



(21)申请号 201310632696.5

(22)申请日 2013.11.29

(65)同一申请的已公布的文献号

申请公布号 CN 104683409 A

(43)申请公布日 2015.06.03

(73)专利权人 华为终端(东莞)有限公司

地址 523808 广东省东莞市松山湖高新技术
产业开发区新城大道2号南方工厂
厂房(一期)项目B2区生产厂房-5

(72)发明人 汪婵 吴黄伟 黄洁静 黄曦

(74)专利代理机构 北京龙双利达知识产权代理

有限公司 11329

代理人 王君 肖鹏

(51)Int.Cl.

H04L 29/08(2006.01)

(56)对比文件

CN 103339602 A,2013.10.02,

CN 101860591 A,2010.10.13,

审查员 杜少凤

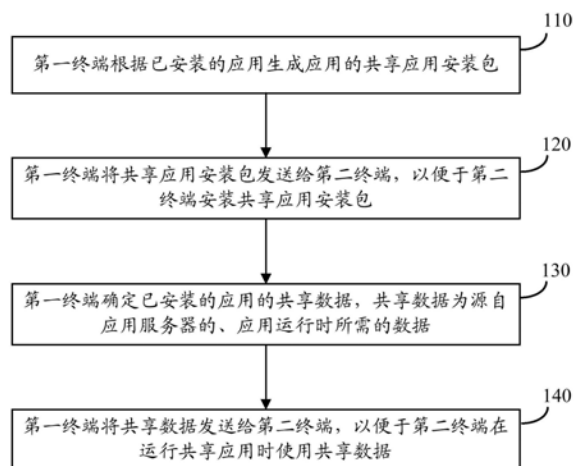
权利要求书2页 说明书26页 附图19页

(54)发明名称

终端间应用共享的方法和终端

(57)摘要

本发明实施例提供一种终端间应用共享的方法和终端,以方便接收端用户的操作。该方法包括:第一终端根据已安装的应用生成该应用的共享应用安装包;该第一终端将该共享应用安装包发送给第二终端,以便于第二终端安装该共享应用安装包;该第一终端确定该已安装的应用的共享数据,该共享数据为源自应用服务器的、该应用运行时所需的数据;该第一终端将该共享数据发送给该第二终端,以便于该第二终端在运行该共享应用时使用该共享数据。本发明实施例中,当两个终端共享应用时,不仅共享该应用的安装包,还共享该应用的共享数据,避免接收端去应用服务器下载该共享数据,方便了接收端用户的操作,提高用户体验。



1. 一种终端间应用共享的方法,其特征在于,包括:

第一终端根据已安装的应用生成所述应用的共享应用安装包;

所述第一终端将所述共享应用安装包发送给第二终端,以便于第二终端安装所述共享应用安装包;

所述第一终端确定所述已安装的应用的共享数据,所述共享数据为源自应用服务器的、所述应用运行时所需的数据;

所述第一终端将所述共享数据发送给所述第二终端,以便于所述第二终端在运行共享应用时使用所述共享数据;

还包括:

所述第二终端接收所述共享应用安装包,并从所述共享应用安装包中提取验证信息,所述验证信息用于确定所述共享应用安装包是否源自应用服务器;

当所述共享应用安装包源自所述应用服务器时,所述第二终端运行所述共享应用安装包。

2. 如权利要求1所述的方法,其特征在于,所述共享数据存储在该第一终端的公用数据文件中,所述确定所述已安装的应用的共享数据包括:

从所述公用数据文件中提取所述共享数据。

3. 如权利要求2所述的方法,其特征在于,所述公用数据文件在该第一终端的存储路径为运行所述安装包时、按照所述安装包的指示定义的存储路径。

4. 如权利要求2所述的方法,其特征在于,所述公用数据文件在该第一终端的存储路径为所述第一终端定义的存储路径。

5. 如权利要求1所述的方法,其特征在于,所述共享数据为所述应用服务器提供的离线数据包中的数据,

在所述确定所述已安装的应用的共享数据之前,还包括:

记录所述离线数据包中数据的存储位置;

所述确定所述已安装的应用的共享数据,包括:

从记录的所述存储位置中提取所述离线数据包中的数据作为所述共享数据。

6. 一种终端间应用共享的方法,其特征在于,包括:

第二终端从第一终端接收应用的共享应用安装包,并接收所述应用的共享数据,所述共享数据为源自应用服务器的、所述应用运行时所需的数据,所述应用的共享应用安装包是由所述第一终端根据已安装的所述应用生成的;

所述第二终端存储所述共享数据;

还包括:

所述第二终端从所述共享应用安装包中提取验证信息,所述验证信息用于确定所述共享应用安装包是否源自应用服务器;

当所述共享应用安装包源自所述应用服务器时,所述第二终端运行所述共享应用安装包。

7. 一种终端,其特征在于,包括:

生成单元,用于根据已安装的应用生成所述应用的共享应用安装包;

发送单元,用于将所述生成单元生成的所述共享应用安装包发送给第二终端,以便于

第二终端安装所述共享应用安装包；

确定单元，用于确定所述已安装的应用的共享数据，所述共享数据为源自应用服务器的、所述应用运行时所需的数据；

所述发送单元还用于将所述确定单元确定的所述共享数据发送给所述第二终端，以便于所述第二终端在运行共享应用时使用所述共享数据，所述第二终端接收所述共享应用安装包，并从所述共享应用安装包中提取验证信息，所述验证信息用于确定所述共享应用安装包是否源自应用服务器；当所述共享应用安装包源自所述应用服务器时，所述第二终端运行所述共享应用安装包。

8. 如权利要求7所述的终端，其特征在于，所述共享数据存储在该终端的公用数据文件中，所述确定单元具体用于从所述公用数据文件中提取所述共享数据。

9. 如权利要求8所述的终端，其特征在于，所述公用数据文件在该终端的存储路径为运行所述安装包时、按照所述安装包的指示定义的存储路径。

10. 如权利要求8所述的终端，其特征在于，所述公用数据文件在该终端的存储路径为该终端定义的存储路径。

11. 如权利要求7所述的终端，其特征在于，所述共享数据为所述应用服务器提供的离线数据包中的数据，

所述终端还包括：

记录单元，用于记录所述离线数据包中数据的存储位置；

所述确定单元具体用于从记录的所述存储位置中提取所述离线数据包中的数据作为所述共享数据。

12. 一种终端，其特征在于，包括：

接收单元，用于从第一终端接收应用的共享应用安装包，并接收所述应用的共享数据，所述共享数据为源自应用服务器的、所述应用运行时所需的数据，所述应用的共享应用安装包是由所述第一终端根据已安装的所述应用生成的；

存储单元，用于存储所述共享数据；

还包括：

确定单元，用于从所述共享应用安装包中提取验证信息，所述验证信息用于确定所述共享应用安装包是否源自应用服务器；

所述确定单元还用于当所述共享应用安装包源自所述应用服务器时，运行所述共享应用安装包。

终端间应用共享的方法和终端

技术领域

[0001] 本发明实施例涉及通信领域,并且更为具体地,涉及终端间应用共享的方法和终端,

背景技术

[0002] 随着移动终端的发展,移动终端上的应用越来越多。当终端的用户需要某个应用时,会在移动应用商店去下载,比如Google Play、App Store或其他应用商店(如第三方应用商店),也可以让好友通过终端间的应用共享,将自己需要的应用传给自己。

[0003] 但是,现有技术中,终端间在应用共享时,发送端(应用的发送端)仅向接收端(应用的接收端)发送应用的安装包。接收端接收到应用的安装包后,还需要去应用服务器下载该应用运行时所需的数据,不够便捷。

发明内容

[0004] 本发明实施例提供一种终端间应用共享的方法和终端,以方便接收端用户的操作。

[0005] 第一方面,提供一种终端间应用共享的方法,包括:第一终端根据已安装的应用生成所述应用的共享应用安装包;所述第一终端将所述共享应用安装包发送给第二终端,以便于第二终端安装所述共享应用安装包;所述第一终端确定所述已安装的应用的共享数据,所述共享数据为源自应用服务器的、所述应用运行时所需的数据;所述第一终端将所述共享数据发送给所述第二终端,以便于所述第二终端在运行所述共享应用时使用所述共享数据。

[0006] 结合第一方面,在第一方面的一种实现方式中,所述共享数据存储在所述第一终端的公用数据文件中,所述确定所述已安装的应用的共享数据包括:从所述公用数据文件中提取所述共享数据。

[0007] 结合第一方面或其上述实现方式的任一种,在第一方面的另一种实现方式中,所述公用数据文件在所述第一终端的存储路径为运行所述安装包时、按照所述安装包的指示定义的存储路径。

[0008] 结合第一方面或其上述实现方式的任一种,在第一方面的另一种实现方式中,所述公用数据文件在所述第一终端的存储路径为所述第一终端定义的存储路径。

[0009] 结合第一方面或其上述实现方式的任一种,在第一方面的另一种实现方式中,所述共享数据为所述应用服务器提供的离线数据包中的数据,在所述确定所述已安装的应用的共享数据之前,还包括:记录所述离线数据包中数据的存储位置;所述确定所述已安装的应用的共享数据,包括:从记录的所述存储位置中提取所述离线数据包中的数据作为所述共享数据。

[0010] 第二方面,提供一种终端间应用共享的方法,包括:第二终端从第一终端接收应用的共享应用安装包,并接收所述应用的共享数据,所述共享数据为源自应用服务器的、所述

应用运行时所需的数据,所述应用的共享应用安装包时由所述第一终端根据已安装的所述应用生成的;所述第二终端存储所述共享数据。

[0011] 第三方面,提供一种验证应用安全性的方法,包括:第一终端接收应用的第一安装包,并从所述第一安装包中提取验证信息,所述验证信息用于确定所述第一安装包是否源自应用服务器;所述第一终端根据所述验证信息确定所述第一安装包是否源自所述应用服务器;当所述第一安装包不是源自所述应用服务器时,所述第一终端从所述应用服务器获取所述应用的第二安装包,并用所述第二安装包覆盖所述第一安装包;当所述第一安装包源自所述应用服务器时,所述第一终端运行所述第一安装包。

[0012] 结合第三方面,在第三方面的一种实现方式中,所述根据所述验证信息确定所述第一安装包是否源自所述应用服务器,包括:向所述应用服务器发送所述验证信息,以便所述应用服务器根据所述验证信息与源信息的匹配,检验所述第一安装包是否源自所述应用服务器,其中所述源信息为所述应用服务器从所述第二安装包中提取的;接收所述应用服务器的检验结果。

[0013] 第四方面,提供一种验证应用安全性的方法,包括:应用服务器接收第一终端发送的验证信息,所述验证信息是所述第一终端从应用的第一安装包中提取的,且所述验证信息用于确定所述第一安装包是否源自所述应用服务器;所述应用服务器从所述应用服务器中存储的所述应用的第二安装包中提取源信息;所述应用服务器根据所述源信息与所述验证信息的匹配确定所述第一安装包是否源自所述应用服务器,并向所述第一终端发送匹配的结果。

[0014] 第五方面,提供一种处理应用方法,包括:接收第一应用的安装包,所述安装包中包括所述第一应用的标识符和第二应用的标识符,所述第二应用是所述第一应用的旧版本;根据所述第二应用的标识符检查系统中是否已安装所述第二应用,若系统中已安装所述第二应用,则安装所述第一应用并移除所述第二应用。

[0015] 第六方面,提供一种终端,包括:生成单元,用于根据已安装的应用生成所述应用的共享应用安装包;发送单元,用于将所述生成单元生成的所述共享应用安装包发送给第二终端,以便于第二终端安装所述共享应用安装包;确定单元,用于确定所述已安装的应用的共享数据,所述共享数据为源自应用服务器的、所述应用运行时所需的数据;所述发送单元还用于将所述确定单元确定的所述共享数据发送给所述第二终端,以便于所述第二终端在运行所述共享应用时使用所述共享数据。

[0016] 结合第六方面,在第六方面的一种实现方式中,所述共享数据存储在该终端的公用数据文件中,所述确定单元具体用于从所述公用数据文件中提取所述共享数据。

[0017] 结合第六方面或其上述实现方式的任一种,在第六方面的另一种实现方式中,所述公用数据文件在该终端的存储路径为运行所述安装包时、按照所述安装包的指示定义的存储路径。

[0018] 结合第六方面或其上述实现方式的任一种,在第六方面的另一种实现方式中,所述公用数据文件在该终端的存储路径为该终端定义的存储路径。

[0019] 结合第六方面或其上述实现方式的任一种,在第六方面的另一种实现方式中,所述共享数据为所述应用服务器提供的离线数据包中的数据,所述终端还包括:记录单元,用于记录所述离线数据包中数据的存储位置;所述确定单元具体用于从记录的所述存储位置

中提取所述离线数据包中的数据作为所述共享数据。

[0020] 第七方面,提供一种终端,包括:接收单元,用于从第一终端接收应用的共享应用安装包,并接收所述应用的共享数据,所述共享数据为源自应用服务器的、所述应用运行时所需的数据,所述应用的共享应用安装包时由所述第一终端根据已安装的所述应用生成的;存储单元,用于存储所述共享数据。

[0021] 第八方面,提供一种终端,包括:第一接收单元,用于接收应用的第一安装包;提取单元,用于从所述第一接收单元接收的所述第一安装包中提取验证信息,所述验证信息用于确定所述第一安装包是否源自应用服务器;确定单元,用于根据所述提取单元提取的所述验证信息确定所述第一安装包是否源自所述应用服务器;当所述第一安装包不是源自所述应用服务器时,从所述应用服务器获取所述应用的第二安装包,并用所述第二安装包覆盖所述第一安装包;当所述第一安装包源自所述应用服务器时,运行所述第一安装包。

[0022] 结合第八方面,在第八方面的一种实现方式中,所述确定单元具体用于向所述应用服务器发送所述验证信息,以便所述应用服务器根据所述验证信息与源信息的匹配,检验所述第一安装包是否源自所述应用服务器,其中所述源信息为所述应用服务器从所述第二安装包中提取的;接收所述应用服务器的检验结果。

[0023] 第九方面,提供一种应用服务器,包括:接收单元,用于接收第一终端发送的验证信息,所述验证信息是所述第一终端从应用的第一安装包中提取的,且所述验证信息用于确定所述第一安装包是否源自所述应用服务器;提取单元,用于从所述应用服务器中存储的所述应用的第二安装包中提取源信息;匹配单元,用于根据所述提取单元提取的所述源信息与所述接收单元接收的所述验证信息的匹配确定所述第一安装包是否源自所述应用服务器;发送单元,用于向所述第一终端发送所述匹配单元的匹配结果。

[0024] 第十方面,提供一种终端,包括:接收单元,用于接收第一应用的安装包,所述安装包中包括所述第一应用的标识符和第二应用的标识符,所述第二应用是所述第一应用的旧版本;检查单元,用于根据所述接收单元接收的所述安装包中的所述第二应用的标识符检查系统中是否已安装所述第二应用;若系统中已安装所述第二应用,安装所述第一应用并移除所述第二应用。

[0025] 第十一方面,提供一种处理应用方法,包括:向应用服务器发送请求,所述请求用于请求第一应用的安装包和包含所述第一应用的应用信息列表;所述应用信息列表中包括所述第一应用的标识符和至少一个第二应用的标识符,所述第二应用是所述第一应用的旧版本,所述第一应用的标识符和所述第二应用的标识符不同;根据所述第二应用的标识符检查系统中是否已安装所述第二应用,若系统中已安装第二应用,则安装所述第一应用并移除所述第二应用。

