(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 105550595 A
(43)申请公布日 2016.05.04

(21)申请号 201510974308.0

(22)申请日 2015.12.22

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 奇智软件(北京)有限公司

(72)发明人 李常坤

(74)专利代理机构 北京商专永信知识产权代理事务所(普通合伙) 11400
代理人 方挺 黄谦

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/45(2013.01)

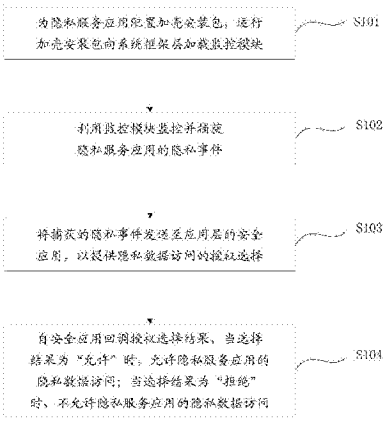
权利要求书2页 说明书11页 附图6页

(54)发明名称

用于智能通信设备的隐私数据访问方法及系统

(57)摘要

本发明提出了一种用于智能通信设备的隐私数据访问方法及系统。其中方法包括:为隐私服务应用配置加壳安装包,运行加壳安装包向系统框架层加载监控模块;利用监控模块监控并捕获隐私服务应用的隐私事件;将捕获的隐私事件发送至应用层的安全应用,以提供隐私数据访问的授权选择;自安全应用回调授权选择结果,当选择结果为"允许"时,允许隐私服务应用的隐私数据访问;当选择结果为"拒绝"时,不允许隐私服务应用的隐私数据访问。本发明通过在系统框架层加载监控模块,将对隐私权限管理的时间进行提前处理,在系统框架层对隐私事件进行监控,提升了权限管理的效率;对系统进行免ROOT处理,提高了系统的安全性和稳定性,改善了用户体验。



CN 105550595 A

1.一种用于智能通信设备的隐私数据访问方法，所述智能通信设备包括系统框架层和应用层，所述方法包括：

为隐私服务应用配置加壳安装包，运行所述加壳安装包向所述系统框架层加载监控模块；

利用所述监控模块监控并捕获所述隐私服务应用的隐私事件；

将捕获的隐私事件发送至所述应用层的安全应用，以提供隐私数据访问的授权选择；

自所述安全应用回调授权选择结果，当所述选择结果为“允许”时，允许所述隐私服务应用的隐私数据访问；当所述选择结果为“拒绝”时，不允许所述隐私服务应用的隐私数据访问。

2.根据权利要求1所述的方法，其中，为隐私服务应用配置加壳安装包，运行所述加壳安装包向所述系统框架层加载监控模块包括：

获取所述隐私服务应用的安装包的副本；

解析所述隐私服务应用的安装包的副本，以获取所述隐私服务应用的二进制可执行的代码文件；

修改或者替换所述代码文件，注入加载模块，以配置所述加壳应用安装包；

运行所述加壳应用安装包，启动所述加载模块，利用所述加载模块加载监控模块，挂钩隐私服务应用的隐私事件行为。

3.根据权利要求1或2所述的方法，其中，利用所述监控模块监控并捕获所述隐私服务应用的隐私事件为：

利用所述监控模块从后台沙箱的钩子插件框架中获取对应于所述隐私服务应用的隐私事件的钩子插件，利用所述钩子插件捕获相应的隐私事件。

4.根据权利要求3所述的方法，其中，通过将所述钩子插件配置在以下隐私数据访问接口中的至少一个接口中以利用所述钩子插件捕获相应的隐私事件：

拨打电话接口、发送短信接口、获取手机号接口、读取通话记录接口、读取地理位置接口、读取已安装应用列表接口、读取设备id接口、读取通信录接口、读取短信接口、写通话记录接口、写通信录接口、写短信接口、录音接口、打开摄像头接口、打开wifi开关接口、打开蓝牙开关接口。

5.根据权利要求1-4中任一项所述的方法，其中，所述智能通信设备为Android通信设备。

6.一种用于智能通信设备的隐私数据访问系统，其中，所述智能通信设备包括系统框架层和应用层，所述系统包括：

加载模块，用于为隐私服务应用配置加壳安装包，运行所述加壳安装包向所述系统框架层加载监控模块；

监控模块，用于监控并捕获所述隐私服务应用的隐私事件；

选择模块，用于将捕获的隐私事件发送至所述应用层的安全应用，以提供隐私数据访问的授权选择；

处理模块，用于自所述安全应用回调授权选择结果，当所述选择结果为“允许”时，允许所述隐私服务应用的隐私数据访问；当所述选择结果为“拒绝”时，不允许所述隐私服务应用的隐私数据访问。

7.根据权利要求6所述的系统，其中，所述加载模块包括：

获取单元，用于获取所述服务应用的安装包的副本；

解析单元，用于解析所述服务应用的安装包的副本，以获取所述服务应用的二进制可执行的代码文件；

注入单元，用于修改或者替换所述代码文件，注入加载模块，以配置所述加壳应用安装包；

挂钩单元，用于运行所述加壳应用安装包，启动所述加载模块，利用所述加载模块加载监控模块，挂钩隐私服务应用的隐私事件行为。

8.根据权利要求6或7所述的系统，其中，所述监控模块用于从后台沙箱的钩子插件框架中获取对应于所述隐私服务应用的隐私事件的钩子插件，利用所述钩子插件捕获相应的隐私事件。

9.根据权利要求8所述的系统，其中，所述监控模块通过将所述钩子插件配置在以下隐私数据访问接口中的至少一个接口中以利用所述钩子插件捕获隐私事件：

拨打电话接口、发送短信接口、获取手机号接口、读取通话记录接口、读取地理位置接口、读取已安装应用列表接口、读取设备id接口、读取通信录接口、读取短信接口、写通话记录接口、写通信录接口、写短信接口、录音接口、打开摄像头接口、打开wifi开关接口、打开蓝牙开关接口。

10.根据权利要求6-9中任一项所述的系统，其中，所述监控模块包括：

设置监听器接口，用于将所述安全应用设置的回调接口通过binder传递给所述监控模块；

授权检查接口，用于调用所述安全应用设置的回调接口，将捕获的隐私事件发送至所述应用层的安全应用进行授权选择，回调授权选择结果，以允许或不允许隐私数据访问。

用于智能通信设备的隐私数据访问方法及系统

技术领域

[0001] 本发明涉及网络安全技术领域，尤其涉及一种用于智能通信设备的隐私数据访问方法及系统。

背景技术

[0002] 随着网络技术的快速发展，智能设备不再局限于为用户提供通话、短信等服务，而且会提供例如位置定位、费用支付等各种功能的应用服务。用户在享受便捷服务的同时，也面临着隐私数据泄露等问题的困扰。以Android(安卓)系统为例，一些服务应用出于商业目的，申请访问隐私数据的权限，获取用户隐私数据。比如读取用户的通话记录、短信内容、位置信息等。

