[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 9/445 (2006.01)
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 02814974.2

[45] 授权公告日 2006 年 5 月 31 日

[11] 授权公告号 CN 1258141C

[22] 申请日 2002.5.23 [21] 申请号 02814974.2
[30] 优先权
[32] 2001. 5.31 [33] US [31] 09/872,418
[86] 国际申请 PCT/US2002/016485 2002.5.23
[87] 国际公布 WO2002/097620 英 2002.12.5
[85] 进入国家阶段日期 2004.1.29
[71] 专利权人 高通股份有限公司
地址 美国加利福尼亚州
[72] 发明人 L·朗德布拉德 M·S·菲利普斯
B·米尼尔 Y·庄 A·克里施男
S·A·斯普里格 M·奇梅特里
M·奥利弗 G·豪雷尔
K·克罗斯兰德
审查员 谢志远

[74] 专利代理机构 上海专利商标事务所有限公司
代理人 李家麟

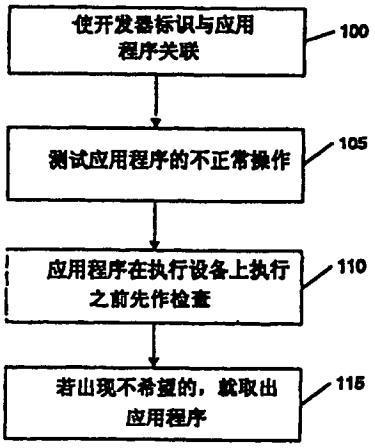
权利要求书 5 页 说明书 12 页 附图 7 页

[54] 发明名称

处理应用程序的方法和系统和执行应用程序无线装置

[57] 摘要

本发明提供了安全、保密的应用程序分配和执行，其途径是提供测试应用程序的系统和方法，以确保其满足与其所执行的环境相关的预定准则。另外，通过采用规则及准许表、应用程序去除和修正检测技术如数字签名特征，本发明还通过判断是否已经修改了应用程序、判断是否已被允许在给定的无线装置环境中执行以及去除该应用程序，提供了安全分配和执行测试的或未经测试的应用程序的机理。