[0026] 第十二方面,提供一种处理应用方法,包括:向应用服务器发送请求,所述请求用于请求第一应用的安装包和包含所述第一应用的应用信息列表;所述应用信息列表中包括所述第一应用的证书信息和至少一个第二应用的证书信息,所述第二应用是所述第一应用的旧版本,所述第一应用的证书信息和所述第二应用的证书信息不同;根据所述第二应用的证书信息检查系统中是否已安装所述第二应用,若系统中已安装第二应用,则安装所述第一应用并移除所述第二应用。

[0027] 第十三方面,提供一种处理应用方法,包括:接收应用的第一安装包,所述第一安

安装包对应于第一数字证书,且所述第一安装包包含所述第一数字证书的公钥和第一验证信息;接收所述应用的第二安装包,所述第二安装包对应于第二数字证书,且所述第二安装包包含所述第二数字证书的公钥和第二验证信息;根据所述第一数字证书、所述第一验证信息、与所述第二数字证书的公钥以及所述第二验证信息验证所述第二安装包对应的应用是否为所述第一安装包对应的应用的新版本;当验证成功时,利用新版本的应用覆盖旧版本的引用。

[0028] 第十四方面,提供一种终端,包括:发送单元,用于向应用服务器发送请求,所述请求用于请求第一应用的安装包和包含所述第一应用的应用信息列表;所述应用信息列表中包括所述第一应用的标识符和至少一个第二应用的标识符,所述第二应用是所述第一应用的旧版本,所述第一应用的标识符和所述第二应用的标识符不同;检查单元,用于根据所述第二应用的标识符检查系统中是否已安装所述第二应用,若系统中已安装第二应用,则安装所述第一应用并移除所述第二应用。

[0029] 第十五方面,提供一种终端,包括:发送单元,用于向应用服务器发送请求,所述请求用于请求第一应用的安装包和包含所述第一应用的应用信息列表;所述应用信息列表中包括所述第一应用的证书信息和至少一个第二应用的证书信息,所述第二应用是所述第一应用的旧版本,所述第一应用的证书信息和所述第二应用的证书信息不同;检查单元,用于根据所述第二应用的证书信息检查系统中是否已安装所述第二应用,若系统中已安装第二应用,则安装所述第一应用并移除所述第二应用。

[0030] 第十六方面,提供一种终端,包括:第一接收单元,用于接收应用的第一安装包,所述第一安装包对应于第一数字证书,且所述第一安装包包含所述第一数字证书的公钥和第一验证信息;第二接收单元,用于接收所述应用的第二安装包,所述第二安装包对应于第二数字证书,且所述第二安装包包含所述第二数字证书的公钥和第二验证信息;验证单元,用于根据所述第一数字证书、所述第一验证信息、与所述第二数字证书的公钥以及所述第二验证信息验证所述第二安装包对应的应用是否为所述第一安装包对应的应用的新版本;当验证成功时,利用新版本的应用覆盖旧版本的引用。

[0031] 本实施例中,当两个终端共享应用时,不仅共享该应用的安装包,还共享该应用的共享数据,避免接收端去应用服务器下载该共享数据,方便了接收端用户的操作,提高用户体验。

附图说明

[0032] 为了更清楚地说明本实施例的技术方案,下面将对本实施例中所需要使用的附图作简单地介绍,显而易见地,下面所描述的附图仅仅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。

[0033] 图1是根据本实施例的终端间应用共享的方法的示意性流程图。

[0034] 图2是根据本实施例的终端间应用共享的方法的示意性流程图。

[0035] 图3是根据本实施例的终端间应用共享的方法的流程图。

[0036] 图4是根据本实施例的终端间应用共享的方法的流程图。

[0037] 图5是根据本实施例的终端间应用共享的方法的流程图。

- [0038] 图6是根据本发明实施例的应用共享的UI场景图。
- [0039] 图7是根据本发明实施例的验证应用安全性的方法的示意性流程图。
- [0040] 图8是根据本发明实施例的验证应用安全性的方法的示意性流程图。
- [0041] 图9是根据本发明实施例的验证应用安全性的方法的流程图。
- [0042] 图10是根据本发明实施例的判断是应用是官方引用的流程图。
- [0043] 图11是根据本发明实施例的验证应用安全性的方法的流程图。
- [0044] 图12是根据本发明实施例的验证应用安全性的方法的流程图。
- [0045] 图13是根据本发明实施例的处理应用方法的示意性流程图。
- [0046] 图14是根据本发明实施例的处理应用方法的流程图。
- [0047] 图15是根据本发明实施例的处理应用方法的流程图。
- [0048] 图16是根据本发明实施例的处理应用方法的流程图。
- [0049] 图17是根据本发明实施例的终端的示意性框图。
- [0050] 图18是根据本发明实施例的另一终端的示意性框图。
- [0051] 图19是根据本发明实施例的终端的示意性框图。
- [0052] 图20是根据本发明实施例的另一终端的示意性框图。
- [0053] 图21是根据本发明实施例的终端的示意性框图。
- [0054] 图22是根据本发明实施例的应用服务器的示意性框图。
- [0055] 图23是根据本发明实施例的终端的示意性框图。
- [0056] 图24是根据本发明实施例的应用服务器的示意性框图。
- [0057] 图25是根据本发明实施例的终端的示意性框图。
- [0058] 图26是根据本发明实施例的终端的示意性框图。

具体实施方式

[0059] 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的一部分实施例,而不是全部实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例,都应属于本发明保护的范围。

[0060] 应理解,本发明实施例中的终端包括但不限于移动电话、移动电脑、平板电脑、个人数字助理(Personal Digital Assistant,PDA)、媒体播放器、智能电视、智能手表、智能眼镜、智能手环等。

[0061] 还应理解,本发明实施例中的应用可以是应用在Android平台上的应用,也可以是应用在iOS平台上的应用。例如,当该应用是Android平台上的应用时,该应用的安装包通常为以“.apk”为后缀名的文件,即Android平台下应用的安装包文件为appname.apk。该apk文件通常包含:META-INF文件夹,AndroidManifest.xml,classes.dex,resources.arsc等。

[0062] 图1是根据本发明实施例的终端间应用共享的方法的示意性流程图。该方法包括:

[0063] 110、第一终端根据已安装的应用生成应用的共享应用安装包。

[0064] 120、第一终端将共享应用安装包发送给第二终端,以便于第二终端安装共享应用安装包。

[0065] 130、第一终端确定已安装的应用的共享数据,共享数据为源自应用服务器的、应

用运行时所需的数据。

[0066] 应理解,第一终端确定共享数据的方式可以有多种,例如,第一终端在应用共享时,逐个查看该应用的数据,搜索出哪些是共享数据;或者,预先对该应用的数据进行分类,记录共享数据的存储位置,在应用共享时,从共享数据的存储位置提取出该共享数据即可。

[0067] 140、第一终端将共享数据发送给第二终端,以便于第二终端在运行共享应用时使用共享数据。

[0068] 本发明实施例中,当两个终端共享应用时,不仅共享该应用的安装包,还共享该应用的共享数据,避免接收端去应用服务器下载该共享数据,方便了接收端用户的操作,提高用户体验。

[0069] 在现有技术中,某些应用的正常使用除了需要安装包,还需要具有一些其他数据文件。例如地图类应用,如果仅向目标终端传送地图类应用的安装包,目标终端运行该安装包后,仍需要去应用服务器下载地图数据才能正常使用。但是,下载地图数据对终端的流量耗费大。

[0070] 进一步地,第一终端与第二终端通过无线局域网(例如,通过蓝牙、WiFi、WLAN等)或者有线的传输方式传输上述共享数据,避免了接收端去应用服务器下载该共享数据造成的流量消耗问题。

[0071] 应注意,步骤130中的共享数据源自应用服务器提供具体可指:该共享数据的最初来源是应用服务器,并非指该共享数据是第一终端从应用服务器下载的,该共享数据可以是第一终端从应用服务器下载的,也可以是第一终端从其他终端获得的。例如,地图类应用的开发者会将设计好的地图数据放到应用服务器上,以供下载;终端可以根据自己的实际需要去应用服务器下载相应的地图。

[0072] 应注意,步骤130中的共享数据是运行应用时所需的数据,具体可指该应用正常运行所必须的数据,也可以指该应用运行时可能需要从应用服务器下载的数据。例如,该应用为地图类应用,需要一些基本的地图数据才能启动该应用,那么该共享数据可包括该基本的地图数据;或者,该应用为游戏应用,当需要实现某些游戏功能时,需要获得应用服务器提供的对应的游戏数据,那么该共享数据可包括该游戏数据。

[0073] 进一步地,图1的方法中,第一终端还可以向第二终端发送其他数据,例如,共享第一终端的一些隐私数据,如第一终端的游戏记录、第一终端的好友列表等。

[0074] 进一步地,共享数据存储在第一终端的公用数据文件中,步骤130可包括:从公用数据文件中提取共享数据。

[0075] 具体地,终端上每个应用对应一个公用数据文件夹,上述共享数据存放在该公用数据文件夹中。在终端间应用共享时,除了传输安装包,发送端从该公用数据文件夹中选出上述共享数据即可。

[0076] 可选地,第一终端还可包括隐私数据文件,隐私数据文件包括第一终端运行应用时产生的、与第一终端的用户关联的隐私数据。

[0077] 上述隐私数据具体可指与用户本身强相关的数据,例如,用户的账号信息、用户的好友列表、用户的聊天记录、用户的游戏记录、用户使用该应用所产生的缓存文件、用户使用下载软件下载的数据文件、用相机拍摄的照片、用户自己标识出的隐私文件等,这些数据是与用户本身强相关的,是用户特别关心的,即应用的隐私数据。

[0078] 可选地,公用数据文件和隐私数据文件在第一终端的存储路径为运行安装包时、按照安装包的指示定义的存储路径。

[0079] 具体地,终端在运行该安装包时,根据安装包的指示会自动建立预先定义的路径,该路径中包含公用数据文件和隐私数据文件各自的存放位置。该路径可以是该应用的开发者预先在安装包中定义好的,也可以是应用服务器定义的。

[0080] 可选地,公用数据文件和隐私数据文件在第一终端的存储路径为第一终端定义的存储路径。换句话说,该公用数据文件和隐私数据文件的存储路径还可以是终端自己定义的,例如,终端在解压该应用时,自动建立与该应用对应的文件存储体系,该体系指明了公用数据文件夹和隐私数据文件夹各自的存储路径。

[0081] 可选地,作为一个实施例,共享数据为应用服务器提供的离线数据包中的数据,在步骤130之前,图1的方法还可包括:记录离线数据包中数据的存储位置;步骤130可包括:从记录的存储位置中提取离线数据包中的数据作为共享数据。

[0082] 举例说明,第一终端从应用服务器下载离线数据包,在解析该离线数据包时,建立离线数据包中的文件与存储路径的对应关系的列表。当共享应用时,根据该列表即可提取出离线数据包中的数据,并发送至第二终端。

[0083] 可选地,作为一个实施例,第一终端可包括公用数据文件和隐私数据文件,公用数据文件包括源自应用服务器提供的、应用运行时所需的下载数据,隐私数据文件包括第一终端运行应用时生成的、与第一终端的用户关联的隐私数据,步骤130可包括:第一终端从公用数据文件和隐私数据文件中选择共享数据。

[0084] 以Android的App为例举例说明,Android引用除了包含appname.apk文件之外,还可包括public data(对应于上述公用数据文件)和private data(对应于上述隐私数据文件)两个数据文件。其中public data中存储于应用强相关的数据,即公用数据;private data中存储与用户强相关的数据,即隐私数据。

[0085] 具体地,区分应用的数据为公用数据或隐私数据的方法可以如下:

[0086] 例如,可以判断数据是与应用本身强相关的数据,还是与用户本身强相关的数据。与应用本身强相关的数据可以看作是应用的公用数据,与用户本身强相关的数据可以看作是应用的隐私数据。具体地,与应用本身强相关的数据可以为应用的配置文件、应用的离线数据文件、应用的数据库文件等,比如游戏应用的资源文件、地图类应用的离线地图。此类数据仅与各个应用自身相关,即应用的公用数据。与用户本身强相关的数据可以是用户比较关心的数据,比如:用户的账号信息、用户的好友列表、用户的聊天记录、用户的游戏记录、用户使用该应用所产生的缓存文件、用户使用下载软件下载的数据文件、用相机拍摄的照片、用户自己标识出的隐私文件等,这些数据是与用户本身强相关的,是用户特别关心的,即应用的隐私数据。

[0087] 若移动终端不能明确的判断某些数据文件是属于公用数据文件还是隐私数据文件,可以通过移动终端引导用户设置已安装的应用所产生的数据文件保存在存放公用数据文件的路径下还是存放隐私数据文件的路径下。

[0088] 或者,可以根据所共享应用之外的其他应用是否能够访问该共享应用的某些数据文件来判断是公用数据文件还是隐私数据文件。若所共享应用之外的其他应用能够访问该共享应用的某些数据文件,则这些数据文件为公用数据文件;若所共享应用之外的其他应

用不能访问该共享应用的某些数据文件,则这些数据文件为隐私数据文件。

[0089] 可选地,公用数据文件和隐私数据文件在第一终端的存储路径为运行安装包时、按照安装包的指示定义的存储路径。

[0090] 可选地,公用数据文件和隐私数据文件在第一终端的存储路径为第一终端定义的存储路径。

[0091] 上文中结合图1,从第一终端的角度详细描述了根据本发明实施例的终端间应用共享的方法,下面将结合图2,从第二终端的角度描述根据本发明实施例的终端间应用共享的方法。

[0092] 应理解,第二终端侧描述的第一终端与第二终端的交互及相关特性、功能等与第一终端侧的描述相应,为了简洁,适当省略重复的描述。

[0093] 图2是根据本发明实施例的终端间应用共享的方法的示意性流程图。该方法包括:

[0094] 210、第二终端从第一终端接收应用的共享应用安装包,并接收应用的共享数据,共享数据为源自应用服务器的、应用运行时所需的数据;

[0095] 上述应用的共享应用安装包时由第一终端根据已安装的该应用生成的。

[0096] 220、第二终端存储共享数据。

[0097] 本发明实施例中,当两个终端共享应用时,不仅共享该应用的安装包,还共享该应用的共享数据,避免接收端去应用服务器下载该共享数据,方便了接收端用户的操作,提高用户体验。

[0098] 可选地,作为另一实施例,图2的方法还包括:将共享数据存储在第一终端的公用数据文件中。

[0099] 根据本发明的实施例,公用数据文件在第一终端的存储路径为运行安装包时、按照安装包的指示定义的存储路径。

[0100] 根据本发明的实施例,公用数据文件在第一终端的存储路径为第一终端定义的存储路径。

[0101] 根据本发明的实施例,共享数据为应用服务器提供的离线数据包中的数据。

[0102] 下面结合具体例子,更加详细地描述本发明实施例。应注意,图3至图6的例子仅仅是为了帮助本领域技术人员理解本发明实施例,而非要将本发明实施例限于所例示的具体数值或具体场景。本领域技术人员根据所给出的图3至图6的例子,显然可以进行各种等价的修改或变化,这样的修改或变化也落入本发明实施例的范围内。

