



(12) 发明专利

(10) 授权公告号 CN 1705334 B

(45) 授权公告日 2012.04.25

(21) 申请号 200510075934.2

(22) 申请日 2005.06.01

(30) 优先权数据

04253251.5 2004.06.01 EP

(73) 专利权人 捷讯研究有限公司

地址 加拿大安大略省

(72) 发明人 尼尔·P·亚当斯

希尔伯特·A·莱特

迈克尔·G·基尔库普

雷蒙德·P·范德维恩

(74) 专利代理机构 中科专利商标代理有限责任
公司 11021

代理人 王玮

(51) Int. Cl.

H04M 3/533 (2006.01)

H04L 12/58 (2006.01)

H04L 9/00 (2006.01)

(56) 对比文件

CN 1283023 A, 2001.02.07, 全文.

WO 01/24485 A1, 2001.04.05, 全文.

JP 61267432 A, 1986.11.27, 说明书第2页
左栏第8行至第3页右栏第20行, 附图1-2.

CN 1082289 A, 1994.02.16, 全文.

CN 1371568 A, 2002.09.25, 全文.

US 20020076039 A1, 2002.06.20, 全文.

US 20030059007 A1, 2003.03.27, 全文.

审查员 门晓晶

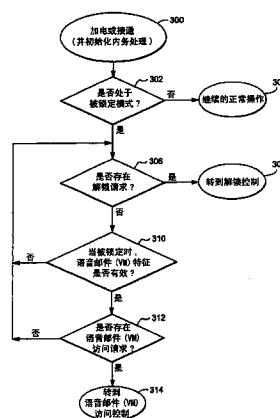
权利要求书 2 页 说明书 6 页 附图 7 页

(54) 发明名称

增强的语音邮件口令安全性

(57) 摘要

一种在用于输入口令的设备处、在本地增强语音邮件口令安全性的方法和设备,当访问受口令保护的语音邮件服务时,该通信设备(及其相关操作方法)可以调用至少有效地掩蔽口令数值、以防通过用户反馈来识别该口令数值的增强安全特征。在便携式无线通信设备可以具有供自动化语音邮件访问之用的预存口令数据的情况下—即使在“被锁定”模式下,这是尤其重要的。这种设备的未被授权拥有者可能利用口令发送期间的常规可听反馈,来译解口令值。然而,即便要,也通过掩蔽口令数据值以防可听和/或可见的用户反馈,来避免这种安全性不足。



1. 一种在用于输入口令的通信设备处、在本地增强语音邮件口令安全性的方法,所述方法的特征在于:

接收来自中心 IT 控制部的输入数据,其中所述中心 IT 控制部远离所述用于输入口令的通信设备;

在集中式控制选项存在时基于所述输入数据选择用于掩蔽设备生成的可听反馈的口令数据值掩蔽方案,所述口令数据值掩蔽方案只用来发送语音邮件口令,而不提供识别口令数据值的人类可检测反馈;

在所述通信设备处接收语音邮件口令数据输入;

根据所述输入发送语音邮件口令数据,以访问远程受口令保护的语音邮件系统;以及在所述通信设备(100)处,根据所述口令数据值掩蔽方案向用户提供反馈。

2. 根据权利要求 1 所述的方法,其中,根据所述口令数据值掩蔽方案,在本地不提供任何种类的人类可检测反馈。

3. 根据权利要求 1 所述的方法,其中,根据所述口令数据值掩蔽方案,通过不与被发送的口令数据值唯一对应的可听声音,来提供本地人类可检测反馈。

4. 根据权利要求 3 所述的方法,其中所述可听声音包括对于被发送的口令数据的每个数字实质上相同的不变音调。

5. 根据权利要求 3 所述的方法,其中所述可听声音包括为被发送的口令数据的每个数字随机选择的音调。

6. 根据权利要求 3 所述的方法,其中所述可听声音包括与被发送的口令数据的序列数值无关的、固定的预定音调序列。

7. 根据权利要求 6 所述的方法,其中用于特定通信设备的所述预定音调序列被预编程到该通信设备中。

8. 根据权利要求 7 所述的方法,其中被预编程到一个通信设备中的预定音调序列不同于被预编程到至少另一通信设备中的预定音调序列。

9. 根据权利要求 1-8 中任一项所述的方法,其中所述语音邮件口令数据被预存在通信设备中,并连同发送语音邮件电话访问号码一起自动地从该通信设备被发送。

10. 根据权利要求 1-8 中任一项所述的方法,其中所述语音邮件口令数据的每个数字都由通信设备用户手动地输入。

11. 根据权利要求 1-8 中任一项所述的方法,其进一步包括:

向通信设备用户提供选项,以便即使当通信设备另外处于被锁定和安全状态下也允许进行自动化语音邮件访问,所述被锁定和安全状态防止仅仅是拥有通信设备的人使用所述通信设备的至少一些其它功能性。

12. 根据权利要求 1-8 中任一项所述的方法,其中所述口令数据值掩蔽方案包括以下方案之一:

(a) 避免任何可听反馈;

(b) 为口令的每个数字播放相同的不变可听反馈音调;

(c) 为口令的每个数字播放随机的可听反馈音调;以及

(d) 为口令的每个数字播放来自固定的预定序列音调的可听反馈音调。

13. 一种在用于输入口令的通信设备处、在本地增强语音邮件口令安全性的装置,所述

装置的特征在于包括：

适于接收来自中心 IT 控制部的输入数据的装置，其中所述中心 IT 控制部远离所述用于输入口令的通信设备；以及

用于在集中式控制选项存在时基于所述输入数据选择用于掩蔽设备生成的可听反馈的口令数据值掩蔽方案的装置，所述口令数据值掩蔽方案只用来发送语音邮件口令，而不提供识别口令数据值的人类可检测反馈；