1.一种分配与处理应用程序的方法，其特征在于，包括步骤：

接收应用程序和与应用程序关联的标识信息；

验证应用程序符合预定的指标；

对应用程序指定许可；

用修正检测技术向一设备发送应用程序、许可和标识信息；

判断应用程序在传输中是否被改过；

在设备上存贮一规则；

判断应用程序能否用许可与规则处理；和

从设备中取出应用程序。

2.如权利要求1所述的方法，其特征在于，还包括步骤：

在设备上启动应用程序的执行；

监视应用程序的执行；和

探测试图作不当操作的应用程序。

3.如权利要求1所述的方法，其特征在于，不许可在设备上处理应用程序。

4.如权利要求1所述的方法，其特征在于，设备检索标识信息。

5.如权利要求1所述的方法，其特征在于，还包括探测应用程序的修改的步骤。

6.如权利要求1所述的方法，其特征在于，还包括探测许可的修改的步骤。

7.如权利要求1所述的方法，其特征在于，修正检测技术应用一数字特征。

8.一种分配与处理应用程序的方法，其特征在于，包括步骤：

接收应用程序和与应用程序关联的标识信息；

验证应用程序符合预定的指标；

对应用程序指定许可；

向无线设备发送应用程序、许可和标识信息；

在设备上存贮规则；和

判断能否用许可与规则在设备上处理应用程序。

9.如权利要求8所述的方法，其特征在于，还包括步骤：

在无线设备上启动应用程序的执行；

监视应用程序的执行；

探测试图作不当操作的应用程序；和

从无线设备中取出应用程序。

10. 如权利要求 8 所述的方法，其特征在于，不许可在无线设备上处理应用程序，还包括从设备中取出应用程序的步骤。

11. 如权利要求 8 所述的方法，其特征在于，标识信息由无线设备确定。

12. 如权利要求 8 所述的方法，其特征在于，用修正检测技术发送应用程序、许可和标识信息。

13. 如权利要求 12 所述的方法，其特征在于，修正检测技术应用一数字特征。

14. 如权利要求 12 所述的方法，其特征在于，还包括步骤：

探测发送给设备的应用程序的修改；和

从设备中取出应用程序。

15. 如权利要求 12 所述的方法，其特征在于，还包括步骤：

探测发送给设备的许可的修改；和

从设备中取出应用程序。

16. 一种分配和处理应用程序的方法，其特征在于，包括步骤：

接收应用程序和与应用程序关联的标识信息；

对应用程序指定许可；

用修正检测技术向设备发送应用程序、许可和标识信息；

判断应用程序在传输中是否被改过；

在设备上存贮一规则；

判断能否用许可和规则处理应用程序；和

从设备中取出应用程序。

17. 如权利要求 16 所述的方法，其特征在于，还包括步骤：

在无线设备上启动应用程序的执行；

监视应用程序的执行；

探测试图作不当操作的应用程序；和

从无线设备中取出应用程序。

18. 如权利要求 16 所述的方法，其特征在于，不许可在无线设备上处理应用程序，还包括从设备中取出应用程序的步骤。

19. 如权利要求 16 所述的方法，其特征在于，标识信息由无线设备确定。

20. 如权利要求 16 所述的方法，其特征在于，用修正检测技术发送应用程序、许可和标识信息。

21. 如权利要求 20 所述的方法，其特征在于，修正检测技术应用数字特征。

22. 如权利要求 20 所述的方法，其特征在于，还包括步骤：

探测发送给设备的应用程序的修改；和

从设备中取出应用程序。

23. 如权利要求 20 所述的方法，其特征在于，还包括步骤：

探测发送给设备的许可的修改；和

从设备中取出应用程序。

24. 一种在无线设备上分配并执行应用程序的系统，其特征在于，包括：

接收应用程序和与应用程序关联的标识信息的装置；

验证应用程序符合预定的指标的装置；

对应用程序指定许可的装置；

向无线设备发送应用程序、许可和标识信息的装置；

在设备上存贮规则的装置；和

判断能否用许可与规则在设备上处理应用程序的装置。

25. 如权利要求 24 所述的系统，其特征在于，所述向无线设备发送应用程序、许可和标识信息的装置还能用修正检测技术向无线设备发送应用程序。

26. 如权利要求 24 所述的系统，其特征在于，所述向无线设备发送应用程序、许可和标识信息的装置还能用修正检测技术向无线设备发送许可。

27. 如权利要求 24 所述的系统，其特征在于，所述验证应用程序符合预定的指标的装置是中央服务器。

28. 如权利要求 24 所述的系统，其特征在于，还包括用存贮在无线设备中的规则评估指定的许可的装置。

29. 一种在无线设备上分配并执行应用程序的系统，其特征在于，包括：

接收应用程序和与应用程序关联的标识信息的装置；

对应用程序指定许可的装置；

用修正检测技术向设备发送应用程序、许可和标识信息的装置；

判断应用程序在传输中是否被改过的装置；

在设备上存贮规则的装置；

判断能否用许可和规则处理应用程序的装置；和

从设备中取出应用程序的装置。

30.一种处理应用程序分配的方法，其特征在于，包括步骤：

接收应用程序和与应用程序关联的标识信息；

验证应用程序符合预定的指标；

对应用程序指定许可；

用修正检测技术向设备发送应用程序、许可和标识信息；和

提出从设备中取出应用程序的请求。

31.如权利要求30所述的方法，其特征在于，还包括步骤：

评估收到的应用程序和标识信息，确定应用程序开发器的身份。

32.如权利要求30所述的方法，其特征在于，修正检测技术应用数字特征。

33.一种应用程序分配系统，其特征在于，包括：

接收应用程序和与应用程序关联的标识信息的装置；

验证应用程序符合预定的指标的装置；

对应用程序指定许可的装置；

用修正检测技术向设备发送应用程序、许可和标识信息的装置；和

提出从设备中取出应用程序的请求的装置。

34.一种在无线设备上执行应用程序的方法，其特征在于，包括步骤：

存贮一种评估许可的规则；

用修正检测技术接收含应用程序、许可和与应用程序关联的标识的信息；

接收在无线设备上执行应用程序的请求；

评估收到的信息，判断收到的信息是否被改过；

在收到的信息未被改过时，评估与应用程序关联的许可；和

在同意许可时，执行应用程序。

35.如权利要求34所述的方法，其特征在于，修正检测技术应用数字特征。

36.如权利要求34所述的方法，其特征在于，还包括步骤：监视应用程序的执行，判断是否试图作不当操作。

37.如权利要求34所述的方法，其特征在于，还包括从无线设备中取出应用程序的步骤。

38.一种在无线设备上执行应用程序的方法，其特征在于，包括步骤：

存贮一种评估许可的规则；

用修正检测技术接收包含应用程序、许可和与应用程序关联的标识的信

息；

接收在无线设备上执行应用程序的请求；

评估与应用程序关联的许可；和

在信息被改过时，从无线设备中取出应用程序。

39. 如权利要求 38 所述的方法，其特征在于，还包括步骤：

在收到的信息未被改过时，评估与应用程序关联的许可；和

在同意许可时，执行应用程序。

40. 如权利要求 38 所述的方法，其特征在于，修正检测技术应用数字特征。

41. 如权利要求 38 所述的方法，其特征在于，还包括步骤：监视应用程序的执行，判断是否试图作不当操作。

42. 如权利要求 38 所述的方法，其特征在于，还包括步骤：在试图作不当操作时，从无线设备中取出应用程序。

43. 一种执行应用程序的无线设备，其特征在于，包括：

存贮一种评估许可的规则的装置；

用修正检测技术接收包含应用程序、许可和与应用程序关联的标识的信息的装置；

接收在无线设备上执行应用程序的请求的装置；

评估与应用程序关联的许可的装置；和

在信息被改过时，从无线设备中取出应用程序的装置。

44. 一种执行应用程序的无线设备，其特征在于，包括：

存贮评估许可的规则的装置；

用修正检测技术接收含应用程序、许可和与应用程序关联的标识的信息的装置；

接收在无线设备上执行应用程序的请求的装置；

评估收到的信息以判断其是否被改过的装置；

在收到的信息未被改过时，用来评估与应用程序关联的许可的装置；和

在同意许可时执行应用程序的装置。

处理应用程序的方法和系统和执行应用程序无线装置

发明领域

本发明涉及处理用于无线装置的应用程序，尤其涉及提高在无线装置上执行应用程序的保密性、安全性与完整性。

背景

无线通信在近年经历了蓬勃发展。由于消费者与各种经营活动更依赖于其无线装置，诸如移动电话与电子记事簿(PDA)，故无线服务者即承运者尽力对这些无线装置提供附加的功能。这类附加功能不仅增大了对无线装置的需求量，也扩大了在当今用户中间的使用。然而，增加功能，尤其是增加能为无线装置访问的应用程序，既费钱又复杂，妨碍了承运者提供这种功能。

而且，一旦将应用程序装在无线装置上，不能保证正确地执行。目前，对应用程序在无线装置上执行的能力的依赖性寄托在开发器、无线装置制造商和/或承运者身上。随着开发出更多的应用程序和在无线装置上数量的增多，无线装置环境变得更富动态性，例如无线装置可在任何指定时间从大型现有应用程序库中检出大量不同的应用程序来执行，因而保证将对无线装置分配任一指定应用程序并安全地执行就变得更难以管理。

对此要特别加以关注，因为应用程序执行不当不仅会有害地影响无线装置，还有害于承运网络和其它网络元件，包括其它无线装置。例如，若对一条应用程序不加限制，它就会控制无线装置的功率控制并在其它无线装置之间引起干扰，降低该无线装置服务小区的整体能力。

在动态应用程序分配与执行环境中，目前无线装置制造商与承运者都未予以装备支持应用程序的测试与安全分配，因而担心在无线装置上分配与执行应用程序会损害该无线装置承运网络或其它网络元件。

另由于开发出更多的应用程序和向无线装置发送应用程序的环境变得更富动态性，出现了另一安全性问题。由于应用程序数量和正在创建这些应用程序的开发器数量增多了，也更希望知道任一指定应用程序的来源即开发器。承运或手机制造商以某种可靠性程度想知道他们能确定应用程序来源是否会造

成伤害应用程序。

因此，本领域要求有一种系统与方法能为在无线装置上分配和执行应用程序提供一种更安全的环境。

发明内容

符合本发明的诸系统和方法通过以下办法克服了现有系统的不足：对应用程序分配与执行创造一种按预定标准测试应用程序的更安全的环境，向开发器提供用于否定的可跟踪性，检查对应用程序无意识的修改，允许从无线装置中取出应用程序，以及/或者运用规则与许可来限定应用程序执行的环境。

应用程序符合预定标准的证明提供了提前捕捉执行期间可能出现的差错的优点，这有助于防止应用程序执行的有害影响。

可跟踪性提供了否定的优点。若应用程序有问题，则追寻该应用程序的来源即开发器有利于纠正该问题。此外，可跟踪性能阻止开发器创建有有害结果的应用程序，不论是有意还是无意。

而且，判断应用程序在无线装置接收前是否被修改的能力，通过保证该接收的应用程序是发送的同一应用程序，有利于提高安全性。由于在无线环境中更自由地分配应用程序，故判断应用程序是否被修改的能力提高了无线装置接收的应用程序未被偶然或有意修改的置信度。

设置一套规定应用程序可执行的时间的规则与许可，通过防止在未获准的平台上即未经核准的系统或环境执行应用程序，也提高了应用程序分配与执行系统的安全性。

从无线装置中取出应用程序的能力也提高了应用程序分配系统的安全性。若由制造商或通过应用程序下载把应用程序装在手机上，则拥有一种因不可预见的负面结果而取出该应用程序的机理，通过消除有害和不希望的有害代码，可提高应用程序分配与执行系统的安全性。

符合本发明的诸系统与方法可以引用一种或多种本文所揭示的技术。但通过引用本文揭示和参照的所有技术，符合本发明的诸系统与方法可对应用程序提供高质量和安全的分配与执行。

在本发明一实施例中，分配与处理应用程序的方法包括步骤：接收应用程序和标识信息，证明该应用程序满足一预定指标，对应用程序指定许可，运用修正检测技术向设备发送应用程序、许可与标识信息，判断应用程序在传输中

是否被修改，在设备上存贮某种规则，判断该应用程序是否用该许可与规则处理，以及从该设备中取出该应用程序。

在本发明另一实施例中，在无线装置上执行应用程序的方法包括步骤：存贮评估许可的规则，用修正检测技术接收包含应用程序、许可与标识的信息，接收在无线装置上执行应用程序的请求，评估收到的信息以判断其是否被修改过，在收到信息未被修改的情况下，评估与该应用程序关联的许可，而在同意许可的情况下，就执行该应用程序。