[0003] 目前，用户主要利用智能设备上的安全软件来对服务应用访问隐私数据进行管理。具体的，用户可以通过安全软件来控制设备上的服务应用访问系统中隐私数据权限，从而保护用户的隐私。现有的安全软件主要是通过进程注入的方式来实现隐私权限管理的。具体的，安全软件通过向Android的service manager、phone等系统进程注入自己的动态库文件，在系统读取关键数据的接口中加入HOOK(钩子)插件，调用安全软件的回调接口，根据用户的选择情况返回相应的结果，以决定是否要授权。只有获得授权，隐私数据访问接口才会继续原来的流程，否则直接忽略。然而，现有的主流智能设备采用了Linux操作系统。以Android为典型代表，Android具有相对较为严格的用户权限管理机制。默认状态下，用户的权限较低。要突破权限限制，需要将系统的权限提高到最高级别(即进行ROOT授权)。获得最高权限后，安全应用便可对服务应用访问隐私数据进行管理。如果不进行ROOT授权，传统的安全防御软件则不能完全阻止恶意程序的破坏。但是，即使安全软件获得ROOT授权仍会存在如下的问题：Android设备产商众多，各家多少都会对系统本身有修改，所以现有技术方式可能存在不兼容的问题，导致ROOT授权在某些机型上不太稳定；一般用户并不掌握ROOT授权的专业知识，不能对智能设备进行ROOT授权；ROOT授权在为安全软件开放更高权限的同时，也给了恶意程序以可乘之机。

发明内容

[0004] 本发明提出了一种用于智能通信设备的隐私数据访问方法及系统，用以解决现有技术中对智能设备进行ROOT授权后带来的安全性和稳定性差、隐私权限管理时间滞后且效率低等问题。

[0005] 本发明实施例一方面提供了一种用于智能通信设备的隐私数据访问方法。所述智能通信设备包括系统框架层和应用层。该方法包括：

[0006] 为隐私服务应用配置加壳安装包，运行所述加壳安装包向所述系统框架层加载监控模块；

[0007] 利用所述监控模块监控并捕获所述隐私服务应用的隐私事件；

[0008] 将捕获的隐私事件发送至所述应用层的安全应用，以提供隐私数据访问的授权选

择；

[0009] 自所述安全应用回调授权选择结果，当所述选择结果为“允许”时，允许所述隐私服务应用的隐私数据访问；当所述选择结果为“拒绝”时，不允许所述隐私服务应用的隐私数据访问。

[0010] 在一些实施方式中，为隐私服务应用配置加壳安装包，运行所述加壳安装包向所述系统框架层加载监控模块包括：

[0011] 获取所述服务应用的安装包的副本；

[0012] 解析所述服务应用的安装包的副本，以获取所述服务应用的二进制可执行的代码文件；

[0013] 修改或者替换所述代码文件，注入加载模块，以配置所述加壳应用安装包；

[0014] 运行所述加壳应用安装包，启动所述加载模块，利用所述加载模块加载监控模块，挂钩隐私服务应用的隐私事件行为。

[0015] 在一些实施方式中，利用所述监控模块监控并捕获所述隐私服务应用的隐私事件为：

[0016] 利用所述监控模块从后台沙箱的钩子插件框架中获取对应于所述隐私服务应用的隐私事件的钩子插件，利用所述钩子插件捕获相应的隐私事件。

[0017] 在一些实施方式中，通过将所述钩子插件配置在以下隐私数据访问接口中的至少一个接口中以利用所述钩子插件捕获相应的隐私事件：

[0018] 拨打电话接口、发送短信接口、获取手机号接口、读取通话记录接口、读取地理位置接口、读取已安装应用列表接口、读取设备id接口、读取通信录接口、读取短信接口、写通话记录接口、写通信录接口、写短信接口、录音接口、打开摄像头接口、打开wifi开关接口、打开蓝牙开关接口。

[0019] 在一些实施方式中，所述智能通信设备为Android通信设备。

[0020] 本发明实施例另一方面还提供了一种用于智能通信设备的隐私数据访问系统。智能通信设备包括系统框架层和应用层。系统包括：

[0021] 加载模块，用于为隐私服务应用配置加壳安装包，运行所述加壳安装包向所述系统框架层加载监控模块；

[0022] 监控模块，用于监控并捕获所述隐私服务应用的隐私事件；

[0023] 选择模块，用于将捕获的隐私事件发送至所述应用层的安全应用，以提供隐私数据访问的授权选择；

[0024] 处理模块，用于自所述安全应用回调授权选择结果，当所述选择结果为“允许”时，允许所述隐私服务应用的隐私数据访问；当所述选择结果为“拒绝”时，不允许所述隐私服务应用的隐私数据访问。

[0025] 在一些实施方式中，所述加载模块包括：

[0026] 获取单元，用于获取所述服务应用的安装包的副本；

[0027] 解析单元，用于解析所述服务应用的安装包的副本，以获取所述服务应用的二进制可执行的代码文件；

[0028] 注入单元，用于修改或者替换所述代码文件，注入加载模块，以配置所述加壳应用安装包；

[0029] 挂钩单元，用于运行所述加壳应用安装包，启动所述加载模块，利用所述加载模块加载监控模块，挂钩隐私服务应用的隐私事件行为。

[0030] 在一些实施方式中，所述监控模块利用所述监控模块从后台沙箱的钩子插件框架中获取对应于所述隐私服务应用的隐私事件的钩子插件，利用所述钩子插件捕获相应的隐私事件。

[0031] 在一些实施方式中，所述监控模块通过将所述钩子插件配置在以下隐私数据访问接口中的至少一个接口中以利用该钩子插件捕获隐私事件：

[0032] 拨打电话接口、发送短信接口、获取手机号接口、读取通话记录接口、读取地理位置接口、读取已安装应用列表接口、读取设备id接口、读取通信录接口、读取短信接口、写通话记录接口、写通信录接口、写短信接口、录音接口、打开摄像头接口、打开wifi开关接口、打开蓝牙开关接口。

[0033] 在一些实施方式中，所述监控模块包括：

[0034] 设置监听器接口，用于将所述安全应用设置的回调接口通过binder传递给所述监控模块；

[0035] 授权检查接口，用于调用所述安全应用设置的回调接口，将捕获的隐私事件发送至所述应用层的安全应用进行授权选择，回调授权选择结果，以允许或不允许隐私数据访问。