用于在所述通信设备处接收语音邮件口令数据输入的装置；

用于根据所述输入发送语音邮件口令数据以访问受口令保护的远程语音邮件系统的装置；以及

用于在所述通信设备 (100) 处根据所述口令数据值掩蔽方案向用户提供反馈的装置。

14. 根据权利要求 13 所述的装置，其中，根据所述口令数据值掩蔽方案，在本地不提供任何种类的人类可检测反馈。

15. 根据权利要求 13 所述的装置，其中，根据所述口令数据值掩蔽方案，通过不与被发送的口令数据值唯一对应的可听声音，来提供本地人类可检测反馈。

16. 根据权利要求 15 所述的装置，其中所述可听声音包括对于被发送的口令数据的每个数据实质上相同的不变音调。

17. 根据权利要求 15 所述的装置，其中所述可听声音包括为被发送的口令数据的每个数字随机选择的音调。

18. 根据权利要求 15 所述的装置，其中所述可听声音包括与口令数据的序列数值无关的、固定的预定音调序列。

19. 根据权利要求 18 所述的装置，其中用于特定通信设备的所述预定音调序列被预编程到该通信设备中。

20. 根据权利要求 19 所述的装置，其中被预编程到一个通信设备中的预定音调序列不同于被预编程到至少另一通信设备中的预定音调序列。

21. 根据权利要求 13 至 20 中任一权利要求所述的装置，其中所述语音邮件口令数据被预存在所述通信设备中，并连同发送语音邮件电话访问号码一起自动地被发送。

22. 根据权利要求 13 至 20 中任一权利要求所述的装置，其中所述语音邮件口令数据的每个数字都由通信设备用户手动地输入。

23. 根据权利要求 13 至 20 中任一权利要求所述的装置，其进一步包括：

用于向通信设备用户提供选项以便即使当通信设备另外处于被锁定和安全状态下也允许进行自动化语音邮件访问的装置，所述被锁定和安全状态防止仅仅是拥有通信设备的人使用所述通信设备的至少一些其它功能性。

24. 根据权利要求 13 至 20 中任一权利要求所述的装置，其中所述口令数据值掩蔽方案包括以下方案之一：

(a) 避免任何可听反馈；

(b) 为口令的每个数字播放相同的不变可听反馈音调；

(c) 为口令的每个数字播放随机的可听反馈音调；以及

(d) 为口令的每个数字播放来自固定的预定序列音调的可听反馈音调。

增强的语音邮件口令安全性

技术领域

[0001] 本发明涉及可以使用受口令保护的语音邮件服务的通信设备。本发明尤其可用于具有供自动化语音邮件访问能力自动使用的被存储口令数据的移动无线通信设备。

背景技术

[0002] 语音邮件工具如今是实际上所有电话系统的众所周知特征。大多数语音邮件服务是受口令保护的,以致甚至对于被授权的用户,也只有正确输入预先定义的秘密口令,才允许访问这些语音邮件服务。

[0003] 移动或无线通信设备也可用于访问这种语音邮件工具。常常,这种便携式无线通信设备具有预存的、用于访问语音邮件特征的电话号码—通常包括必需的口令数据(例如,作为访问电话号码的附加号码,或者作为在通过第一电话号码建立了到语音邮件工具的连接之后接着要拨的第二伪电话号码)—的能力。当然,也能通过用户对常见键盘的操作—包括输入用于访问语音邮件数据的必需口令,来手动地访问语音邮件工具。

[0004] 典型地,按照惯例向这种通信设备的用户提供可听反馈(audible feedback)。典型地,对于访问电话号码和口令的每个数字,都产生用户听得见的清晰可辨音调。通常,可听反馈可以是传统上用于把用户的键击数据发送给传统普通老式电话业务(POTS)中电话交换设备的常见双音多频(DTMF)音调。如果使用替换的反馈可听音调,则按照惯例也使它们和特定数值唯一关联。即,传统上,在给定音频(或在DTMF音调情况下的频率组合)和被手动键入或自动发送的特定数值之间,存在一对一的唯一对应关系。

[0005] 如果便携式(即无线)通信设备包括自动化语音邮件访问特征(包括必需的口令),则未被授权的用户(例如扒手或攻击者)可能非法占有设备,并发出未被授权的电话呼叫—包括对语音邮件服务的未被授权访问。这样做时,如果有一些识别正被发送的口令数据值的人类可检测反馈(humanly detectable feedback),则在未被授权的非法占有期间,未被授权用户可以获知秘密口令值。如果是这样的话,甚至可能在合法用户不知道这种未被授权访问发生了的情况下,也获得这种信息,因此提出了未来受口令保护的语音邮件服务的安全性风险。例如,未被授权的用户可能利用录音机来仅仅记录音调序列,然后获知音频与数值之间的唯一对应关系,重放被记录的音调来弄清语音邮件口令值。

[0006] 已公开的美国专利申请 US 2002/0076039A1 是针对,通过在远程应答机站点插入合适的干扰信号,来干扰从远程应答机反射的DTMF口令音调。该技术用于挫败电话线或蜂窝网络上可能正在收听从远程应答机反射的返回信号的偷听者。然而,该方法根本没有提到,对由在输入口令的设备处本地产生的本地用户反馈生成的口令数据提供本地保护的问题。

[0007] 至少因为这样的原因,增强的语音邮件口令安全性是所希望的。

发明内容

[0008] 我们现在认识到了,通过发送语音邮件口令数据而不提供识别口令数据值的人类

可检测反馈,能够基本上避免这种语音邮件口令安全性问题。在示范性实施例中,能够以以下方式中至少一种方式来实现这种增强的安全性:

[0009] (a) 当输入口令时,不提供任何人类可检测反馈;

[0010] (b) 通过不与被发送的口令数据值唯一对应的可听声音,来提供人类可检测反馈(例如,可以为输入的数的每个数字使用相同的音频);

[0011] (c) 随机选择的音频(或多种音频)可以用于可听反馈;以及

[0012] (d) 固定的预定序列音频可以用于可听反馈,而与口令值可能是什么无关(例如,每个单独的设备甚至可能有不同的要播放的预编程音调序列)。

[0013] 虽然这些掩蔽方案中的一种或多种、或不同的掩蔽方案可能用于整个电话号码和口令输入(手动的、或预存并自动的),但是我们主要关心为至少语音邮件口令而使用这种掩蔽方案。

[0014] 可以提供被掩蔽的可见反馈—单独地、或者与被掩蔽的可听反馈组合。例如,当在发送每个口令数字时,可能显示不与实际数值唯一对应的掩蔽可见字符(例如星号),来代表口令数字的发送。类似于上述可听掩蔽方案,也可以定义各种不同的可见反馈掩蔽方案。

[0015] 也可以为多个通信设备的集中式控制,而提供实施多种可能数据值掩蔽方案之一的选项。当然,可以将设备配置成只有一种这样的掩蔽方案,并完全避免任何选择。作为选择,可以允许用户选择是否实施并可以得到多种这样的掩蔽方案。

[0016] 可以用硬件、软件或硬件与软件组合,来体现本发明。通过可以用常规无线通信设备的物理程序存储介质体现的可执行计算机程序代码,来完全实现示范性实施例。

附图说明

[0017] 连同以下参考附图进行的示范性实施例详细描述,本发明的这些及其它目的和优点将变得更容易理解和评价,其中:

[0018] 图1是根据本发明一个示范性实施例的、结合了具有增强语音邮件口令安全性的移动无线通信设备的示范性无线邮件通信系统的整个系统示意图;

[0019] 图2是示范性移动无线通信设备内包括的硬件的缩略示意图;