[0103] 应理解,图3至图5中的移动终端A对应于图1与图2中的第一终端;移动终端B对应于图1与图2中的第二终端。

[0104] 图3和图4的实施例均是将应用的数据分别存放在公用数据文件夹和隐私数据文件夹,该公用数据文件夹中存放与应用强相关的数据,包括上述共享数据;该隐私数据文件夹中存放与用户强相关的数据。应用共享时,可以将公用数据文件夹中的全部或部分共享给对端,同时,也可以将部分或全部隐私数据文件共享给对端,本发明实施例对此不作具体限定。图3和图4的区别在于该公用数据文件夹和隐私数据文件夹的存储路径的定义者不同。

[0105] 图3是根据本发明实施例的终端间应用共享的方法的流程图。图3的方法中,公用数据文件夹和隐私数据文件夹的存储路径在安装包中定义,即运行安装包时就会生成对应

的存储路径。

[0106] 310、在应用S的安装包中定义应用S的公用数据文件存放在什么路径,隐私数据文件存放在什么路径。应用S的数据文件,按照类别存放至相应的路径。

[0107] 320、移动终端A下载应用S并安装。

[0108] 330、移动终端A在运行应用S的过程中产生数据文件,移动终端A按照应用S的定义将应用S运行过程中产生的数据文件存放在相应的路径。

[0109] 340、移动终端A共享已安装的应用S给移动终端B,移动终端A提取用户A选择的所要共享的应用S的安装包。默认情况下,移动终端A向移动终端B共享应用S时,共享应用S的安装包和所有公用数据文件,包括公用数据的配置文件,不共享应用S的隐私数据文件。可选的,在应用S的公用数据文件中,可以标识出应用S的哪些公用数据文件是必须的,哪些公用数据文件是可选的;也可以在移动终端A中自定义,在移动终端A的显示面板上提供用户选项,由用户A在移动终端A上输入,选择要共享应用S的哪些数据文件。

[0110] 350、移动终端A提取用户A所要共享的应用S的公用数据文件及隐私数据文件的路径,并打包允许共享的应用S的数据文件及应用S的安装包文件,其中包括每个数据文件对应的路径和哈希。上述打包允许共享的应用S的数据文件,可以是打包应用S的所有公用数据文件,也可以是打包标识出的应用S所必须的公用数据文件,还可以是打包用户A在移动终端A的显示面板上所选择的数据文件。此外,打包的文件中包含每个数据文件对应的路径和哈希,目的是验证这些数据文件的完整性。

[0111] 360、移动终端A通过蓝牙、WiFi发送打包后的允许共享的应用S的数据文件及应用S的安装包文件给移动终端B。

[0112] 370、移动终端B检测接收到的应用S的安装包的完整性,若具备完整性则安装应用S;否则移动终端B丢弃接收到的安装包,向移动终端A请求新的安装包或终止操作。

[0113] 检测安装包的完整性的具体方法为:计算接收到的允许共享的应用S的数据文件的哈希值,与接收到的哈希结果进行比对,若相等则认为接收到的允许共享的数据文件具备完整性;若计算得到的结果与接收到的哈希结果比对发现不相等,则认为接收到的允许共享的数据文件不具备完整性。

[0114] 380、移动终端B安装接收到的共享应用S后,提取共享应用S的公用数据文件和隐私数据文件的路径,并将所共享的数据文件存放在应用S定义的路径。

[0115] 本发明实施例中,当两个终端共享应用时,不仅共享该应用的安装包,还共享该应用的公用数据文件和隐私数据文件中的数据,提高了应用共享的灵活性。

[0116] 进一步地,在应用共享时,当共享的数据中包含从应用服务器下载的数据时,目标终端无需再去应用服务器获取该下载数据,从而节省了目标终端的流量,并简化了用户的操作。

[0117] 在本发明实施例中,并非所有步骤都是必选的,例如,步骤350、370、380等就可以不执行。顺序执行步骤310、320、330、340、360,能够实现“移动终端A向移动终端B共享应用的安装包文件和应用的公用数据文件”的基本功能。若执行步骤350中的“打包每个数据文件对应的路径和哈希”,则执行步骤370中的“验证数据文件的完整性”,哈希主要是用于验证完整性的。步骤380“安装接收到的共享应用后,提取共享应用的文件路径,将文件分类别存放在应用定义的路径”是可选的,不执行步骤380并不影响用户安装并使用接收到的共享

应用;执行步骤380主要是为下一次的共享做准备。

[0118] 在本发明的具体实施方式中,移动终端A的存储单元用于存储应用的安装包文件和数据文件。应用的数据文件包括应用的公用数据文件和应用隐私数据文件。例如,应用的安装包存放在所述存储单元的appname.apk中,应用的公用数据文件存放在所述存储单元的“public data”文件夹中,应用的隐私数据文件存放在所述存储单元的“private data”文件夹中。

[0119] 移动终端A的处理器单元用于在运行应用S的过程中,将产生的公用数据文件和隐私数据文件按照类别分别存放至所述存储单元的相应路径。

[0120] 移动终端A的处理器单元还用于调用存储在存储单元内的应用S的安装包文件和应用S的公用数据文件。默认情况下,移动终端A的处理器单元用于调用存储在存储单元内的应用S的安装包文件和应用S的所有公用数据文件,包括公用数据的配置文件,不调用应用S的隐私数据文件。可选的,移动终端A的处理器单元也用于识别出在应用S的所有公用数据文件中,应用S的哪些公用数据文件是必须的,应用S的哪些公用数据文件是可选的;移动终端A的处理器单元还用于通过识别用户A在其显示面板上的操作,判断调用存储在存储单元内的哪些数据文件。

[0121] 移动终端A的处理器单元用于调用存储在存储单元内的应用S的公用数据文件及隐私数据文件的相应路径,并打包所调用的应用S的数据文件及应用S的安装包文件,其中包括每个数据文件所对应的存储单元的相应路径和由处理器单元所计算的每个数据文件的哈希。这里提到的移动终端A的处理器单元打包所调用的应用S的数据文件,可以是打包应用S的所有公用数据文件,也可以是打包处理器单元识别出的应用S所必须的公用数据文件,还可以是打包处理器单元识别出的用户A在移动终端A的输入单元所选择的数据文件,具体为用户A在移动终端A的显示面板上所选择的数据文件。此外,移动终端A的处理器单元还包括一个验证模块,用于验证数据文件的完整性。

[0122] 移动终端A通过通信单元将存储单元所调用的打包后的应用S的数据文件及应用S的安装包文件发送给移动终端B,所述通信单元可以是蓝牙模块、WiFi模块。

[0123] 移动终端B的处理器单元还用于检测接收到的应用S的安装包文件的完整性,若具备完整性则安装应用S;否则移动终端B的处理器单元丢弃接收到的安装包,向移动终端A发送请求新的安装包文件的指令或终止操作的指令。

[0124] 移动终端B的处理器单元检测安装包文件的完整性的具体方法为:移动终端B的处理器单元的计算模块用于计算其存储单元所接收到的应用S的数据文件的哈希值,并与存储单元所接收到的哈希值进行比对,若二者相等则认为存储单元所接收到的数据文件具备完整性;若处理器单元的计算模块计算得到的哈希值与存储单元所接收到的哈希值比对结果不相等,则存储单元所接收到的数据文件不具备完整性。

[0125] 若移动终端B的处理器单元检测结果为安装包文件具备完整性,则移动终端B将接收到的数据文件存放在其存储单元的相应路径。

[0126] 图4是根据本发明实施例的终端间应用共享的方法的流程图。图4的方法中,公用数据文件夹和隐私数据文件夹的存储路径由终端自己定义,即运行安装包时,终端会自己选择各个文件夹的存储路径。

[0127] 410.移动终端A定义应用S的公用数据存放在什么路径,应用S的隐私数据存放在

什么路径。应用S的数据文件,按照类别存放至相应的路径。

[0128] 420.移动终端A下载应用S并安装。

[0129] 430.移动终端A在运行应用S的过程中产生数据文件,按照移动终端A的定义,移动终端A将应用S运行过程中产生的数据文件存放在相应的路径。

[0130] 440.移动终端A共享已安装的应用S给移动终端B,移动终端A提取用户A选择的所要共享的应用S的安装包文件。

[0131] 默认情况下,移动终端A向移动终端B共享应用S时,共享应用S的安装包文件和所有公用数据文件,包括公用数据的配置文件,不共享隐私数据文件。可选的,在应用S的公用数据文件中,可以标识出应用S的哪些公用数据文件是必须的,哪些公用数据文件是可选的;也可以在移动终端A中自定义,在移动终端A的显示面板上提供用户选项,由用户A在移动终端A上输入,选择要共享应用S的哪些数据文件。

[0132] 450.移动终端A提取用户A所要共享的应用S的公用数据文件及隐私数据文件的路径,并打包允许共享的应用S的数据文件及应用S的安装包文件,其中包括每个数据文件对应的路径和哈希。

[0133] 这里提到的打包允许共享的应用S的数据文件,可以是应用S的所有公用数据文件,也可以是标识出的应用S所必须的公用数据文件,还可以是用户A在移动终端A的显示面板上所选择的数据文件。此外,打包的文件中包含每个数据文件对应的路径和哈希,目的是验证这些数据文件的完整性。

[0134] 460.移动终端A通过蓝牙、WiFi发送打包后的允许共享的应用S的数据文件及应用S的安装包文件给移动终端B。

[0135] 470.移动终端B检测接收到的应用S的安装包文件的完整性,若具备完整性则安装应用S;否则移动终端B丢弃接收到的安装包文件,向移动终端A请求新的安装包文件或终止操作。

[0136] 检测安装包文件的完整性的具体方法为:计算接收到的允许共享的应用S的数据文件的哈希值,与接收到的哈希结果进行比对,若相等则认为接收到的允许共享的数据文件具备完整性;若计算得到的结果与接收到的哈希结果比对发现不相等,则认为接收到的允许共享的数据文件不具备完整性。

[0137] 480.移动终端B安装接收到的共享应用S后,提取共享应用S的公用数据文件和隐私数据文件的路径,并将所共享的数据文件存放在移动终端A定义的路径。

[0138] 本发明实施例中,当两个终端共享应用时,不仅共享该应用的安装包,还共享该应用的公用数据文件和隐私数据文件中的数据,提高了应用共享的灵活性。

[0139] 进一步地,在应用共享时,当共享的数据中包含从应用服务器下载的数据时,目标终端无需再去应用服务器获取该下载数据,从而节省了目标终端的流量,并简化了用户的操作。

[0140] 同样地,在本发明实施例中,步骤410、420、430主要描述应用S的数据存储方法,步骤440、450、460、470、480主要描述分享应用S的方法。

[0141] 在本发明实施例中,并非全部步骤均是必选的,可以根据实际情况进行调整,例如,可以不执行步骤450、470、480。顺序执行步骤410、420、430、440、460,能够实现“移动终端A向移动终端B共享应用的安装包文件和应用的公用数据文件”的基本功能。若执行步骤

450中的“打包每个数据文件对应的路径和哈希”，则执行步骤470中的“验证数据文件的完整性”，哈希主要是用于验证完整性的。步骤480“安装接收到的共享应用后，提取共享应用的文件路径，将文件分类别存放在移动终端定义的路径”可做可不做，不执行步骤480并不影响用户安装并使用接收到的共享应用；执行步骤8主要是为下一次的共享做准备。

[0142] 图5是根据本发明实施例的终端间应用共享的方法的流程图。图5的方法中，并非通过定义公用文件夹和隐私文件夹的方式选择可共享数据的。本发明实施例的关键点在于，移动终端对用户下载的应用的离线数据包中的所有数据文件进行识别，并将识别出的所有已下载的离线数据文件保存为一个列表。离线数据包是指将在线的数据按照功能或类别分别打包，提供用户下载。下载下来的离线数据包是一个压缩包，打开该压缩包，可以看到其所包含的多个离线数据文件。下载离线数据包后，用户的移动终端不需要联网，就可以使用应用的相应功能。

[0143] 510. 移动终端A下载应用S并安装。

[0144] 520. 移动终端A在运行应用S的过程中，下载应用S的离线数据包。

[0145] 530. 移动终端A对已下载的应用S的离线数据包中的所有文件进行识别，并将所有已下载的离线数据文件保存为一个列表，列表中包含离线数据文件的名称及相应的路径。

[0146] 540. 移动终端A共享应用S给移动终端B。

[0147] 默认情况下，共享应用S时，共享应用S的安装包文件和应用S所保存的列表中的离线数据文件；也可以在移动终端A中自定义，在移动终端A的显示面板上提供用户选项，由用户A在移动终端A的显示面板上输入，选择要共享应用S的哪些离线数据文件。

[0148] 550. 移动终端A提取所要共享的应用S的安装包文件，并根据移动终端A所保存的应用S的列表信息中的路径提取相应的离线数据文件。

[0149] 560. 移动终端A打包允许共享的应用S的离线数据文件及安装包文件，其中包括每个文件对应的路径和哈希。

[0150] 打包的文件中包含每个文件对应的路径和哈希，目的是验证这些文件的完整性。

[0151] 570. 移动终端A通过蓝牙、WiFi发送打包后的允许共享的应用S的离线数据文件及应用S的安装包文件给移动终端B。

[0152] 580. 移动终端B检测接收到的应用S的安装包文件的完整性，若具备完整性则安装应用S；否则用户B丢弃接收到的应用S的安装包文件，向移动终端A请求应用S的新的安装包文件或终止操作。

[0153] 检测安装包文件的完整性的具体方法为：计算接收到的允许共享的应用S的数据文件的哈希值，与接收到的哈希结果进行比对，若相等则认为接收到的允许共享的数据文件具备完整性；若计算得到的结果与接收到的哈希结果比对发现不相等，则认为接收到的允许共享的数据文件不具备完整性。

[0154] 590. 移动终端B安装接收到的共享应用S后，提取共享应用S的离线数据文件的路径，并将所共享的应用S的离线数据文件存放在移动终端A定义的路径。

[0155] 本发明实施例中，可共享数据中包含从应用服务器下载的数据，目标终端无需再去应用服务器获取该下载数据，从而节省了目标终端的流量，并简化了用户的操作。

[0156] 在本发明实施例中，步骤510、520、530主要描述应用S的数据存储方式，步骤540至步骤590主要描述分享应用S的方式。

[0157] 在本发明实施例中,并非全部步骤均是必选的,可以根据实际情况调整,例如,可以不执行步骤550、560、580、590。顺序执行步骤510、520、530、540、570,能够实现“移动终端A向移动终端B共享应用的安装包文件和离线数据文件”的基本功能。若执行步骤5中的“提取安装包文件和离线数据文件”,以及步骤560中的“打包每个数据文件对应的路径和哈希”,则执行步骤580中的“验证数据文件的完整性”,哈希主要是用于验证完整性的。步骤590“安装接收到的共享应用后,提取共享应用的离线数据文件路径,将离线数据文件存放在移动终端定义的路径”可做可不做,不执行步骤590并不影响用户安装并使用接收到的共享应用;执行步骤590主要是为下一次的共享做准备。

[0158] 具体地,移动终端A的存储单元用于存储应用S的安装包文件和应用S的离线数据文件。

[0159] 移动终端A的处理器单元用于在运行应用S的过程中,下载应用S的离线数据包至应用S的存储单元。

[0160] 移动终端A的处理器单元还用于识别所述已下载的应用S的离线数据包中的所有文件,并将所有已下载的应用S的离线数据文件保存为一个离线数据文件列表,存放至应用S的存储单元。其中,离线数据文件列表中包含离线数据文件的名称及离线数据文件在应用S的存储单元的相应路径。

