

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G06F 9/30 (2006.01)

G06F 9/318 (2006.01)

G06F 9/45 (2006.01)



[12] 发明专利说明书

专利号 ZL 02155777.2

[45] 授权公告日 2007 年 11 月 28 日

[11] 授权公告号 CN 100351779C

[22] 申请日 2002.12.4 [21] 申请号 02155777.2

[30] 优先权

[32] 2001.12.5 [33] US [31] 10/005, 959

[73] 专利权人 微软公司

地址 美国华盛顿州

[72] 发明人 I·B·皮夫 H·M·丹格

K·J·萨瓦吉 S·R·谢尔

N·M·霍夫梅斯特

[56] 参考文献

CN1221147A 1999.6.30

US5768566A 1998.6.16

EP0811942A2 1997.12.7

WO9956207A1 1999.11.4

US6199204B1 2001.3.6

审查员 王学睿

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 张政权

权利要求书 7 页 说明书 16 页 附图 5 页

[54] 发明名称

利用配置管理器的回滚与安全特性在移动计算设备上安装软件

[57] 摘要

使用配置管理器安装软件，从而可以在安装过程中利用配置管理器的回滚与安全特性。一台移动计算设备访问将要安装在该移动计算设备上的文件，以及定义了如何将这些文件安装到该移动计算设备上的计算机可执行指令。然后配置管理器使这些计算机可执行指令得以执行（如使用配置服务供应器），并使一个镜像回滚文档得以构造。如果安装失败，就通过执行该回滚文档倒转安装过程。通过检查判定每个安装指令的执行是否已授权，配置管理器还可以用来在执行安装指令时实现安全性。

1、在一个包含了一套计算机可执行指令来源和多台移动计算设备的网络环境中，使至少其中一台移动计算设备利用驻留在该移动计算设备上的配置管理器的回滚特性作为一个事务来安装该套计算机可执行指令的一种方法，其特征在于该方法包含：

该移动计算设备访问将要安装在该移动计算设备上的至少一个文件的至少一个版本的一个动作；

该移动计算设备访问定义了如何将该至少一个文件安装到该移动计算设备上的计算机可执行安装指令的一个动作，而这些安装指令直接由与该移动计算设备相关的一个配置管理器来解释；

该移动计算设备判定这些安装指令是否会成功的一个动作；

该配置管理器使这些安装指令得以执行的一个动作；

该配置管理器使一个回滚文档得以构造的一个动作；以及

该配置管理器将一个安装前状态包含在该回滚文档中的一个动作。

2、如权利要求 1 所述的一种方法，其特征在于所述移动计算设备判定这些安装指令是否会成功的动作包含：

询问多个将要执行某些安装指令的配置服务供应器就它们相应的安装指令而言安装是否会成功的一个动作。

3、如权利要求 2 所述的一种方法，其特征在于进一步包含：

根据询问的结果判定安装是否会成功的一个动作；以及

包括将这些安装指令作为一个整体执行的事务提交的一个动作。

4、如权利要求 1 所述的一种方法，其特征在于该移动计算设备判定这些安装指令是否会成功的动作包含：

判定这些安装指令都已成功执行的一个动作。

5、如权利要求 1 所述的一种方法，其特征在于该移动计算设备判定这些安装指令是否会成功的动作包含：

判定这些安装指令作为整体已执行失败的一个动作；以及

通过执行回滚文档来倒转安装过程的一个动作。

6、如权利要求 1 所述的一种方法，其特征在于其中的该移动计算设备访问将要安装在该移动计算设备上的至少一个文件的至少一个版本的动作包含：

该移动计算设备访问将要安装在该移动计算设备上的至少一个文件的一个压缩版本的一个动作；以及

该移动计算设备解压将要安装在该移动计算设备上的至少一个文件的该压缩版本的一个动作。

7、如权利要求 1 所述的一种方法，其特征在于其中的该移动计算设备访问将要安装在该移动计算设备上的至少一个文件的至少一个版本的动作包含：

该移动计算设备访问将要安装在该移动计算设备上的至少一个文件的一个未压缩版本的一个动作。

8、如权利要求 1 所述的一种方法，其特征在于其中的该移动计算设备访问定义了如何将至少一个文件安装到该移动计算设备上的计算机可执行安装指令的动作包含：

该移动计算设备访问按照由配置管理器解释的一个模式构造安装指令的一个动作。

9、如权利要求 1 所述的一种方法，其特征在于其中的该移动计算设备访问定义了如何将至少一个文件安装到该移动计算设备上的计算机可执行安装指令的动作包含：

该移动计算设备访问按照可扩展标记语言 XML 构造安装指令的一个动作。

10、如权利要求 1 所述的一种方法，其特征在于其中的该移动计算设备访问定义了如何将至少一个文件安装到该移动计算设备上的安装指令的动作包含：

该移动计算设备访问至少一个安装指令以提取一个文件的一个压缩版本的一个动作。

11、如权利要求 1 所述的一种方法，其特征在于其中的该移动计算设备访问定义了如何将至少一个文件安装到该移动计算设备上的安装指令的动作包含：

该移动计算设备访问至少一个安装指令以将一个文件从一个源目录位置

移动到一个目标目录位置的一个动作。

12、如权利要求 1 所述的一种方法，其特征在于其中的该移动计算设备访问定义了如何将至少一个文件安装到该移动计算设备上的安装指令的动作包含：

该移动计算设备访问至少一个安装指令以将一个文件从一个源目录位置复制到一个目标目录位置的一个动作。

13、如权利要求 1 所述的一种方法，其特征在于其中的该移动计算设备访问定义了如何将至少一个文件安装到该移动计算设备上的安装指令的动作包含：

该移动计算设备访问至少一个安装指令以删除一个文件的一个动作。

14、如权利要求 1 所述的一种方法，其特征在于其中的该移动计算设备访问定义了如何将至少一个文件安装到该移动计算设备上的安装指令的动作包含：

该移动计算设备访问至少一个安装指令以改变一个配置设定的一个动作。

15、如权利要求 1 所述的一种方法，其特征在于其中的该配置管理器使这些安装指令得以执行的动作包含：

该配置管理器直接执行这些安装指令的一个动作。

16、如权利要求 1 所述的一种方法，其特征在于其中的该配置管理器使这些安装指令得以执行的动作包含：

该配置管理器让至少一个其它模块来执行这些安装指令的一个动作。

17、如权利要求 16 所述的一种方法，其特征在于其中的该配置管理器让至少一个其它模块来执行这些安装指令的动作包含：

该配置管理器将文件命令传递给一个文件配置服务供应器的一个动作。

18、如权利要求 16 所述的一种方法，其特征在于其中的该配置管理器让至少一个其它模块来执行这些安装指令的动作包含：

该配置管理器将配置命令传递给一个注册表配置服务供应器的一个动作。

19、如权利要求 1 所述的一种方法，其特征在于其中的该配置管理器将一个安装前状态包含在该回滚文档中的动作包含：

为每个改变一个文件的安装指令备份该文件原始版本的一个动作。

20、如权利要求 1 所述的一种方法，其特征在于其中的该配置管理器将一个安装前状态包含在该回滚文档中的动作包含：

为每个将一个配置设定从一个原始值改变为一个改变了值的安装指令备份该配置设定原始值的一个动作。

21、如权利要求 1 所述的方法，其特征在于，该配置管理器使一个回滚文档得以构造的一个动作包括：

接收一个供应文档；

根据所述供应文档，识别将需要被实例化以执行安装指令的相应的配置服务供应器；

从所述配置服务供应器识别可能在安装指令的执行期间被改变的文件和数据；以及

创建包含所识别的文件和数据的当前状态的回滚文档。

22、如权利要求 1 所述的方法，其特征在于，该移动计算设备判定这些安装指令是否会成功的动作至少部分地基于对角色掩码的使用。

23、如权利要求 1 所述的方法，其特征在于，仅当首先判定所述安装指令的执行将会成功时，配置管理器提交安装指令。

24、如权利要求 1 所述的方法，其特征在于，所述移动计算设备包括无线电话或 PDA。

25、在一个包含了一套计算机可执行指令来源和多台移动计算设备的网络环境中，使至少其中一台移动计算设备利用驻留在该移动计算设备上的配置管理器的安全特性来安装该套计算机可执行指令的一种方法，其特征在于该方法包含：

