

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04Q 7/32 (2006.01)



[12] 发明专利说明书

专利号 ZL 01802131.X

[45] 授权公告日 2008 年 9 月 24 日

[11] 授权公告号 CN 100421484C

[22] 申请日 2001.6.19 [21] 申请号 01802131.X

[30] 优先权

[32] 2000.6.22 [33] FR [31] 00/07978

[86] 国际申请 PCT/FR2001/001903 2001.6.19

[87] 国际公布 WO2001/099448 法 2001.12.27

[85] 进入国家阶段日期 2002.3.21

[73] 专利权人 CP8 技术公司

地址 法国卢旺茨那斯

[72] 发明人 阿蒙德·纳切夫

[56] 参考文献

WO98/53628A1 1998.11.26

WO99/63767A2 1999.12.9

CN1254482A 2000.5.24

审查员 何永春

[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 李德山

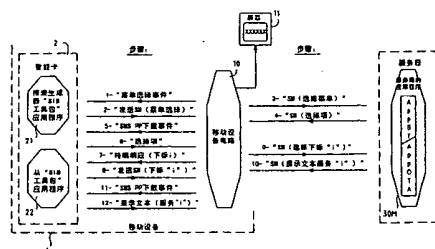
权利要求书 3 页 说明书 19 页 附图 4 页

[54] 发明名称

在具体使用 GSM 标准的移动电话网络上处理
和发送数字数据的方法和嵌入式微芯片系统

[57] 摘要

本发明涉及在具体为 GSM 的移动电话网络上处理和发送数字数据的方法，更具体地的是涉及在移动设备(1)的 SIM 智能卡上记录的 SIM 工具包应用程序的方法。该方法的特征在于，在移动设备(1)与之通信的一个远程服务器(3)上传送所谓的主应用程序(30M)。上述应用程序(30M)通过移动设备电路(10)和分别被称作报表生成器(21)和从应用程序(22)的第一和第二类 SIM 工具包应用程序与 SIM 智能卡(2)通信。本发明还涉及机载微芯片系统，尤其是智能卡。



1.移动电话网络中处理数字数据的方法，上述移动电话网络包括一个与具有嵌入式芯片的智能卡可操作地相连的移动单元，上述嵌入式芯片具有信息处理器和数据存储单元，所述数据存储单元包括报表生成器类型应用程序以及从属类型应用程序，所述方法包括：

由所述智能卡中的所述报表生成器类型应用程序接收从上述移动单元发送的事件；

报表生成器类型应用程序响应于接收上述事件，将智能卡操作的执行分配给远程应用服务器的数据存储单元中存储的附加应用程序，上述附加应用程序是主控类型应用程序，其中上述分配包括经由上述移动电话网络的信道从报表生成器类型应用程序向远程应用服务器的主控类型应用程序发送处理消息；

由上述从属类型应用程序使用上述移动电话网络来接收来自主控类型应用程序的命令；

使用上述智能卡的上述嵌入式芯片的上述信息处理器来执行上述命令；

以及使用上述移动电话网络将上述执行命令的结果重发到上述主控类型应用程序。

2.如权利要求1所述的方法，其特征在于智能卡的数据存储单元存储通过发送命令来控制上述移动单元的至少一个程序，并且至少一个程序对从上述移动单元发送的事件进行响应，上述程序执行与上述事件相关联的指令以便执行与至少一个预定应用相关联的功能。

3.根据权利要求2所述的方法，其特征在于报表生成器类型应用程序向上述远程应用服务器重发从上述移动单元接收的上述事件的特征数据，并且

当接收上述特征数据时，上述远程应用服务器中的附加应用程序执行上述指令中的与上述至少一个预定应用相关的至少一个指令并且向上述智能卡中的上述嵌入式芯片重发上述执行的结果。

4.如权利要求3所述的方法，其特征在于，上述嵌入式芯片受一个操作系统的控制，并且

上述远程应用服务器向上述嵌入式芯片的上述操作系统发送包括命令的上述执行结果，以便进行指定操作，并且

上述指定操作的结果被重发到远程应用服务器。

5.如权利要求1所述的方法，其特征在于报表生成器类型应用程序和从属类型应用程序中的至少一个是自治类型应用程序，其直接在上述智能卡的嵌入式芯片中执行至少一个预定应用的预先设定部分。

6.如权利要求1所述的方法，其特征在于上述移动电话网络符合GSM标准，并且

上述报表生成器类型应用程序符合 GSM 11.14标准。

7.如权利要求1所述的方法，其特征在于上述电话网络包括至少两个不同的传输信道，其中一个传输信道是语音数据信道，另一个传输信道是消息信道，并且

处理的上述数字数据包括通过上述消息信道发送的短类型消息，该短类型消息包括140个八位字节或160个七位字节。

8.如权利要求2所述的方法，其中上述报表生成器类型应用程序和从属类型应用程序中的至少一个是自治类型应用程序，其直接在上述智能卡的上述嵌入式芯片中执行上述至少一个预定应用的预先设定部分。

9.一种智能卡，适于连接到移动电话网络中的移动单元，该智能卡包括：

嵌入式芯片，该嵌入式芯片包括：

(a) 信息处理器；以及

(b) 数据存储单元，其中存储有报表生成器类型应用程序以及从属类型应用程序，上述报表生成器类型应用程序适于生成用于将智能卡操作的执行分配给远程应用服务器的数据存储单元中存储的附加应用程序的信息，并且上述报表生成器类型应用程序响应于从上述移动单元接收的事件而生成上述信息；

上述远程应用服务器中存储的上述附加应用程序是主控类型应用程序，其中上述分配包括用于经由上述移动电话网络的信道从报表生成器类型应用程序向远程应用服务器的主控类型应用程序发送处理消息；并且

上述从属类型应用程序使用上述移动电话网络从上述远程应用服务器的主控类型应用程序接收命令，并且使用上述信息处理器执行上述命令并且使用上述移动电话网络向远程应用服务器的主控类型应用程序重发上述命令的执行结果。

10.如权利要求9所述的智能卡，其特征在于，上述智能卡是用户识别模块（SIM）类型的卡。

11.如权利要求9所述的智能卡，其特征在于，上述报表生成器类型应用程序和从属类型应用程序中的至少一个是直接执行预定应用的自治类型应用程序。

12.如权利要求11所述的智能卡，其特征在于上述智能卡是用户识别模块（SIM）类型的卡。

在具体使用 GSM标准的移动电话网络上处理
和发送数字数据的方法和嵌入式微芯片系统

技术领域

本发明涉及在移动电话网络中处理和发送数字数据的方法。

更具体的是涉及符合"GSM"标准 (在 900 MHz带宽上工作的全球移动通信系统的缩写)的移动电话网络。

本发明还涉及配备了实现该方法的微芯片的嵌入式系统。

背景技术

在本发明的范围内,应当广义地理解术语"网络"。它包含网络自身的传输部件(无线传输子系统,传输电缆,微波无线系统,地面"有线"子系统,等等),以及所有与移动电话网络相连的系统(基站,工作站控制器,交换系统,目录,等等,更概括地是指所有与网络相连的数据处理系统和服务器),其中包含移动电话网络用户(客户)拥有的移动电话,设备或工作站。