[0161] 移动终端A的处理器单元还用于调用存储在存储单元内的应用S的安装包文件和应用S的离线数据文件列表中的离线数据文件。

[0162] 默认情况下,移动终端A的处理器单元用于调用存储在存储单元内的应用S的安装包文件和应用S的离线数据文件列表中的所有离线数据文件。可选的,移动终端A的处理器单元也可以用于通过识别用户A在其显示面板上的操作,判断调用存储在存储单元内的哪些离线数据文件。

[0163] 移动终端A的处理器单元还用于调用存储在存储单元内的应用S的安装包文件及离线数据文件列表,根据离线数据文件列表中的相应路径调用存储在存储单元内的应用S的离线数据文件,并打包所调用的应用S的安装包文件及应用S的离线数据文件。此外,移动终端A的处理器单元计算每个离线数据文件的哈希。这里提到的移动终端A的处理器单元打包所调用的应用S的离线数据文件,可以是应用S的离线数据文件列表中的所有离线数据文件,也可以是处理器单元识别出的用户A在移动终端A的输入单元所选择的离线数据文件,具体为用户A在移动终端A的显示面板上所选择的离线数据文件。此外,移动终端A的处理器单元还包括一个验证模块,用于验证安装包文件和离线数据文件的完整性。

[0164] 移动终端A通过通信单元将存储单元所调用的打包后的应用S的离线数据文件及应用S的安装包文件发送给移动终端B,所述通信单元可以是蓝牙模块、WiFi模块。

[0165] 移动终端B的处理器单元还用于检测接收到的应用S的安装包文件的完整性,若具备完整性则安装应用S;否则移动终端B的处理器单元丢弃接收到的安装包文件,向移动终端A发送一条请求新的安装包文件的指令或终止操作的指令。移动终端B的处理器单元检测安装包文件的完整性的具体方法为:移动终端B的处理器单元的计算模块计算其存储单元所接收到的应用S的数据文件的哈希值,并与存储单元所接收到的哈希值进行比对,若二者相等则认为存储单元所接收到的数据文件具备完整性;若处理器单元的计算模块计算得到的哈希值与存储单元所接收到的哈希值比对结果不相等,则存储单元所接收到的数据文件

不具备完整性。若移动终端B的处理器单元检测结果为安装包文件具备完整性,则移动终端B将接收到的离线数据文件存放在其存储单元的相应路径。

[0166] 以上结合图3-图5详细描述了引用的共享方法,下面给出本发明实施例的UI实现实施例。

[0167] 图6是根据本发明实施例的应用共享的UI场景图。具体步骤如下:

[0168] 第一步、移动终端A获取到用户A在移动终端A的显示面板上长按应用S的图标这一操作后,移动终端A的显示面板上呈现“好友共享”的标签提示用户分享应用。

[0169] 第二步、移动终端A获取到用户A在移动终端A的显示面板上选择“好友共享”标签这一操作后,移动终端A的显示面板上呈现通信链路的列表供用户选择,以使用户A可以通过选择所述移动终端A的显示面板上呈现的通信链路向用户B共享应用S。

[0170] 第三步、当移动终端A检测到用户A选择某个所述通信链路后,移动终端A提取应用S的安装包文件和应用S的公用数据文件,并打包应用S的安装包文件和应用S的公用数据文件,通过用户A在移动终端A的显示面板上选定的某个通信链路将打包后的应用S的安装包文件和应用S的公用数据文件发送给用户B的移动终端B,实现共享应用的目的。

[0171] 在现有技术中,同Google Play一样,亚马逊和腾讯应用商店中也拥有不少质量上乘的应用,但用户直接从网上下载Android应用却依旧存在着不少风险,因为网络中虽然拥有不少优质应用,但也有可能包含很多恶意软件和盗版应用。因此,谷歌宣布修改应用商店政策:Google play全面禁止应用自动升级。

[0172] 根据已有的应用推荐的方案(如通过推送应用链接或传送应用安装包的形式等),可以实现终端针对特定用户进行应用的推荐和共享。

[0173] 终端不能保证其推荐的应用是否来源合法(如非官方应用),则若安装了之后会给终端带来一定的安全隐患。

[0174] 图7是根据本发明实施例的验证应用安全性的方法的示意性流程图。图7的方法包括:

[0175] 710、第一终端接收应用的第一安装包,并从第一安装包中提取验证信息,验证信息用于确定第一安装包是否源自应用服务器。

[0176] 本发明实施例对第一终端的第一安装包的来源不作具体限定,例如,可以来从其他终端接收,或者从其他路径下载。

[0177] 720、第一终端根据验证信息确定第一安装包是否源自应用服务器。

[0178] 可选地,每个正版的安装包中包含某种标识信息,第一终端从第一安装包中提取出该标识信息,验证其真伪,即可判断出该第一安装包是否源自应用服务器;或者,该第一终端提取出第一安装包的签名、数字证书、哈希等信息,并将上述信息发送至应用服务器,以便应用服务器从正版的安装包中提取出上述信息对应的信息进行比较,确定该第一安装包是否为正版安装包(即是否源自应用服务器)。

[0179] 730、当第一安装包不是源自应用服务器时,第一终端从应用服务器获取应用的第二安装包,并用第二安装包覆盖第一安装包。

[0180] 740、当第一安装包源自应用服务器时,第一终端运行第一安装包。

[0181] 本发明实施例中,在第一终端获取安装包后,从安装包中提取验证信息,并根据该验证信息验证该安装包是否源自应用服务器,提高了应用安装的安全性。

[0182] 可选地,作为一个实施例,步骤720可包括:向应用服务器发送验证信息,以便应用服务器根据验证信息与源信息的匹配,检验第一安装包是否源自应用服务器,其中源信息为应用服务器从第二安装包中提取的;接收应用服务器的检验结果。

[0183] 图8是根据本发明实施例的验证应用安全性的方法的示意性流程图。图8的方法包括:

[0184] 810、应用服务器接收第一终端发送的验证信息,验证信息是第一终端从应用的第一安装包中提取的,且验证信息用于确定第一安装包是否源自应用服务器;

[0185] 820、应用服务器从应用服务器中存储的应用的第二安装包中提取源信息;

[0186] 830、应用服务器根据源信息与验证信息的匹配确定第一安装包是否源自应用服务器,并向第一终端发送匹配的结果。

[0187] 本发明实施例中,在第一终端获取第一安装包后,从第一安装包中提取验证信息,并将验证信息发送至应用服务器,应用服务器根据该验证信息与源信息的匹配检测该第一安装包是否源自应用服务器,提高了应用安装的安全性。

[0188] 下面结合具体例子,更加详细地描述本发明实施例。应注意,图9至图12的例子仅仅是为了帮助本领域技术人员理解本发明实施例,而非要将本发明实施例限于所例示的具体数值或具体场景。本领域技术人员根据所给出的图9至图12的例子,显然可以进行各种等价的修改或变化,这样的修改或变化也落入本发明实施例的范围内。

[0189] 图9是根据本发明实施例的验证应用安全性的方法的流程图。本发明实施例四的关键点:移动终端对获取到的应该安装包文件进行验证,此处提到的验证可包含:移动终端对安装包的完整性验证以及应用服务器对安装包的合法性验证。完整性验证是由移动终端对获取到的应用安装包的验证,确保该安装包是未被恶意篡改。合法性验证是由应用服务器对移动终端上传的安装包文件的信息作验证,与正版应用安装包文件作比对,排除盗版应用的安装包文件。该方法包括:

[0190] 901.移动终端B获取到一个应用安装包文件,这个安装包文件不是从官方的应用服务器下载的,可以是其他移动终端共享给移动终端B的安装包文件也可以是从其他途径获取的(如第三方应用服务器)。

[0191] 902.移动终端B对获取到的应用安装包文件执行安装操作。

[0192] 903.在安装之前,移动终端B对该安装包文件作完整性的验证。

[0193] 904、移动终端B成功验证了安装包文件的完整性之后,提取出该安装包文件的相关信息(这个相关信息可以是安装包文件的包名、签名、证书信息、hash值、版本信息等)。

[0194] 905.移动终端B将上步骤提取出来的信息发送到对应的应用服务器作后续的验证处理。

[0195] 906.应用服务器接收到移动终端B提取的安装包文件信息,并对该安装包文件作合法性验证。

[0196] 关于步骤906的比对情况可以参照图10。

[0197] 907.假设移动终端B的安装包文件通过了应用服务器的合法性验证,应用服务器将给移动终端B发送确认信息,表示该应用安装包文件属于正版应用可正常安装。

[0198] 908.移动终端B正常安装该应用的安装包文件。

[0199] 909.移动终端B安装了该应用安装包文件之后,应用服务器会对移动终端B这一合

法的安装作记录,方便后续与该应用相关的操作(如更新和升级消息的推送等)。

[0200] 910.假设移动终端B的安装包文件未通过了应用服务器的合法性验证,应用服务器将给移动终端B发送相关的提示(如提示该应用安装包文件与正版应用的安装包文件不匹配),并发送对应的正版应用的安装包文件。

[0201] 911.移动终端B接收应用服务器的提供的正版应用的安装包文件并安装。

[0202] 912.移动终端B安装了该正版应用的安装包文件之后,应用服务器会对移动终端B的合法安装作记录,方便后续与该应用相关的操作(如更新和升级消息的推送等)。

[0203] 本发明实施例中,在目标终端获取安装包后,从安装包中提取验证信息,并在引用服务器端检验该安装包是否为官方应用,提高了应用安装的安全性。

[0204] 在图9的实施例中,顺序执行步骤901、902、904、905、906、907、908、909,能够实现“移动终端B接收移动终端A发送的应用安装包文件并将该安装包发送至应用服务器作合法性认证,若安装包文件合法则正常安装,若安装包文件非法则替换成正版应用安装包文件”的基本功能。步骤902“移动终端B对获取到的应用安装包文件进行完整性验证”可做可不做,不影响方案的执行,但执行了步骤902后能保证移动终端B接收到的应用安装包在发送过程中未被篡改。

[0205] 具体地,移动终端A的存储器单元用于存储移动终端A上安装或未安装的应用安装包文件,对应于相应的存储路径。

[0206] 移动终端A的处理器单元用于根据某应用安装包的存储路径将移动终端A上的存储器单元存储的某个应用安装包文件传送至移动终端A的输出单元。这一过程实现移动终端A给移动终端B发送一个应用安装包文件的操作。

[0207] 移动终端B的输入单元用于接收移动终端A发送过来的应用安装包文件,并送到移动终端B上的处理器单元进行处理。

[0208] 移动终端B的处理器单元包含提取模块、验证模块、安装模块等。

[0209] 移动终端B的处理器单元用于将输入单元获取到的安装包文件,处理器单元中的验证模块用于提取该安装包文件的相关信息作完整性验证,验证成功后由验证模块将该安装包文件送至移动终端B的输出单元。其中,相关信息可以是安装包文件的哈希值,公钥信息等。

[0210] 移动终端B的处理器单元的输出单元将该安装包文件发送至应用服务器做合法性验证。

[0211] 图10是根据本发明实施例的判断是应用是官方引用的流程图,包括:

[0212] 1001、对安装包文件作完整性验证;

[0213] 1002、以安装包文件的包名作为索引信息查找对应的官方应用安装包文件;

[0214] 1003、将该安装包文件与官方应用的安装包文件作签名及版本信息的比对;

[0215] 1004、证书相同,版本相同即判断该安装包文件为官方应用;

[0216] 1005、证书相同,版本不同即需要根据版本的高低分情况处理;

[0217] 1006、证书不同,版本不同即判断该安装包文件为非官方应用;

[0218] 1007、判断该安装包文件版本信息是否高于官方应用安装包文件的版本信息;

[0219] 1008、默认该应用合法,允许该安装包文件的安装;

[0220] 1009、向用户确认是否用官方最新版本替换当前旧版本;

[0221] 1010、替换为正版的官方应用的安装包文件；

[0222] 1011、正常安装应用的安装包文件后，由应用服务器记录下该移动终端的安装信息。

[0223] 图11是根据本发明实施例的验证应用安全性的方法的流程图。本发明实施例的关键点在于，在移动终端未联网的情况下，移动终端对获取的安装包文件进行完整性验证，安装该应用安装包文件，但由于未联网验证，故安装好的应用不能正常使用，等到联网后由应用服务器进行合法性验证之后，该应用能正常使用。

[0224] 1101.移动终端B获取到一个应用安装包文件，这个安装包文件不是从官方应用服务器下载的，可以是其他移动终端共享的安装包也可以是从其他途径获取的（如第三方应用服务器）；

[0225] 1102.移动终端B对获取到的应用安装包文件执行安装操作，在安装之前，移动终端B对该安装包文件作完整性的验证；

[0226] 1103.移动终端B安装该应用安装包文件；

[0227] 1104.由于该安装包文件未经过合法性验证（移动终端B未联网），故安装之后的应用图标显示为灰色且不能正常使用，且移动终端B会对这些灰显的应用进行记录，等到联网后作后续的合法性验证；

[0228] 1105.联网后，移动终端B将灰色图标的应用的相关信息（如安装包的包名、签名、证书信息、hash值、版本信息等）发送到应用服务器去进行合法性的验证；

[0229] 1106.联网后的合法性验证与图9的实施例情况类似，可参照图9的实施例；

[0230] 1107.经应用服务器确认并记录后，灰色图标的应用正常显示并可正常使用。

[0231] 本发明实施例中，顺序执行步骤1101、1103、1104、1105、1106、1107，能够实现“移动终端B在未联网时，接收移动终端A发送的应用安装包文件并安装，但由于未经过应用服务器进行合法性验证，故安装之后的应用不能正常使用，等到移动终端B连网时再将该安装包文件送至应用服务器作合法性认证，若安装包文件合法则正常安装，若安装包文件非法则替换成正版应用安装包文件”的基本功能。步骤1102“移动终端B对获取到的应用安装包文件进行完整性验证”可做可不做，不影响方案的执行，但执行了步骤1102后能保证移动终端B接收到的应用安装包在发送过程中未被篡改。

[0232] 图12是根据本发明实施例的验证应用安全性的方法的流程图。本发明实施例的关键点在于，在移动终端未联网的情况下，移动终端对获取的安装包文件进行完整性验证，安装该应用安装包文件，安装之后的应用能正常使用。但由于未联网验证，移动终端要对该应用作下未验证的记录，等到联网后由应用服务器再进行合法性验证。

[0233] 1201.移动终端B获取到一个应用安装包文件，这个安装包文件不是从官方应用服务器下载的，可以是其他移动终端共享的安装包文件也可以是从其他途径获取的（如第三方应用服务器）；

[0234] 1202.移动终端B对获取到的应用安装包文件执行安装操作，在安装之前，移动端B对该安装包文件作完整性的验证；

[0235] 1203.移动终端B在安装该应用安装包文件时，移动终端B提示要求打开“允许未知来源的安装”（默认情况下移动终端关闭此项设置）；

[0236] 1204.移动终端B安装该应用，安装之后该应用可以正常使用；

[0237] 1205. 移动终端B对未联网时安装的应用作记录,等到联网后作后续的合法性验证;

[0238] 1206. 联网后,移动终端B将步骤1205作了记录的应用的相关信息(如安装包的包名、签名、证书信息、hash值、版本信息等)发送到应用服务器去进行合法性的验证;