该移动计算设备访问将要安装在该移动计算设备上的至少一个文件的至少一个版本的一个动作；

该移动计算设备访问确定如何将该至少一个文件安装到该移动计算设备上的计算机可执行安装指令的一个动作，而这些安装指令直接由与该移动计算设备相关的一个配置管理器来解释；

该配置管理器使这些计算机可执行指令得以执行的一个动作；以及

对这些计算机可执行指令中的至少一个，该配置管理器判定这些计算机可

执行指令的执行是否已授权的一个动作。

26、如权利要求 25 所述的一种方法，其特征在于其中的该移动计算设备访问将要安装在该移动计算设备上的至少一个文件的至少一个版本的动作包含：

该移动计算设备访问将要安装在该移动计算设备上的至少一个文件的一个压缩版本的一个动作；以及

该移动计算设备解压将要安装在该移动计算设备上的至少一个文件的该压缩版本的一个动作。

27、如权利要求 25 所述的一种方法，其特征在于其中的该移动计算设备访问将要安装在该移动计算设备上的至少一个文件的至少一个版本的动作包含：

该移动计算设备访问将要安装在该移动计算设备上的至少一个文件的一个未压缩版本的一个动作。

28、如权利要求 25 所述的一种方法，其特征在于其中的该移动计算设备访问确定如何将该至少一个文件安装到该移动计算设备上的计算机可执行安装指令的动作包含：

该移动计算设备访问按照由配置管理器可解释的一个模式构造的安装指令的一个动作。

29、如权利要求 25 所述的一种方法，其特征在于其中的该移动计算设备访问确定如何将该至少一个文件安装到该移动计算设备上的计算机可执行安装指令的动作包含：

该移动计算设备访问按照可扩展标记语言 XML 规定构造的安装指令的一个动作。

30、如权利要求 25 所述的一种方法，其特征在于其中的该移动计算设备访问确定如何将该至少一个文件安装到该移动计算设备上的计算机可执行安装指令的动作包含：

该移动计算设备访问至少一个安装指令以提取析一个文件的一个压缩版本的一个动作。

31、如权利要求 25 所述的一种方法，其特征在于其中的该移动计算设备

访问确定如何将该至少一个文件安装到该移动计算设备上的计算机可执行安装指令的动作包含：

该移动计算设备访问至少一个安装指令以将一个文件从一个源目录位置移动到一个目标目录位置的一个动作。

32、如权利要求 25 所述的一种方法，其特征在于其中的该移动计算设备访问确定如何将该至少一个文件安装到该移动计算设备上的计算机可执行安装指令的动作包含：

该移动计算设备访问至少一个安装指令以将一个文件从一个源目录位置复制到一个目标目录位置的一个动作。

33、如权利要求 25 所述的一种方法，其特征在于其中的该移动计算设备访问确定如何将该至少一个文件安装到该移动计算设备上的计算机可执行安装指令的动作包含：

该移动计算设备访问至少一个安装指令以删除一个文件的一个动作。

34、如权利要求 25 所述的一种方法，其特征在于其中的该移动计算设备访问确定如何将该至少一个文件安装到该移动计算设备上的计算机可执行安装指令的动作包含：

该移动计算设备访问至少一个安装指令以改变一个配置设定的一个动作。

35、如权利要求 25 所述的一种方法，其特征在于其中的该配置管理器使这些安装指令得以执行的动作包含：

该配置管理器直接执行这些安装指令的一个动作。

36、如权利要求 25 所述的一种方法，其特征在于其中的该配置管理器使这些安装指令得以执行的动作包含：

该配置管理器让至少一个其它模块来执行这些安装指令的一个动作。

37、如权利要求 36 所述的一种方法，其特征在于其中的该配置管理器让至少一个其它模块来执行这些安装指令的动作包含：

该配置管理器将文件命令传递给一个文件配置服务供应器的一个动作。

38、如权利要求 36 所述的一种方法，其特征在于其中的该配置管理器让至少一个其它模块来执行这些安装指令的动作包含：

该配置管理器将配置命令传递给一个注册表配置服务供应器的一个动作。

39、如权利要求 25 所述的一种方法，其特征在于其中的该配置管理器判

定这些计算机可执行指令的执行是否已授权的动作包含：

该配置管理器访问与该套计算机可执行指令相应的一个角色掩码的一个动作；以及

使用该角色掩码来判定这些计算机可执行指令的执行是否已授权的一个动作。

40、如权利要求 25 所述的一种方法，其特征在于其中的该配置管理器判定这些计算机可执行指令的执行是否已授权的动作包含：

该配置管理器判定这些计算机可执行指令中的至少一个未授权的一个动作。

41、如权利要求 40 所述的一种方法，其特征在于进一步包含：

在该配置管理器判定这些计算机可执行指令中的至少一个未授权的动作后，停止或放弃该配置管理器使这些安装指令得以执行的动作的一个动作。

42、一种系统，用于实现权利要求 25 所述的方法，所述系统包含了一套计算机可执行指令来源和多台移动计算设备，该系统用于在一台移动计算设备上利用驻留在该移动计算设备上的配置管理器的安全特性来安装该套计算机可执行指令，该系统包含：

配置来将该套计算机可执行指令解析成将要安装的一个或多个文件和安装指令的一个安装模块；

配置来从该安装模块接收安装指令的一个配置管理器；

配置来从该配置管理器接收表示文件或目录操作的任何安装指令，并配置来执行所接收到的安装指令的一个文件配置服务供应器；以及

配置来从该配置管理器接收表示配置设定操作的任何安装指令，并配置来执行所接收到的安装指令的一个注册表配置服务供应器。

利用配置管理器的回滚与安全特性在移动计算设备上安装软件

(1) 技术领域

本发明涉及软件安装技术领域，特别是涉及使用一种配置管理器的回滚与安全特性在移动计算设备上安装软件的方法、系统、计算机程序产品和数据结构。

(2) 背景技术

计算机变革了我们的生活方式。一台通用的计算设备的功能部件可以分为两个总类，即，硬件和软件。举例而言，硬件包括一个或多个处理器、多种的存储器（如 RAM、ROM、FLASH、硬盘驱动器、CD-ROM 等）、用户接口（如显示器、键盘、鼠标、扬声器、打印机、扫描仪等）和联网设备（如调制解调器、网络接口卡、天线等）。软件则包含在由处理器执行时控制硬件的多种操作，使硬件能以某种方式交互作用，完成某些任务。典型的计算设备包含多种软件，能实现大量的功能。

为了进一步改善计算设备的操作能力，经常希望能在计算设备上添加额外的软件。为安装这样的软件，计算设备要访问某个安装文件。安装文件一般包含存储在计算设备上某个合适目录处的许多最终需要解开的压缩文件。安装文件还包括为了以恰当地安装这些解压文件需循序的一系列指令。举例来说，这样的指令可以引导计算设备解压文件、移动文件、复制文件、删除文件或设定配置信息。

一个典型的安装过程本质上是由计算设备的用户启动的。举例来说，用户可以购买在计算机可读取媒介如硬盘、CDROM 等上的软件，或可以通过网络下载软件。可是，在移动计算设备上要采用某种相对新的安装形式。特别是，移动计算设备能接收到新软件可用的通知，然后一般会给用户一个接受该新软件的选项。如果接受，就可以潜在地将该软件下载到要安装的移动计算设备上。