[0020] 图3是可以和图2的移动通信设备一起使用的设备控制程序逻辑的示范性缩略示意图;

[0021] 图4是可以用于图2设备中以便为至少语音邮件口令提供增强安全性的计算机软件(即程序逻辑)的示范性缩略示意图;

[0022] 图5是可以用于图2设备中以便提供要在多个通信设备中实施对语音邮件口令掩蔽方案的集中式控制的选项的计算机软件(即程序逻辑)的示范性缩略示意图;

[0023] 图6是对于内容保护特征被使能的被锁定通信设备的可能屏幕的示范性表示;

[0024] 图7是对于仍然允许进行电话呼叫的被锁定通信设备的屏幕显示的示范性表示;以及

[0025] 图8是对于仍然提供允许进行语音邮件呼叫的菜单的被锁定通信设备的可能屏幕显示的示范性表示。

具体实施方式

[0026] 图 1 是根据本发明的可以使用无线通信设备 100 的示范性通信系统的概略图。本领域技术人员将要理解,有数百种不同的系统拓扑。也可以有许多消息发送器和接收器。图 1 所示的简单示范性系统只是说明性的,并且可能显示了当前最流行的因特网邮件环境。

[0027] 图 1 显示了邮件发送器 10、因特网 12、消息服务器系统 14、无线网关 16、无线基础设施 18、无线网 20 和移动通信设备 100。

[0028] 例如,邮件发送器 10 可以连接到位于公司内部、有可能连接到局域网 (LAN)、连接到因特网 12、并且上面具有系统用户帐户的因特网服务提供商 (ISP),或者可以通过诸如 America Online™ (AOL) 的大应用服务提供商 (ASP) 连接到因特网 12。本领域技术人员将要理解,图 1 所示的系统可以改为连接到除因特网以外的广域网 (WAN),虽然邮件传输一般是通过如图 1 所示的因特网连接配置来实现的。

[0029] 例如,可以在公司防火墙内的网络计算机、ISP 或 ASP 系统内的计算机等上面实施消息服务器 14,并且消息服务器 14 充当因特网 12 上邮件交换的主接口。虽然其它消息收发系统可能不需要消息服务器系统 14,但是为接收并有可能发送邮件而配置的移动设备 100 将正常地和消息服务器上的帐户联系。可能两种最普通的消息服务器是 Microsoft Exchange™ 和 Lotus Domino™。这些产品常常和路由并传递邮件的因特网邮件路由器一起使用。在图 1 中没有显示这些中间部件,因为它们不直接在下述本发明中起作用。诸如服务器 14 的消息服务器的功能典型地刚好扩展到邮件发送与接收以外;它们也包括动态数据库存储引擎,该动态数据库存储引擎具有为诸如日历、要做事情列表、任务列表、邮件和文件的数据而预先定义的数据库格式。

[0030] 无线网关 16 和无线基础设施 18 提供因特网 12 与无线网 20 之间的链接。当用户在国家或网络之间漫游时,无线基础设施 18 确定用于定位给定用户的最可能网络,并跟踪用户。然后,典型地以射频 (RF),通过无线传输把消息从无线网络 20 中的基站传送给移动设备 100。特殊网络 20 实际上可以是可以通过其与移动通信设备交换消息的任何无线网络。

[0031] 如图 1 所示,位于因特网 12 某处的邮件发送器 10 发送组成邮件消息 22。该消息 22 典型地利用传统的简单邮件传输协议 (SMTP)、RFC 822 头和多用途因特网邮件扩展 (MIME) 体部分,来定义邮件消息的格式。这些技术对于本领域技术人员是众所周知的。消息 22 到达消息服务器 14,并且正常地被存储在消息存储器中。最为人所知的消息收发系统支持所谓的“推送”消息访问方案,其中移动设备 100 必须请求消息服务器 14 把存储的消息转发给移动设备 100。一些系统提供了利用与移动设备 100 关联的特定邮件地址来寻址的这种消息的自动路由。在优选实施例中,当寻址到和诸如属于移动设备 100 的用户的家庭计算机或办公计算机的主系统关联的消息服务器帐户的消息被接收时,这些消息从消息服务器 14 被重新引向移动设备 100。

[0032] 与用于控制消息到移动设备 100 的转发的特定机制无关,消息 22 或者其可能的转化或重新格式化版本,被发送给无线网关 16。无线基础设施 18 包括到无线网络 20 的一系列连接。这些连接可以是综合服务数字网 (ISDN)、使用在整个因特网上使用的 TCP/IP 的帧中继或 T1 连接。当用于此处时,术语“无线网”意欲包括三种不同类型的网络,它们是 (1) 数据中心无线网络, (2) 语音中心无线网络,以及 (3) 通过相同物理基站既能支持语音通信、又能支持数据通信的双模网络。组合双模网络包括但不限于:(1) 码分多址 (CDMA) 网

络, (2) 特别移动组或全球移动通信系统 (GSM) 以及通用分组无线业务 (GPRS) 网络, 以及 (3) 诸如增强数据率全球演进 (EDGE) 和通用移动通信系统 (UMTS) 的未来第三代 (3G) 网络。一些更旧的数据中心网络例子包括 Mobitex™ 无线网络和 DataTAC™ 无线网络。更旧的语音中心数据网络的例子包括诸如 GSM 的个人通信系统 (PCS) 和时分多址 (TDMA) 系统。

[0033] 如图 2 所示, 移动通信设备 100 包括用于和无线网络 20 进行无线通信的合适 RF 天线 102。提供了常规的 RF、解调 / 调制与解码 / 编码电路 104。如本领域技术人员将要理解的, 这种电路可以涉及可能许多数字信号处理器 (DSP)、微处理器、滤波器、模拟和数字电路等。然而, 因为这种电路在该领域中是众所周知的, 因此不进一步描述。

[0034] 如将要理解的, 移动通信设备 100 可以被配置成在公用交换电话系统 (PSTS) 中操作, 以便允许语音电话呼叫以及 / 或者提供对常规语音邮件服务的访问。

[0035] 移动通信设备 100 典型地还包括主控制中央处理器 (CPU) 106, 主控制 CPU 106 在程序存储器 108 中存储的程序的的控制下操作 (并且可以使用数据存储器 110)。CPU 106 与常规的键盘 112、显示器 114 (例如液晶显示器) 及音频换能器或扬声器 116 通信。数据存储器 110a 的一部分可用于存储一个或多个语音邮件 (VM) 访问号码和相应的口令 (PW)。合适的计算机程序可执行代码被存储在程序存储器 108 的几部分中, 以构成关于至少存储的 VM PW 的增强安全性。