[0036] 在上述各实施方式中，所述智能通信设备为Android通信设备。

[0037] 由此，本发明通过在系统框架层加载监控模块，将对隐私权限管理的时间进行提前处理，在系统框架层对隐私事件进行监控，提升了权限管理的效率；对系统进行免ROOT处理，提高了系统的安全性和稳定性，改善了用户体验。

附图说明

[0038] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0039] 图1为本发明用于智能通信设备的隐私数据访问方法的一实施方式的流程示意图；

[0040] 图2为短信应用在读短信时，在智能设备的用户界面上显示的授权选择的一实施方式的示意图；

[0041] 图3为图1实施例中子流程实施例的流程示意图；

[0042] 图4为本发明用于智能设备的访问短信消息方法的具体实施例的流程示意图；

[0043] 图5为本发明用于智能通信设备的隐私数据访问系统的一实施例结构示意图；

[0044] 图6为图5实施例中加载模块的结构示意图；

[0045] 图7为图5实施例中监控模块的结构示意图。

具体实施方式

[0046] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是

本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0047] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能解释为对本发明的限制。

[0048] 本技术领域技术人员可以理解，除非特意声明，这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是，本发明的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件，但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、元件、组件和/或它们的组。应该理解，本技术领域技术人员可以理解，除非另外定义，这里使用的所有术语(包括技术术语和科学术语)，具有与本发明所属领域中的普通技术人员的一般理解相同的意义。还应该理解的是，诸如通用字典中定义的那些术语，应该被理解为具有与现有技术的上下文中的意义一致的意义，并且除非像这里一样被特定定义，否则不会用理想化或过于正式的含义来解释。

[0049] 本技术领域技术人员可以理解，这里所使用的“设备”、“智能设备”既包括无线信号接收器的设备，其仅具备无发射能力的无线信号接收器的设备，又包括接收和发射硬件的设备，其具有能够在双向通信链路上，执行双向通信的接收和发射硬件的设备。这种设备可以包括：蜂窝或其他通信设备，其具有单线路显示器或多线路显示器或没有多线路显示器的蜂窝或其他通信设备；PCS(Personal Communications Service，个人通信系统)，其可以组合语音、数据处理、传真和/或数据通信能力；PDA(Personal Digital Assistant，个人数字助理)，其可以包括射频接收器、寻呼机、互联网/内联网访问、网络浏览器、记事本、日历和/或GPS(Global Positioning System，全球定位系统)接收器；常规膝上型和/或掌上型计算机或其他设备，其具有和/或包括射频接收器的常规膝上型和/或掌上型计算机或其他设备。这里所使用的“设备”、“智能设备”可以是便携式、可运输、安装在交通工具(航空、海运和/或陆地)中的，或者适合于和/或配置为在本地运行，和/或以分布形式，运行在地球和/或空间的任何其他位置运行。这里所使用的“设备”、“智能设备”还可以是通信终端、上网终端、音乐/视频播放终端，例如可以是PDA、MID(Mobile Internet Device，移动互联网设备)和/或具有音乐/视频播放功能的移动电话，也可以是智能电视、机顶盒等设备。

[0050] 本技术领域技术人员可以理解，这里所使用的服务器、云端、远端网络设备等概念，具有等同效果，其包括但不限于计算机、网络主机、单个网络服务器、多个网络服务器集或多个服务器构成的云。在此，云由基于云计算(Cloud Computing)的大量计算机或网络服务器构成，其中，云计算是分布式计算的一种，由一群松散耦合的计算机集组成的一个超级虚拟计算机。本发明的实施例中，远端网络设备、终端设备与WNS服务器之间可通过任何通信方式实现通信，包括但不限于，基于3GPP、LTE、WIMAX的移动通信、基于TCP/IP、UDP协议的计算机网络通信以及基于蓝牙、红外传输标准的近距无线传输方式。

[0051] 本领域技术人员应当理解，本发明所称的“应用”以及类似表述的概念，是业内技术人员所公知的相同概念，是指由一系列计算机指令及相关数据资源有机构造的适于电子运行的计算机软件。除非特别指定，这种命名本身不受编程语言种类、级别，也不受其赖以运行的操作系统或平台所限制。理所当然地，此类概念也不受任何形式的终端所限制。

[0052] 图1为本发明用于智能通信设备的隐私数据访问方法的一实施例流程示意图。在

本实施方式中，所述智能通信设备包括系统框架层和应用层。如图1所示，该方法包括：

[0053] S101：为隐私服务应用配置加壳安装包，运行所述加壳安装包向所述系统框架层加载监控模块。

[0054] 在本实施方式中，隐私服务应用为可以获取到用户的隐私数据的服务应用。例如短信应用、通话应用、地图应用、微博应用、淘宝应用等。以微博应用为例，可以对其管理的权限为：发送文本短信、发送文本信息、发送数据信息安装应用、录音等。该步骤的具体实现方式将在下面的图2的实施方式中详细描述。

[0055] S102：利用所述监控模块监控并捕获所述隐私服务应用的隐私事件。

[0056] 在本实施方式中，隐私事件可以是拨打电话事件、发送短信事件、获取手机号事件、读取通话记录事件、读取地理位置事件、读取已安装应用列表事件、读取设备身份标识号(id)(包括国际移动设备标识(IMEI)、国际移动用户识别码(IMSI))事件、读取通信录事件、读取短信事件、写通话记录事件、写通信录事件、写短信事件、录音事件、打开摄像头事件、打开wifi开关事件、打开蓝牙开关事件中的一种或者多种，也可以是其他可能涉及到隐私数据的事件，例如：

[0057] (1)智能设备、联网有关的操作。例如获取运营商信息。具体可以通过getSimOperatorName()函数可以获得智能设备的IMSI。

[0058] (2)通知栏广告操作。

[0059] (3)命令操作。例如：利用Execve()函数进行SU提权操作或执行命令操作。

[0060] (4)界面及访问操作。例如：利用SentBroacast()函数创造快捷方式，和利用Sentto()、Write()等函数访问HTTP网络。

[0061] S103：将捕获的隐私事件发送至所述应用层的安全应用，以提供隐私数据访问的授权选择。

[0062] 在本实施方式中，授权结果通常可以是“允许”或者“拒绝”。本领域的技术人员可以理解，也可以通过“询问”的方式与用户进行信息交互后再获取“允许”或者“拒绝”的选择。当然，也可以通过预设的程序直接进行选择，而无需与用户进行信息交互。

[0063] 下面以短信应用读短信为例，说明提供隐私数据访问的授权选择的实现方式。图2为短信应用在读短信时，在智能设备的用户界面上显示的授权选择的一个实施方式的示意图。应用层的安全软件(例如360的手机卫士的安全应用)在判断是否允许短信应用读短信的授权结果时，可以通过弹屏的方式与用户进行信息交互。参见图2，弹屏的内容可以是：隐私权限请求，应用名称：短信，隐私权限：读短信，uid:10024，pid:27185，“不用再问我”的复选框，“允许”的按钮和“拒绝”的按钮。