后一种设备可以是便携电话或更加复杂终端,例如合并电话和管理器功能的终端。为了简单,在不限制本发明的范围的情况下这些设备此后被称作"移动电话"。移动电话具体配备一个嵌入式系统,而嵌入式系统配备了数据处理和存储装置,其中包含一个缩写表示成"SIM"("用户识别模块")的功能模块。为了简单,此后还假定"SIM"模块被安装在智能卡内。还提供操作智能卡的软件(被称作"OS",表示"操作系统")。

在现有技术状况下, GSM网络移动电话不再单纯用于打电话。它们也可以被用来处理和发送具体为短消息形式(被称作"GSM数据"的服务)的数字数据。

根据应用程序的情况,这些消息通常长度为 160个七位字节或 140个八位字节。

最近出现了被称作"SIM工具包"的标准化技术。这种技术已经被包含在某些 GSM网络移动电话运营商提供的补充服务内。实际上在电话的"SIM"智能卡中实现了一个特定的软件片段。

这种标准允许在移动电话的智能卡 ("SIM")上运行的应用程序向相关移动设备发送命令以便:

- 在移动电话屏幕上显示文本;
- 提示用户向应用程序输入文本;
- 向一个号码请求电话呼叫;
- 请求向一个服务器或另一个电话发送包含文本或数据的短消息;
- 请求在移动设备中的一个辅助智能卡中执行命令;
- 等等。

这些命令被称作"主动"命令。

"SIM工具包"标准还允许"SIM"智能卡的应用程序在接收某个数量从移动设备发出的事件时作出反应。这些事件包含:

- 通过移动设备配备的键盘发出的所谓"菜单"命令选择应用程序;
- 接收向"SIM"智能卡的应用程序或操作系统发送的短消息;
- 编程到移动设备定时器中的时间超时;
- 请求呼叫一个电话号码;
- 等等。

这个标准提供的功能允许在智能卡中开发出大量不同的应用程序以便为用户提供所谓的"增值"服务。

为了更加详细地描述"SIM工具包"技术,最好参照 GSM 11.14标准。

总之,在现有技术条件下,"SIM工具包"标准包括在智能卡中开发能够控制支持智能卡的移动设备并且响应来自其设备的事件的应用程序。今天,这个标准已经被大多数移动设备和智能卡厂商采用。它是一个允许编写功能强大并且安全的应用程序的标准。

"SIM工具包"应用程序通常通过短消息信道与服务器中安装的一或多个应用程序通信。这个信道独立于语音信道并且被 GSM标准加

以标准化。无论是安装在 SIM卡还是服务器内，应用程序均可以发送和接收包含文本或二进制数据的短消息。(更多有关点对点模式短消息的信息参见 GSM 03.40标准。)

然而，虽然上述增值 GSM服务的数量和性质在本质上是无限的，但电话运营商和软件应用开发人员经常受智能卡中有限的可用资源的限制。

"SIM工具包"技术本质上的两个主要缺点是：

1)由于智能卡只包含几万字节的存储器，所以智能卡中没有足够的存储器来存储"SIM工具包"应用程序；虽然非常有经验的软件应用开发人员进行了各种优化，但电话服务运营商在加载和/或运行大量"SIM工具包"应用程序时仍然会遇到存储器缺乏的问题；和

2)智能卡的长响应时间；本质上这个技术在执行上述应用程序期间需要智能卡完成最复杂的计算，而智能卡与移动设备的处理器尤其是服务器相比只具有最小的计算能力。

显然提出了相反的需求。首先，电话运营商希望为其用户提供尽可能多的附加服务。此外，智能卡进行的操作必须在最小时间内完成。由于存在相互影响，可用应用程序增加到最大数量也会因增加处理时间而带来降低性能的风险。

尽管今后并且在可预知的未来智能卡技术会有根本的改进，但上述限制因素仍然存在并且仍将是一个重要的障碍。

最近提出了第二个被称作"WAP"("无线应用协议")的标准化技术。这个标准的目的是为了允许移动电话用户通过无线链路从其移动电话访问因特网。

这个技术仍然有其缺点。

首先，由于其具有不同于常规 Web浏览器的特征，所以有必要安装一个特定类型的"WAP"浏览器。这个浏览器被安装在移动设备中，移动设备的存储器肯定多于智能卡，但通常小于微型计算机，当然也小于服务器。并且，虽然这个技术具有允许接入因特网的优点，但不包括 SIM工具包应用程序的所有功能。为了提供一个非限制性的例

子,象在使用 SIM工具包应用程序时那样, WAP应用程序不能控制电话呼叫。此外, WAP应用程序不能保证与 SIM工具包应用程序相同的安全强度。本质上SIM工具包应用程序使用被存储在 SIM智能卡上的私有密钥。例如, WAP应用程序不能在任意服务器上请求认证应用程序。此外,这并不是转移到 SIM智能卡上的唯一安全功能。它还保证发送信息的安全性和保密性。

为了提供所有这些功能,智能卡存储确定数量的所谓"敏感"数据,加密算法和相关密钥,其中包含:

- 用户国际号码或"IMSI" (for "国际移动用户标识");
- 当移动站移动时为其分配的临时身份或"TMSI"("临时移动用户标识");
- 一个单个认证密钥,即被用来加密和解密无线信道上的所谓信令和传输数据的加密密钥,和三个不同的加密与解密或密钥生成算法;和
- 一个加密密钥序列号或"CKSN" ("加密密钥序号"),上述序列号指示上述有效加密数值以避免移动站和网络使用不同的密钥。

事实上这种敏感信息或数据被存储在智能卡中并且在智能卡中执行对应操作以便能够获得高度安全和保密性。

最终,在现有技术条件下,支持 WAP技术的移动设备的费用仍然高于支持 SIM工具包技术的设备的费用。

发明内容

本发明的目标是消除现有技术设备和系统的上述缺点并且满足不断提出的需求。

本发明的目标是在具体使用 GSM标准的移动电话网络中处理和发送数字数据的方法,该方法允许为这个网络中的移动电话用户提供所有通过符合 SIM工具包技术要求的应用程序可以提供的服务,并且消除在开发智能卡中的应用程序时遇到的存储器和性能限制,至少是大部分限制。