在本发明再一实施例中，在无线装置上执行应用程序的方法包括步骤：存贮评估许可的规则，用修正检测技术接收包含应用程序、许可与标识的信息，接收在无线装置上执行应用程序的请求，评估收到的信息以判断该信息是否被修改，在收到的信息未被修改的情况下，评估与该应用程序相关联的许可，而在同意许可的情况下，就执行应用程序。

附图说明

配入并构成本说明书一部分的诸附图，示出本发明目前较佳的诸实施例，与上述一般说明和以下对诸较佳实施例的详述一起说明本发明的原理。附图中：

图 1 是一流程图，示出本发明一示例性实施例中安全应用程序分配与执行的高层次处理；

图 2 是一框图，示出可实现本发明一示例性实施例的系统结构；

图 3 是本发明一示例性实施例的框图，示出可实现安全应用程序分配处理系统的无线网络结构；

图 4 是本发明一示例性实施例的框图，示出一无线装置和一些内部元件；

图 5 是本发明一示例性实施例的框图，示出用于建立数字特征并发送给无线装置的信息；

图 6 是本发明一示例性实施例的流程图，示出 1 只或多只伺服器在分配应用程序时使用的步骤；和

图 7 是本发明一示例性实施例的流程图，示出无线装置在执行应用程序时使用的步骤。

较佳实施例的详细描述

现参照图示的本发明示例性较佳实施例，图中用同样的标号表示通篇附图中相应的部件。在参阅了以下结合附图的详述后，本领域技术人员将更清楚本发明的特征、目的和优点。

本发明通过提供测试应用程序的系统与方法以保证该应用程序满足与执行环境有关的预定指标，提供安全而可靠的应用程序分配与执行。而且，通过应用规则与许可清单、应用程序取出和修正检测技术，诸如数字特征，本发明提供安全地分配与执行一经测试或未经测试应用程序的机理，其方法是判断该应用程序是否被修改这，判断该应用程序是否许可在指定的无线装置环境中执行，并在需要时取出该应用程序。

本领域的技术人员将明白，为便于描述，前面描述了一种可分配与执行的应用程序文件类型。“应用程序”还可包括具有诸如下列可执行内容的文件：目标代码、字符数字(script)、java 文件、书签文件(或 PQA 文件)、WML 正本、字节码与 perl 正本。此外，这里的“应用程序”还可包括实质上不可执行的文件，如要求公开的文件或其它要求被访问的数据文件。

图 1 是一流程图，示出以一种符合本发明一示例性实施例的方式对安全应用程序分配与执行作高层次的处理。本发明一实施例能使开发器标识与应用程序相关联，对准备执行应用程序的环境作应用程序测试，指定可决定执行应用程序的设备或系统的许可，并在应用程序执行非法或不希望的动作时取出应用程序。

最好是，诸系统和方法应用所有这些技术来提高应用程序的安全分配与执行，但应明白，即使应用一种或多种这类技术也能提高应用程序的安全分配与执行。

高层次处理通过使开发器标识与应用程序关联而开始(步骤 100)。当它被分配时，该处理通过将开发器标识与分配的应用程序捆绑在一起而实现，或者在系统的服务器上把关联的开发器标识与相应的应用程序一起存贮，而把开发器标识信息存贮起来并与应用程序信息相关联而使它不能被轻易修改，此方法也不错。

然后测试该应用程序的不正常操作(步骤 105)。应用程序可应用于这样一种环境，即不正常操作不仅会影响正在运行该应用程序的设备，而且还会影响与之连接或联网的其它设备。最好测试该应用程序，使它不让不正常系统在操作期间调用或负面地影响该设备或其它连接的设备。在一实施例中，由验证处

理作这一测试，其中测试该应用程序，判断它是否符合预定的指标。使用与开发器无关的验证处理来测试应用程序也较佳。验证处理的独立性促成了更加精确与可靠的测试。

应用程序在执行前，先作检验，判断是否“允许”它在设备上执行(步骤110)。检验可运用下述的许可与规则，或通过其它本领域技术人员已知的允许机理进行。再者，在每次执行应用程序前，先检验一下应用程序较佳。这种持久的检验过程提高了执行应用程序的安全性，例如可防止在执行设备上通过另一应用程序把具有特洛伊木马的应用程序插入该应用程序。

然后，从设备中取出作不正常或不希望操作的应用程序(步骤 115)，以防该应用程序造成进一步伤害并让设备里的存储器用作他用。或者，不要求从应用中取出该应用程序。取出应用程序可以指使该应用程序禁用但仍留在设备上。

图 2 示出可实现本发明一实施例的系统结构。开发器 200 建立一供无线装置 230 应用的应用程序。如上所述，本领域技术人员将明白，虽然前面的说明包括应用程序文件类型，但也可使用其它文件类型。而且他们还明白，本发明可应用于其它无线或非无线的设备，并可应用无线网络、非无线网络或它们的组合形式。

通常，开发器 200 有一套开发规程供开发在无线装置 230 上执行的应用程序。在一实施例中，无线装置包括一帮助应用程序与其接口的软件平台，如 QUALCOMM 公司(总部在 San Deigo, California)开发的 BREW™ 软件。开发器可以建立符合该软件平台或 BREW™ 软件、规范标准与协定的应用程序。

在一实施例中，把开发器 200 接中央服务器 205，使它以电子技术方式向中央服务器 205 发送该应用程序。在一实施例中，中央服务器是向无线装置分配应用程序的“应用程序管理中心总部(ACCHQ)”服务器。开发器 200 能以数字方式对应用程序加记号，以判断该应用程序是否修改过。应该明白，不必对中央服务器作物理连接，例如开发器 200 可通过头等邮件向贮存在 CD-ROM 上的中央服务器 205 发送应用程序。

此外，开发器还向中央服务器 205 发送各种源标识信息，包括任一类与应用程序关联的识别开发器的信息，诸如公司名称、公司纳税标识或其它识别信息。

在应用程序分析与验证中，或者使用单独的中央服务器 205，或者使用应

用验证服务器 210 的中央服务器。在一实施例中，把应用程序管理中心(ACC)用作验证服务器。验证服务器 210 分析应用程序，判断它是否满足预定的验证指标。该指标包括应用程序是否满足在无线装置或平台上执行的开发规程，不过可以是应用程序在无线装置或平台上执行之前必须满足的任一指标。这类指标包括验证：(a)开发器所申明的应用程序功能，使应用程序不伤害无线装置的操作(如不损坏电话)；(b)应用程序不访问不该访问的数据或存储器(如不访问其它应用程序拥有的数据或文件、操作系统或平台软件)；和(c)不负面地影响无线装置资源，如有害地独占无线装置的输入与输出。

中央服务器 205 还可以在与应用程序有关的清单中指定一组许可。该许可清单由各种因素决定，包括分析应用程序是否通过验证处理，批准应用程序在其上执行的网络 220，无线装置是否支持该应用程序。确定许可清单的因素很多，留待本领域技术人员在实施本发明时定夺。

中央服务器 205 接收开发器标识信息并将其与开发器 200 建立的应用程序相关。若应用程序有问题，该服务器能识别应用程序的来源。在一实施例中，将开发器信息传给无线装置 230，从而由该无线装置或与之连接的其它系统作相关。

在一实施例中，中央服务器还接至应用程序下载服务器(ADS)215，后者经无线网络 220 与无线装置接口而下载应用程序。中央服务器还向 ADS 发送许可清单和与应用程序有关的开发器标识并存贮在其中，直到传输给无线装置。较佳地，为提高修改的保密性，中央服务器以数字方式对应用程序、许可清单与开发器标记加记号。

