设备生产）
在通信终端接口设备中设定接入鉴权系统密钥和接入鉴权用户密钥（用户设置）
在智能型SIM卡卡座设备中设定（相同的）接入鉴权系统密钥和接入鉴权用户密钥（用户设置）
通信终端接口设备运行随机接入请求鉴权算法（以系统密钥和用户密钥为输入），得到随机接入请求数据
通信终端接口设备在无线接口（随机接入信道）传输随机接入请求数据
智能型SIM卡卡座设备在随机接入信道上接收到随机接入请求数据
智能型SIM卡卡座设备以系统密钥和接收到的随机接入请求数据为输入，运行随机接入请求鉴权算法，得到接入鉴权用户密钥
续下图
通信终端接口设备通过无线接口（随机接入信道），接收到回复响应数据给通信终端接口设备
智能型SIM卡卡座设备通过无线接口（随机接入信道），传输回复响应数据给通信终端接口设备
智能型SIM卡卡座设备产生一次性的随机数序列，并包含在回复响应数据中
是
否
运行结果的鉴权密钥是否和存储的设定密钥相同？
智能型SIM卡卡座设备对随机接入请求不予响应，结束随机接入过程
智能型SIM卡卡座设备比较运行结果的鉴权密钥和先前用户设定的接入鉴权用户密钥

图 9

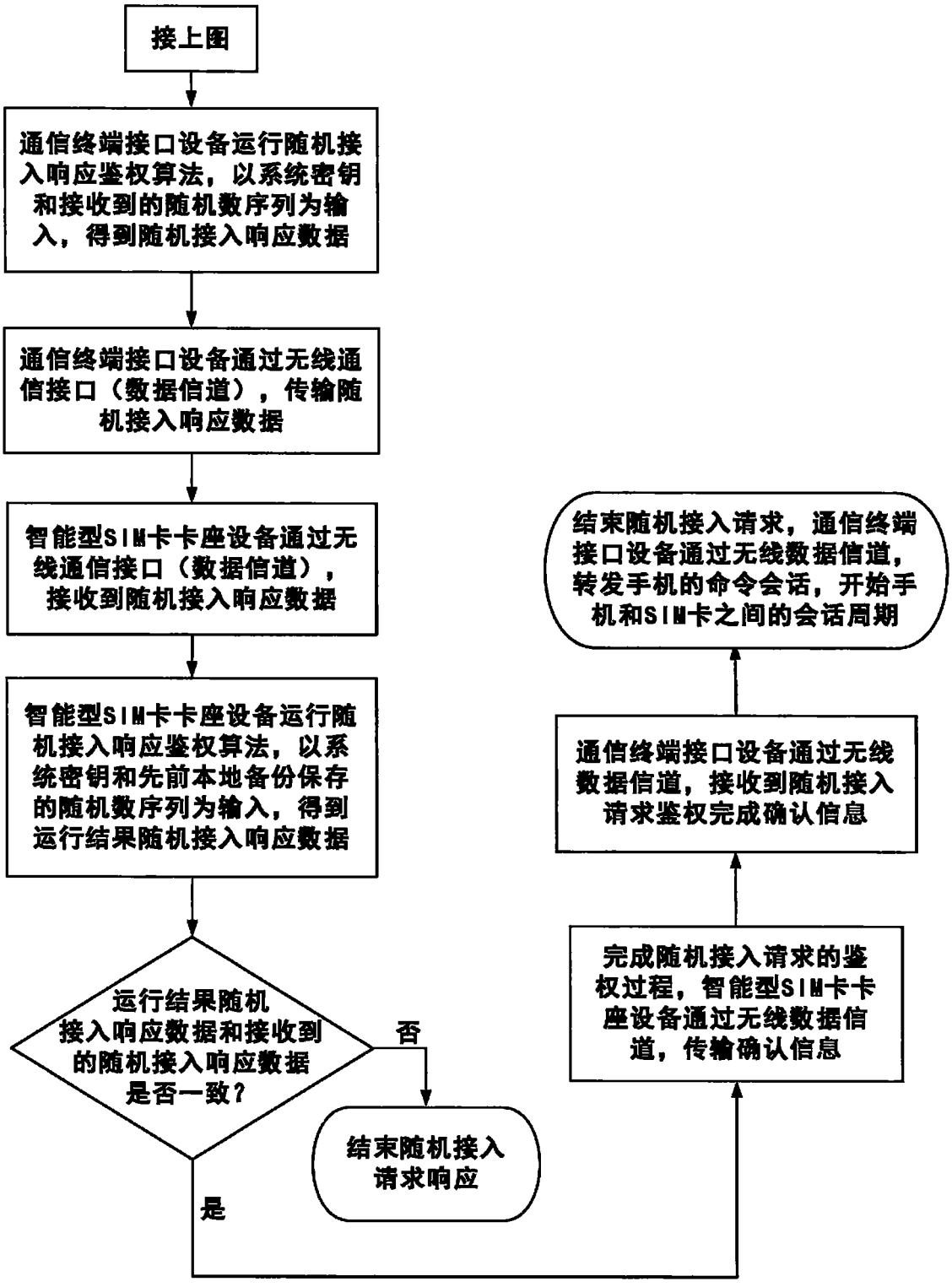

接上图
通信终端接口设备运行随机接入响应鉴权算法，以系统密钥和接收到的随机数序列为输入，得到随机接入响应数据
通信终端接口设备通过无线通信接口（数据信道），传输随机接入响应数据
智能型SIM卡卡座设备通过无线通信接口（数据信道），接收到随机接入响应数据
智能型SIM卡卡座设备运行随机接入响应鉴权算法，以系统密钥和先前本地备份保存的随机数序列为输入，得到运行结果随机接入响应数据
运行结果随机接入响应数据和接收到的随机接入响应数据是否一致？
否
结束随机接入请求响应
是
完成随机接入请求的鉴权过程，智能型SIM卡卡座设备通过无线数据信道，传输确认信息
通信终端接口设备通过无线数据信道，接收到随机接入请求鉴权完成确认信息
结束随机接入请求，通信终端接口设备通过无线数据信道，转发手机的命令会话，开始手机和SIM卡之间的会话周期

图 10