为此,本发明较好得利用了符合 SIM工具包技术要求的应用程序

可以具体发送短消息并且也可以在接收向其发送的其它短消息时执行指令的特性。

基于本发明的移动电话网络体系结构是这样一种体系结构，即SIM工具包应用程序：

1)向至少一个与上述电话网相连的远程服务器中安装的应用程序通知从一个移动设备单元发出的事件已经到达；这些应用程序此后被称作"SIM工具包报表生成器应用程序"；并且

2)根据上述服务器中实现的应用程序的请求执行命令和指令；这些应用程序此后被称作"SIM工具包从应用程序"；

因此可以向在这些服务器中实现的应用程序分配在现有技术中在SIM智能卡中执行的、使用大量计算机资源的高强度运算处理。

上述服务器本质上不具有任何象SIM智能卡那样的内在限制，无论是在可用存储器数量方面还是在计算能力方面。因此可以大大增加SIM智能卡的可用SIM工具包应用程序数量(和提供的服务的数量)并且允许达到高处理速度。

并且，象在现有技术中那样，由于涉及安全和保密的功能在SIM智能卡中仍然受到限制，仍然要保证服务质量的高水平。

因此，本发明的主题是在移动电话网络中发送和处理数字数据的方法，上述网络包括至少一个移动设备单元和一个远程服务器，上述远程服务器包括通过上述移动电话网络彼此通信的信息处理和数据存储装置，上述移动设备与一个嵌入式微芯片系统协同工作，上述嵌入式微芯片系统包括被用来存储至少某些能够通过发送指定命令来控制上述移动设备而且通过执行与上述事件相关的指令对这些设备发出的事件作出响应的软件片段以便完成与至少一个预定应用相关的功能，其特征在于该方法包含实现存储在上述嵌入式微芯片系统的上述数据存储装置中的所谓报表生成器(repporteuse)类型软件的至少一个第一特定片段，并且实现存储在一个上述远程服务器的上述数据存储装置中的软件的至少一个相关片段，其特征还在于报表生成器类型软件的上述片段向上述与数据相关的软件片段重发从上述移动设备接收的

上述事件的特征数据，上述软件相关片段在接收上述特征数据时使用上述远程服务器的上述信息处理装置执行与一个上述预定应用相关的所有或某些上述指令并且向上述移动设备和/或上述嵌入式微芯片系统重发上述执行的结果。

本发明的另一个主题是一个嵌入式系统，上述嵌入式系统配备了一个微芯片，上述微芯片与一个被相连到上述移动电话网络的移动设备单元协同工作。

附图说明

现在参照附图更详细地描述本发明，其中：

-图1图解了一个基于本发明的一个方面，属于所谓"报表生成器"类型并且位于 SIM智能卡内的应用程序激活远程服务器中的 SIM工具包应用程序的主要步骤；

-图2根据本发明的另一个方面图解了远程服务器内的所谓"主"类型应用程序和SIM智能卡内的所谓"从"类型SIM工具包应用程序之间如本发明所述的相互关系；

-图3图解了本发明发送基于 GSM 11.14标准的主动命令的方法的主要步骤；

-图4根据现有技术针对一个具体例子图解了在 SIM智能卡内的SIM工具包应用程序和远程服务器内的应用程序之间交换数据和命令的主要步骤；和

-图5根据本发明的方法针对这个具体例子图解了SIM智能卡内的SIM工具包应用程序和远程服务器内的应用程序之间交换数据和命令的主要步骤。

具体实施方式

现在我们更详细地描述基于本发明的移动电话网络体系结构的一个最优示例性实施例。

如上所示，根据本发明的一个特征，现有技术条件下在 SIM卡中完成的高强度运算被分配到在一或多个与网络连接的远程服务器中实现的应用程序内。

根据本发明的另一个特征, 提供两个主要类别的 SIM工具包应用程序, 即分别在 SIM智能卡中实现的"报表生成器 SIM工具包应用程序"和"从 SIM工具包应用程序".

现在我们更详细地描述两类应用程序。

报表生成器SIM工具包应用程序

首先, SIM工具包应用程序响应来自移动电话或更常见的来自用户移动设备的事件。这些事件通过被称为"信封"的命令到达 SIM智能卡。"信封"命令可以包含"菜单选择"事件, 其中以其选择下标作为这个 SIM工具包应用程序的选择下标。因此这个事件允许从移动电话配备的显示器装置上显示的菜单上选择一个应用程序。在 GSM 11.14标准中可以找到有关这个命令的详细描述。

移动设备不知道在服务器中找到的应用程序。为了使服务器中的应用程序响应 SIM工具包标准中定义的事件, 有必要将其与 SIM卡内安装的 SIM工具包应用程序相连接, 上述 SIM工具包应用程序此后被称作"报表生成器SIM工具包应用程序"。移动设备将报表生成器应用程序看作常规 SIM工具包应用程序。它不知道位于服务器内的对应应用程序。因此是完全透明的。

报表生成器应用程序被写入 SIM卡以便侦听服务器内实现的对应应用程序必须响应的事件。一旦报表生成器应用程序从移动设备接收一个事件, 它准备一个将被发送到其对应应用程序的短消息。这个短消息包含所有代表接收的事件的特征的数据。实际上通过上述"主动命令"类型的命令发送上述数据。

服务器的对应应用程序接收短消息。这个消息向上述应用程序通知出现了一个来自移动设备的事件。接着执行涉及上述事件接收的操作。这个操作可以连接到一个 Web站点。也可以是另一个在 SIM智能卡中实现的所谓从应用程序的所谓主应用程序。因此可以控制从应用程序使其向移动设备发送主动命令, 并且使其也调用 SIM智能卡内安装的库中存储的方法。

图1图解了移动设备单元1的SIM智能卡2内的"报表生成器SIM工具包"应用程序21激活远程服务器3内的SIM工具包应用程序30M的主要步骤。远程服务器3和用户Ab的移动设备1均被连接到移动电话网络RT(未示出)。这个本领域的技术人员众所周知并且本身属于常规类型的网络不需要因本发明的方法而进行任何修改。因而任何基于现有技术的网络先天上均是可用的,这是本发明的一个附加优点。没有必要进一步描述这种网络及其各种部件。作为一个非限制性例子,可以参照Jean Cellmer标题为" Réseaux Cellulaires, Systeme GSM "的文章,该文章发表在" Techniques de l'Ingénieur ", Volume TE 7364, 1999年11月,1-23页。

诸如便携电话的移动设备1包含常规电子电路(存储器,处理器等等)10。后者可以通过一个读取器(未示出)与SIM智能卡2连接。SIM智能卡2也包含电子电路20,具体是处理器和存储装置,其中可以存储SIM工具包应用程序(由于是现有技术本身所固有的,上述SIM工具包应用程序被称作常规应用程序(未示出))以及一或多个基于本发明一个特征的报表生成器SIM工具包应用程序21。在图1中,为了使处理的图解更加简单,只在SIM智能卡2的电路20的外部示出一个应用程序。实际上就象常规应用程序那样在智能卡2的存储装置中存储这个应用程序21。