本领域技术人员将明白，可将 ADS 接多个网络 220，以对各种无线装置 230 分配应用程序、文件和其它信息。而且，可用无线与非无线网向无线装置发送应用程序的许可清单和开发器标识。

根据对应用程序的请求，ADS215 经网络 220 向无线装置 230 发送应用程序、许可清单、开发器标识与数字特征。在一实施例中，为判断应用程序、许可清单和/或开发器信息是否被修改，无线装置 230 有一查验数字特征的电钥。

较佳的是，若在本发明中应用数字特征，则中央服务器用密钥建立该数字特征，并在无线装置上装一评估该数字特征的电钥。应用密钥，无线装置将具有更高的可靠性，即数字特征由中央服务器而不是起供者产生。

若应用程序在无线装置上出错或出于另一理由，无线装置可以取出应用程

序。而且，根据 ADS 或中央服务器的请求，可从无线装置中取出应用程序。服务器可根据任何理由发出这种请求，例如用该应用程序在另一设备上操作不正常、发布了该应用程序的新版本或者甚至经营上的原因强行取出应用程序，服务器可从无线装置中取出应用程序。这一应用程序取出处理可防止无线装置环境反复地执行不可靠和/或损坏的应用程序。

图 3 示出本发明一实施例中可实现应用程序分配系统的无线网络结构。中央服务器 302 是依靠自己或与验证服务器一起验证应用程序与一套规定的编程标准或协定是否兼容的机构。如前所述，可以建立这些编程标准，从而在软件平台如 BREW™ 平台上执行应用程序。

在一实施例中，中央服务器数据库 304 包括一种记录，它记录了在任一时间被下载到网络 300 中各无线装置 330 上的各应用程序的标识、各下载应用程序的“电子服务编号(ESN)”和携带该应用程序的无线装置 330 持有的“移动标识编号(MIN)”。或者，中央服务器数据库 304 对网络 300 中的每个无线装置 330 记录了无线装置型号、无线网络承运器、使用无线装置 330 的区域以及任何其它有用于识别哪一无线装置 330 正携带哪一应用程序的信息。此外，该数据库还可存贮这种与应用程序有关的开发器标识信息。

在一实施例中，中央服务器 302 还包括一取出命令源 322，该源 322 是人或者机构，可决定取出一条或多条目标的应用程序。源 322 也是构成取出命令 316(下面讨论)的机构，该取出命令播送给识别的携带目标应用程序的无线装置 330。或者在没有限止的情况下，取出命令源 322 可以是一个或多个人或机构，他们涉及开发和颁布目标应用程序、制造无线装置 330 的人或机构和/或网络 300 的任何部分功能的人或机构。

中央服务器 302 通过网络 308 诸如因特网与一个或多个计算机服务器 306 如 ADS 通信，最好是安全的。服务器 306 还通过网络 308 与承运网络 310 通信，而承运网络 310 靠因特网与简易普通电话系统(POTS)二者(图 3 中一起标为 311)与 MSC312 通信。承运网络 310 与 MSC312 之间的因特网连接 311 传递数据，POTS311 传递话音信息。再将 MSC312 接多个基站(BTS)314，并通过因特网 311(数据传递)与 POTS311(话音信息)二者接 BTS。BTS314 利用短消息服务(SMS)或任何其它空中传播方法向无线装置 330 无线发送消息。

本发明中一例 BTS314 发送的消息是取出命令 316。正如本文进一步讨论的，响应于收到的取出命令 316，不安装存贮在无线装置 330 上的目标应用程序。

在一实施例中，可附加或交替地对取出程序编程，以禁止目标应用程序或对它再编程以不同地执行。无线装置也可删除该应用程序和任何相关信息，如许可清单。

取出命令 316 由取出命令源 322 构成(可以是或可以不是决定取出目标应用程序的同样的人或机构)，取出命令源 322 通过网络 300 发送取出命令 316 而向无线装置 330 广播。

利用上例的取出命令，通过设置一种不安装不可靠或不希望的应用程序的机理，提高了应用程序分配与执行的安全性。本领域的技术人员将明白，虽然前面描述了由中央服务器启动的取出命令，但是无线装置也可取出或不装应用程序及其相关信息。

同样地，以上网络可通过 MSC 与 BTS 将来自中央服务器至各种服务器 306(如 ADS')的应用程序、许可清单和有关数字特征发送给无线装置 330。

图 4 示出本发明一实施例的无线装置和某些内部元件，虽然该例针对无线装置 400，但它仅是个例子而不是任何限制。或者，本发明可在能通过网络通信的任一形式的远地模块上实施，包括但不限制无线与非无线的设备，诸如电子记事簿(PDA)、无线调制解调器、PCMCIA 卡、访问终端、个人计算机、无显示或键板的设备或它们的任意组合或分组合。这些远地模块的例子也可具有用户接口，如键板、目视显示器或声响显示器。

图 4 的无线装置 400 在制造时装了一块专用集成电路(ASIC)415，该电路是一硬件元件，由包含在其内的软件驱动。无线装置 400 在制造时还装有应用程序编程接口(APT)410。在一实施例中，API 代表 BREW API 或软件平台。API410 是配置成与 ASIC 交互的软件程序，用作装在无线装置 400 上的 ASIC415 硬件与应用程序(下面讨论)之间的接口。或者，无线装置 400 含有任何其它形式的使程序以与无线装置 400 硬件配置兼容的方式操作的电路。无线装置 400 还具有存储器 405，包括 RAM 与 ROM，或是任存储器形式如 EPROM、EEPROM 或闪卡插件。

无线装置的存贮区 405 可存贮收到的应用程序与许可清单 425，还可存贮一个或多个“电钥”405，这些电钥可用特征算法应用于数字特征，判断加记号的信息是否被修改过。

规则 435 也装在无线装置 400 上，可与许可清单一起判断是否允许执行应用程序。例如，如在许可清单中设置了验证标志(即表示该应用程序已通过验

证)，规则就申明允许执行该应用程序。根据是否通过验证，许可清单将具有设置或不设置的验证标志。对包含在许可清单里的信息应用该规则，或同意或否定执行应用程序的许可。

制造商(未示出)可在制造无线装置 400 时把应用程序下载到其存储器 405 上，这些应用程序可以是任何可能对无线装置用户有用或感兴趣的程序，如游戏、书籍或其它类的数据或软件程序。无线装置制成后，也可通过空中将应用程序下载到无线装置 400 上。

在无线装置 400 执行取出程序时，不装来自贮存在无线装置 400 上的应用程序之一的一条或多条目标应用程序。目标应用程序是一种因下述各种原因而不要求无线装置 400 安装的应用程序。

无线装置 400 有一制造商安装的本地数据库 420。无线装置的 API 经编程，用记录的存贮在无线装置 400 上的各应用程序的标识信息自动地更新本地数据库 420，后者包含各存贮在无线装置 402 上的应用程序独特的特征标识记录。另外，本地数据库 420 包含诸应用程序在无线装置 400 上存储器 405 内位置的记录，以及任何其它有利于跟踪下载在无线装置 400 上的应用程序及其位置的信息。

图 5 是本发明一实施例的框图，示出用于建立数字特征并发送给无线装置的信息。本领域的技术人员知道，可用数字特征来跟踪数字文件是否已改过。正如描述的那样，数字特征可应用于任何数字文件，包括文件、应用程序、数据库等。通常数字特征通过运用特征算法对文件应用电钥而形成，这种数字特征用包含在文件里的信息构成。一般，数字特征与文件一起发送给收件者，然后收件者对收到的文件和数字特征用电钥判断该文件在传输给收件者时是否被改过。