用于常规通用计算机的操作系统一般提供某些安全层次，以确保能适当地将进程和个人所可能执行的操作类型限制在特定的文件上或特定的目录中。但是，由于移动计算设备与膝上或桌面计算机相比相对有限的存储和处理能力，用于移动设备的操作系统可能只具有削弱了的功能。

由于如此的处理和存储限制，这样的操作系统经常可能在安全控制的种类上受限。况且，当响应某个对移动计算设备的异步通知而下载某个安装软件时，软件提供者的可信度就更成问题。因此，当在某个处理和存储能力受限的环境中安装软件时，就希望有能提供安全性的系统、方法、计算机程序产品和数据结构。

而且，安装过程可能由于这样那样的原因而失败。举例来说，计算系统可能会崩溃，或者安装软件可能会试图操作未授权该安装软件操作的文件、目录或配置设定。如果软件安装失败，操作系统可能会存储错误的预示软件安装成功的配置设定。而且，安装的部分文件可能会被存储在计算设备上，即使由于安装失败这些文件已经无用。此外，无用的文件占据大量的存储空间，这在如移动计算设备那样的有限存储器的环境内特别不利。因此，如果在某个移动计算环境中安装失败，就进一步希望有能倒转安装效果的系统、方法、计算机程序产品和数据结构。

(3)发明内容

描述了使移动计算设备能使用配置管理器安装软件，从而可以在安装过程中利用配置管理器的回滚与安全特性的系统、方法、计算机程序产品和数据结构。如果安装由于某种原因未成功或需要倒转，回滚特性能完全倒转安装的效果。关于操作中在哪个目录与文件上可以执行什么操作，安全特性能实现适当的访问控制。

在某实例中，已经利用配置管理器在设定配置信息的环境中实现了这些回滚与安全特性。通过不仅在配置设定环境而且在目录和文件操作环境中将这一功能应用于安装，就最大限度地减小了将回滚与安全功能应用于安装过程的存储和处理的负担。这在与膝上或桌面计算机相比一般只有相对有限的存储和处理能力的移动计算设备如蜂窝电话和个人数字助理（PDA）环境中特

别重要。

本发明可以在某个驻留了可用于安装软件，如某个新的应用或补丁的安装文件的网络环境中实现。该网络也包括了某种移动计算设备。举例来说，该网络环境可以包括一台服务器，通过一个蜂窝电话网向蜂窝电话下载安装文件，也可以包括一台桌面个人计算机，通过一个坞架(docking cradle)向PDA传送安装文件。

如本发明所述，作为安装的一部分，移动计算设备会访问将要安装在该移动计算设备上的一个或多个文件的至少一个版本。举例而言，这些文件可以是压缩形式的，以保证网络带宽的有效利用，或者也可以是未压缩的。

移动计算设备还访问定义了如何将文件安装到该移动计算设备上的计算机可执行指令。举例而言，这样的指令可以包括对复制、移动或删除文件的指示，以及对设定配置信息的指示。要安装的文件以及安装指令可以作为部分而包含在单个的安装文件中。

这些计算机可执行指令是可直接由一个与该移动计算设备相关的配置管理器来解释的。举例而言，这些计算机可执行指令可以按照某种特定模式，如以可扩展标记语言(XML)规范定义的语言的特定模式来构造。这种特定模式可以是一套规则，在其中，结构内值的意义可从该结构内值的上下文环境获得。

而后配置管理器使这些计算机可执行指令得以执行。举例而言，配置管理器可以直接执行这些指令，或者可能让另一组件(如配置服务供应器)来执行某些指令。举例来说，配置管理器可能会让一个文件配置服务供应器来执行文件操作指令，而让一个注册表服务供应器来执行配置操作指令。

在这些指令的执行中，配置管理器可以实现回滚与安全功能。如果由于某种原因安装失败或不再需要，回滚特性能使安装的效果倒转。

这样，如果安装失败，移动计算设备就能回到其原来的状态。不再有预示成功安装的不希望的配置设定的改变。因此，移动计算设备的处理就不会被错误的配置设定所妨碍。而且，也不再有着眼于成功安装而安装的无用的散乱文件。因此，移动计算设备的存储器就能被节省，而不必存储作为失败安装的结果的无用信息。在处理和存储能力相对有限的移动计算设备环境中，

这是特别有益的。

在执行安装指令时，通过检查判定每个安装指令的执行是否被授权，配置管理器还可以用来实现安全性。以这种方式，移动计算设备可以保护其自身，不让无聊或疏忽的新软件提供者执行对该移动计算设备总体上有有害的安装指令。

本发明另外的特性与益处将在后面的描述中阐明，其在描述中部分地将是明显的，或可以通过本发明的实践来获悉。本发明的特性与益处可以通过在所附权利要求中所特别指出的设备与组合的手段来认识与获得。本发明的这些与其它特性通过下面的描述和所附的权利要求将更充分地彰显，或可以如下文中所阐明的那样，通过本发明的实践来获悉。

(4)附图说明

为了描述可以获得本发明上述及其它益处和特性的方式，将通过参照在附图中例示的详细实施例来呈现对上面已简要描述的本发明更为详细的描述。请理解这些图只是描述了本发明的典型实施例，因此不可认为是对其范围的限制，而本发明可以通过使用附图以另外的特性与细节来加以描述和解释。这些附图包括：

图 1 例示了一个可以用于向移动计算设备递送安装文件的示例网络环境；

图 2 例示了一个可按照本发明原则在其上可安装新软件的移动计算设备的操作部件；

图 3 例示了一个可以用于在移动计算设备上安装新软件的各种部件的架构；

图 4 例示了一个使用配置管理器的回滚与安全特性在移动计算设备上安装新软件的方法的流程图；

图 5 例示了一个包括要安装的文件及一个引导安装的指令部分的安装文件的数据结构。

(5)具体实施方式

本发明提供了使用配置管理器安装软件，从而可以在安装过程中利用配

置管理器的回滚与安全特性的系统、方法、计算机程序产品和数据结构。如果安装由于某种原因未成功或需要倒转，回滚特性能完全倒转安装的效果。关于安装过程中在哪个目录与文件上可以执行什么操作，安全特性能实现适当的访问控制。

一台移动计算设备访问一个安装文件。该安装文件包含一个或多个要安装在该移动计算设备上的文件（此处也称作“要安装的文件”），以及用于安装这些文件的计算机可执行指令（此处也称作“安装指令”）。安装器将这些安装指令传递给配置管理器并解压要安装的文件。这些安装指令是某种可由配置管理器直接解释的格式。然后配置管理器通过例如解析这些安装指令并将指令传递给适当的配置服务供应器来使这些安装指令得以执行。

为了实现回滚特性，配置管理器构造一个回滚文档。如果安装最终成功，则将这次安装作为一次单独的事务而提交。相反，如果安装失败，则通过执行该回滚文档来倒转安装过程。在一个实施例中，将在持久性的存储器中维护关于事务的状态信息。这样，如果移动计算设备掉电，事务状态在供电恢复时仍可用于继续该事务。如此，该事务就可以挺过供电的中断。

通过检查判定每条安装指令的执行是否已授权，配置管理器还可以用来在执行安装指令时实现安全性。特别是，在接收到一个安装文件后，该安装文件就被根据与安装文件一起提供的信任状而赋予一个角色掩码。角色掩码被用来确定在移动计算设备上的什么文件与设定上可以进行什么安装操作。如果该安装指令表现为任何未经授权的操作，则配置管理器会确保不执行该安装，并使移动计算设备保持在其安装前的状态。通过这样做，移动计算设备就可以保护其自身，不让新软件提供者执行对该移动计算设备有害的安装操作。