[0064] S104：自所述安全应用回调授权选择结果，当所述选择结果为“允许”时，允许所述隐私服务应用的隐私数据访问；当所述选择结果为“拒绝”时，不允许所述隐私服务应用的隐私数据访问。

[0065] 在本实施方式中，利用所述监控模块从后台沙箱的HOOK插件框架(可设置在普通的存储设备内，也可以设置在云服务器内)中获取对应于所述隐私服务应用的隐私事件的HOOK插件，利用所述HOOK插件捕获相应的隐私事件。

[0066] 由此，本发明监控模块可以采用HOOK技术，利用丰富的HOOK函数对相关调用指令的入口点进行监视，截获调用指令，转向执行相应的钩子函数，由该钩子函数依据沙箱自身

逻辑来应答该调用指令，不对设备进行破解ROOT的情况下，实现多种类的隐私权限管理的目的，使得用户可以主动选择对隐私数据访问的授权，避免隐私信息被恶意软件窃取或者后台乱发短信等造成资费的损失。

[0067] 在本实施方式中，通过将所述HOOK插件配置在以下隐私数据访问接口中的至少一个接口中以利用所述HOOK插件捕获相应的隐私事件：

[0068] 拨打电话接口、发送短信接口、获取手机号接口、读取通话记录接口、读取地理位置接口、读取已安装应用列表接口、读取设备身份标识号(id)(包括国际移动设备标识(IMEI)、国际移动用户识别码(IMSI))接口、读取通信录接口、读取短信接口、写通话记录接口、写通信录接口、写短信接口、录音接口、打开摄像头接口、打开wifi开关接口、打开蓝牙开关接口中的一种或者多种，也可以是其他可能涉及到隐私数据的接口。在本实施方式中，所述智能通信设备为Android通信设备。

[0069] 由此，本发明在涉及用户隐私数据的接口中均配置了相应的HOOK插件，提高了系统的安全性，确保了用户的隐私数据不会被泄露。

[0070] 此外，本发明中的隐私服务应用通过Android sdk接口访问数据，最终都会调用到framework(系统框架层)中的上述相关接口来访问实际数据。将隐私权限管理的时间从应用层提前至系统框架层，提高了管理的效率。对系统进行免ROOT处理，提高了系统的安全性和稳定性，改善了用户体验。

[0071] 具体的，本发明在Android系统的访问隐私数据的接口中加入HOOK插件，中断原来的直接调用过程，先回调安全软件的接口，得到授权之后才继续原来的流程。一旦隐私应用要调用相关接口访问隐私的数据，framework会回调安全软件设置的接口，根据用户的选择返回授权结果，直接在系统层就解决了这个问题，无需安全软件应用通过获取ROOT权限注入系统进程，从而提高了系统安全性和稳定性。

[0072] 图3为图1中子流程实施例的示意图。图1中的S101步骤(为隐私服务应用配置加壳安装包，运行所述加壳安装包向所述系统框架层加载监控模块)包括：

[0073] S1011：获取所述隐私服务应用的安装包的副本。

[0074] S1012：解析所述隐私服务应用的安装包的副本，以获取所隐私述服务应用的二进制可执行的代码文件(classes.dex代码文件)。

[0075] 本实施方式通过解析所述服务应用的安装包的副本，可以获得如下面表1中所附的目录和文件：

[0076]

文件名或目录名称	说明
META-INF\	该目录下一般有 MANIFEST.MF 和以.RSA、.SF 结尾的文件，这些文件记录了其它目录文件的证书签名，Android 系统在安装 APK 安装包的时候会逐个检查 APK 内部各文件是否与本目录记录的证书签名一致，如果不一致，则认为文件已被篡改，拒绝该 APK 的安装和运行。
res\	该目录下是 Android 应用所使用的图片、文件等资源文件。系统会为此类资源文件给出 ID。
assets\	该目录下是 Android 应用所使用的其它资源文件，此类资源文件不能被赋予 ID，但可用路径访问。
resources.arsc	二进制的资源索引表。

[0077]

lib\	该目录下是 JNI 库文件。
AndroidManifest.xml	对本 APK 所包含的 Android 应用程序的全局描述文件，如应用的包名、版本号、模块入口等。
classes.dex	.dex 是 Dalvik Executable（Dalvik 虚拟机可执行文件）的缩写。

[0078] 表1

[0079] S1013:修改或者替换所述代码文件,注入加载模块(stub()),以配置所述加壳应用安装包。

[0080] 在本实施方式中,在为加壳应用安装包命名时,将加壳应用安装包的包名与被加壳的隐私服务应用的包名命名成一致的包名。

[0081] S1014:运行所述加壳应用安装包,启动所述加载模块,利用所述加载模块加载监控模块,挂钩隐私服务应用的隐私事件行为。

[0082] 具体的,在本实施方式中,可以将上述表1中的文件加入到加壳应用安装包内。其中,Androidmanifest.xml文件(安装包中较为重要的全局配置文件,其负责向系统注册Android系统的四大组件,以及向系统申请权限等)。由于快捷应用的安装包中的Androidmanifest.xml文件与原安装包的为同名文件(其包名相同),故加壳安装包在系统中安装运行宿主应用程序(被加壳的应用的安装包程序)之后,以Androidmanifest.xml向系统注册各个组件和申请系统权限,以此便建立了各个组件的入口,使经反射调用的隐私服务应用的各个组件均可以被ActivityManagerService调用,而不必为所述各个组件构造

ActivityThread和提供相应的LoadedApk对象，省去运行上下文环境的程序实现环节。同理，反射调用所导致的PackageManagerService对各大组件是否合法注册的问题，也将因Androidmanifest.xml的注册而被克服。

[0083] 通过该加载模块stub()，可以进一步启动监控模块。该监控模块用于监控经反射调用的隐私服务应用程序的活动过程(隐私事件)。监控模块会先于隐私服务应用的程序加载。该监控模块便是沙箱运行环境的实现者，负责实现两方面的功能。一方面，通过监控隐私服务应用对资源的访问，对资源引用进行重定向，使隐私服务应用程序进程能够实现对正确资源的正常引用。具体而言，如果相关资源是被反射调用的原安装包的资源，则通过反射调用机制调用该原安装包的资源供引用，实现重定向。如果是系统资源或者指向宿主应用程序的已安装资源，则可允许其默认引用保证其正常引用关系。如果是I/O操作，也可以藉此进行重定向。另一方面，通过监控应用程序对系统资源的访问(例如是否请求发送短信息)，来依据安全策略确定是否允许其操作。当不允许这种实施这种行为时，可以向相关调用指令返回自定义数据(例如返回空值)，从而确保能杜绝一些非法操作。