建立和评估数字特征的电钥可判断加记器的身份，如某一机构可生成形成数字特征的电钥并秘密保持，而该机构可分配一相应的电钥用于评估该数字特征。若该电钥秘密保持而不泄露，则评估数字特征的收件者不仅能判断信息是否被改过，还能判断加记器身份。

或者，第三方以保密方式对特定机构形成电钥，这样拥有与某特定身份有关的电钥的收件者将能判断该机构是否是加记器。

在本发明一实施例中，通过把加记器的电钥 525 如中央服务器电钥(图 2)、应用程序 500、许可清单 505 和开发器身份信息 510 用作数字特征算法 530 的

输入，生成数字特征 515，它依赖于输入里包含的信息。

数字特征 515 形成后，把应用程序 500、许可清单 505、开发器身份信息 510 与数字特征 515 都发送给无线装置 520，然后该无线装置用数字特征判断该应用程序或有关信息(即许可清单与开发器身份信息)有无改过。此外，应用上述技术之一，如保密电钥，无线装置还可对向其发送该信息的加记器的身份产生置信度。

图 6 是一流程图，示出伺服器按本发明一实施例的方式分配应用程序所用的步骤。本例中，过程开始时接收应用程序与数字特征(步骤 600)，该特征是有关应用程序的信息，因而可判断应用程序在接收前是否被改过。再者，对数字特征加记号的电钥最好由第三方指定，以便确认对应用程序加记号的机构或开发器是接收该指定电钥的开发器。

接收了应用程序与数字特征后，对该数字特征作评估，判断发送应用程序的开发器是否为对应用程序加记号的同一开发器(步骤 605)。若第三方对开发器指定形成数字特征的电钥，则第三方也将评估数字特征的电钥分配给接收方，如参照图 2 描述的中央服务器。

然后把开发器或无论哪个加记号和/或形成应用程序的机构的标识存贮起来，并与该应用程序相关联(步骤 610)。存贮形式可以是表格、数据库或其它方式，在要求确定开发器身份时可加以检索。在一实施例中，把开发器标识存贮在无线装置中，不存入服务器。

接着验证收到的应用程序，判断是否符合规定的指标(步骤 615)。在一实施例中，把应用程序编制成在特定平台上执行，如 QUALCOMM 公司(总部在 San Diego California)开发的在无线装置中使用的 BREW™ 平台。特定平台或设备具有应用程序在其上执行前必须满足的特殊要求，例如平台或设备可能要求应用程序不得访问该设备中的特定存储位置，从而不损害该设备或存储器里其它应用程序的完整性。这些指标规定后，可对应用程序作测试，判断是否符合这些指标。最好这些指标预定后供给开发器以引入应用程序的开发。

验证后，对给定的环境指定与应用程序关联的许可(步骤 620)。许可根据多种因素指定，具体取决于实施本发明的环境。在一实施例中，应用程序用于无线装置。该例中，例如可根据承运网络、无线装置的要求、验证测试结果以及开发器、承运器或其它测试环境来指定许可。因此，许可清单说明该应用程序已通过验证测试，可在特定承运器网上执行。

然后，服务器对应用程序、许可清单和开发器标识加数字记号(步骤 625)。在一实施例中，用一密钥制作特征，让接收该加上数字记号的信息的一方确定服务器身份，不要求服务器接收的开发器特征也加记号，也不要求向无线装置发送开发器特征。

接着，向无线装置发送应用程序、许可清单、开发器标识和在步骤 625 形成的特征(步骤 630)。

图 7 是一流程图，示出无线装置按本发明一实施例的方式执行应用程序时使用的步骤。本例中，无线装置存贮了评估与应用程序关联的许可的规则(步骤 700)。本领域的技术人员将明白，虽然本发明描述了规则/许可的样式，但对特定设备或平台而言，有多种样式可用于对应用程序同意许可，且被视为在本发明范围之内。

于是，该无线装置接收应用程序、许可清单、开发器标识与数字特征(步骤 705)。在一实施例中，无线装置评估收到的数字特征，确定加记器身份。还可用该数字特征判断应用程序、许可清单或开发器标识在加上记号后是否被改过。

接着，无线装置接收执行应用程序的请求(步骤 710)。该请求可能来自想执行程序的无线装置的用户。或者，请求由无线装置自己提出，或来自通过网络或与无线装置直接连接的方法发送给该无线装置的某种请求。

收到请求后，在程序执行之前，无线装置先评估数字特征和与该应用程序关联的许可清单(步骤 720)。如上所述，在一实施例中，无线装置用规则评估许可清单。通过评估，若断定应用程序、许可清单或开发器标识未被改过，无线装置就用存贮的规则评估许可清单。若没有修改而且规则对许可清单的评估表明已同意该应用程序许可在无线装置上执行，则处理进到在该设备上执行该应用程序(步骤 730)。

若步骤 720 的评估表明应用程序、许可清单或开发器标识在加上记号后被改过了，或者不同意在无线装置上执行该应用程序，则不执行该应用程序(步骤 725)。过程进到从无线装置中取出该应用程序(步骤 750)。最好还从无线装置中取出许可清单和开发器标识。

在步骤 730 之后，监视应用程序的执行，判断它是否执行非法或不正常的操作(步骤 735)。无线装置或其应用的平台可以规定某些非法或不当的操作，包括那些访问受限制的存贮区或为其它程序或文件使用的存储位置的操作。此

外，这些操作还会涉及有害地利用无线装置的资源，这不仅会影响该无线装置，还会影响无线装置联网的其它设备。

若试图作这种非法或不当的操作，就停止应用程序的执行(步骤 745)，并从无线装置中将其与开发器标识和许可清单一起取出(步骤 750)。或者如上所述，取出处理可以涉及禁止应用程序启动，从而防止其执行，并把应用程序保持在无线装置上。

若在步骤 735 未执行非法、不当或不希望的操作，则允许继续执行该应用程序(步骤 740)。

结论

利用验证与检测修改、确定源身份、指定许可和引入取出应用程序能力的机理，符合本发明的诸系统与方法提高了安全与可靠的应用程序分配与执行。系统与方法可实施少量或全部这些机理，实施的机理越多，得到的安全度越高。

在一实施例中，开发器向服务器发送应用程序，开发器可对应用程序加记号以防未经批准的修改。服务器检查开发器身份，和对应用程序进行验证测试。服务器还对应用程序指定许可，形成许可清单。应用程序、许可清单和开发器标识被服务器加上数字记号后，与数字特征一起发送给无线装置。无线装置在执行应用程序之前，先对照存贮的规则查验数字特征的修改和许可清单。在一实施例中，每次试图在无线装置上执行应用程序之前，先作这些查验，若查验表明该应用程序已被改过或不许可执行，该应用程序就不执行并从无线装置中取出；若在执行期间该应用程序试图作非法或不当的操作，则该应用程序被终止并从无线装置中取出。

前述的本发明实施法仅作示例和说明，并不详尽，并不将本发明限于所揭示的拘谨的形式。根据以上进授内容或实践本发明的经验，可作出各种修正与变化，例如所述实施法包含软件，但本发明一实施例可用软硬件的组合或单独用硬件来实施。本发明可实施为以目标为对象与不以目标为对象的二种编程系统。另外，虽然把本发明诸方面描述成存贮在存储器中，但本领域的技术人员将明白，这些方法还可存贮在其它类型的计算机可读媒体上，诸如辅助存储设备，像硬盘、软盘或 CD-ROM 等；来自因特网或其它传播媒体的载波；或其它形式的 RAM 或 ROM。本发明的范围由权利要求及其等效文件来限定。