如将在下面更详细讨论的那样，本发明的实施例可以包含一台包括了多种计算机硬件的专用或通用的计算设备。本发明范围内的实施例还包括用来在其上承载或存储计算机可执行指令或数据结构的计算机可读取媒介。这样的计算机可读取媒介可以是能由通用或专用计算机访问的任何可用媒介。举例而言，但非限制，这样的计算机可读取媒介可以包括物理存储媒介，如 RAM、ROM、EEPROM、CD-ROM 或其它光盘存储器、磁盘存储器或其它磁存储设

备，或可以用来承载或存储所期望的以计算机可执行指令或数据结构形式并可由通用或专用计算机访问的程序代码手段的任何其它媒介。

当通过一个网络或另一通信连接（可以是硬连线的、无线的或硬连线与无线组合的）将信息传送或提供给一台计算机时，该计算机可以恰当地将该连接看作一个计算机可读取媒介。上述的组合也包括在计算机可读取媒介的范围内。因此，任何这样的连接都可被恰当地称为计算机可读取媒介。计算机可执行指令则包括例如让通用计算机、专用计算机或专用处理设备执行某些功能或功能组的指令和数据。

尽管没有要求，仍将在由计算设备执行的计算机可执行指令，如程序模块的一般环境中描述本发明。一般而言，程序模块包括执行特定任务或实现特定抽象数据类型的例程序、程序、对象、组件、数据结构等。计算机可执行指令、相关数据结构和程序模块表示了用以执行此处披露的方法步骤的程序代码手段的示例。这些可执行指令或相关数据结构的特定序列则表现了用以实现在这些步骤中所描述功能的相应动作的示例。

相关领域的行家将会理解，本发明可以在具有多种计算机系统配置的网络计算环境中实现，这些计算机系统配置包括个人计算机、手持设备、多处理器系统、基于微处理器的或可编程的消费电子产品、网络 PC、小型计算机、大型计算机等。本发明也可以在分布式计算环境中实现，其中由本地的或通过一个通信网络而相联接（通过硬连线链路、无线链路或硬连线链路 & 无线链路的组合）远端处理设备来执行任务。在一个在分布式计算环境中，程序模块可以位于本地和远端者的记忆存储设备上。

图 1 例示了一个网络环境 100，在其中可以将一个安装文件递送给一台移动计算设备。网络环境 100 主要包括一台通过一个无线链路 103 与移动计算设备 102 通信的服务器 101。

服务器 101 可以是移动计算设备 102 的主要连接点，如公共无线服务提供者（如某个蜂窝运载者）或某个专用无线通信网络（如某个公司通信网络）。服务器 101 也还可以是一台与主要连接点合作的专用服务器。

移动计算设备 102 在下面参考图 2 和 3 来进一步详细例示与描述。简要地说，移动计算设备 102 是一台包括了移动电话功能及典型个人数字助理

（PDA）功能的手持计算设备。

服务器 101 和移动计算设备 102 通过一个无线链路 103 互相通信，无线链路 103 可以是任何无线通信的装置，如无线电频率链路等。举例而言，服务器 101 可以检测到可用于安装到移动计算设备 102 上的新软件（如新的应用、更新或补丁）。然后服务器 101 通过无线链路 103 向移动计算设备 102 发出一个安装通报 104，通知移动计算设备 102 有新的可用的软件。在图 1 中以第一个箭头来表示这一通报。这一通报可以通过一个无线网络，使用无线应用协议（WAP）推送通报、超文本传输协议（HTTP）推送通报或无论是当前存在还是将要开发的任何其它可能的通报方法来予以实现。

这样的通报方法有很多种。举例来说，用户可以使用移动计算设备 102 的一个浏览器来导引一个公司网络或互联网，找到某个下载站点。用户通过选择某个与安装文件相应的链接来同意安装。然后浏览器就提交一个对该安装文件的请求（如一个 HTTP GET 命令），而该安装文件就将会自动下载。

可作替换的是，移动计算设备 102 也可以插入一个经由通用串行总线（USB）或串行线缆与桌面计算机或膝上计算机连接的坞架。桌面计算机就可以使用同步软件（如 ActiveSync）来向移动计算设备下载安装文件。用户通过让安装文件下载到移动计算设备 102 来允许安装。

在另一个例子中，安装文件作为附件或链接被包含在发往移动计算设备 102 的电子邮件或文本短消息内。用户可以通过选择该附件或链接来允许安装。

运载者还可以将服务提示（SI）和服务加载（SL）消息通过推送代理网关（PPG）发送给移动计算设备 102。移动计算设备 102 可以配置成将这些专用的文本短消息服务（SMS）的消息放置到一个收件箱中。如果是一个 SI 消息，用户就通过选择该消息中的一个链接来允许安装。如果是一个 SL 消息，设备就自己试图下载安装文件。

安装文件可以存储在一块“多媒体卡”（MMC）存储卡上。如果该 MMC 卡包含一个“自动运行”文件，而“自动运行”在该移动计算设备上可以实现，MMC 甚至可以自动启动一个安装脚本。在这种情况下，用户通过插入 MMC 设备来允许安装。

如果移动计算设备 102 允许安装,就提交一个对与新软件相关的安装文件的请求。这可以是一个 HTTP GET 请求的形式,在图 1 中以第二个箭头表示。而后安装文件 105 就被下载到移动计算设备 102 上。举例来说,安装文件 105 可以在响应 HTTP GET 请求的同一会话中下载。安装文件 105 的下载在图 1 中以第三个箭头表示。而后移动计算设备 102 如下面与图 3 至 6 相关而进一步描述的那样,使用安装文件 105 来安装新软件。

尽管这里主要描述了通过无线链路 103 将安装文件 105 递送给移动计算设备 102 的环境,可以理解这只是下载安装文件 105 的一种实施例。上面描述了将安装文件 105 递送给移动计算设备 102 的几种方法,某些是面向网络的,某些不是。因此,图 1 中的第二个和第三个箭头可以表示任何形式的通信,用户在其中允许安装,而安装文件在移动计算设备 102 上执行。

图 2 进一步详细例示了移动计算设备 102。移动计算设备 102 包含了一个用户接口 201,用以让用户通过一个输入用户接口 203 输入信息,并经由一个输出用户接口 202 检查所显示的信息。举例来说,输出用户接口 202 包括一个用以向用户表现音频信息的扬声器 204,及一个用以向用户表现视频信息的显示器。移动计算设备 102 还有一根用以通过无线链路 103 与服务器 101 无线通信的天线 209。

输入用户接口 203 可以包括一个用以将音频信息呈现为电子形式的话筒 206。另外,输入用户接口 203 还包括以 12 个按键表示的拨号控件 207,用户通过它可以拨出电话号码、输入文本消息或指示移动计算设备 102 发送数据消息。输入用户接口 203 还包括导引控制按键 208,它帮助用户引导在显示器 205 上可能列出的多个条目与选项。

尽管移动计算设备 102 具有移动电话的外观,其看不见的特性可以实现复杂与灵活的通用处理能力。举例而言,移动计算设备还包括了一个处理器 211 和一个存储器 212,它们互相连接,并经由一个总线 210 与用户接口 201 相连。从历史上看,移动计算设备如蜂窝电话与 PDA 的处理和存储能力与膝上和桌面个人计算机相比是相对有限的。存储器 212 一般表现为可以使用的很多种易失和/或不易失的存储器。在移动计算设备 102 中使用的存储器的特定种类对本发明是不重要的。

由一个或多个程序模块组成的程序代码手段可以存储在存储器 212 中。多个程序模块之一可以包括一个操作系统 213、一个或多个应用程序 214、其它程序模块 215 和程序数据 216。在图 2 中例示的环境只是示例性的，并不代表本发明的原则可在其中得以实现的多种移动计算设备中的即使一小部分。

图 3 示意性地例示了一个可以由移动计算设备 102 实现的架构 300。详细来说，在图 2 中例示的组件包括了几个功能性的组件如调度程序 301、安装器 302、配置管理器 303、解析器 304、回滚起草器 305、反安装器 306、安全模块 307、文件配置服务供应器（CSP）308 和注册表 CSP309。这些功能组件可以是如移动计算设备 102 的应用程序 214、程序模块 215 或操作系统 213 各部分之一。回滚文档 310 可以是如移动计算设备 102 的程序数据 216 的一部分。