[0036] 控制 CPU 106 典型地受如图 3 所示的主控制程序所控制。在此, 一旦在 300 加电或接通, 如果在 302 没有检测到被锁定模式, 则在 304 可以允许继续的正常操作。然而, 如果设备处于被锁定模式, 则在 306 检查解锁请求。如果检测到了解锁请求, 则可以将控制传递给常规解锁例程 308。然而, 如果设备保持被锁定模式并且没有解锁请求, 则在 310 进行检查, 看设备是否具有即使在被锁定模式下也允许进行呼叫 (例如语音邮件访问) 的当前有效模式。如果是这样的话, 则在 312 对语音邮件访问请求进行进一步测试。如果检测到这种请求, 则在 314 将控制传递给语音邮件例程。否则, 继续贯穿测试单元 306、310 和 312 的循环, 等待适当的输入。

[0037] 如本领域技术人员将要理解的, 虽然在此 (以上和以下) 将示范性实施例描述为使用循环逻辑, 但是在专用硬件和 / 或操作系统平台上的实施中, 优选地可以使用中断事件驱动的逻辑来代替一些或所有这种逻辑。

[0038] 图 4 中描述了可能的语音邮件访问控制逻辑, 并在 400 进入该语音邮件访问控制逻辑。在 402 将循环计数器 n 初始化为 1 值。然后, 在 404 进行测试, 看预存的带有口令的语音邮件访问的自动拨号是否有效。如果没有, 则在 406 进入等待循环, 以等待语音邮件访问电话号码和口令的数字的适当用户键入。如将要理解的, 如果希望的话, 可以回避图 4 逻辑中关于电话邮件电话访问号码的增强安全特征, 而只为口令发送采用图 4 逻辑中的增强安全特征。

[0039] 当 (语音邮件电话访问号码和 / 或秘密口令的) 下一个数字 D(n) 可用于发送时, 则在 408 以常用和常规的方式、利用合适的数字信令协议、通过合适的数字信道, 来发送该下一个数字 D(n)。当然, 把数字协议等用于电话交换网的该常规实际信令本身不向用户提供任何可听的 (或可见的) 反馈。

[0040] 在 410 提供关于可能的可听和 / 或可见用户反馈的规定。如本领域技术人员将要

理解的,现代微处理器和 / 或 DSP 具有软件控制音调发生器 (或者能够利用合适的操作系统或应用程序软件对现代微处理器和 / 或 DSP 编程,以提供这种特征)。如图 4 中的 410 所示,一个选项仅仅是,根本不提供可听的用户反馈。然而,该选项不是优选的,因为期望将给予一些可听的用户反馈 (例如,使得用户知道实际上数字已通过信令电路被发送)。410 中的第二选项是总是为每个被发送的数字产生相同的固定音调 T。410 所示的第三种可能掩蔽方案 (masking scheme) 是利用随机数 RN 随机选择音调,以便为每个连续数字选择可能不同的音调 (RN)。410 所示的另一种可能掩蔽方案规定了要发送的固定序列音调 $T(n)$ - 与可能为连续数字发送什么值无关。也可以提供类似的掩蔽可见反馈方案的逻辑。如将要理解的,所有这些都只是可能被用来发送语音邮件口令,而不提供识别口令数据值的人类可检测反馈的掩蔽方案的例子。

[0041] 在 412 进行合适的测试,看是否有附加数字要发送。如果是这样的话,则在 414 使循环计数器 n 递增,并将控制传回给 404 处的循环顶部。如果发送了一组完整的数字,则将在 412 检测到这一点,并且例程将在 416 退出。

[0042] 当然,如本领域技术人员将要理解的,有许多用于确定序列最后数字何时到达的常规技术。例如,不是计数到预期最多数量的数字 (可以在为特殊电话系统接口而配置该设备的期间设置的数量), 而是可以进入等待循环,看在某一预定长时间以后是否 (自动或手动地) 输入了另一个数字。如果没有,则可以假定所有期望的数都被输入了,并且照这样,例程可以在 416 退出。本领域技术人员也要认识到其它用于实现期望最终结果的技术。

[0043] 如果希望的话,可以提供如图 5 所示的掩蔽方案选择例程,并在 500 进入该掩蔽方案选择例程。该示范性实施例使能在 502 被测试的集中式控制选项。如果存在,则在 504 只响应来自中心 IT 控制部等的输入数据、才允许掩蔽方案选择发生,以便选择 (例如,如上及如下描述的方案 a、b、c 或 d 之一)。

[0044] 如果集中式控制选项没有变成有效,则在 506 接受各个用户输入,以便选择多种可能的掩蔽方案之一。视情况而定,按照惯例在 508 或 510 退出到其它处理例程。

[0045] 如果通信设备 100 被锁定 (即内容保护特征有效), 则对于未被授权的用户,设备的可见屏幕可以看上去实际上是空白的。例如,屏幕可以看上去如图 6 所示。然而,如果即使在该被锁定模式下仍然允许语音邮件呼叫,则用户能够调用如图 7 所示的菜单 (例如通过用户移动滚轮或按键), 并选择发出呼叫的选项。如果该选项被选中,则可以提供如图 8 所示的屏幕,以允许自动化语音邮件访问呼叫。同样如图 7 所示,可以提供多个选项,以允许预编程的紧急情况呼叫或发出其它期望电话呼叫 (例如,用于语音邮件访问—可能是预编程的、并且被自动或手动实施)。

[0046] 如果设备用户具有使允许他或她不登录他们的设备就从被锁定屏幕发出电话呼叫的特征有效的选项,这允许攻击者盗窃用户的设备,并发出电话呼叫。使能该特征的用户必定冒这个风险。然而,在没有本发明的情况下,当设备被偷时—即使该设备被锁定,这也使用户预存的语音邮件口令容易被得到。例如,在没有本发明的情况下,攻击者只须拨 (即选择) 预编程的语音邮件号码,并且当系统自动输入口令 (访问号码) 时记录音调。如果音调是每个号码所特有的 (按照惯例), 则通过重放被记录的音调,攻击者能够弄清用户的语音邮件口令。

[0047] 然而,如上所述,我们的示范性实施例提供了对该问题的四种解决方案 :

[0048] a) 当自动输入口令时,不播放任何音调;

[0049] b) 当自动输入口令时,播放不变音调(例如为每个输入的数字播放相同的音调);

[0050] c) 当自动输入口令时,播放随机音调(例如为每个输入的数选择新的随机音调);以及/或者

[0051] d) 当自动输入口令时,播放固定的预定序列音调(例如总是播放相同序列的音调,而与口令数值序列是什么无关)—每个设备甚至可以有被播放的不同预编程音调序列。