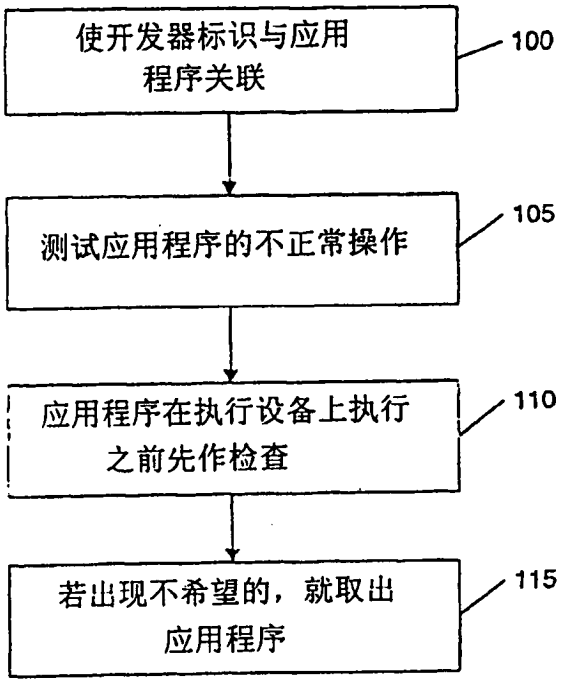

使开发器标识与应用程序关联
100
测试应用程序的不正常操作
105
应用程序在执行设备上执行之前先作检查
110
若出现不希望的，就取出应用程序
115

图 1

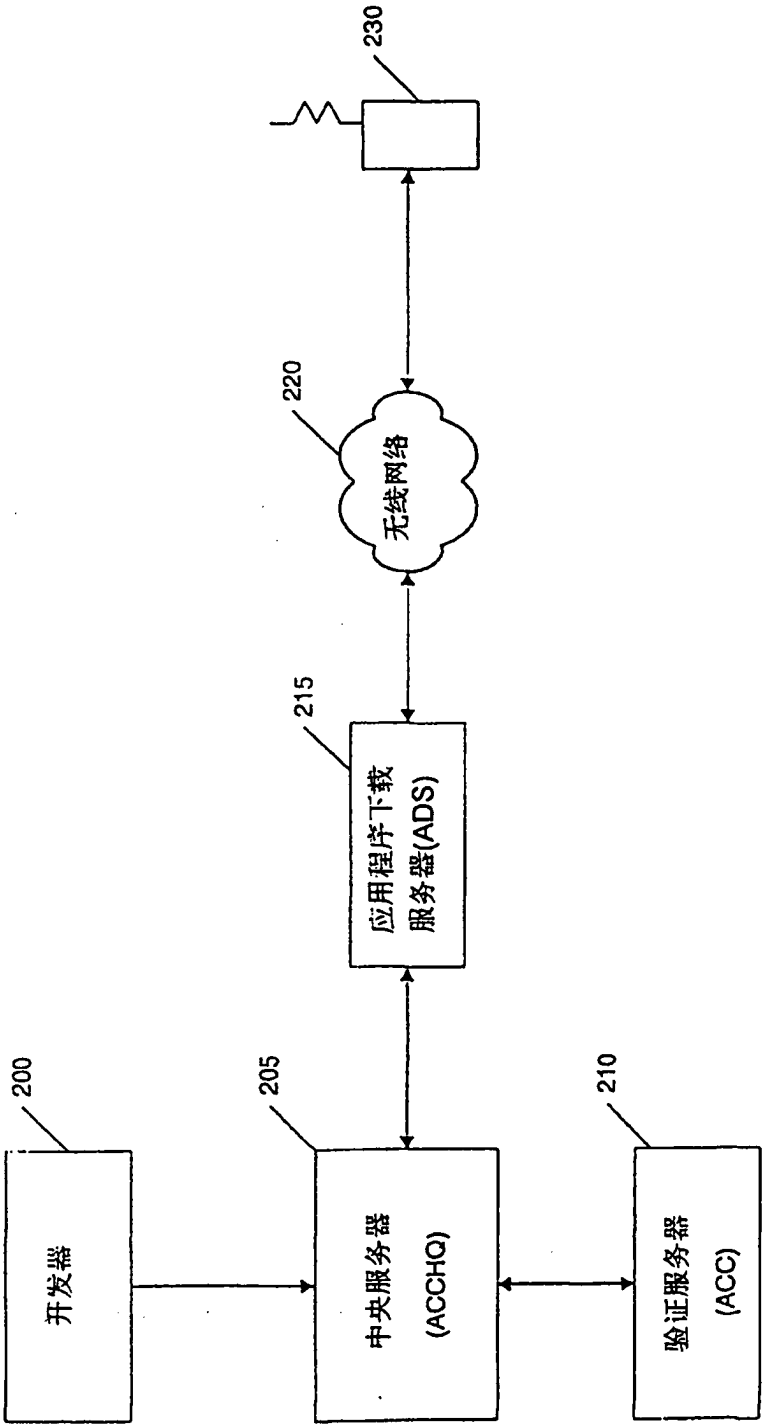

230
220
无线网络
215
应用程序下载
服务器(ADS)
200
205
210
开发端
中央服务器
(ACCHQ)
验证服务器
(ACC)