如果安装文件 105 的递送要通过网络，则调度程序 301 接收安装通报 104，并可选地从服务器 101 检索安装文件 105。然后调度程序 301 触发安装器 302 使用安装文件 105 安装新软件。而后图 3 的架构 300 就可以使用图 4 的方法来利用配置管理器的回滚与安全特性安装新软件。因此，图 3 架构的余下部分（实质上是除调度程序 310 外的所有组件）将频繁参照图 4 来予以描述。

参照图 4 的方法 400，移动计算设备 102 访问将要安装到该移动计算设备上作为新软件安装的一部分的一个或多个文件的至少一个版本（动作 401）。举例来说，为了确保网络带宽的有效利用，这些文件可以是压缩形式的，在这种情况下移动计算设备将访问这些文件的一个压缩版本。但是，一个安装文件也可以包含这些文件自身，不用任何压缩。

移动计算设备 102 还访问定义了如何将这些文件安装到该移动计算设备上的计算机可执行指令（动作 402）。举例来说，这些指令可以包括对复制、移动或删除文件的指示，以及对设定配置信息的指示。

所要安装的文件及安装指令可以包含为安装文件 105 的一部分。在这种情况下，访问所要安装的文件的动作（动作 401）和访问安装指令的动作（动作 404）可以由安装器 302 简单地访问一个单独的安装文件如安装文件 105 来实现。图 5 示意性地例示了安装文件 105 的一个数据结构 500。数据结构 500 包含了所要安装的多个文件，如文件 503a 至 503d。数据结构 500 还包含了用于指示如何在移动计算设备 102 上安装文件 503 的安装指令 501。

安装指令 501 直接由配置管理器 303 解释。举例而言，安装指令 501 可以按照某种特定的模式来构造。在图 5 中以由粗线突出标注的模式 502 的安装指令 501 来表示安装指令 501 遵循这一模式。在下面将进一步描述一个遵循某个使用可扩展标记语言（XML）规范的模式安装指令示例。在这一描述和权利要求中，“模式”被定义为一套规则，通过其可以组织某种数据结构，在该结构内数值的意义可从该结构内数值的上下文环境获得。

按常规途径，安装指令直接由一个专门化的安装器来执行。然而，按照本发明，安装器 302 只是辅助安装过程。详细来说，安装器 302 将所要安装的文件解压（假设它们是压缩形式的），然后将它们存储到存储器 212 中。安装器 302 还将安装指令 501 传递给配置管理器。在某些实施例中，配置管理器 302 可以直接执行安装指令。然而，在这里描述的实施例中，配置管理器 303 使用一个解析器 304 解析安装指令，并将适当的安装指令路由给其它适当的组件。举例来说，配置管理器 303 可以让一个文件配置服务供应器 308 来执行文件操作指令（如移动文件、复制文件或删除文件），而让一个注册表配置服务供应器 309 来执行配置操作指令。

以前，配置管理器 303 仅仅是利用一个配置服务供应器来负责改变或者说管理配置设定。可是，本发明的原则将监视全部安装操作的责任也分配给了配置管理器 303。这样，配置管理器提供给配置信息设定的任何功能就都被应用于文件操作。文件操作和配置设定指令都按照配置管理器 303 所遵循的某种模式来构造。这样，配置管理器 303 就可以在对配置管理器 303 的操作与编码作最小改动下，解析配置设定指令及文件操作指令两者。最低限度，配置管理器 303 只需要识别出文件操作指令，并将文件操作指令传递给某个能够实现文件操作的组件（如文件 CSP 308）。

以这种方式，配置管理器 303 在设定配置信息环境下的功能就可以被扩展到安装过程。举例而言，在动作 405 中执行安装指令的过程中，配置管理器可以实现回滚与安全功能。如果由于某种原因安装失败或不再被需要，回滚特性允许安装的效果被倒转。首先将描述安装过程的回滚特性，接着是对安装过程的安全特性的描述。

参照图 3，配置管理器 303 的回滚特性由该配置管理器 303 可直接或间接

访问的回滚起草器 305、回滚文档 310 和反安装器 306 来予以支持。在名为“用于连续提供移动服务的系统与方法”的一般拥有并且未决的美国专利申请（序列编号 09/895471，2001 年 6 月 29 日归档，在此完整附录以供参考）中，描述了有关配置管理器如何使用回滚特性来在事务基础上设定配置信息的细节。

尽管在上面附作参考的相应申请中已描述了详细的回滚操作，现在这里还是参照图 4 简要地描述一下回滚操作。图 4 例示了一个使用配置管理器 303 以某种事务方式来安装新软件的步骤（步骤 402）。该步骤包括了前已描述的相应的动作 404 和 405，以及相应的动作 406 和 407。

详细来说，配置管理器 303 使回滚文档 310 得以构造（动作 406）。作为安装的一部分，移动计算设备 102 可以接收一个可能是或包括安装文件 105 的供应文档。该供应文档包含了关于需要哪些配置服务供应器来完成安装的信息，因此就识别出哪些配置服务供应器需要实例化。配置管理器 303 根据这些信息实例化文件 CSP308 和注册表 CSP309（以及任何其它所需要的 CSP）。

然后配置管理器 303 识别出可能作为安装结果被改变的文件和/或其它数据项。举例而言，配置管理器 303 询问文件 CSP308 要作为安装的一部分而被改变的任何文件的当前状态，并询问注册表 CSP309 要作为安装的一部分而被改变的任何配置变化的当前状态。而后配置管理器 303 将这些当前状态编入回滚文档 310。这样，回滚文档 310 就表示了移动计算设备那些很有可能作为安装的结果而改变的数据项在安装前的状态。

然后配置管理器 303 判定安装是否已经或将要成功（动作 407）。举例而言，配置管理器 303 将相应的指令传递给相应的 CSP，并询问每个 CSP 这是否将得到成功安装。如果 CSP 中的任何一个提示安装将不成功，配置管理器 303 就判定该安装将不成功（在判定框 407 中为 NO）。例如，可能有某个 CSP 检测出一个或多个安装指令对于安装文件的识别并未授权执行。在某种实施例中，这使用赋予安装文件的角色掩码来完成。关于 CSP 如何使用角色掩码来实现安全性将在后面描述。如果在执行安装指令前就判定安装将不成功，就没有必要在动作 410 中执行回滚文档。取而代之的是，配置管理器 303 可以简单地拒绝执行该安装。

如果通过这一询问过程判定安装很有可能成功（在判定框 407 中为 YES），则配置管理器 303 提交该事务（动作 409）。详细来说，配置管理器 303 指示每个 CSP 实施它们相应的安装指令。如果由于某种原因，安装尽管有预备询问仍失败了，则配置管理器 303 判定安装为未成功（在判定框 407 中为 NO）。由于在这一判定的时刻安装指令已经被执行，所以配置管理器 303 要使用回滚文档 310 来将移动计算设备 102 恢复到其安装前的状态（动作 410）。这就以某种事务方式完成了安装新软件的步骤。

这样，如果安装失败，移动计算设备 102 就回到其原来的状态。不再有预示成功安装的不需要的配置设定的变化。因此，移动计算设备的处理就不会被错误的配置设定所妨碍。而且，也不再有着眼于成功安装而安装的无用的散乱文件。因此，移动计算设备 102 的存储器就能被节省，而不必存储作为失败安装的结果的无用信息。

在图 3 中所例示的架构 300 不仅支持在某种事务基础上安装新软件，而且利用配置管理器 303 所提供的安全特性来有条件地安装新软件。具体来说，安全模块 307 特别地支持这些安全特性，而安全模块 307 对于配置管理器 303 是直接或间接可访问的。在名为“用于经过空中的配置安全的系统与方法”的一般拥有并且未决的美国专利申请（序列编号 09/843901，2001 年 4 月 27 日归档，在此完整附录以供参考）中，描述了配置管理器如何在设定配置信息时提供安全性的细节。