上述步骤如下所述(如图1中的实箭头所示):

F1)移动设备1的电路10向SIM智能卡2的电路20发送一个"信封"类型的命令;这个"信封"命令包含一个在上述GSM 11.14标准中提供的事件;

F2)SIM卡2的电路20向一个报表生成器SIM工具包应用程序21发送这个事件,而上述报表生成器SIM工具包应用程序21能够响应该事件;和

F3)报表生成器SIM工具包应用程序21通过网络RT以短消息的方式向服务器3内的一个对应应用程序30M发送相同的事件。

其中下面会解释的原因,应用程序30M被称作"主应用程序"。

从SIM工具包应用程序

通过一种已知的方式，现有技术的 SIM工具包应用程序具体可以：

a) 向移动设备发送基于 GSM 11.14标准的主动命令；它可以请求移动设备显示文本；

b) 不通过移动设备，向 SIM智能卡的操作系统发送基于上述 GSM 11.11标准的命令；和

c) 请求执行 SIM智能卡中实现的库中存储的方法：它可以调用 SIM智能卡中的一个方法请求使用这个卡中存储的密钥加密消息。

根据本发明的一个附加方面，远程服务器中实现的应用程序具有这些功能。因而能够为其分配在现有技术中使用智能卡中实现的常规 SIM工具包应用程序执行的操作。

为了使远程服务器3中实现的应用程序能够执行这些操作，需要其能够与 SIM智能卡2中实现的 SIM工具包应用程序通信。接着它向第二种应用程序发送命令，而后者应用程序执行上述命令。此后远程服务器中实现的应用程序被称作"主应用程序"，而 SIM智能卡中安装的 SIM工具包应用程序被称作"从SIM工具包应用程序"。

图2图解了两种应用程序之间的相互关系。

一个"主"应用程序30M向一个从SIM工具包应用程序 22发送一个命令 (图2中的实线)。后一种应用程序执行命令，通过在处理之后返回命令结果 (虚线)来响应"主"应用程序30M。

现在我们详细描述"主"应用程序30M如何可以发送上述类型 a)-c) 的命令。

发送基于 GSM 11.14标准的主动命令

下面参照图3描述基于本发明的方法的主要步骤：

a) 主应用程序30M准备一个被移动设备单元1的电路10执行的主动命令：它被包含在发送到一个从SIM工具包应用程序 22的短消息的

数据中(通过移动设备单元1的电路10, 其中执行主动命令) - 图3中的箭头 F' 1和 F' 2;

b) 从SIM工具包应用程序 22分析接收的短消息数据: 它理解主应用程序30M请求其向其移动设备1的电路10发送主动命令; 因此它向移动设备1传送这个命令并且自身等待返回应答 - 箭头 F' 3;

c) 移动设备1的电路10接收主动命令: 它们执行命令并且以通称为"终端应答"的命令形式向 SIM卡2发送一个应答 - 箭头 F' 4 - , 该命令包含移动设备1的电路10执行主动命令的结果(例如如果主动命令包括请求在移动设备1中启动一个辅助智能卡, 未示出, "终端应答"命令中发送的结果包含一个字节串, 该字节串是辅助卡的置0应答);

d) 从发送主动命令开始处于后备状态的从SIM工具包应用程序 22在接收到上述"终端应答"命令时被释放出来;

e) 从SIM工具包应用程序 22准备一个短消息, 该短消息包含其在通过移动设备1的电路10发出的"终端应答"命令中找到的主动命令结果;

f) 从SIM工具包应用程序 22以主动命令的形式通过移动设备1的电路10向主应用程序30M发送这个短消息-箭头F'5;

g) 移动设备1的电路10向主应用程序30M传送短消息-箭头 F' 6;
和

h) 主应用程序30M接收短消息并且处理其先前发送的主动命令所得到的应答。

发送"非主动"命令, 即基于 GSM 11.11标准的命令

主应用程序30M (图3)可以使用两个不同方法向 SIM智能卡2发送 GSM 11.11命令, 其中可以使用两个方法中的任一个。

方法1

a) 一个主应用程序30M准备一个基于 GSM 11.11标准的命令, 该命令将被发送到一个在 SIM智能卡2中实现的从SIM工具包应用程序

22: 它以短消息的形式通过移动设备1的电路10进行发送;

b) 从SIM工具包应用程序 22分析接收的短消息数据: 它向 SIM智能卡2的操作系统 23发送在这个消息中找到的命令;

c) SIM智能卡2的操作系统23执行来自从SIM工具包应用程序22的命令并且向这个应用程序22返回对这个命令的应答;

d)从SIM工具包应用程序22准备一个短消息, 该短消息将被发送到一个在远程服务器3中实现的对应主应用程序30M: 这个消息包含 GSM 11.11命令的结果并且被从应用程序以主动命令的形式发送到移动设备1的电路10;

e)移动设备1的电路10向消息自身所指示的目的地址, 即主应用程序30M传送短消息; 和

f)主应用程序30M接收短消息并且处理接收的应答。

方法2

远程服务器3中实现的主应用程序30根据 GSM 03.40和 GSM 03.48标准通过短消息直接向 SIM智能卡的操作系统23发送一个 GSM 11.11命令。

象在方法1中那样, 由于不需要提供从SIM工具包应用程序, 这个解决方案的优点是简单。

另一方面, 方法2的缺点是很少有 SIM智能卡操作系统完全实现了这个功能。通常, 服务器的应用程序可以通过短消息发送一个命令脚本以便执行, 但是 SIM智能卡不返回命令的结果。如果服务器中实现的应用程序需要知道 SIM智能卡中一个文件的内容, 则在大多数 SIM智能卡中不能做到这一点。

调用 SIM智能卡的库中的函数

如上所示, SIM工具包应用程序可能需要请求执行 SIM智能卡的库中包含的函数(上述操作 c))。在 SIM智能卡中有两个主要类别的函数。

1)在其参数中使用至少一个存储在智能卡中的密钥的函数: 这些函数被用来加密, 解密, 签名或验证签名; 和

2)不使用私有密钥的函数。

如上所述, 如果有必要保证高度安全, 第一类函数不能在服务器外部。一个从应用程序23 (图3)必须能够在主应用程序30M发出请求后调用它们。

在从应用程序 22和主应用程序30M之间必须有一个约定以便允许主应用程序30M使用 SIM智能卡2的密钥执行加密 /解密和签名操作。

例如, 主应用程序30M向从应用程序22发送一个消息, 其中消息指示要执行的加密函数的性质 (例如使用被称为"DES", 即"数据加密系统"的算法的加密)。它还指示要使用的并且在 SIM智能卡2中存储的密钥的索引和要加密的消息。从应用程序22调用适当的加密函数并且向主应用程序30M返回结果。