[0052] 当设置语音邮件拨号时,可以要求用户输入两个值。一个值是“语音邮件号码”,另一个值是“附加号码”。电话应用程序首先拨语音邮件号码,然后拨附加号码。典型地,附加号码包括口令,因此当电话应用程序拨附加号码时,电话应用程序可以自动应用音调重新映射(即掩蔽方案)。当然,附加号码也可以包括电话分机等。

[0053] 中心 IT 管理员可以强制执行哪种重新映射方案(即,通过向设备发送 IT 策略,来强制应该使用哪种重新映射方案)。然而,这样不能提高安全性。按照惯例,IT 管理员可以确定用户是否被允许从被锁定屏幕拨他们的语音邮件。

[0054] 如果设备被解锁,则附加号码(即口令)可以是可见的,并且如果是这样的话,攻击者将可以可见地使用口令,因此在解锁模式下音调的重新映射目前不提供任何安全性。然而,在其中在选项屏幕中掩蔽口令的实施的,即使在解锁模式下也可以享受增强的安全性。典型地,被发送的电话号码的数字被映射到唯一对应的音调,从而当拨号时,用户听到某些音调。在本发明的示范性实施例中,至少在拨口令的时候,改变那个映射。四种不同的示范性映射技术(即无声、不变、随机、随机序列)全部都提供增强的安全性。然而,无声选项可能不是用户友好的,因为合法用户不知道口令是否被拨打。

[0055] 虽然连同目前被认为是最实际和优选的实施例一起描述了本发明,但是应该理解,本发明不限于所公开的实施例,而是相反,意欲覆盖在附加权利要求的精神和范围内包括的变化、更改及等效配置。