参照图 4，例示了一个利用配置管理器 303 的安全特性来有条件地安装新软件的步骤（步骤 403）。该步骤包括了前已描述的相应的动作 404 和 405，以及相应的动作 408。详细来说，配置管理器 303 询问 CSP 它们是否能够执行它们相应的安装指令。作为响应，CSP 检查确定是否每个安装指令是否都已授权（动作 408）。CSP 可以利用赋予安装文件的某个角色掩码来完成这一任务。角色掩码可以随查询而传递给多个 CSP。

角色掩码按现在所描述的这样来赋予和使用。当初始创建一个安装文件时，该安装文件可以是有标记或无标记的。安装文件的标记可以通过使用软件如 Microsoft® Authenticode®来将一个证书包含到安装文件中而完成。然后移动计算设备 102 将该证书与某个相应的角色掩码相匹配。每个角色掩码都

可以对应于一个适当的证书。而后移动计算设备 102 将角色掩码赋予相应的安装文件。如果安装文件是无标记的，或具有一个与角色掩码不匹配的证书，则赋予一个缺省的角色掩码，该角色掩码对应于用于某个未鉴别的安装文件来源的适当的安全权限。在有些情况下，这可能意味着根本没有安全权限。

如果对于给定的角色掩码有任何安装指令没有授权，则配置管理器 303 可以如上面描述的那样制止安装。以这种方式，移动计算设备 102 可以保护其自身，不让无聊或疏忽的新软件提供者执行对该移动计算设备 102 总体上有害的安装操作。

现在描述一个基于 XML 的安装指令 501 的实例。下面的 XML 例示了一个如下的示例 XML 文档中的最高层嵌套标记：

```
1    <?xml version="1.0" encoding="UTF-8"?>
2    <wap-provisioningdoc>
3-47 [Content]
48    </wap-provisioningdoc>
```

在 XML 编码中每一行左边的数字表示了示例 XML 文档中的顺序行号。请注意在该 XML 文档中有 48 行。只有第 1、2 和 48 行表示了嵌套 XML 代码的最高层。因此，在上面只有第 1、2 和 48 行是明确地列出的。XML 代码的较低层次总的用术语 “[Content]” 来表示，在这里情况下它对应于该 XML 文档的第 3 至第 47 行。在说明为术语 “[Content]” 处，这表示在 XML 文档中相应行的确切内容将在下面进一步描述。

如那些 XML 文档编写领域的普通行家所周知，第 1 行表示了该 XML 文档的 XML 版本，以及该 XML 文档的文本编码格式。在这里，第 1 行表示 XML 版本是 1.0，文本以 UTF-8 文本编码格式来编码。

第 2 行和第 48 行分别是开始和结束标记，表示其间的材料（即标识为 “[Content]” 的第 3-47 行）是某种 wap 提供的文档。配置管理器 303 将 wap 提供的文档识别为某种包含了配置指令的文档类型。然而，在软件安装的情况下，wap 提供的文档也可以包含文件指令。

以下表现了在对应于该 XML 文档第 3 至第 7 行的 wap 提供的文档中的一个元素：

```
3    <characteristic type="Registry">
4        <characteristic type="maindir\subdir\config\app">
```

```

5          <para name="Filename" value="newgame"/>
6      </characteristic>
7  </characteristic>

```

归结起来，这个元素识别了发生在“注册表”上的一个操作（见第 3 行），因此指出该元素表示了一个配置操作。配置位置是在一个由“maindir\subdir\config\app”所定义的目录结构内（见第 4 行）。配置设定是“文件名”配置设定，它将接收到值“newgame”（见第 5 行）。请注意值“newgame”的意义可以通过其在该 XML 文档内的上下文来确定。

然而，该 XML 的 wap 提供文档不仅包含配置设定指令，而且还包含实际的文件操作指令。以下的 XML 文档定义了该 XML 文档的一个文件操作元素的代码范围：

```

8      <characteristic type="FileOperation">
9-46      [Content]
47  </characteristic>

```

第 8 行和第 47 行分别是开始和结束标记，表示从第 9 行至第 46 行的内容表现文件操作。以下的 XML 代码表现了组成这内容一部分的一个元素：

```

9      <!--current directory is:\Program Files\My Test App\Temp>
10     <characteristic type="%CE1%\My Test App\Temp">
11         <!--create this directory-->
12         <characteristic type="MakeDir">
13             </characteristic>
14         <!--extract hopen.txt from CAB 00hopen.001-->
15         <characteristic type="hopen.txt">
16             <parm name="Source" value="00hopen001"/>
17             <parm name="NoOverwriteIfNewer"/>
18             <parm name="Shared"/>
19         </characteristic>
20         <!--extract AirSync.txt from CAB 00hopen.002-->
21         <characteristic type="AirSync.txt">
22             <parm name="Source" value="00hopen002"/>
23             <parm name="NoOverwrite"/>
24         </characteristic>
25     </characteristic>

```

第 9 行是不执行的注释代码。第 9 行表示文件操作将发生在目录“Program Files\My Test App\Temp”中。第 10 行是一个开始标记，对应于第 25 行的结束标记，表示从第 11 行至第 24 行的内容将应用于该目录。

如第 11 注释行所显示，第 12 和第 13 行分别是创建目录“Program Files\My Test App\Temp”的开始和结束标记。请注意文本“%CE1%”是文本“Program Files”的一个已编码形式。如第 14 注释行所显示，第 15 至第 19 行从一个称作“CAB 00hpopen.001”的所要安装文件 503 的压缩版本中解出一个称作“hpopen.txt”的文件。如第 20 注释行所显示，第 21 至第 24 行从一个称作“CAB 00hpopen.002”的所要安装文件 503 的压缩版本中解出一个称作“AirSync.txt”的文件。这些所解出的每一个文件的目标是目录“Program Files\My Test App\Temp”。

以下的 XML 元素表示了一个文件复制操作：

```
26  <!--Copy email.bmp to Temp directory>
27  <characteristic type="\Temp\email.bmp">
28      <characteristic type="Copy"/>
29      <parm name="Source" value="My Test App\email.bmp"/>
30      <parm name="NoOverwriteIfNewer"/>
31      <!--If email.bmp is newer, do not overwrite.-->
32      </characteristic>
33  </characteristic>
```

这一元素将一个称作“email.bmp”的文件从临时目录“Program Files\My Test App\Temp”复制到目标目录“Program Files\My Test App”。

以下的 XML 元素表示了一个文件移动操作：

```
34  <!--Move existing file to target file:profile_move.bmp-->
35  <characteristic type="\Temp\profile_move.bmp">
36      <characteristic type="Move"/>
37      <parm name="Source" value="My Test App\profile.bmp"/>
38      </characteristic>
39  </characteristic>
```

这一元素将一个称作“profile_move.bmp”的文件从临时目录“Program Files\My Test App\Temp”以新的文件名“profile.bmp”移动到目标目录“Program Files\My Test App”。

以下的 XML 元素表示了一个文件删除操作：

```
40    <!--Delete target file-->
41    <characteristic type="\Temp\email.bmp">
42        <characteristic type="Delete"/>
43        <parm name="ForceDelete"/>
44    </characteristic>
45 </characteristic>
```

这一元素将一个称作“email.bmp”的文件从临时目录“Program Files\My Test App\Temp”中删除。

请注意安装是通过衡量移动计算设备的已有组件来完成的。配置管理器
303 只需要识别并解析出文件操作的元素，然后将指令传递给适当的配置服务供应器，无论是文件 CSP 308 还是注册表 CSP 309。因此，与只提供配置设定相比，安装新软件所要求增加的处理花费是最小的。因此，本发明的原则在安装过程中实现回滚与安全的同时，实现了在移动计算设备上新软件的有效安装。