图 2

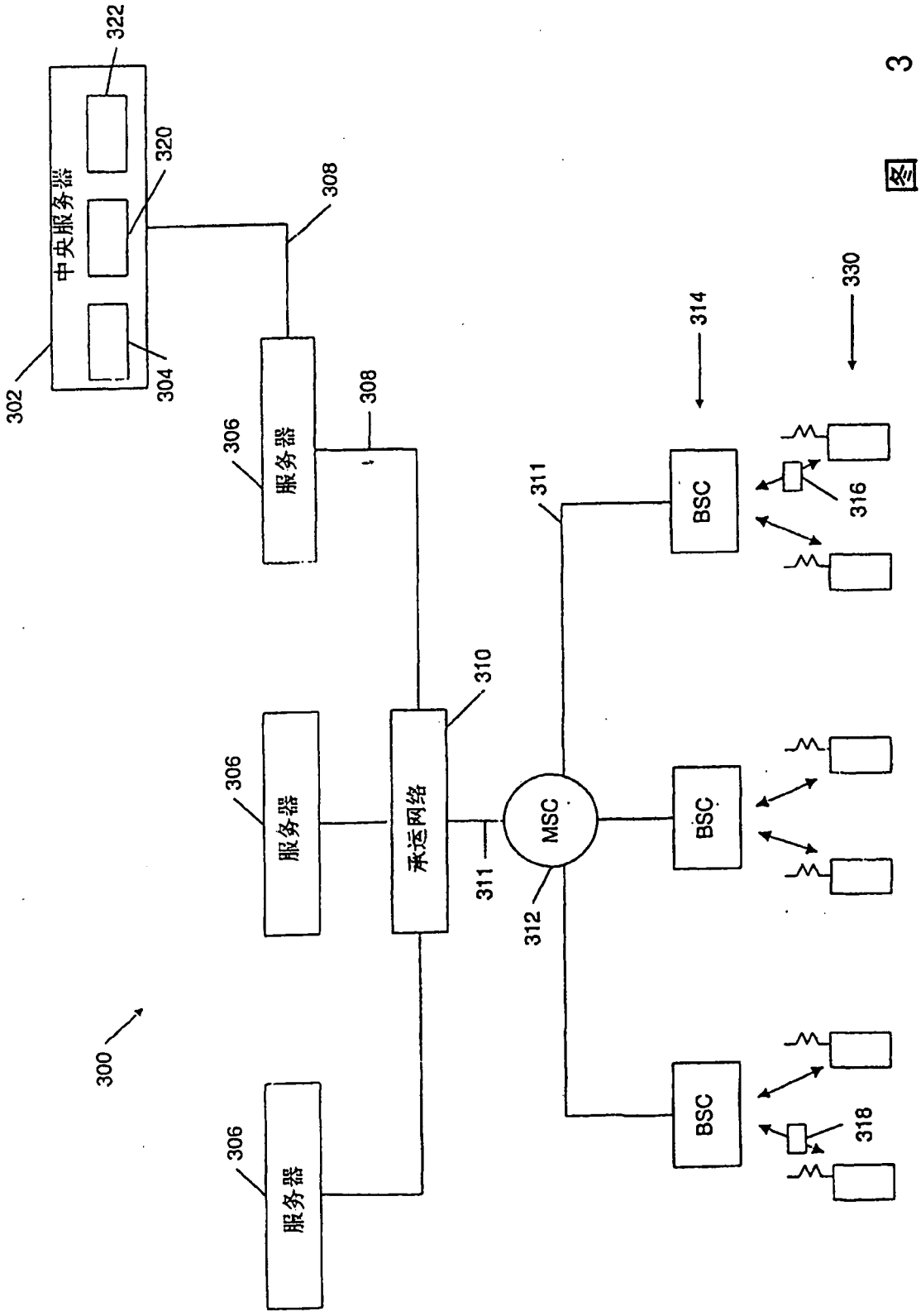

中央服务器
322
320
304
302
308
306
服务器
308
310
承运网络
311
MSC
312
BSC
BSC
BSC
314
316
318
330
300

图 3

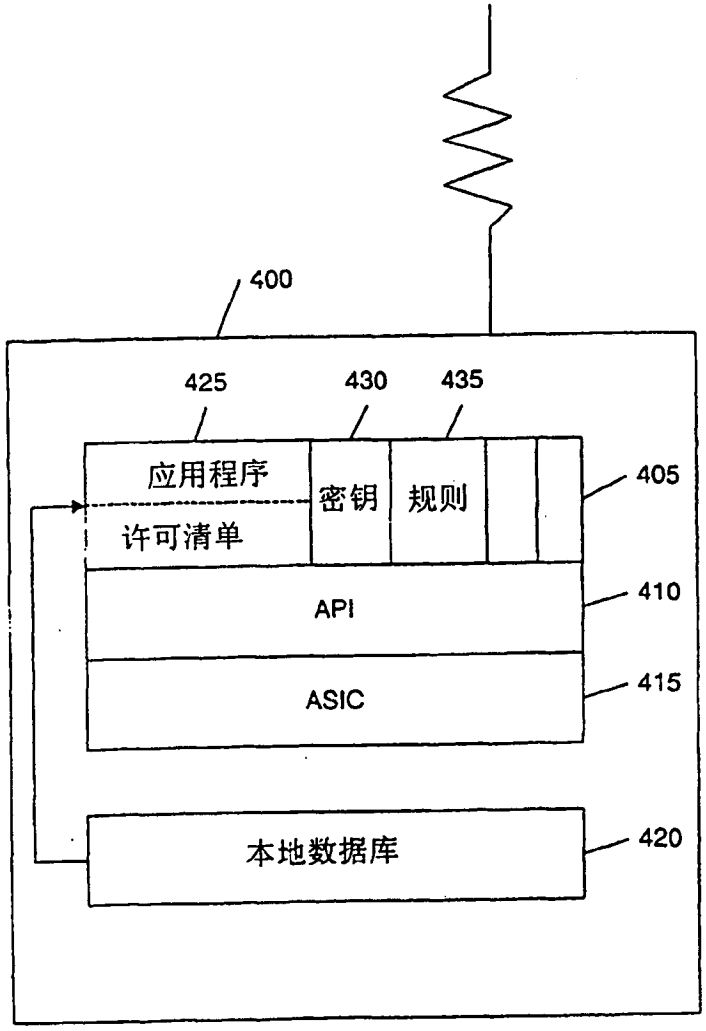


图 4

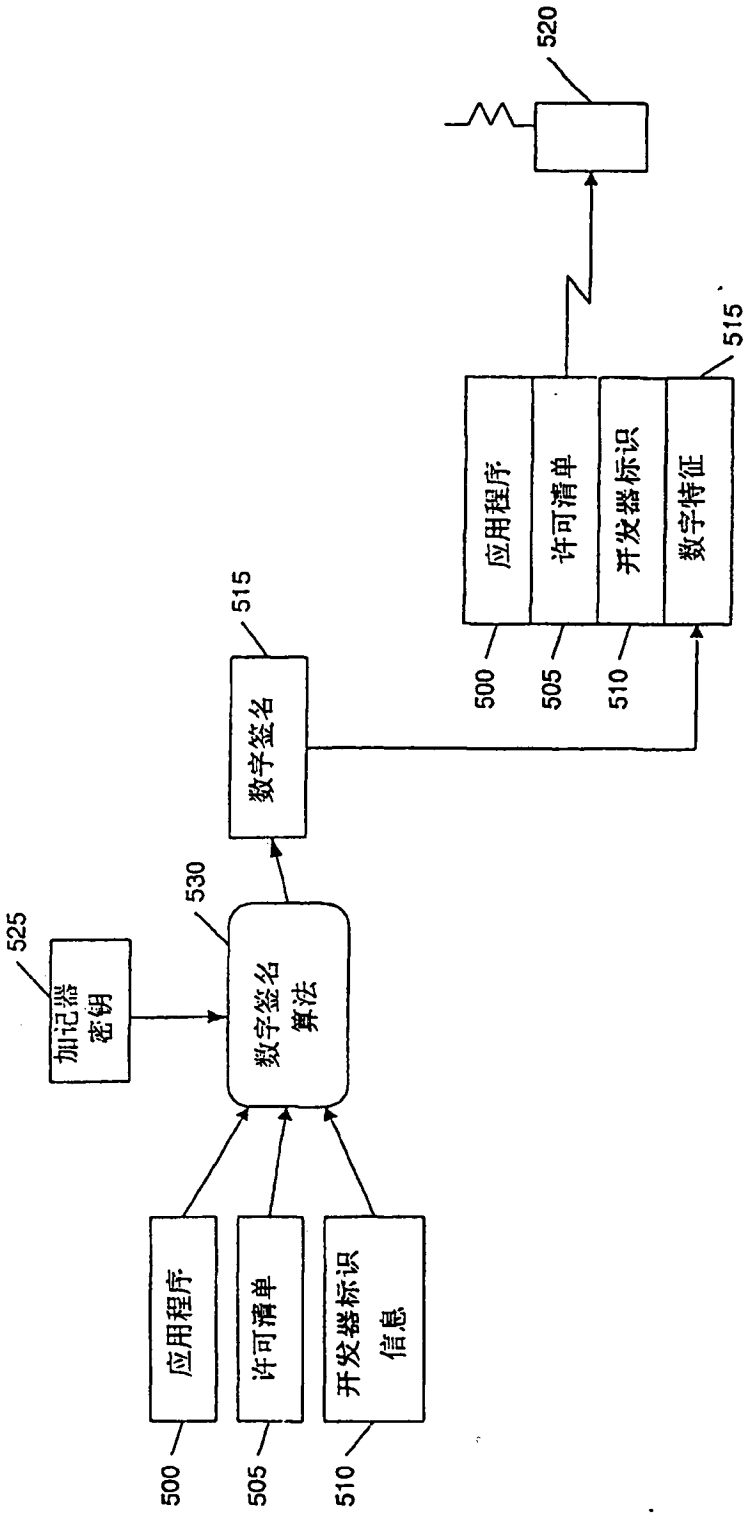

520
515
应用程序
许可清单
开发器标识
数字特征
500
505
510
数字签名
515
加记器密钥
525
530
数字签名算法
应用程序
许可清单
开发器标识信息
500
505
510