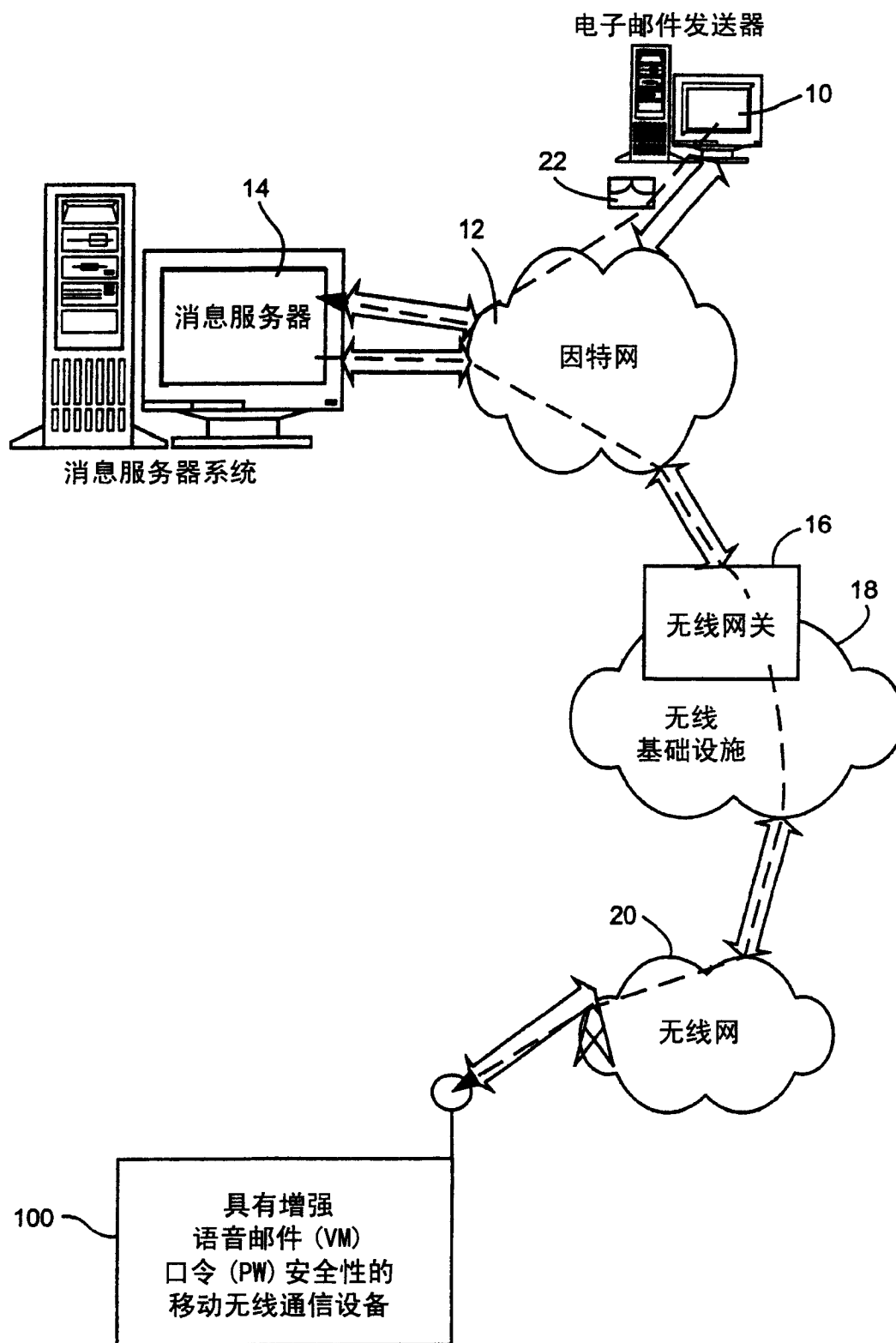


图 1

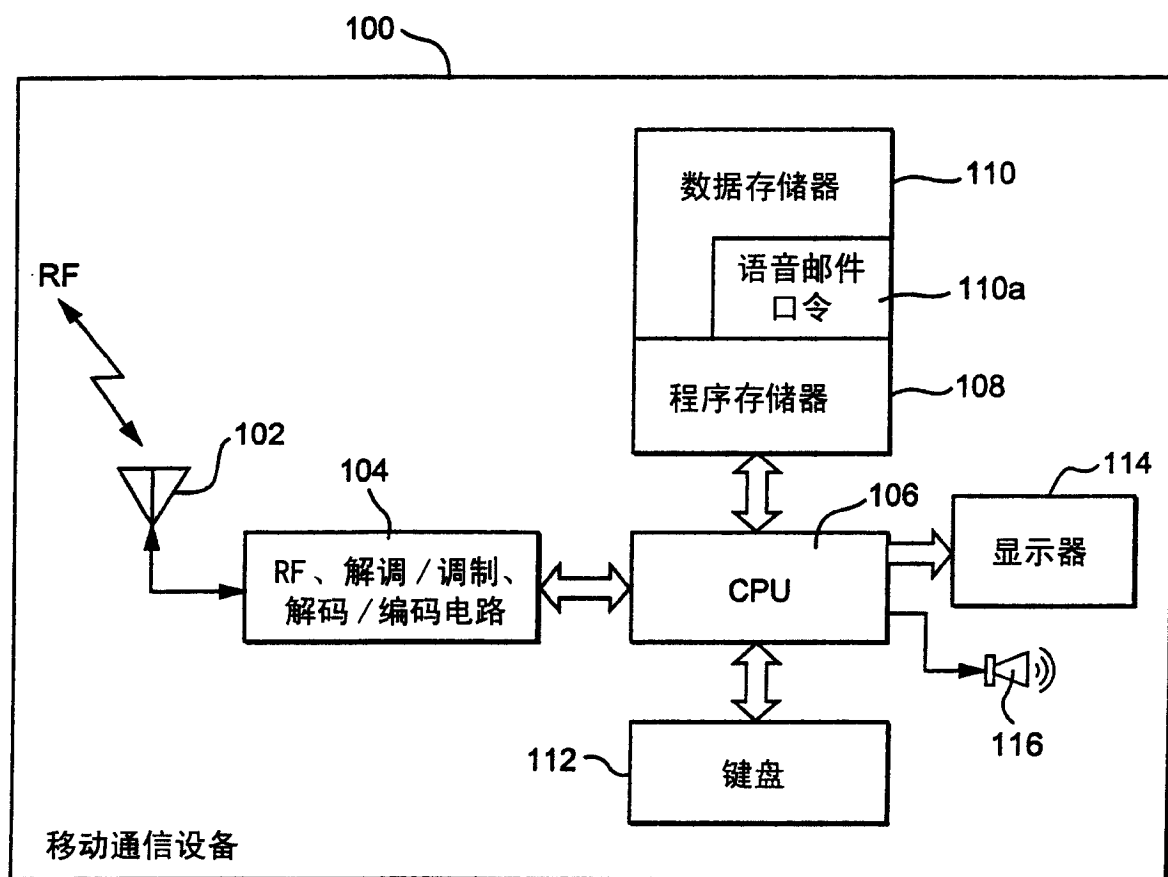


图 2

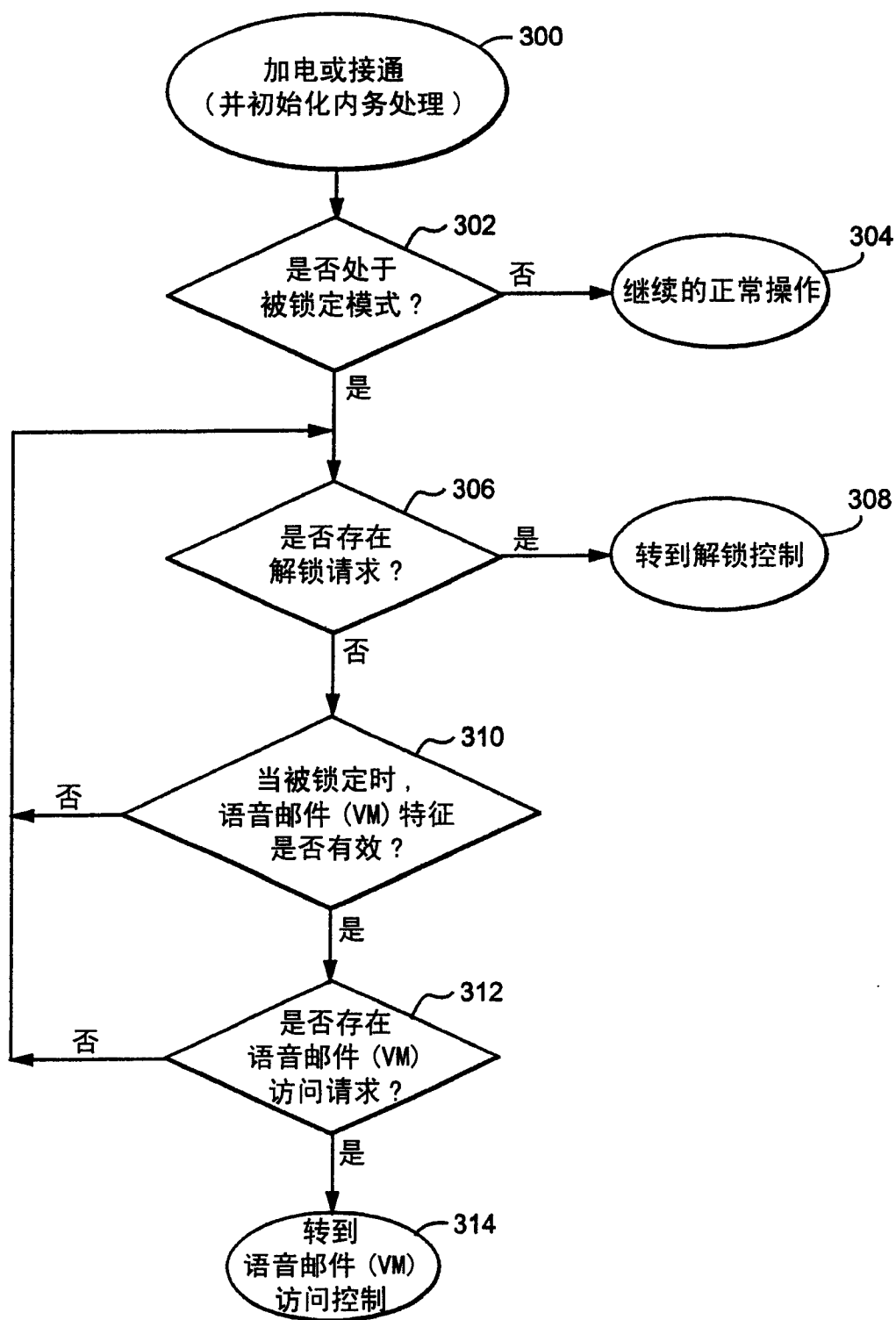


图 3