[0084] 由此，一来，本发明通过相同的包名(为隐私服务应用配置加壳安装包与隐私服务应用的安装包的包名相同)，不必为被反射调用的隐私服务应用的各个组件(例如Activity组件、Service组件、Receiver组件)单独构造主函数入口(ActivityThread.main)，也不必考虑因包名而带来的PackageManagerService校验的程序实现复杂度问题，从而大大提高程序运行效率。

[0085] 二来，本发明通过服务应用的安装包的副本配置含有加载模块的快捷应用的安装包，而服务应用的安装包可以被安全保存。由此，本发明对程序的修改很小，不仅操作简单方便，而且不会影响运行的兼容新。

[0086] 图4为本发明用于智能设备的访问短信消息方法的具体实施例的流程示意图。参照图4，作为智能设备(例如Android手机)应用上述方法的具体操作流程，例如表现如下：

[0087] 在Android手机的系统框架层(向系统框架层加载了监控模块，其中监控模块可以包括安全检查服务和授权处理服务)：

[0088] 短消息接口管理(IccSmsInterfaceManager)发送文本(sendText())(或者发送多部分文本(sendMultipartText()))。

[0089] 安全检查服务(SecurityService)监控并捕获短信应用的发送文本事件。在捕获到发送文本事件后，安全检查服务可通过安全应用的应用管理器(QihooAppManager)和权限监听器(QihooPrivilege Listener)将捕获的发送文本事件发送至所述应用层的安全软件(例如360的手机卫士的安全应用)，以提供隐私数据访问的授权选择。然后，安全检查回调授权选择结果，当所述选择结果为“拒绝”(即没有得到授权)时，中止发送短信消息的活动；当所述选择结果为“允许”(即得到授权)时，允许短消息分发(SmsDispatcher)来发送文本(sendText())或者发送多部分文本(sendMultipartText())。

[0090] 在本实施方式中，安全软件(例如360的手机卫士的安全应用)通过应用程序开发工具集(sdk)和安全检查(SecurityService)进行交互。例如通过QihooAppManager类的setPrivilegeListener()方法设置好回调接口。系统框架层在发送短信调用安全检查(SecurityService)的checkPrivilege()方法进行检查时，回调安全软件的回调接口，以询问是否授权，从而达到权限控制的目的。其中，sdk可以定义见下表2和表3中类和接口：

[0091] 权限监听器

[0092]

接口	
QihooPrivilegeListener	
方法	
boolean	checkPrivilege(String packageName, int uid, int pid, int privilege, Bundle info) 返回 true 表示授权本次操作，返回 false 表示拒绝本次操作。

[0093] 表2

[0094] 权限管理控制类

[0095]

接口	
QihooAppManager	
方法	
boolean	setPrivilegeListener(QihooPrivilegeListener listener) 设置权限管理监听器，参数为 null 时表示不监听。

[0096] 表3

[0097] 图5为本发明用于智能通信设备的隐私数据访问系统的一实施例结构示意图。所述智能通信设备包括系统框架层和应用层。用于智能通信设备的隐私数据访问系统包括：加载模块、监控模块、选择模块和处理模块。其中：

[0098] 加载模块用于为隐私服务应用配置加壳安装包，运行所述加壳安装包向所述系统框架层加载监控模块。

[0099] 监控模块用于监控并捕获所述隐私服务应用的隐私事件。

[0100] 选择模块用于将捕获的隐私事件发送至所述应用层的安全应用，以提供隐私数据访问的授权选择。

[0101] 处理模块用于自所述安全应用回调授权选择结果，当所述选择结果为“允许”时，允许所述隐私服务应用的隐私数据访问；当所述选择结果为“拒绝”时，不允许所述隐私服务应用的隐私数据访问。

[0102] 在本实施方式中，所述监控模块用于从后台沙箱的钩子插件框架中获取对应于所述隐私服务应用的隐私事件的钩子插件，利用所述钩子插件捕获相应的隐私事件。

[0103] 进一步，所述监控模块通过将所述钩子插件配置在以下隐私数据访问接口中的至少一个接口中以利用该钩子插件捕获隐私事件：

[0104] 拨打电话接口、发送短信接口、获取手机号接口、读取通话记录接口、读取地理位置接口、读取已安装应用列表接口、读取设备id接口、读取通信录接口、读取短信接口、写通话记录接口、写通信录接口、写短信接口、录音接口、打开摄像头接口、打开wifi开关接口、

打开蓝牙开关接口。

[0105] 图6为图5中加载模块的结构示意图。如图6所示，加载模块包括：获取单元、解析单元、注入单元和挂钩单元。其中：

[0106] 获取单元用于获取所述服务应用的安装包的副本。

[0107] 解析单元用于解析所述服务应用的安装包的副本，以获取所述服务应用的二进制可执行的代码文件(classes.dex)。

[0108] 注入单元用于修改或者替换所述代码文件，注入加载模块，以配置所述加壳应用安装包。

[0109] 挂钩单元用于运行所述加壳应用安装包，启动所述加载模块(stub())，利用所述加载模块加载监控模块，挂钩隐私服务应用的隐私事件行为。

[0110] 在上述各实施方式中，监控模块通过将所述钩子插件配置在以下隐私数据访问接口中的至少一个接口中以利用该钩子插件捕获隐私事件：

[0111] 拨打电话接口、发送短信接口、获取手机号接口、读取通话记录接口、读取地理位置接口、读取已安装应用列表接口、读取设备身份标识号(id)(包括国际移动设备标识(IMEI)、国际移动用户识别码(IMSI))接口、读取通信录接口、读取短信接口、写通话记录接口、写通信录接口、写短信接口、录音接口、打开摄像头接口、打开wifi开关接口、打开蓝牙开关接口中的一种或者多种，也可以是其他可能涉及到隐私数据的接口。

[0112] 图7为图5中监控模块的结构示意图。如图7所示，所述监控模块包括：设置监听器接口和授权检查接口。其中：

[0113] 设置监听器接口，用于将所述安全应用设置的回调接口通过binder传递给所述监控模块；

[0114] 授权检查接口，用于调用所述安全应用设置的回调接口，将捕获的隐私事件发送至所述应用层的安全应用进行授权选择，回调授权选择结果，以允许或不允许隐私数据访问。

[0115] 作为一种具体的实现方式，本发明的用于智能通信设备的隐私数据访问系统的加载模块、监控模块和处理模块可以嵌入至智能设备(例如Android设备)的框架层内。其中：

[0116] 加载模块用于为隐私服务应用配置加壳安装包，运行所述加壳安装包向所述系统框架层加载监控模块。监控模块用于监控并捕获所述隐私服务应用的隐私事件，将捕获的隐私事件发送至所述应用层的安全应用，以提供隐私数据访问的授权选择。处理模块用于自所述安全应用回调授权选择结果，当所述选择结果为“允许”时，允许所述隐私服务应用的隐私数据访问；当所述选择结果为“拒绝”时，不允许所述隐私服务应用的隐私数据访问。