[0239] 1207. 联网后的合法性验证与图9的实施例情况类似。

[0240] 本发明实施例中,顺序执行步骤1201、1203、1204、1205、1206、1207,能够实现“移动终端B在未联网时,接收移动终端A发送的应用安装包文件并安装,且安装之后的应用能正常使用,但由于未经过应用服务器进行合法性验证,故等到移动终端B连网时再将该安装包文件送至应用服务器作合法性认证,若安装包文件合法则仍可继续正常使用,若安装包文件非法则替换成正版应用安装包文件”的基本功能。步骤1202“移动终端B对获取到的应用安装包文件进行完整性验证”可做可不做,不影响方案的执行,但执行了步骤1202后能保证移动终端B接收到的应用安装包在发送过程中未被篡改。

[0241] 在现有技术中,搭载Android操作系统的电子移动终端越来越多,根据调查机构IDC最新统计数据,Android系统在第三季度已经占到全球智能机市场份额的75%。Android开源和免费的特点,使得各个厂商能够根据自己的需求定制不同的ROM,开发者也可以根据厂商开源的代码编译系统,从而使得整个Android市场更加活跃,部分开发者会在编译系统的时候,对一些应用进行重新签名。

[0242] Google Play是谷歌为Android平台建立的官方应用市场,谷歌同时允许第三方应用市场的存在,国内如,机锋市场,安致市场,小米市场,智慧云市场,百度市场等应用市场层出不穷,开发者可以在多个市场上提交应用,而各个市场有独立的提交和审核机制,开发者在各个市场上提交的应用可以是不同的,也可能因为审核等原因导致当前上架的应用不同,包括版本,签名的数字证书等。

[0243] Android中所有应用都需要经过签名才能正常安装,签名的过程是,先将应用编译成zip文件包,然后对文件包中的所有文件进行哈希,并用MANIFEST.MF文件记录所有哈希值,再对MANIFEST.MF文件以及文件中所有的哈希值进行哈希,并用CERT.SF来记录,最后,使用数字证书中的私钥对*.SF中的记录进行加密,并将加密结果和数字证书信息(公钥和数字证书的其他基本信息)存放在*.RSA文件中。(*一般为数字证书的名字)。

[0244] 现有技术中,如果终端接收到某个应用的新版本,例如应用的包名、版本号、数字签名证书等更新时,在终端上同时存储新旧版本,浪费存储资源。

[0245] 图13是根据本发明实施例的处理应用方法的示意性流程图。图13的方法可以由终端执行,该方法包括:

[0246] 1310、接收第一应用的安装包,该安装包中包括第一应用的标识符和第二应用的标识符,第二应用是第一应用的旧版本,例如,第一应用的标识符可以是第一应用的唯一标识符,第二应用的标识符可以是第二应用的唯一标识符;

[0247] 1320、根据第二应用的标识符检查系统中是否已安装第二应用,若系统中已安装第二应用,则安装第一应用并移除第二应用。

[0248] 本发明实施例中,在接收到第一应用的安装包时,根据该安装包中携带的旧版本的标识符,检测系统中是否安装有该第一应用的旧版本,当检测出旧版本的应用时,移除该旧版本的应用,从而节省了终端的存储资源。

[0249] 下面结合图14至图16,详细说明如何确定接收到的应用为终端上已经存储的应用的新版本。

[0250] 图14是根据本发明实施例的处理应用方法的流程图。图14的方法包括:

[0251] 1401. 在移动终端上安装应用S的版本V1,记录应用S的信息,包括包名,版本号,签名数字证书信息等,应用S的版本V1使用包名APP_S,并由开发者使用数字证书C签名。

[0252] 1402. 下载安装应用S版本V2的APK并开始安装,应用S的版本V2使用包名APP_S2,并由开发者添加了一个标签<old_package android:name="APP_S" version:name="1.0">,用来指示应用S的前一个版本的包名和版本号;使用数字证书C签名。

[0253] 1403. 移动终端提取应用S版本V2的APK的信息。

[0254] 1404. 根据是否有<old_package>标签判断是否有旧版本信息;若有,转至1405,否则,转至1406。

[0255] 1405. 解析旧版本信息,获取旧版本的包名,版本号,签名数字证书等信息。

[0256] 1406. 按照现有技术进行正常安装;

[0257] 1407. 判断系统中是否已安装应用的V1版本;

[0258] 1408. 检测应用V1版本和应用V2版本的签名数字证书是否一致,若一致,进入步骤1409,否则,进入步骤1410;

[0259] 1409. 覆盖安装应用的V1版本,并在系统中记录V2版本的信息

[0260] 1410. 提示用户正在安装的应用有安全风险,并终止安装。

[0261] 在本发明的实施例中,顺序执行步骤1401、1402、1403、1404、1405、1407、1408以及1409,能够实现“移动终端覆盖安装更换了包名的应用S新版本的覆盖升级”,步骤1410是在应用S的版本V2签名与版本V1出现冲突时,给予用户的额外提示,不给于用户提示,也可以。

[0262] 具体地,可以利用终端的以下模块进行上述流程的操作:

[0263] 处理单元的下载模块用于下载应用S的APK;

[0264] 处理单元的安装模块用于下载模块下载应用S的APK之后安装应用S;

[0265] 处理单元的提取模块用于安装模块开始安装应用S之后提取应用S的APK的信息;

[0266] 处理单元的解析模块用于解析提取模块提取的应用S的APK的版本信息;

[0267] 处理单元的判断模块用于根据解析模块解析的应用S的APK的信息判断系统中是否已经安装应用S的V1版本,若已经安装,则激活处理单元的检测模块;

[0268] 处理单元的检测模块用于检测应用S的V1版本与应用S的V2版本签名是否一致;

[0269] 处理单元的用户提示模块用于在检测模块检测到应用有风险后给用户以相应提示;

[0270] 移动终端的通信单元用于提供处理单元中的下载模块进行应用S的APK的下载;

[0271] 下面提供一种处理应用的方法,包括:

[0272] 应用服务器维护第一应用列表,所述应用列表包含所述应用服务器上的应用的基本信息,所述基本信息包括应用的以下信息中的一种或多种:版本号、报名、签名、数字证书;

[0273] 当第一应用的所述基本信息更新时,所述应用服务器更新所述第一应用列表中的所述第一应用的所述基本信息;

[0274] 所述应用服务器向安装了所述第一应用的终端发送信息,所述信息用于指示所述

终端更新所述第一应用的基本信息。

[0275] 下面提供另一种处理应用的方法,包括:

[0276] 终端维护第二应用列表,所述第二应用列表包含所述终端上的应用的基本信息,所述基本信息包括应用的以下信息中的一种或多种:版本号、报名、签名、数字证书;

[0277] 当所述终端的第一应用的所述基本信息更新时,所述终端接收应用服务器发送的指示信息,所述指示信息用于更新所述第二应用列表中所述第一应用的所述基本信息。

[0278] 图15是根据本发明实施例的处理应用方法的流程图。图15的方法包括:

[0279] 1501.移动终端向服务器请求下载安装使用数字证书A签名的应用S;

[0280] 1502.移动终端通知服务器更新用户的应用列表

[0281] 1503.移动终端接收服务器发送的应用S的APK和应用列表;

[0282] 1504.移动终端安装应用S,同时更新移动终端上缓存的应用列表中对应于应用S的项;

[0283] 1505.移动终端接收服务器发送的更新后的应用列表,其中,应用S的数字签名证书由开发者更新为数字证书B;

[0284] 1506.移动终端更新缓存的应用列表;

[0285] 1507.移动终端下载新版本应用S,新版本应用S由开发者使用证书B签名并发布。;

[0286] 1508.移动终端安装应用S时使用最新的应用列表来验证应用S;

[0287] 在本发明的实施例中,顺序执行1502、1503、1504、1505、1506和1508能够完成已更换数字证书信息的应用S的覆盖安装;其中,步骤1501和步骤1507均可用“从其他存储有应用S的APK的设备中获取应用S的APK来替换”。

[0288] 需要说明的是,本实施例中,开发者可以更换给应用做数字签名的数字证书,也可以更换应用的包名,还可以同时更换数字证书和包名,因为安装时是通过最新的应用列表来做验证,所以,不会出现无法覆盖安装的问题。

[0289] 具体地,移动终端的存储单元用于存储移动终端上已安装的应用列表,应用列表用于记录应用的包名,版本号,证书等信息;移动终端中的处理单元包括:请求模块,通知模块,接收模块,安装模块,更新模块,验证模块。各模块相互配合实现上述流程,具体如下:

[0290] 处理单元中的请求模块用于请求应用S的APK;

[0291] 处理单元中的通知模块用于通知服务器更新应用列表;

[0292] 处理单元中的接收模块用于接收应用S的APK和应用列表;

[0293] 处理单元中的安装模块用于在接收模块接收到应用S的APK后安装应用S;

[0294] 处理单元中的更新模块用于更新移动终端中的应用列表;

[0295] 处理单元中的验证模块用于在安装模块安装应用S时使用存储单元中存储的应用列表对应用S进行证书验证;

[0296] 移动终端的通信单元用于为处理单元中的接收模块接收应用S的APK和应用列表提供网络连接。

[0297] 下面提供一种处理应用的方法,包括:

[0298] 接收应用的第一安装包,所述第一安装包对应于第一数字证书,且所述第一安装包包含所述第一数字证书的公钥和第一验证信息;

[0299] 接收所述应用的第二安装包,所述第二安装包对应于第二数字证书,且所述第二

安装包包含所述第二数字证书的公钥和第二验证信息；

[0300] 根据所述第一数字证书、所述第一验证信息、与所述第二数字证书的公钥以及所述第二验证信息验证所述第二安装包对应的应用是否为所述第一安装包对应的应用的新版本；

[0301] 当验证成功时，利用新版本的应用覆盖旧版本的引用。

[0302] 图16是根据本发明实施例的处理应用方法的流程图。本实施例针对包名不变，数字证书更换的情况。

[0303] 1601. 在移动终端D上下载安装应用S版本V1，应用S的版本V1由应用开发者使用数字证书A签名，数字证书A的公钥和验证信息M1保存在应用的APK中；

[0304] 1602. 移动终端记录应用S版本V1中的数字证书A的公钥；

[0305] 1603. 移动终端D下载安装应用S的版本V2，应用S的版本V2是经应用开发者做过如下处理的应用：

[0306] 1) 应用开发者使用数字证书B对应的私钥对应用S版本V2的哈希值H1进行签名，得到签名后的验证信息S1

[0307] 2) 应用开发者使用数字证书A再对得到的验证信息S1进行签名，得到验证信息S2并将哈希值H1和验证信息S2保存在应用S版本V2的APK中；

[0308] 1604. 安装过程中，先使用移动终端中保存的数字证书A的公钥解密验证信息S2，得到验证信息S1；

[0309] 1605. 再使用应用中的数字证书B的公钥解密验证信息S1，得到哈希值H2，并提取APK中的H1，对比H1和H2即可完成验证。

[0310] 1606. 验证成功，继续进行应用S版本V2的安装。

[0311] 在本发明的实施例可以实现覆盖安装已经更换数字证书的应用S。

[0312] 在本发明的具体实施方式中，移动终端的存储单元用于存储应用S的信息，包括应用S的包名，版本信息，数字证书等；移动终端的处理单元包括：下载模块，记录模块，解密模块，对比模块，提取模块，安装模块等。各个模块相互配合，实现上述流程，具体实现方式如下：

[0313] 处理单元的下载模块用于下载应用S的安装包；

[0314] 处理单元的安装模块用于安装下载模块下载的应用S的安装包；

[0315] 处理单元的记录模块用于记录安装模块安装应用S时及安装应用S后应用S的信息；

[0316] 处理单元的解密模块用于解密应用S的APK中的由证书B进行数字签名的内容和由数字证书A进行数字签名的内容，得到由签名前的内容S1和H2；

[0317] 处理单元的提取模块用于提取APK中的验证信息H1；

[0318] 处理单元的对比模块用于对比由提取模块提取的验证信息H1和由解密模块解密的H2，若两者相同，安装模块继续执行安装操作；

[0319] 移动终端的通信单元用于为处理单元的下载模块下载应用S的安装包提供网络连接。

[0320] 上文中结合图1至图6，详细描述了根据本发明实施例的终端间应用共享的方法，下面将结合图17至图20，详细描述根据本发明实施例的终端。

[0321] 图17是根据本发明实施例的终端的示意性框图。图17的终端1700包括：生成单元1710、发送单元1720和确定单元1730。

[0322] 应理解，终端1700能够实现图1至图6中由第一终端（移动终端A）执行的各个步骤，为避免重复，不再详细描述。

[0323] 生成单元1710，用于根据已安装的应用生成应用的共享应用安装包；

[0324] 发送单元1720，用于将生成单元1710生成的共享应用安装包发送给第二终端，以便于第二终端安装共享应用安装包；

[0325] 确定单元1730，用于确定已安装的应用的共享数据，共享数据为源自应用服务器的、应用运行时所需的数据；

[0326] 发送单元1720还用于将确定单元1730确定的共享数据发送给第二终端，以便于第二终端在运行共享应用时使用共享数据。

[0327] 本发明实施例中，当两个终端共享应用时，不仅共享该应用的安装包，还共享该应用的共享数据，避免接收端去应用服务器下载该共享数据，方便了接收端用户的操作，提高用户体验。

[0328] 可选地，作为一个实施例，共享数据存储于终端的公用数据文件中，确定单元1730具体用于从公用数据文件中提取共享数据。

[0329] 可选地，作为另一个实施例，公用数据文件在终端的存储路径为运行安装包时、按照安装包的指示定义的存储路径。

[0330] 可选地，作为另一个实施例，公用数据文件在终端的存储路径为终端定义的存储路径。

[0331] 可选地，作为另一个实施例，共享数据为应用服务器提供的离线数据包中的数据，终端1700还包括：记录单元，用于记录离线数据包中数据的存储位置；确定单元1730具体用于从记录的存储位置中提取离线数据包中的数据作为共享数据。

[0332] 图18是根据本发明实施例的另一终端的示意性框图。图18的终端1800包括：接收单元1810和存储单元1820。

[0333] 应理解，终端1800能够实现图1至图6中由第二终端（移动终端B）执行的各个步骤，为避免重复，不再详细描述。

[0334] 接收单元1810，用于从第一终端接收应用的共享应用安装包，并接收应用的共享数据，共享数据为源自应用服务器的、应用运行时所需的数据，应用的共享应用安装包由第一终端根据已安装的应用生成的；

[0335] 存储单元1820，用于存储接收单元1810接收的共享数据。

[0336] 本发明实施例中，当两个终端共享应用时，不仅共享该应用的安装包，还共享该应用的共享数据，避免接收端去应用服务器下载该共享数据，方便了接收端用户的操作，提高用户体验。

[0337] 图19是根据本发明实施例的终端的示意性框图。图19的终端1900包括：处理器1910和发送器1920。

[0338] 应理解，终端1900能够实现图1至图6中由第一终端（移动终端A）执行的各个步骤，为避免重复，不再详细描述。

[0339] 处理器1910，用于根据已安装的应用生成应用的共享应用安装包；

[0340] 发送器1920,用于将处理器1910生成的共享应用安装包发送给第二终端,以便于第二终端安装共享应用安装包;

[0341] 处理器1910还用于确定已安装的应用的共享数据,共享数据为源自应用服务器的、应用运行时所需的数据;