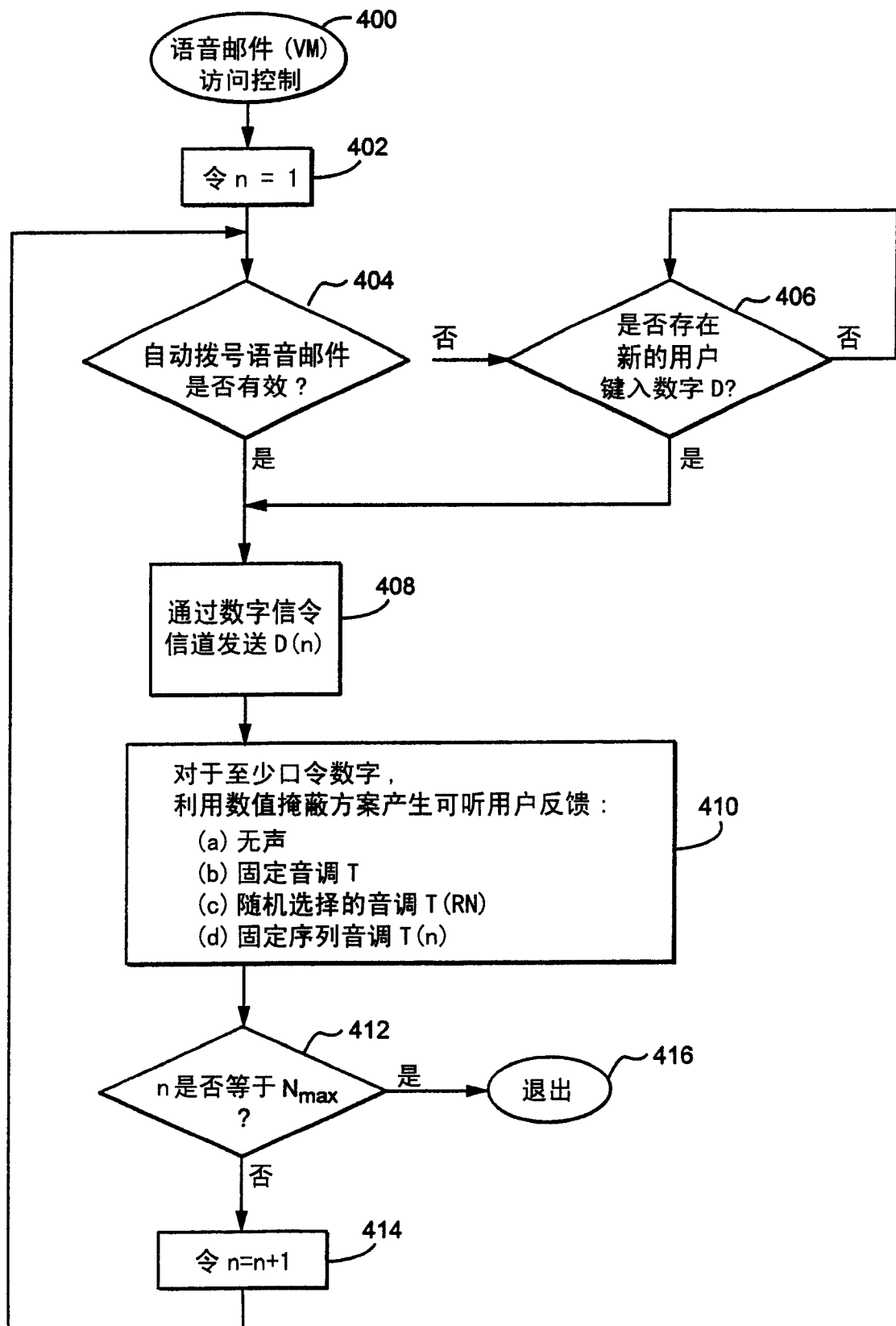


图 4

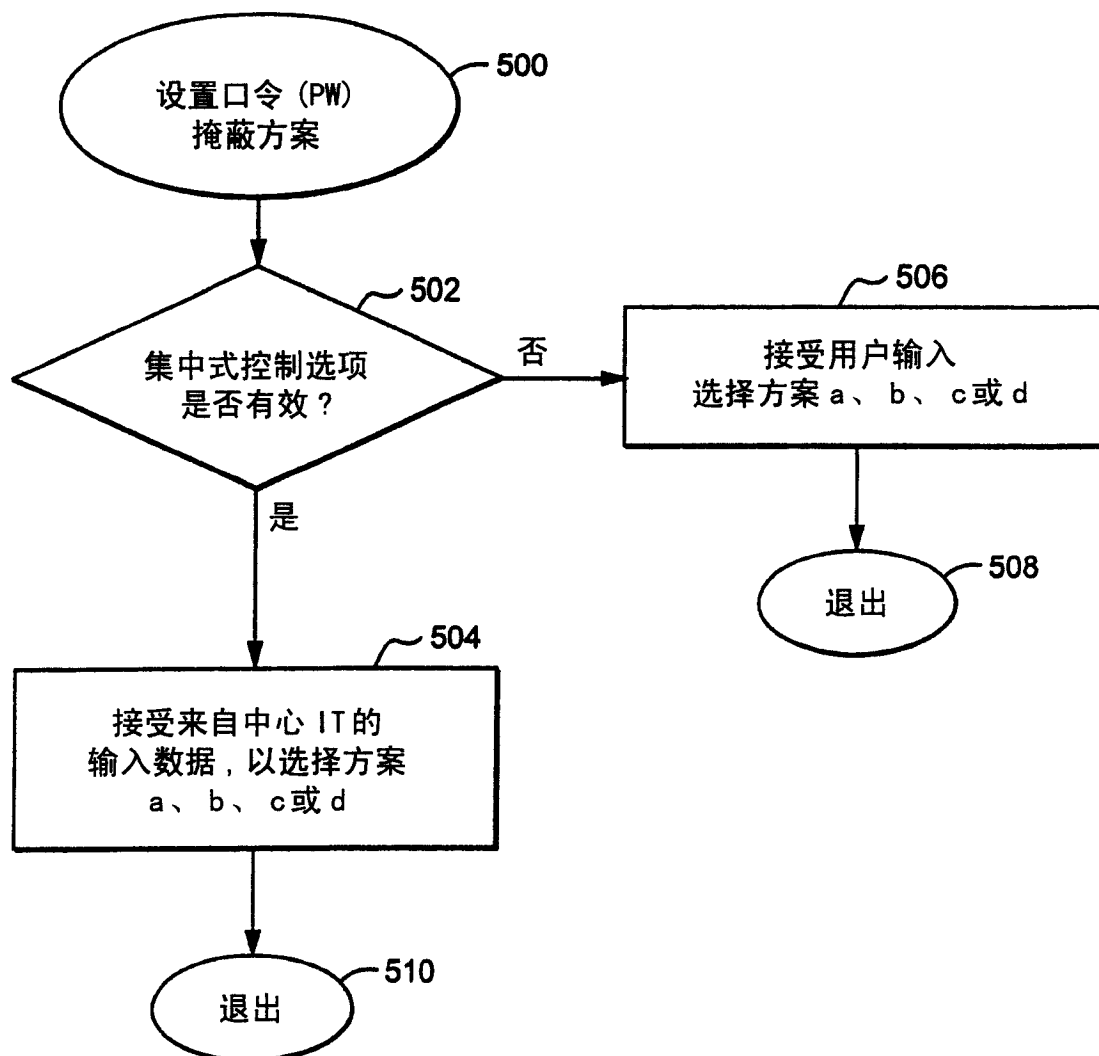
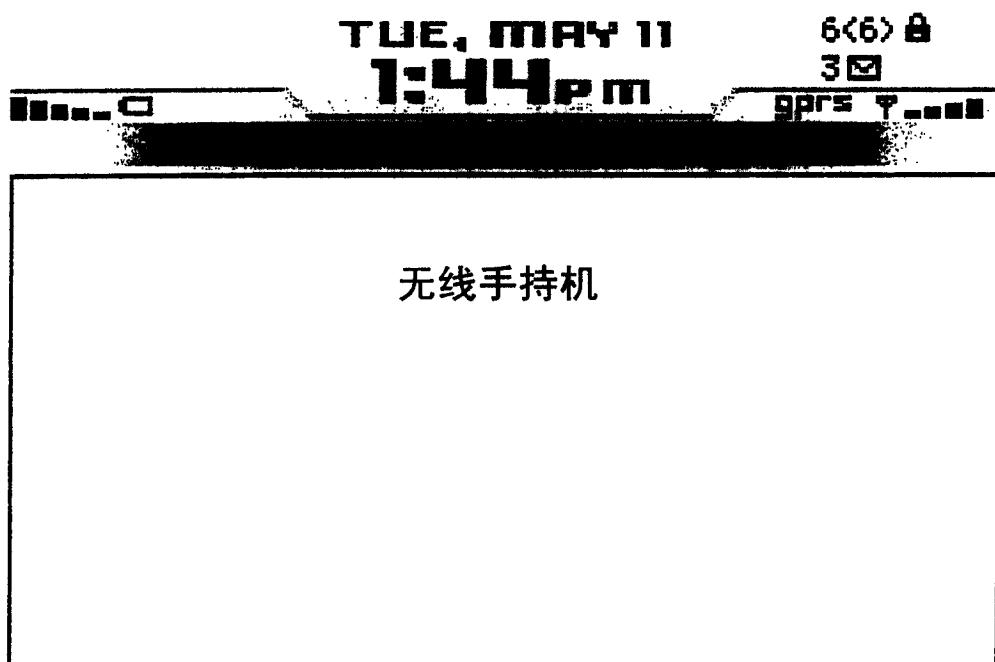