[0117] 在上述各实施方式中，所述智能通信设备为Android通信设备。

[0118] 当然，本发明实施例中可以通过硬件处理器(hardware processor)和各单元来实现相关功能模块的各项功能。

[0119] 上述系统的技术效果与方法的效果相同，在此不再赘述。

[0120] 本领域内的技术人员应明白，本申请的实施例可提供为方法、装置、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包括有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产

品的形式。

[0121] 上述说明示出并描述了本申请的若干优选实施例，但如前所述，应当理解本申请并非局限于本文所披露的形式，不应看作是对其他实施例的排除，而可用于各种其他组合、修改和环境，并能够在本文所述发明构想范围内，通过上述教导或相关领域的技术或知识进行改动。若本领域人员所进行的改动和变化不脱离本申请的精神和范围，则都应在本申请的保护范围内。

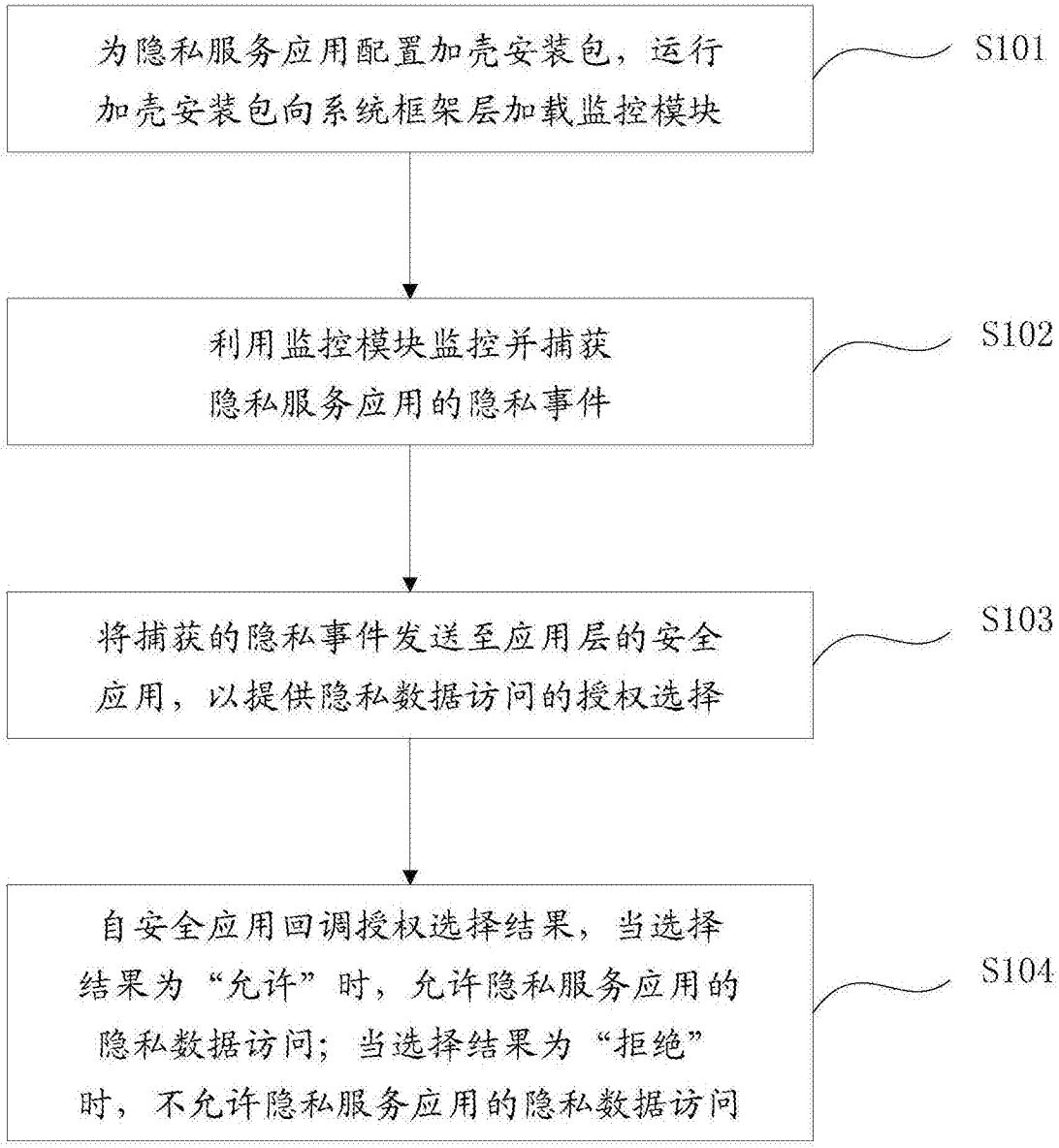

为隐私服务应用配置加壳安装包，运行加壳安装包向系统框架层加载监控模块
S101
利用监控模块监控并捕获隐私服务应用的隐私事件
S102
将捕获的隐私事件发送至应用层的安全应用，以提供隐私数据访问的授权选择
S103
自安全应用回调授权选择结果，当选择结果为“允许”时，允许隐私服务应用的隐私数据访问；当选择结果为“拒绝”时，不允许隐私服务应用的隐私数据访问
S104