[0342] 发送器1920还用于将处理器1910确定的共享数据发送给第二终端,以便于第二终端在运行共享应用时使用共享数据。

[0343] 本发明实施例中,当两个终端共享应用时,不仅共享该应用的安装包,还共享该应用的共享数据,避免接收端去应用服务器下载该共享数据,方便了接收端用户的操作,提高用户体验。

[0344] 可选地,作为一个实施例,共享数据存储于终端的公用数据文件中,处理器1910具体用于从公用数据文件中提取共享数据。

[0345] 可选地,作为另一个实施例,公用数据文件在终端的存储路径为运行安装包时、按照安装包的指示定义的存储路径。

[0346] 可选地,作为另一个实施例,公用数据文件在终端的存储路径为终端定义的存储路径。

[0347] 可选地,作为另一个实施例,共享数据为应用服务器提供的离线数据包中的数据,处理器1910还用于记录离线数据包中数据的存储位置;从记录的存储位置中提取离线数据包中的数据作为共享数据。

[0348] 图20是根据本发明实施例的另一终端的示意性框图。图20的终端2000包括:接收器2010和存储器2020。

[0349] 应理解,终端2000能够实现图1至图6中由第二终端(移动终端B)执行的各个步骤,为避免重复,不再详细描述。

[0350] 接收器2010,用于从第一终端接收应用的共享应用安装包,并接收应用的共享数据,共享数据为源自应用服务器的、应用运行时所需的数据,应用的共享应用安装包由第一终端根据已安装的应用生成的;

[0351] 存储器2020,用于存储接收器2010接收的共享数据。

[0352] 本发明实施例中,当两个终端共享应用时,不仅共享该应用的安装包,还共享该应用的共享数据,避免接收端去应用服务器下载该共享数据,方便了接收端用户的操作,提高用户体验。

[0353] 上文中结合图7至图12,详细描述了根据本发明实施例的验证应用安全性的方法,下面将结合图21至图24,详细描述根据本发明实施例的终端和应用服务器。

[0354] 图21是根据本发明实施例的终端的示意性框图。图21的终端2100包括:第一接收单元2110、提取单元2120和确定单元2130。

[0355] 应理解,图21的终端2100能够实现图7至图12中由终端执行的各个步骤,为避免重复,此处不再赘述。

[0356] 第一接收单元2110,用于接收应用的第一安装包;

[0357] 提取单元2120,用于从第一接收单元2110接收的第一安装包中提取验证信息,验证信息用于确定第一安装包是否源自应用服务器;

[0358] 确定单元2130,用于根据提取单元2120提取的验证信息确定第一安装包是否源自

应用服务器;当第一安装包不是源自应用服务器时,从应用服务器获取应用的第二安装包,并用第二安装包覆盖第一安装包;当第一安装包源自应用服务器时,运行第一安装包。

[0359] 本发明实施例中,在第一终端获取安装包后,从安装包中提取验证信息,并根据该验证信息验证该安装包是否源自应用服务器,提高了应用安装的安全性。

[0360] 可选地,作为一个实施例,确定单元2130具体用于向应用服务器发送验证信息,以便应用服务器根据验证信息与源信息的匹配,检验第一安装包是否源自应用服务器,其中源信息为应用服务器从第二安装包中提取的;接收应用服务器的检验结果。

[0361] 图22是根据本发明实施例的应用服务器的示意性框图。图22的应用服务器2200包括:接收单元2210、提取单元2220、匹配单元2230和发送单元2240。

[0362] 应理解,应用服务器2200能够实现图7至图12中由应用服务器执行的各个步骤,为避免重复,此处不再赘述。

[0363] 接收单元2210,用于接收第一终端发送的验证信息,验证信息是第一终端从应用的第一安装包中提取的,且验证信息用于确定第一安装包是否源自应用服务器;

[0364] 提取单元2220,用于从应用服务器2200中存储的应用的第二安装包中提取源信息;

[0365] 匹配单元2230,用于根据提取单元提取的源信息与接收单元接收的验证信息的匹配确定第一安装包是否源自应用服务器;

[0366] 发送单元2240,用于向第一终端发送匹配单元的匹配结果。

[0367] 本发明实施例中,在第一终端获取安装包后,从安装包中提取验证信息,并根据该验证信息验证该安装包是否源自应用服务器,提高了应用安装的安全性。

[0368] 图23是根据本发明实施例的终端的示意性框图。图23的终端2300包括:接收器2310和处理器2320。

[0369] 应理解,终端2300能够实现图7至图12中由终端执行的各个步骤,为避免重复,此处不再赘述。

[0370] 接收器2310,用于接收应用的第一安装包;

[0371] 处理器2320,用于从接收器2310接收的第一安装包中提取验证信息,验证信息用于确定第一安装包是否源自应用服务器;根据验证信息确定第一安装包是否源自应用服务器;当第一安装包不是源自应用服务器时,从应用服务器获取应用的第二安装包,并用第二安装包覆盖第一安装包;当第一安装包源自应用服务器时,运行第一安装包。

[0372] 本发明实施例中,在第一终端获取安装包后,从安装包中提取验证信息,并根据该验证信息验证该安装包是否源自应用服务器,提高了应用安装的安全性。

[0373] 可选地,作为一个实施例,处理器2320具体用于向应用服务器发送验证信息,以便应用服务器根据验证信息与源信息的匹配,检验第一安装包是否源自应用服务器,其中源信息为应用服务器从第二安装包中提取的;接收应用服务器的检验结果。

[0374] 图24是根据本发明实施例的应用服务器的示意性框图。图24的应用服务器2400包括:接收器2410、处理器2420和发送器2430。

[0375] 应理解,应用服务器2400能够实现图7至图12中由应用服务器执行的各个步骤,为避免重复,此处不再赘述。

[0376] 接收器2410,用于接收第一终端发送的验证信息,验证信息是第一终端从应用的

第一安装包中提取的,且验证信息用于确定第一安装包是否源自应用服务器;

[0377] 处理器2420,用于从应用服务器2400中存储的应用的第二安装包中提取源信息;根据源信息与接收器2410接收的验证信息的匹配确定第一安装包是否源自应用服务器;

[0378] 发送器2430,用于向第一终端发送处理器2420的匹配结果。

[0379] 本实施例中,在第一终端获取安装包后,从安装包中提取验证信息,并根据该验证信息验证该安装包是否源自应用服务器,提高了应用安装的安全性。

[0380] 上文中结合图13至图16,详细描述了根据本实施例的处理应用方法,下面将结合图25至图26,详细描述根据本实施例的终端和应用服务器。

[0381] 图25是根据本实施例的终端的示意性框图。图25的终端2500包括:接收单元2510和检查单元2520。

[0382] 应理解,终端2500能够实现图13至图16中由终端执行的各个步骤,为避免重复,此处不再赘述。

[0383] 接收单元2510,用于接收第一应用的安装包,安装包中包括第一应用的标识符和第二应用的标识符,第二应用是第一应用的旧版本;

[0384] 检查单元2520,用于根据接收单元2510接收的安装包中的第二应用的标识符检查系统中是否已安装第二应用;若系统中已安装第二应用,安装第一应用并移除第二应用。

[0385] 本实施例中,在接收到第一应用的安装包时,根据该安装包中携带的旧版本的唯一标识符,检测系统中是否安装有该第一应用的旧版本,当检测出旧版本的应用时,移除该旧版本的应用,从而节省了终端的存储资源。

[0386] 图26是根据本实施例的终端的示意性框图。图26的终端2600包括:接收器2610和处理器2620。

[0387] 应理解,终端2600能够实现图13至图16中由终端执行的各个步骤,为避免重复,此处不再赘述。

[0388] 接收器2610,用于接收第一应用的安装包,安装包中包括第一应用的标识符和第二应用的标识符,第二应用是第一应用的旧版本,例如,第一应用的标识符可以是第一应用的唯一标识符,第二应用的标识符可以是第二应用的唯一标识符;

[0389] 处理器2620,用于根据接收器2610接收的安装包中的第二应用的标识符检查系统中是否已安装第二应用;若系统中已安装第二应用,安装第一应用并移除第二应用。

[0390] 本实施例中,在接收到第一应用的安装包时,根据该安装包中携带的旧版本的唯一标识符,检测系统中是否安装有该第一应用的旧版本,当检测出旧版本的应用时,移除该旧版本的应用,从而节省了终端的存储资源。

[0391] 本领域普通技术人员可以意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本发明的范围。

[0392] 所属领域的技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的系统、装置和单元的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0393] 在本申请所提供的几个实施例中,应该理解到,所揭露的系统、装置和方法,可以

通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

[0394] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0395] 另外,在本发明各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。

[0396] 所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用,可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0397] 以上所述,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应所述以权利要求的保护范围为准。