本发明能以其它特定的形式来实施而不背离本发明的精神和本质特征。已描述的实施例从所有方面讲都只是示例性的和非限制性的。所以，本发明的范围是通过所附的权利要求来显示，而不是通过前面的描述。与这些权利要求等价的意义上或范围内的所有改变，都包含在其范围内。

通过美国专利特许所要求并期望被保护的是权利要求。

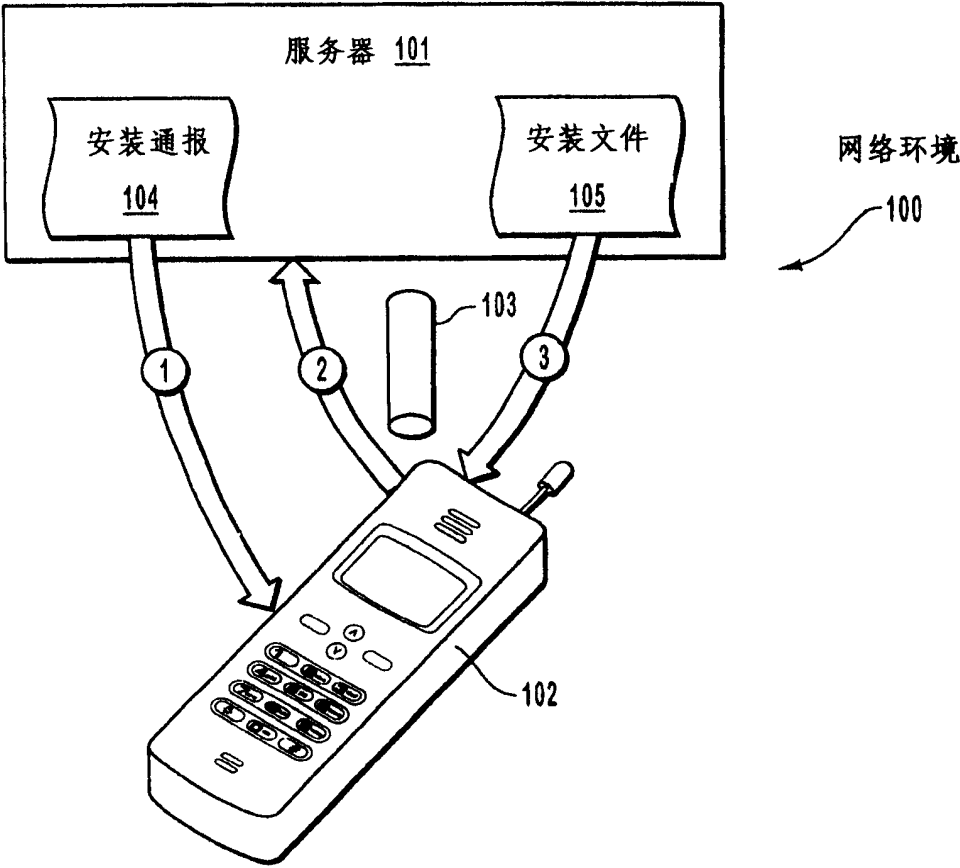