对于第二类函数, 可以使用与第一类相同但基于本发明一个有利特征的方法, 其中直接在一个远程服务器3中实现这些函数。这个解决方案的优点是不需要连接到处理能力高于 SIM智能卡2的机器便可以完成处理。

根据本发明的一个特征, 直接在一或多个远程服务器3中实现部分SIM工具包应用程序。为了保证易于从 SIM智能卡移植这些 SIM工具包应用程序, 还有必要实现所有位于 SIM智能卡的库内的相关函数。

为了图解概念, 如果我们考虑所谓的"Java"(注册商标)卡, 这些函数由"Javacard API", GSM 03.19 API和所谓的"专用", 即特定API构成。"Java"是Sun Microsystems公司开发的面向对象编程语言, API是可编程应用程序接口。Java语言允许开发被称为"applet"的小应用程序。可以根据applet创建SIM工具包应用程序。

使用本发明提供的手段可以保证按照现有技术条件在 SIM智能

卡中执行的现有 SIM工具包技术应用程序也可以在远程服务器中运行，并且不需要修改任何代码，这构成了本发明的一个附加优点。

至此已经假定将所谓的短消息技术（即根据 GSM 03.40标准）被用作传送技术。使用这个技术的优点基于以下原因：

- 1)目前在 GSM网络中广泛地使用该技术；和
- 2)可用于 SIM工具包标准（即基于GSM 11.14标准）的事件和主动命令中。

然而应当理解，也可以使用其它基于 SIM智能卡和远程服务器之间存在的无线传输链路的传送技术，无论这些技术当前或将来是否可用。

前面定义的从和报表生成器SIM工具包应用程序的机制不需要任何修改，这使本发明的方法具有很高的稳定性。

在从和主 SIM工具包应用程序的机制中，假定从SIM工具包应用程序完全处于从属地位。在不出本发明范围的前提下也可以考虑具有某种“智能”的从SIM工具包应用程序。这类被称作“混合”应用程序的应用程序能够服从主应用程序并且还能自主执行本地操作。虽然处于从属地位，SIM工具包应用程序本质上仍然具有常规 SIM工具包应用程序所固有的能力。

同样地，可以向报表生成器应用程序加入类似类型的功能，即某种“智能”。

一个结论是，将可适用于 SIM智能卡的功能转移到远程服务器上增加了网络的传输量，并且由于短消息协议的传送速率较低，在某些不期望的条件下会对响应时间产生很大的影响。

并且实际上最期望使用的 SIM工具包应用程序是从 SIM工具包应用程序和自治 SIM工具包应用程序，和/或报表生成器 SIM工具包应用程序和自治 SIM工具包应用程序，这允许尽量降低上述传输量增加造成的不良影响。

通过实际上等价的方式，在使用 SIM智能卡资源和发送短消息之间寻找一个折衷，这会造成性能的下降。

还应当注意，无论是从 SIM 工具包应用程序还是报表生成器 SIM 工具包应用程序，均必须完成 SIM 智能卡中实现的 SIM 工具包应用程序和直接在服务器上实现的应用程序之间的鉴别。是可以根据 GSM 03.48 标准执行上述操作。

这个标准还为 SIM 智能卡和远程服务器之间的数据交换期间传送的某些信息提供加密。

通常一个主应用程序必须与若干个从应用程序通信。为此最好在实现服务器中的 API 时使用所谓的“线程”技术。

在现有技术条件下，上述实现 GSM 03.19 标准的 Java 类型 SIM 智能卡在不使用一个名称为“`sim.toolkit.ProactiveHandler`”的对象类的情况下不知道如何向移动设备发送命令。当一个从 SIM 工具包应用程序接收主应用程序发送的主动命令时，它必须使用名称为“`ProactiveHandler`”的对象类的方法重构上述命令。显然有必要在向移动设备发送主动命令之前重复发送命令的服务器完成的所有工作。

为了使从和主应用程序的机制保持所有如本发明的一个特征所述的优点，最好在 SIM 智能卡中实现一个函数，上述函数除了向移动设备发送一个由任意字节数组构成的主动命令之外不作任何操作。从 SIM 工具包应用程序接着可以接受接收的主动命令，上述命令被主应用程序准备好并且发送出去。它接着在不执行任何附加操作的情况下向移动设备发送上述命令。

实际示例性实施例

现在我们参照图4和5更详细地描述一个实际的示例性实施例。

假定有必要访问在一个短消息服务器中实现的 n 个服务。此后，这些服务会被任意称作服务1，服务2，...，服务 n 。假定根据 Java applet 创建 SIM 工具包应用程序。

通过常规 SIM 工具包技术，即根据现有技术开发这种应用程序需要开发：

1) 一个在 SIM 智能卡中实现并且可以被称作“AppST”的 SIM 工

具包应用程序；和

2)另一个在远程服务器中实现并且可以被称作"AppOTA"的应用程序，上述远程服务器被称作"OTA"("无线")。

应用程序"AppST"响应两个事件，即"菜单选择"和"SMS PP下载"。

当应用程序"AppST"接收事件"菜单选择"时，它向移动设备发送一个被称作"选择项目"的主动命令，即在 n 个建议的服务中选择一个菜单项目（一个服务）。

例如用户选择具有序号或任意下标 i 的服务或服务 i 。应用程序"AppST"的一个applet通过一个主动命令向应用程序"AppOTA"发送一个短消息以指示用户请求服务 i 。

应用程序"AppOTA"接收来自应用程序"AppST"的短消息并且以通过另一个短消息返回服务 i 的内容的方式响应该消息。

当应用程序"AppST"接收来自应用程序"AppOTA"的短消息时，它发送一个被称作"显示文本"的主动命令以便在移动设备的屏幕上显示其内容。

图4图解了基于现有技术的前八个步骤：

步骤1：移动设备1的电路10向应用程序"AppST"30'发送"菜单选择事件"；

步骤2：应用程序"AppST"30'向移动设备1的电路10发送"选择项目"；

步骤3：这些电路通过向应用程序"AppST"30'发送"终端应答"来应答；

步骤4：后者向应用程序"AppST"30'发送"发送 SM (下标 i)" (发送带下标 i 的短消息)；

步骤5：后者向应用程序"AppOTA"21'发送"短消息(下标 i)" (发送带下标 i 的短消息)；

步骤6：后者作出应答并且发送"短消息 (服务" i ")" (带下标" i " 的服务的短消息)；

步骤7: 移动设备1的电路10向应用程序"AppST"30'发送"SMS PP 下载事件"; 和

步骤8: 应用程序"AppST"30'向移动设备1的电路10发送"显示文本 (服务"i")"以便显示与带下标"i"的服务相关的短消息的内容, 从而在移动设备1的屏幕11上显示出内容。