图 5

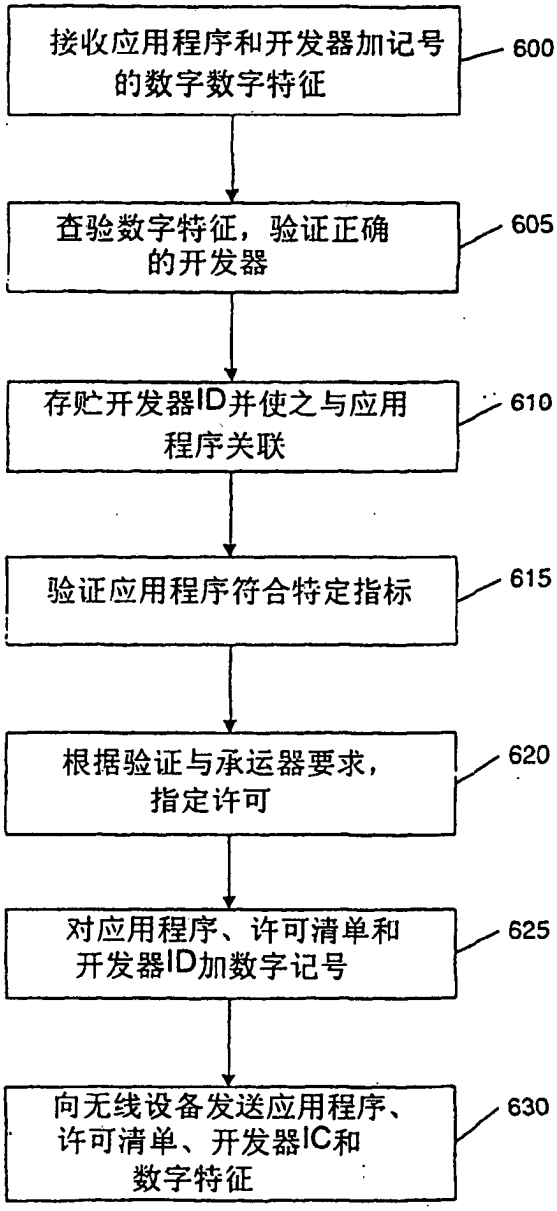

接收应用程序和开发器加记号的数字数字特征
600
查验数字特征，验证正确的开发器
605
存贮开发器ID并使之与应用程序关联
610
验证应用程序符合特定指标
615
根据验证与承运器要求，指定许可
620
对应用程序、许可清单和开发器ID加数字记号
625
向无线设备发送应用程序、许可清单、开发器IC和数字特征
630

图 6

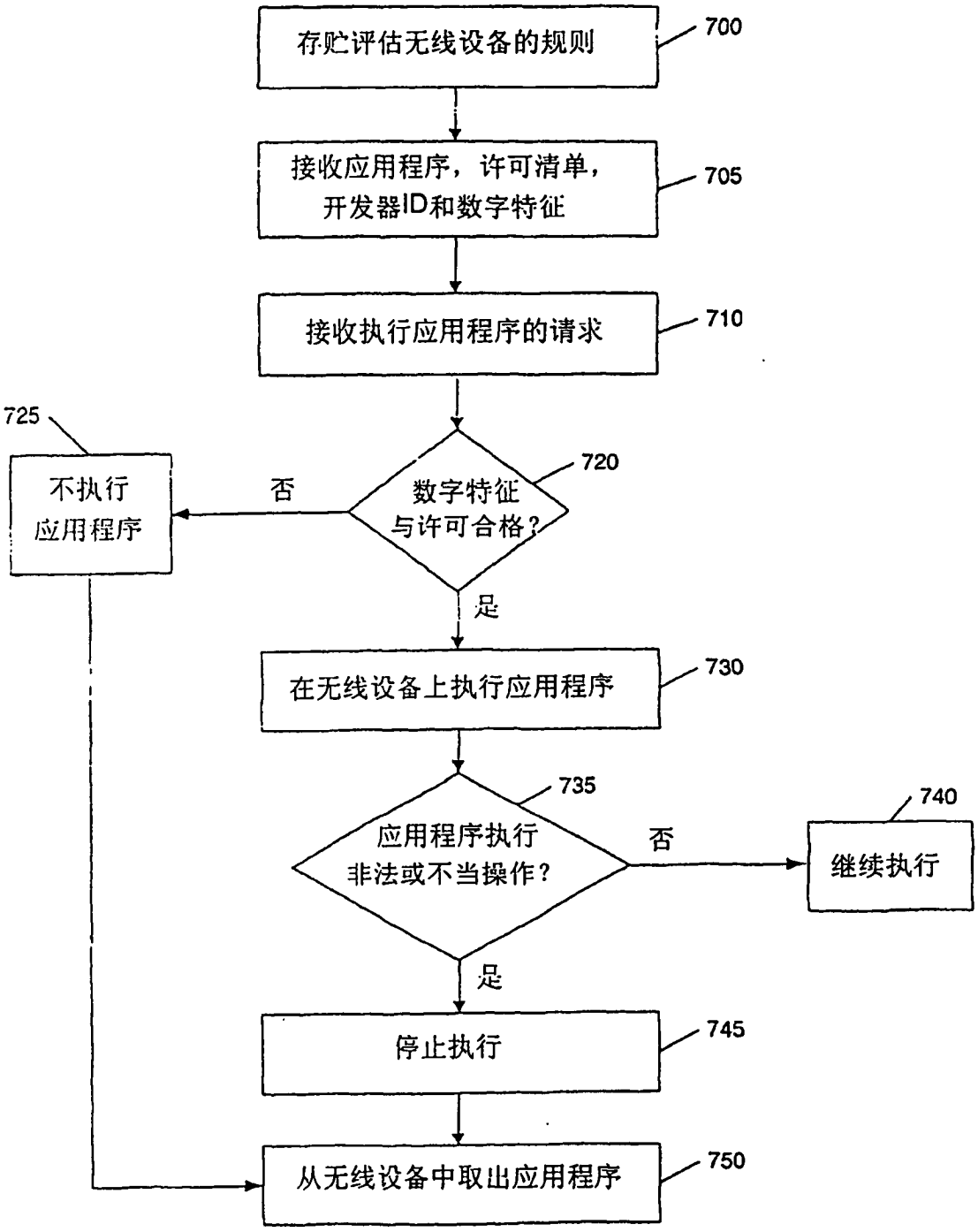

存贮评估无线设备的规则
700
接收应用程序，许可清单，
开发器ID和数字特征
705
接收执行应用程序的请求
710
725
不执行
应用程序
否
数字特征
与许可合格？
720
是
在无线设备上执行应用程序
730
735
应用程序执行
非法或不当操作？
否
740
继续执行
是
停止执行
745
从无线设备中取出应用程序
750

图 7