图1

图2

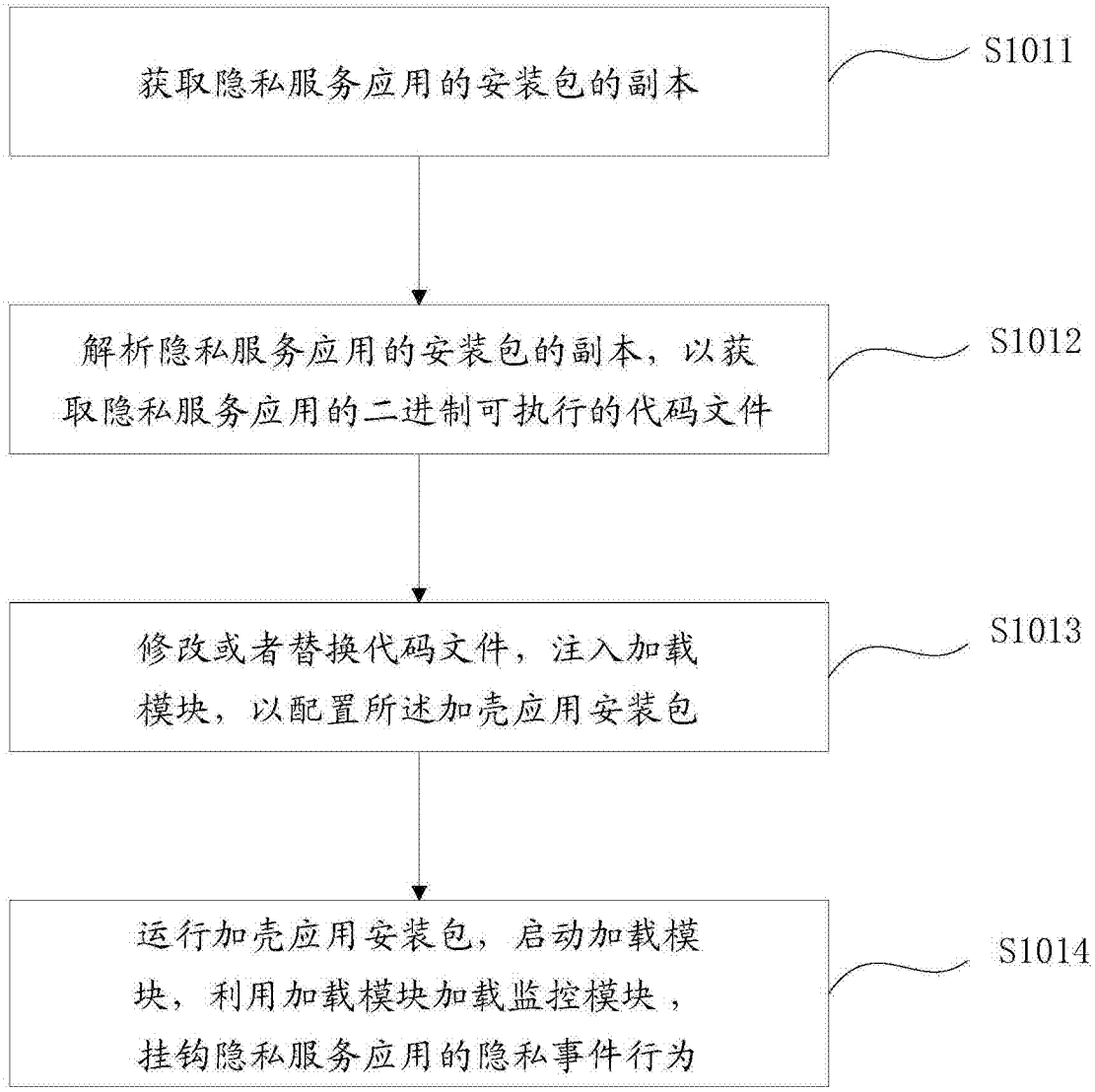

获取隐私服务应用的安装包的副本
S1011
解析隐私服务应用的安装包的副本，以获取隐私服务应用的二进制可执行的代码文件
S1012
修改或者替换代码文件，注入加载模块，以配置所述加壳应用安装包
S1013
运行加壳应用安装包，启动加载模块，利用加载模块加载监控模块，挂钩隐私服务应用的隐私事件行为
S1014

图3

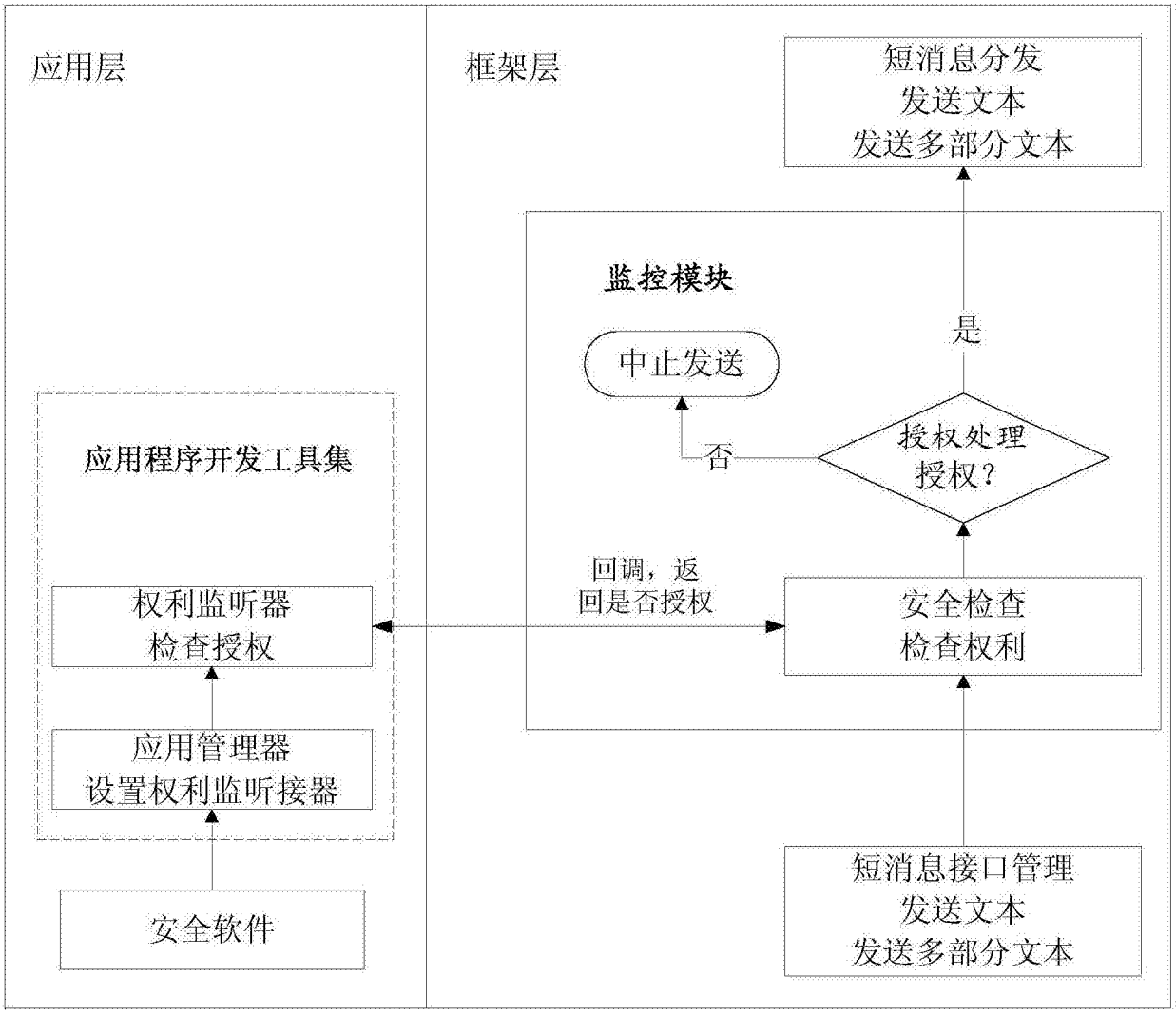

应用层
框架层
短消息分发
发送文本
发送多部分文本
监控模块
中止发送
是
否
授权处理
授权？
应用程序开发工具集
回调，返
回是否授权
权利监听器
检查授权
安全检查
检查权利
应用管理器
设置权利监听接器
短消息接口管理
发送文本
发送多部分文本
安全软件