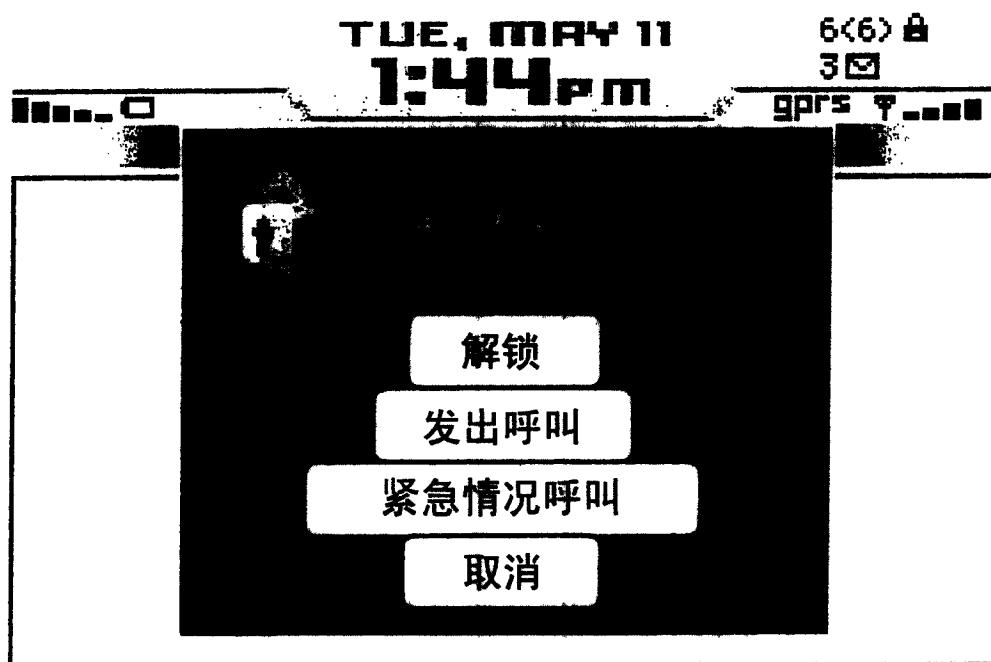


图 5



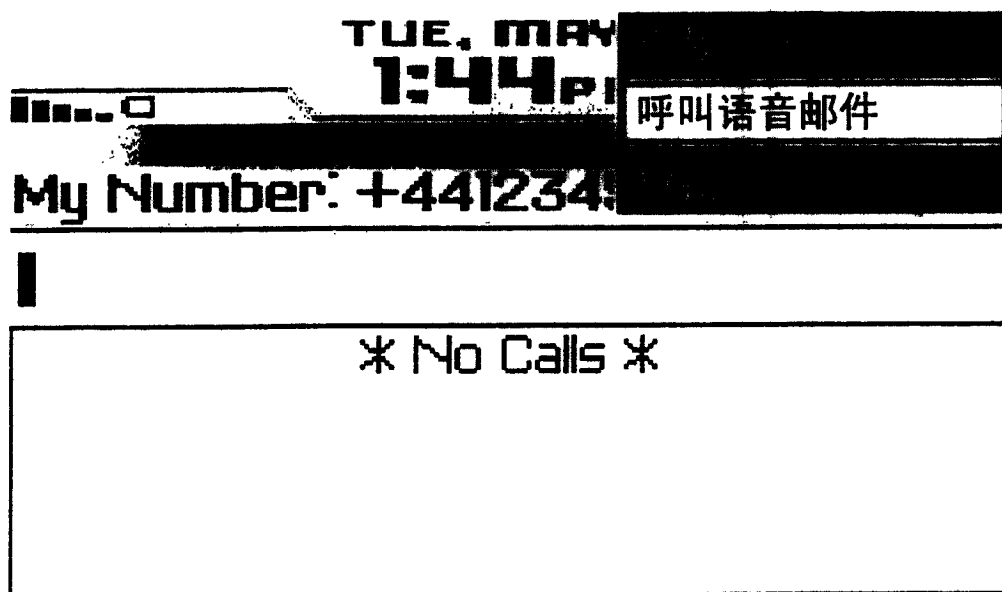
使被锁定设备控制保护有效

图 6



从被锁定设备发出呼叫的选项

图 7



关于被锁定设备的呼叫语音邮件菜单项

图 8