参照图5, 基于本发明方法的相同应用程序的开发如下所述。

由 Java applet构成的两个 SIM工具包应用程序被安装在智能卡2中: 第一个是报表生成器应用程序 21, 上述报表生成器应用程序 21 向一个对应应用程序或服务器3的主应用程序30M发送通过短消息接收的事件。

第二个是执行来自服务器3的主应用程序30M的命令的从应用程序22。

应当注意, 服务器3的主应用程序30M充当图4所示的现有技术应用程序"AppST"和"AppOTA"。

一旦这个应用程序30M接收到事件"菜单选择", 它变成从SIM工具包应用程序22的主应用程序。

它首先请求向移动设备1的电路10发送上述主动命令"选择项目"。当其接收到这个命令的应答时, 它再次请求执行主动命令"显示文本"以便显示选择的服务。

对于所描述的应用程序, 基于本发明的方法接着包含十二个如下所述的步骤:

步骤1: 移动设备1的电路10向报表生成器应用程序发送"菜单选择事件"(由移动设备1的用户启动这个步骤);

步骤2: 报表生成器应用程序21应答并且向移动设备1的电路10发送"发送SM(菜单选择)"(发送一个菜单选择短消息);

步骤3: 移动设备1的电路10向应用程序30M (这个应用程序的"AppST"部分)发送"SM(菜单选择)";

步骤4: 应用程序30M处理并且向移动设备1的电路10发送"SM(选择项目)";

步骤5: 后者向从应用程序22发送"SMS PP下载事件";

步骤6: 从应用程序22处理并且向移动设备1的电路10发送"选择项目";

步骤7: 移动设备1的电路10向从应用程序22发送"终端应答 (下标 i)";

步骤8: 后者向移动设备1的电路10发送"发送 SM (下标" i ")";

步骤9: 移动设备1的电路10向应用程序30M ("AppOTA"部分)发送"SM (选择的下标" i ")"(具有选择下标" i "的待处理短消息);

步骤10: 应用程序30M处理并且向移动设备1的电路10发送"SM (显示文本服务" i ")";

步骤11: 后者向从应用程序22发送"SMS PP下载事件"; 和

步骤12: 处理并向移动设备1的电路10发送"显示文本 (服务" i ")"
以便显示短消息的内容。

由于相同应用程序具有更多的步骤数量, 实现基于本发明的方法导致网络传输量的轻微增加。然而已经将与指定服务相关的主要应用程序从 SIM智能卡2转移到服务器3。因而由于不再需要向 SIM智能卡2加载太多的 applet, 所以服务数量不再受到潜在限制。服务器3的存储器资源事实上远大于 SIM智能卡2上提供的资源。同样地, 由于服务器3中提供的处理器的处理能力比 SIM智能卡2内的处理能力更强, 所以处理速度较高。

并且根据其具体工作范围和本发明的上述一个附加有利方面, 软件应用开发人员仍然具有以优化方式在 SIM智能卡2和服务器3之间分配操作的能力。

为此某些 SIM工具包应用程序可以保留在 SIM智能卡2中。这些应用程序的工作方式与现有技术的应用程序相同, 至少是非常类似。

根据本发明方法允许的实施例的另一个变型, 所有或部分从应用程序 22和/或报表生成器应用程序 21均可以具有上述混合类型, 即它们可以保持某种自治度。因而在这种情况下某些操作在局部继续执行, 这相应减少了 SIM智能卡2和远程服务器2之间的传输量。

通过阅读上述内容显然可以看到本发明实现了上述目标。

具体地，这允许将使用大量计算机资源的"高强度"操作转移到尤其是在数据存储方面没有限制或至少没有根本限制的数据处理系统(远程服务器)上。此外由于在这个系统中提供的计算装置同样非常快速和强力，可以高速执行操作。

根据本发明的另一个方面，虽然基于本发明的方法在某种条件下会产生额外的传输量，但通过优化部分被转移出的操作和部分仍然在本地，即在SIM智能卡或任何充当SIM智能卡的模块中执行的操作可以大大减小这个缺点。

因此，本发明实际上允许提供无限数量的服务并且不必相应增加SIM智能卡中要存储的数据数量，至少是略有增加。

还应当理解，上述转移出的应用程序包含SIM工具包应用程序本身和相关的数据文件。例如，可以将通常被称作其"环境"的用户个人数据转移到一个远程服务器上：地址簿，电话号码本等等。这些文件的长度实际上变成无限的。

最终，可以说本发明在必须更新一或多个应用程序并且应用程序被安装在远程服务器上时提供了这样的优点，即由于更新是集中的，运营商可以通过非常简单和快速的方式进行这种更新。在智能卡中安装的SIM工具包应用程序是标准的，即基于现有技术的应用程序的情况下，相同操作会需要修改所有存储要更新的应用程序的智能卡，即需要经常对其进行更新。

然而应当理解本发明不仅限于刚才具体结合图1至3和5明确描述的示例性实施例。

此外如图所示，本发明不仅限于使用短消息的传输协议。

最终，虽然比较适用于使用GSM标准的电话网，但其它标准也可以适用，尤其是当前正在开发的标准："GPRS"，"UTMS"等等。通常，每当移动设备单元和智能卡或任何类似的嵌入式系统一起使用，并且当这种嵌入式系统中直接安装的函数和移动设备中提供的函数之间存在隔离时，本发明便可以适用。

本发明也允许和 WAP类型的应用程序接口或执行这种函数。例如，远程服务器上提供的主应用程序可以直接根据移动设备的请求访问因特网并且不用首先回传通过移动设备。根据本发明的方法，请求的结果接着被发送到从应用程序。