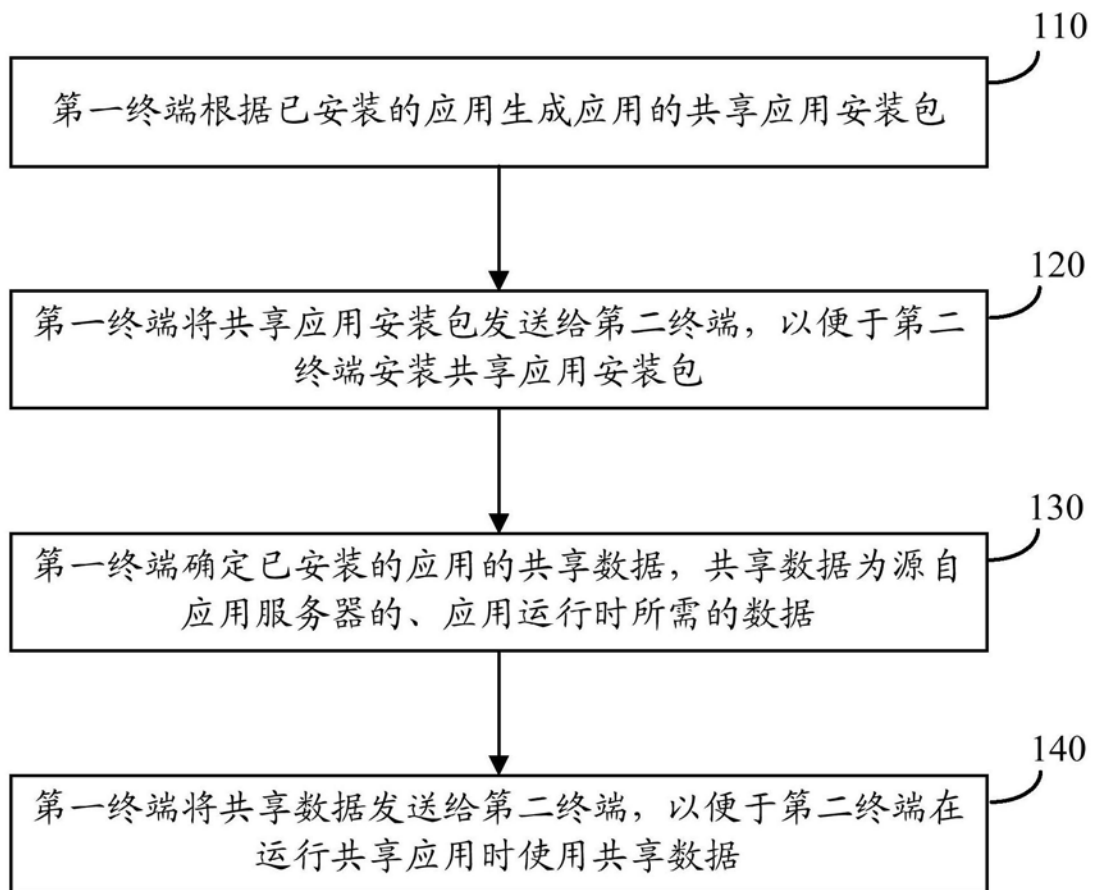


图1

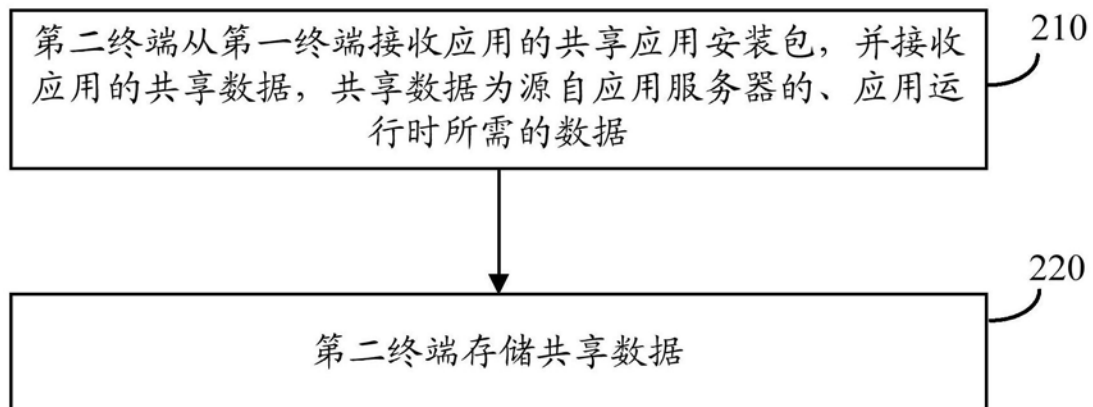


图2

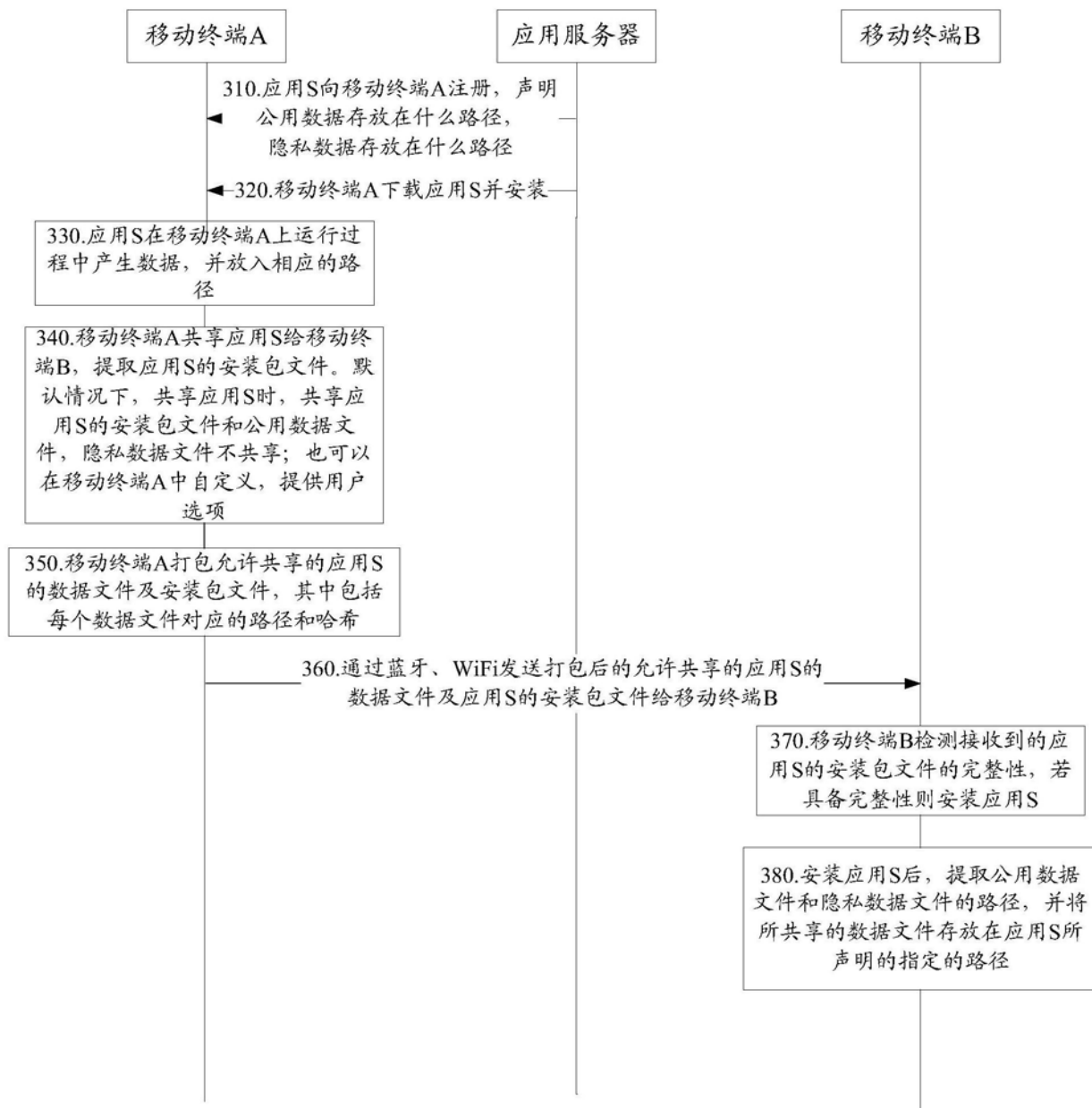


图3

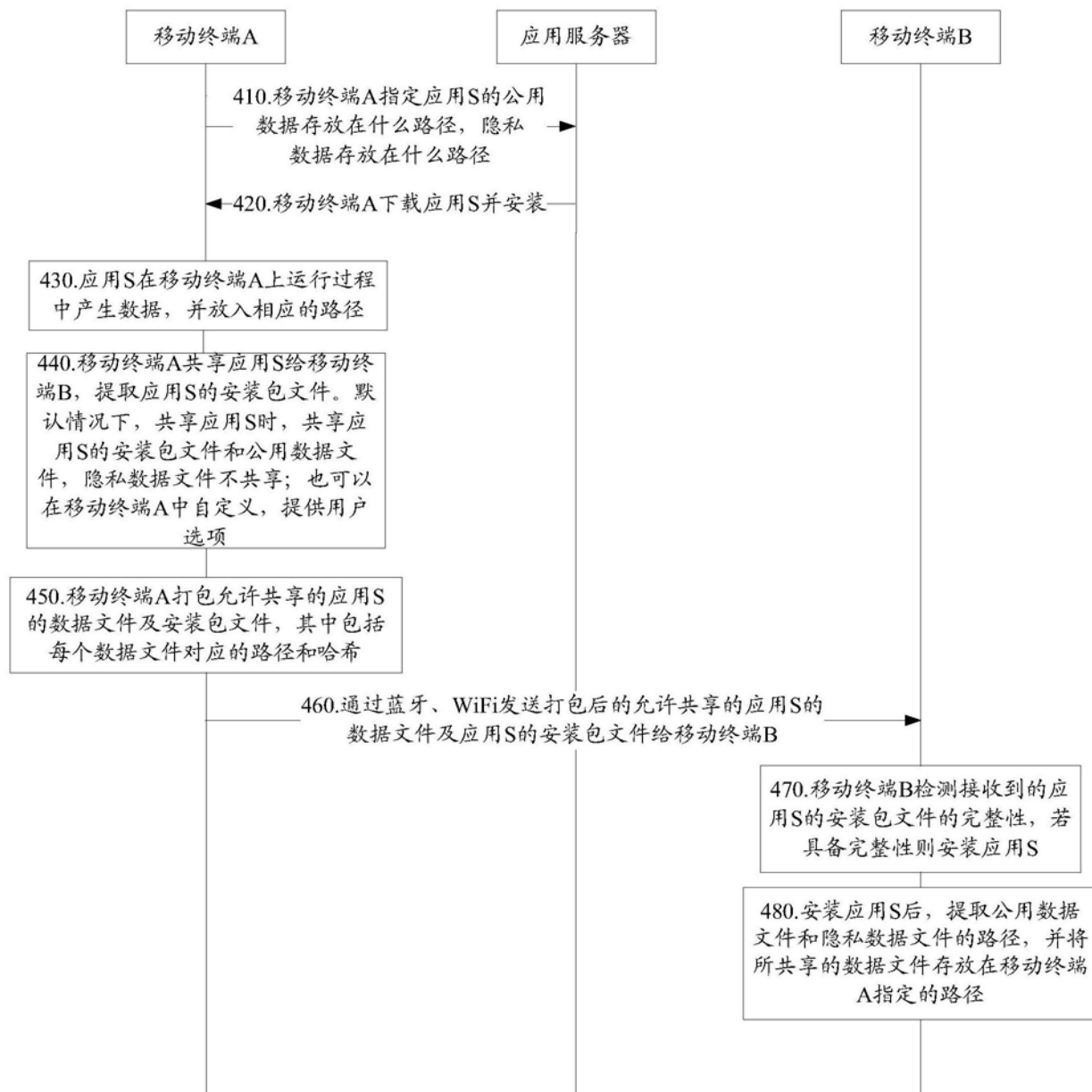


图4



图5

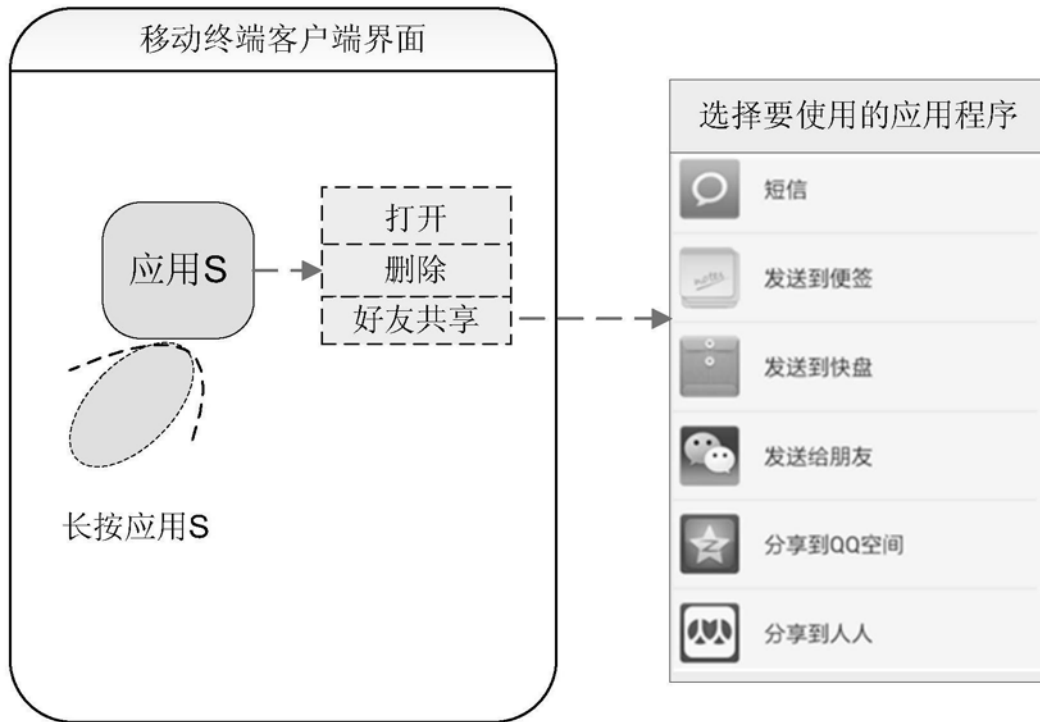


图6

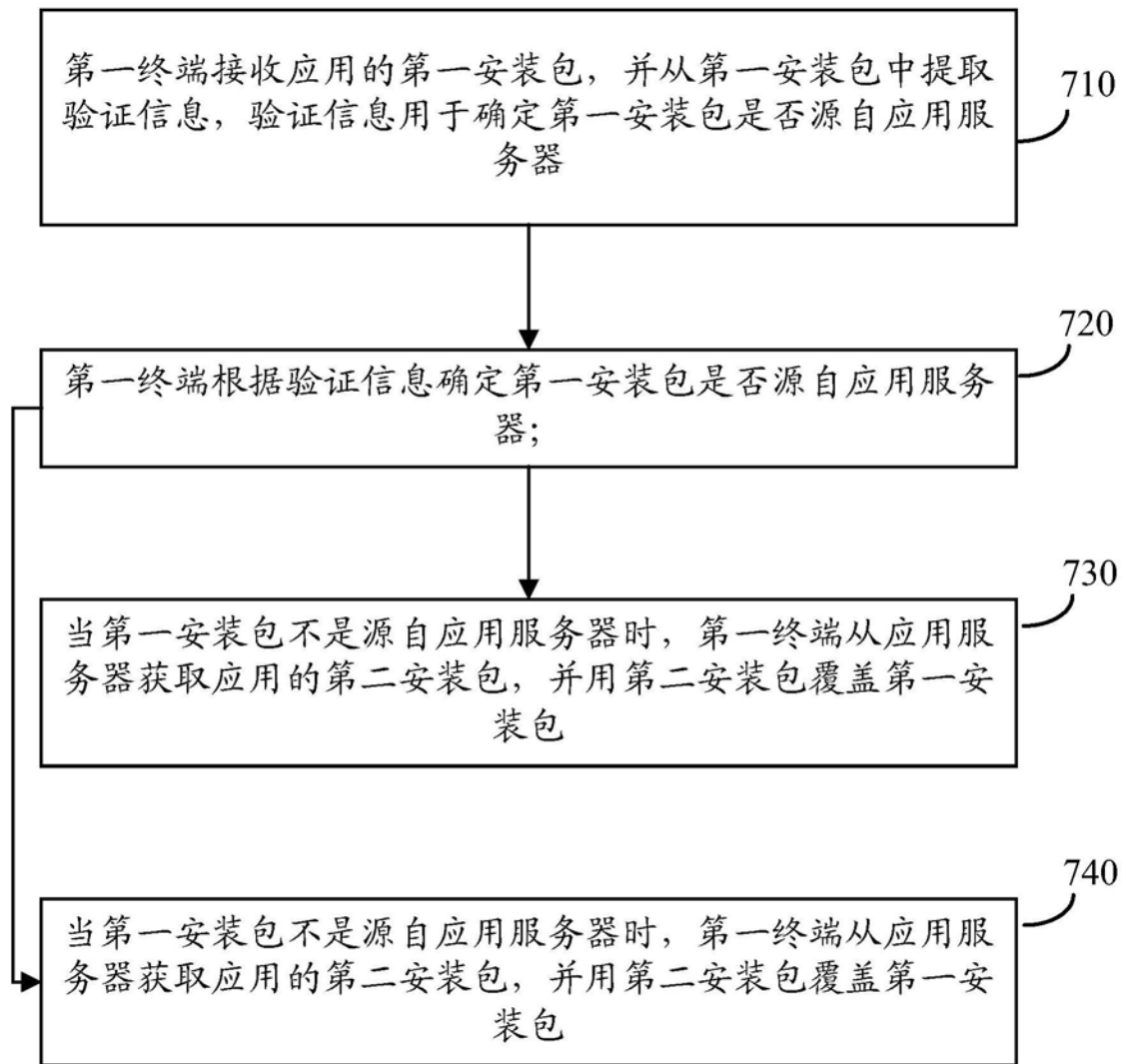


图7