图4

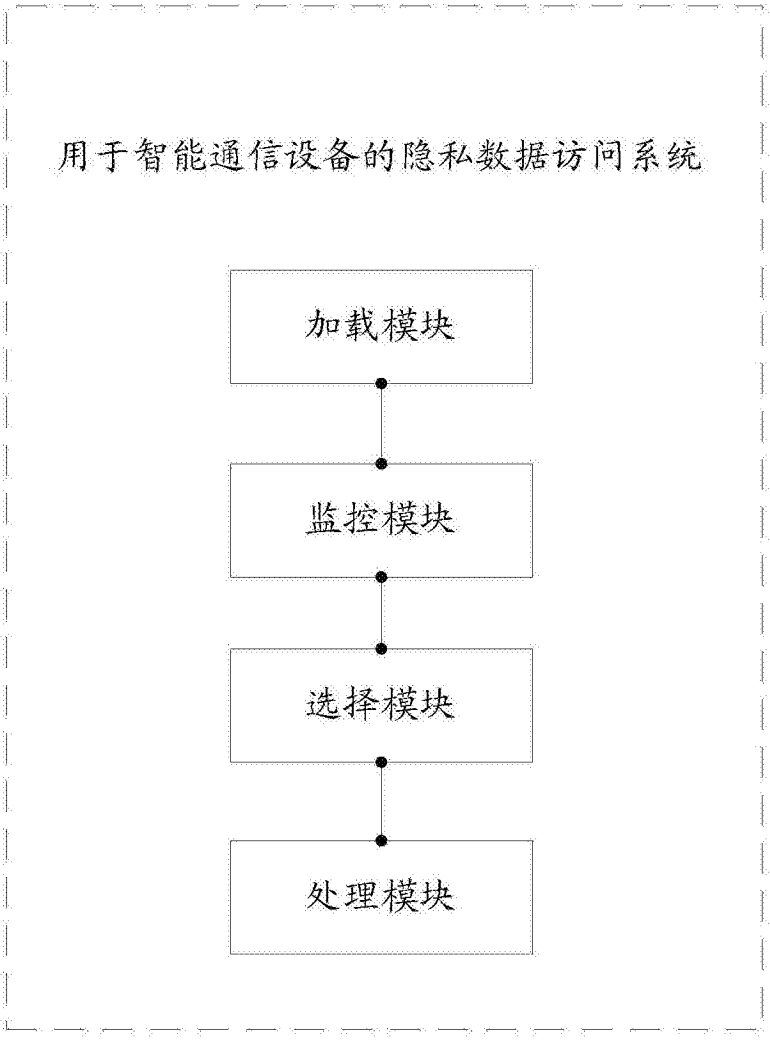


图5

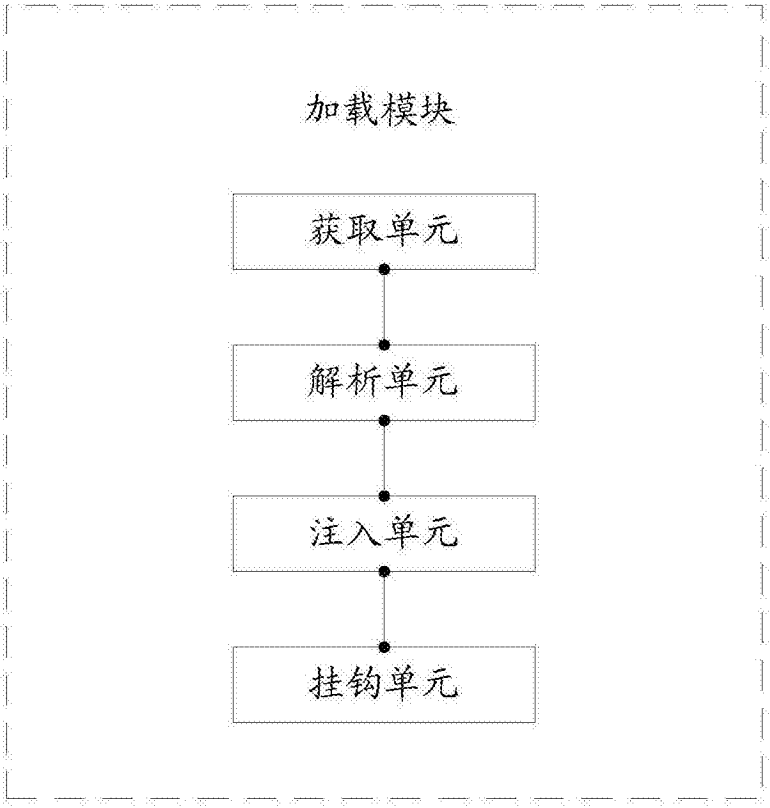


图6

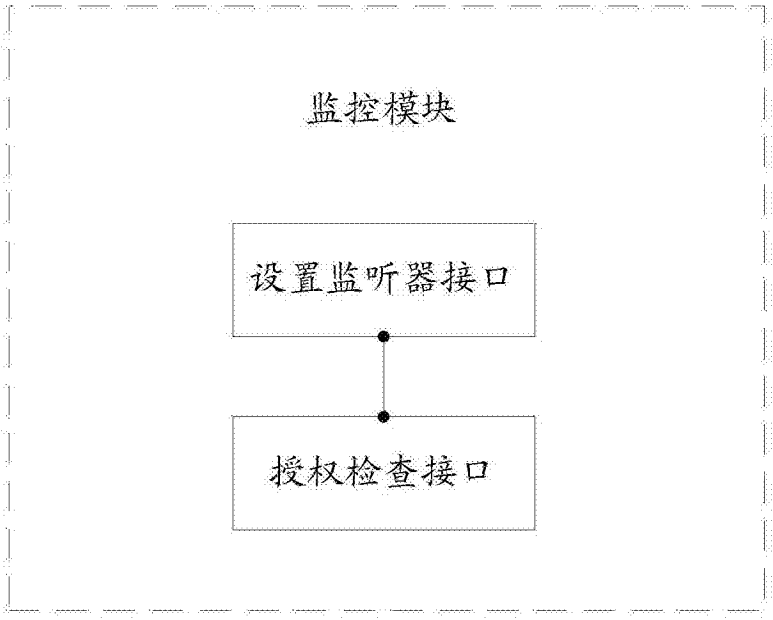


图7