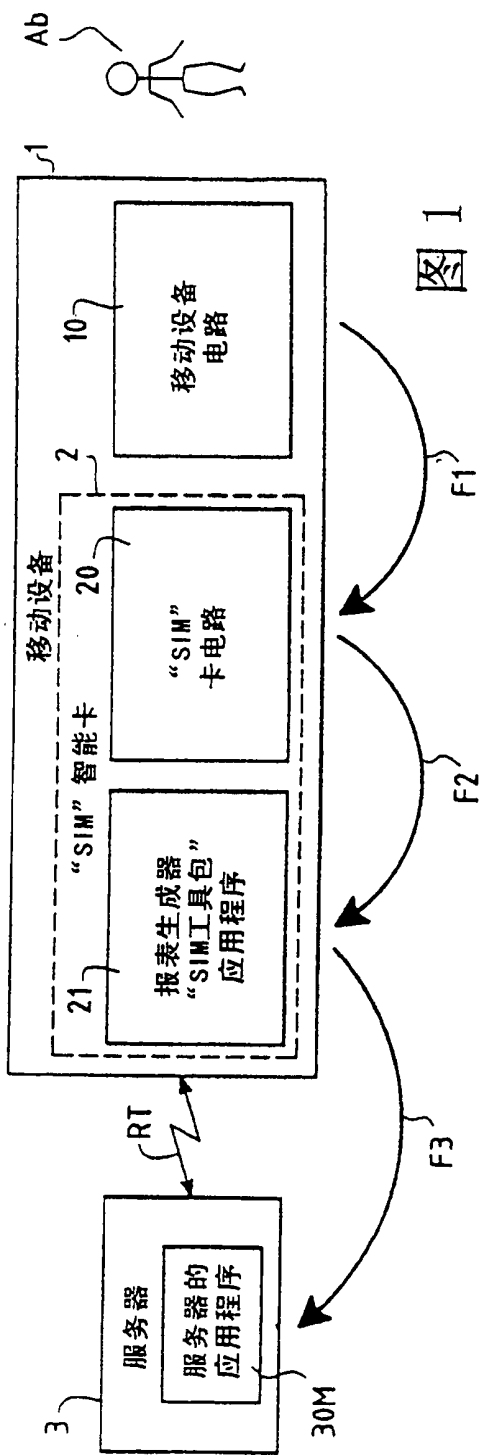


图 1

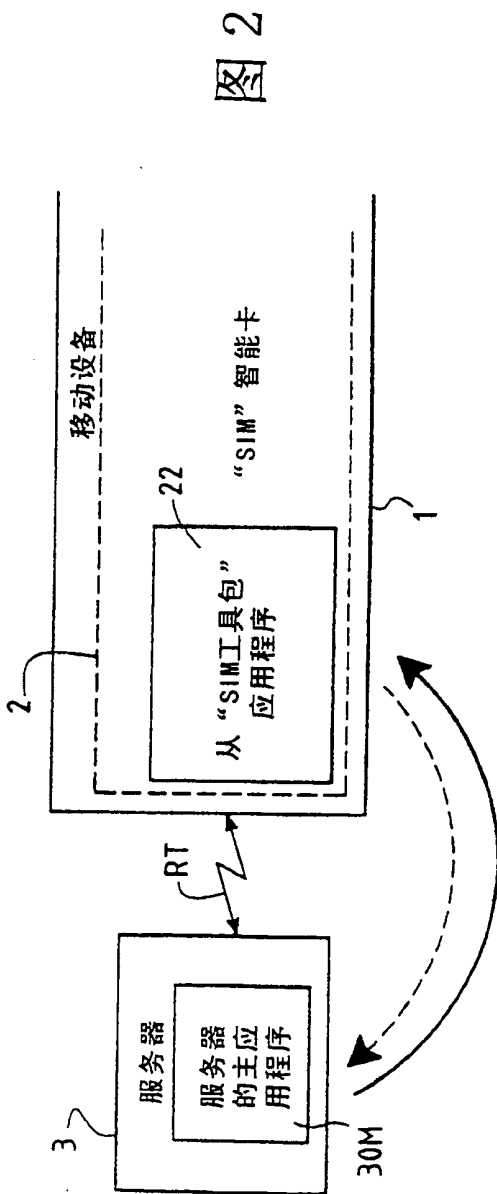


图 2

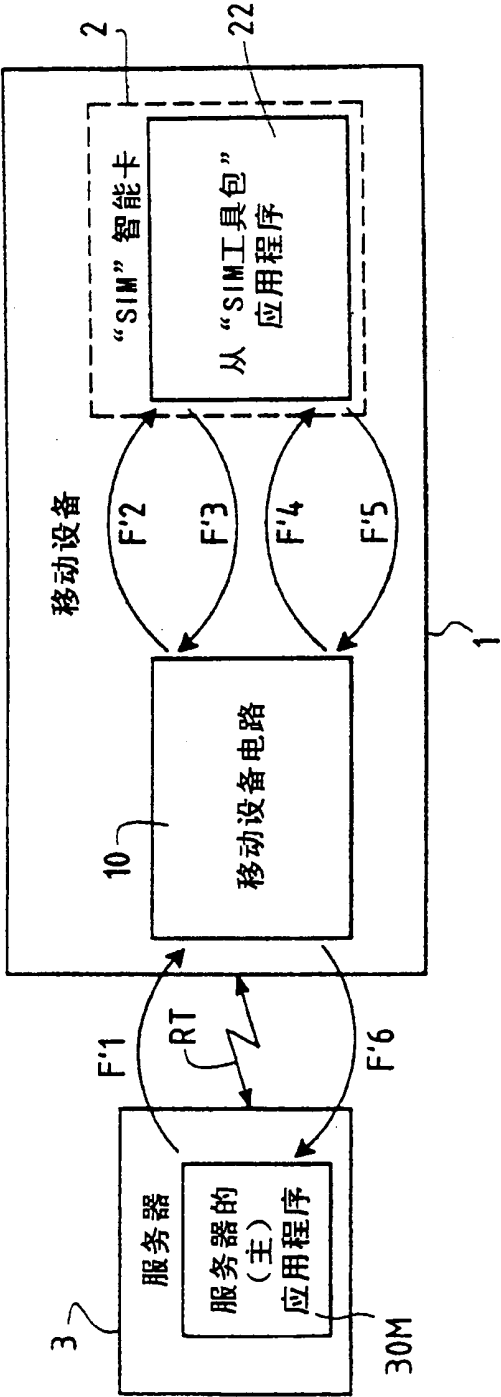