图 1

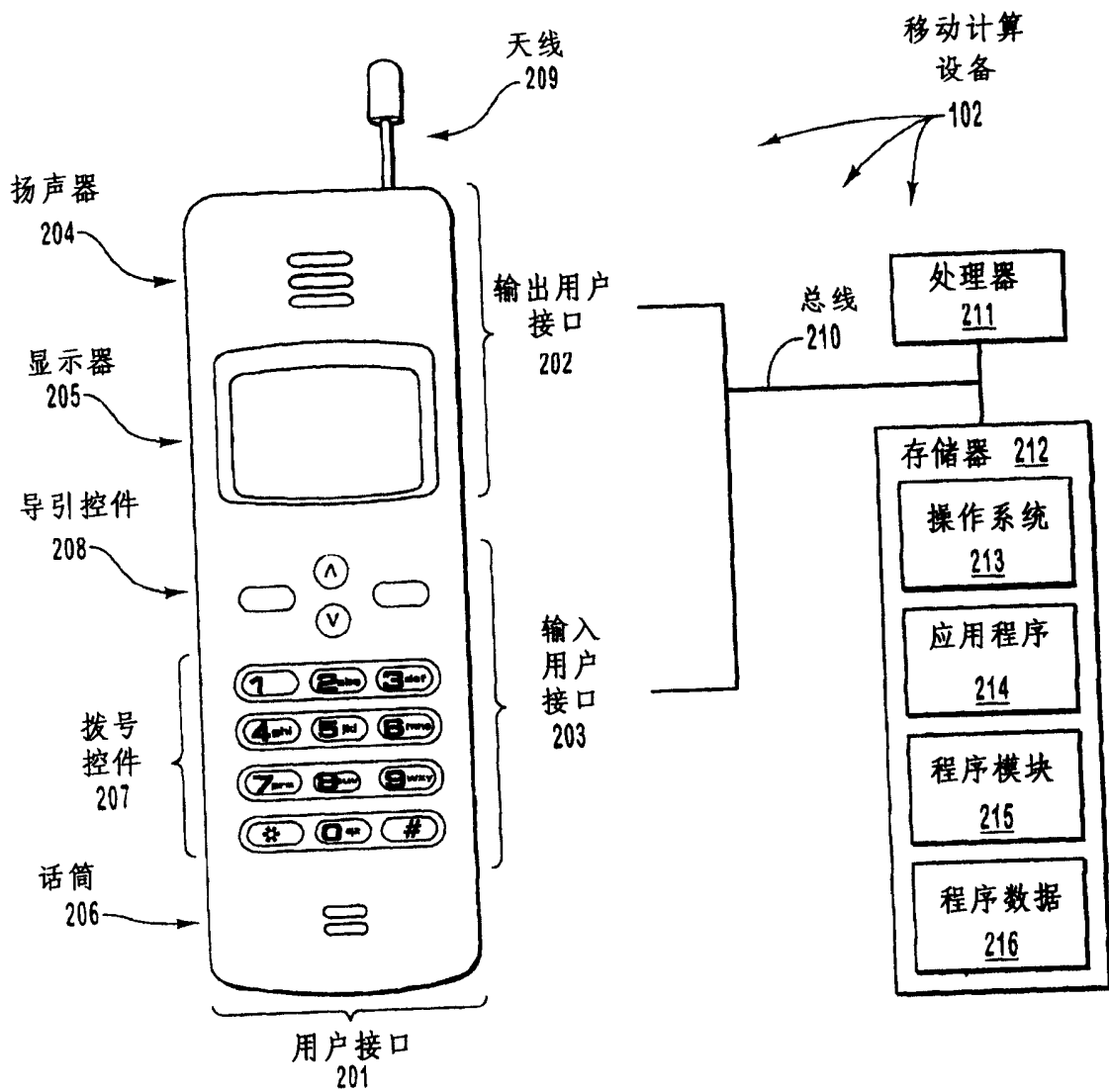


图 2

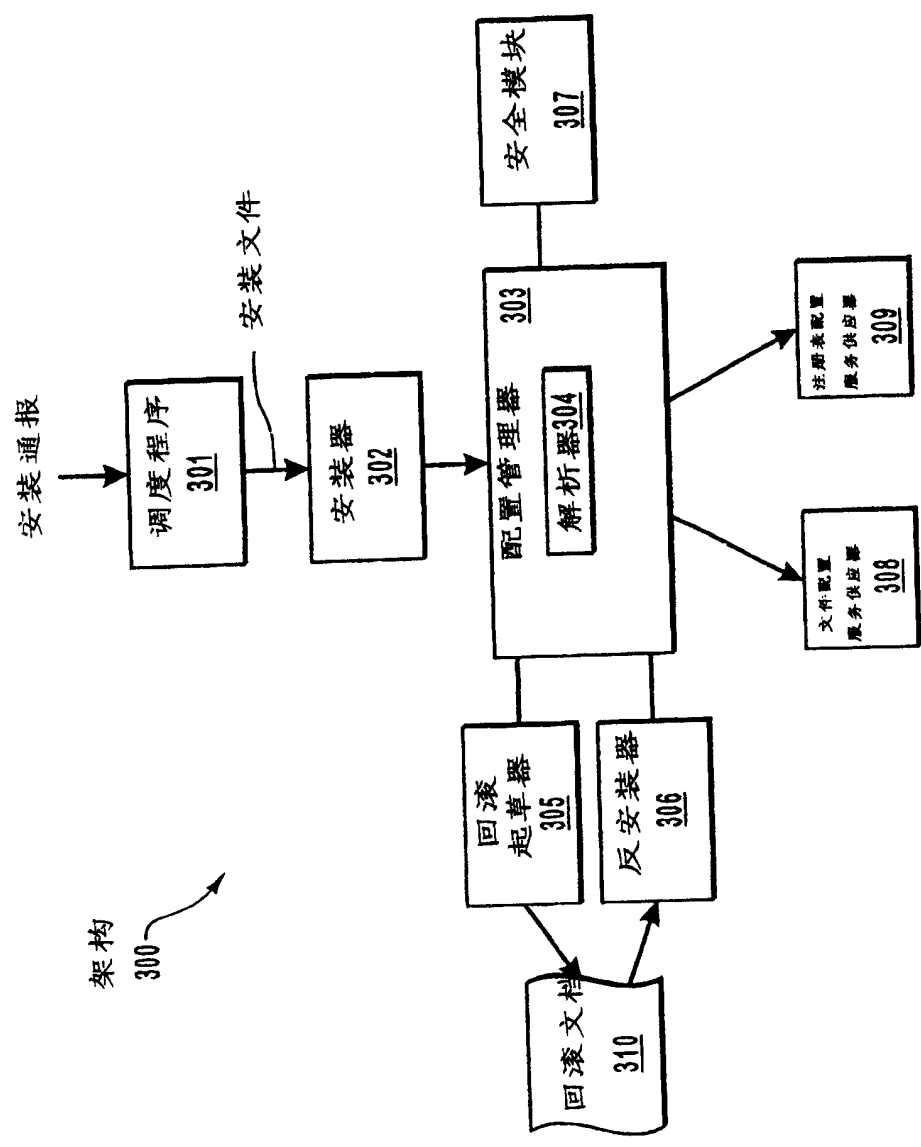


图 3

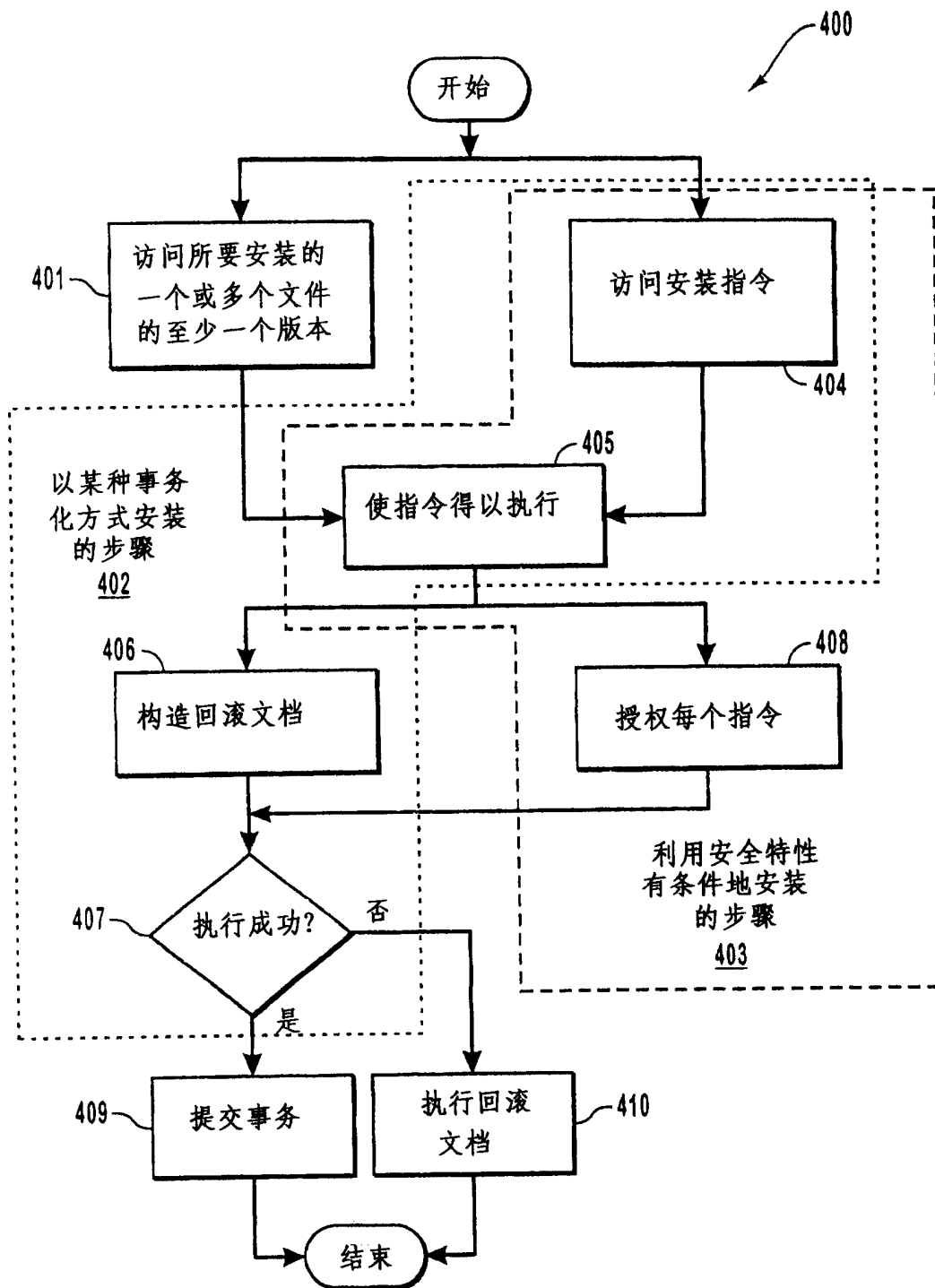


图 4

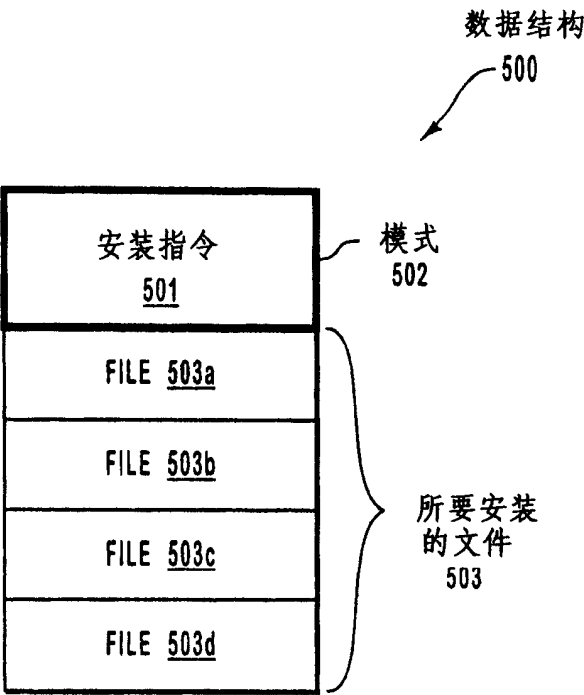


图 5