图 3

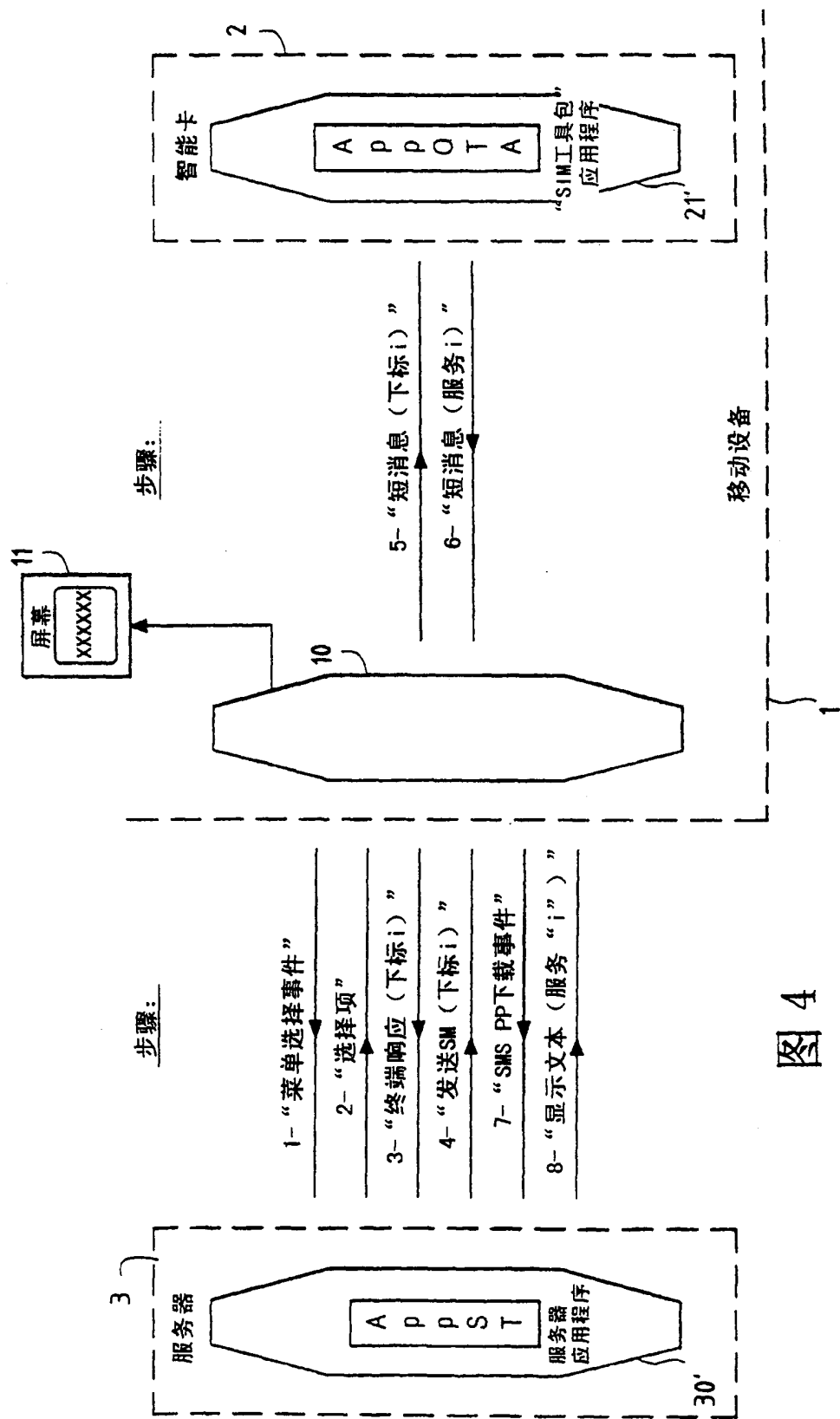


图 4
(现有技术)

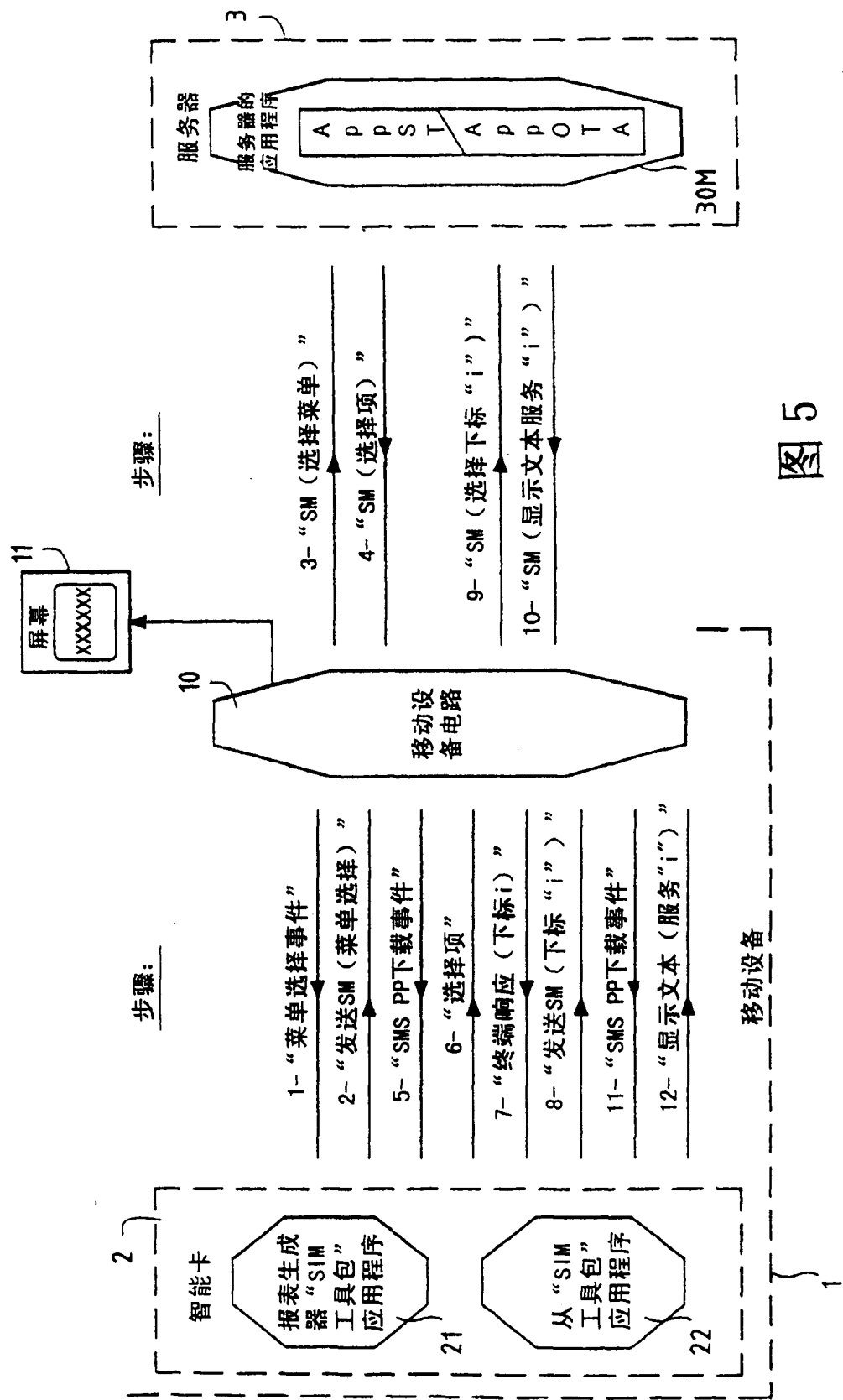


图 5