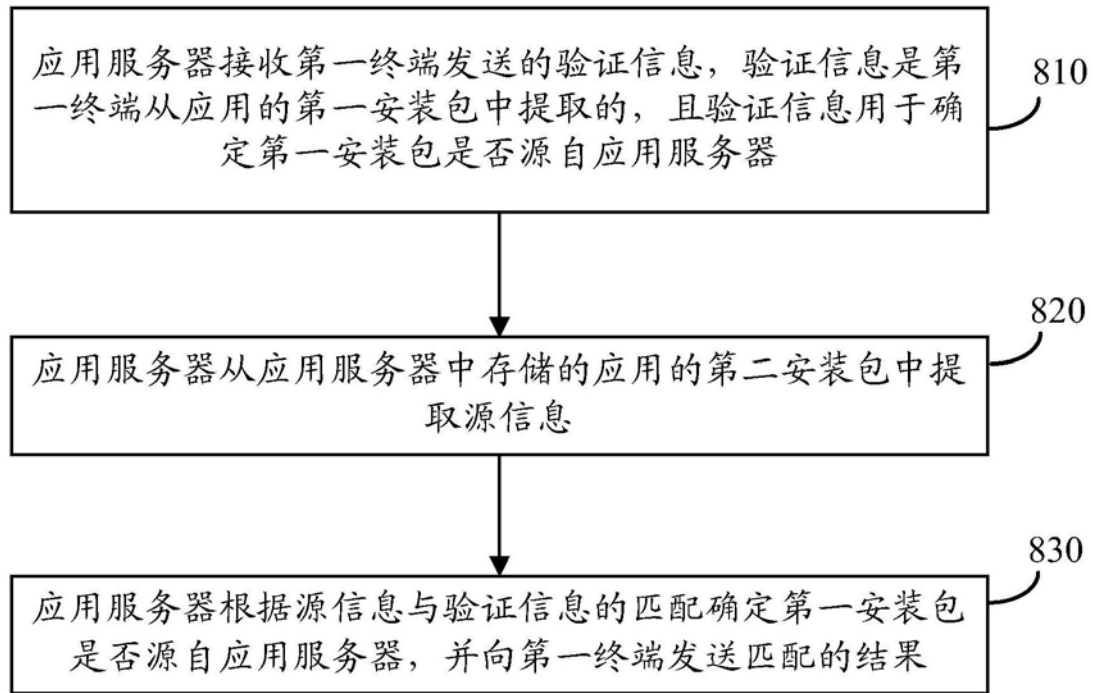


图8

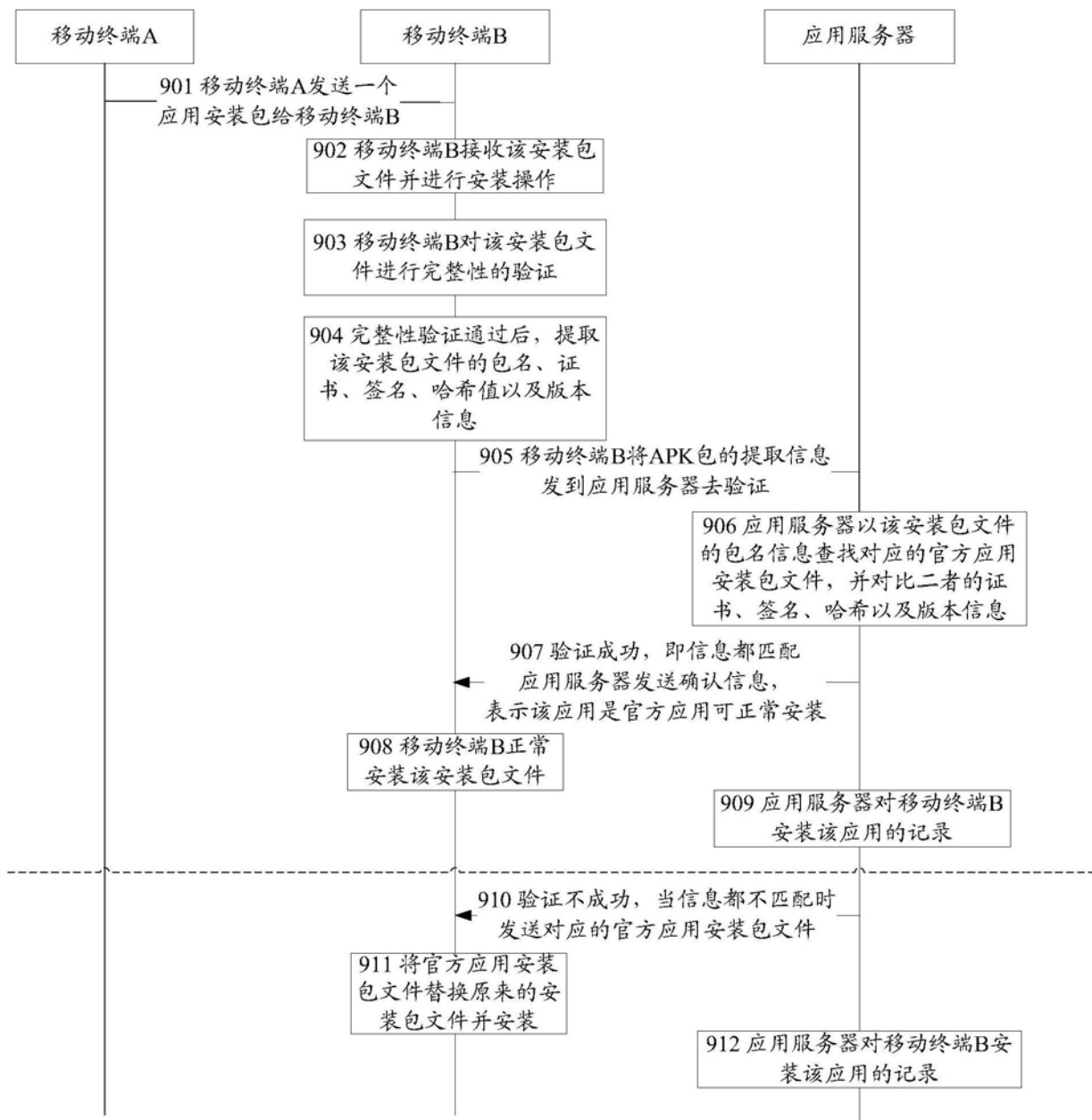


图9

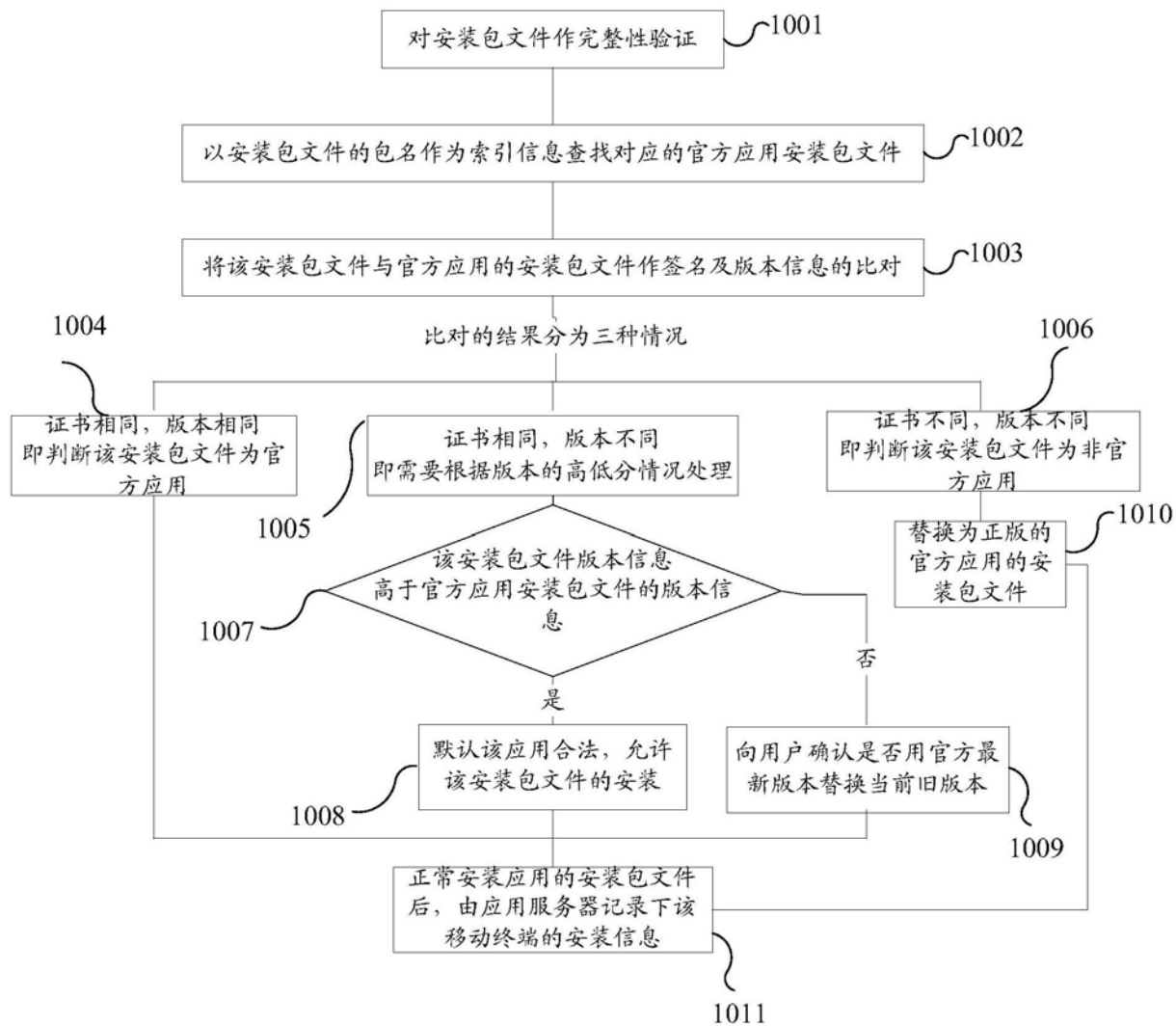


图10

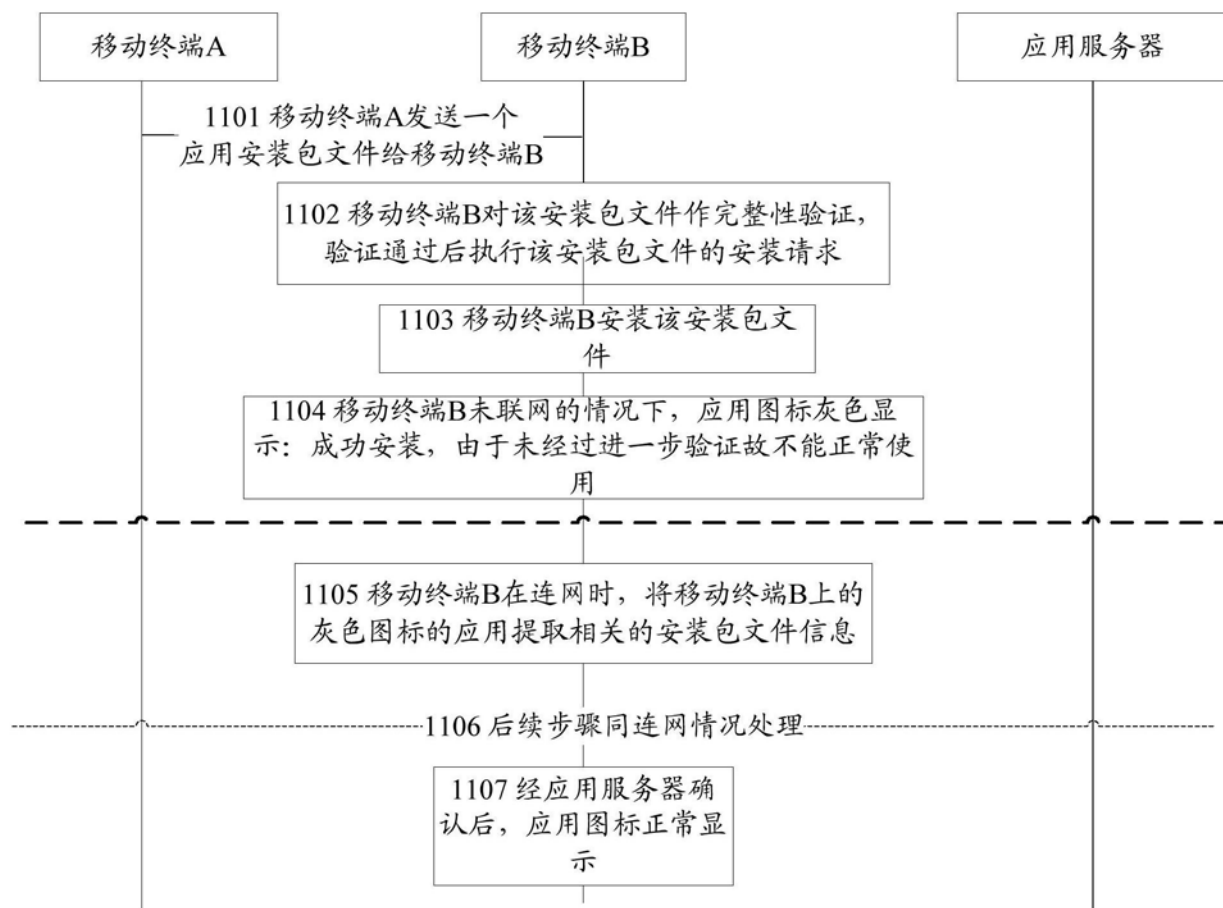


图11

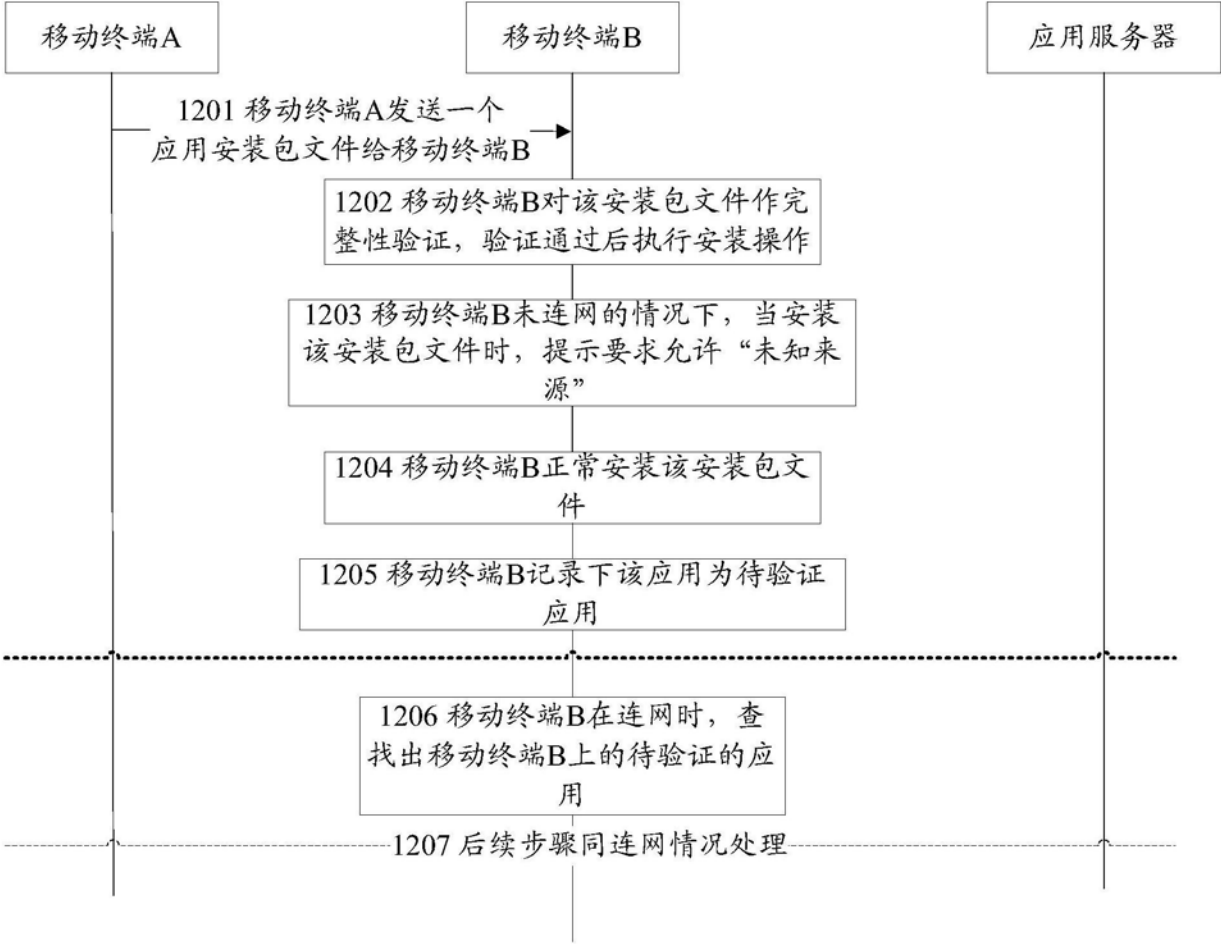


图12

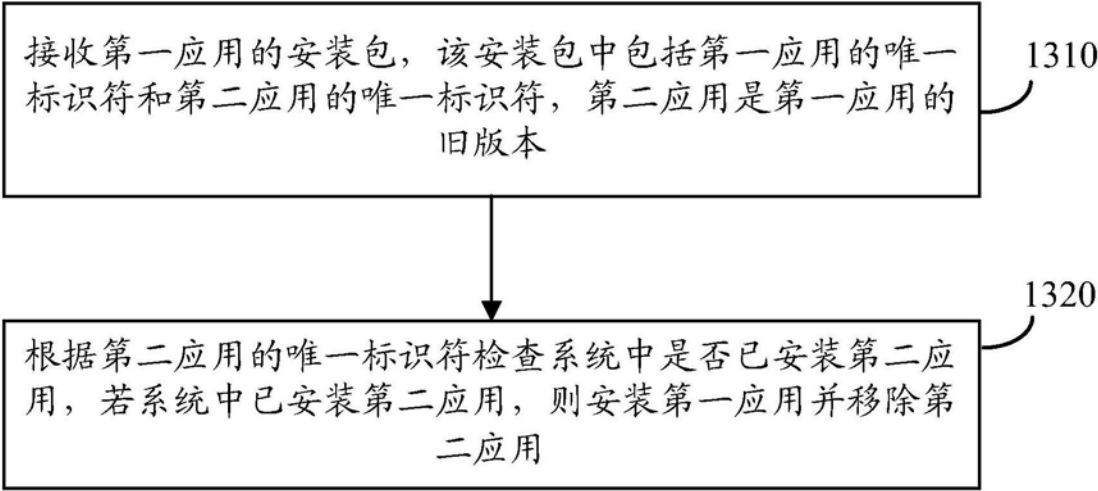


图13

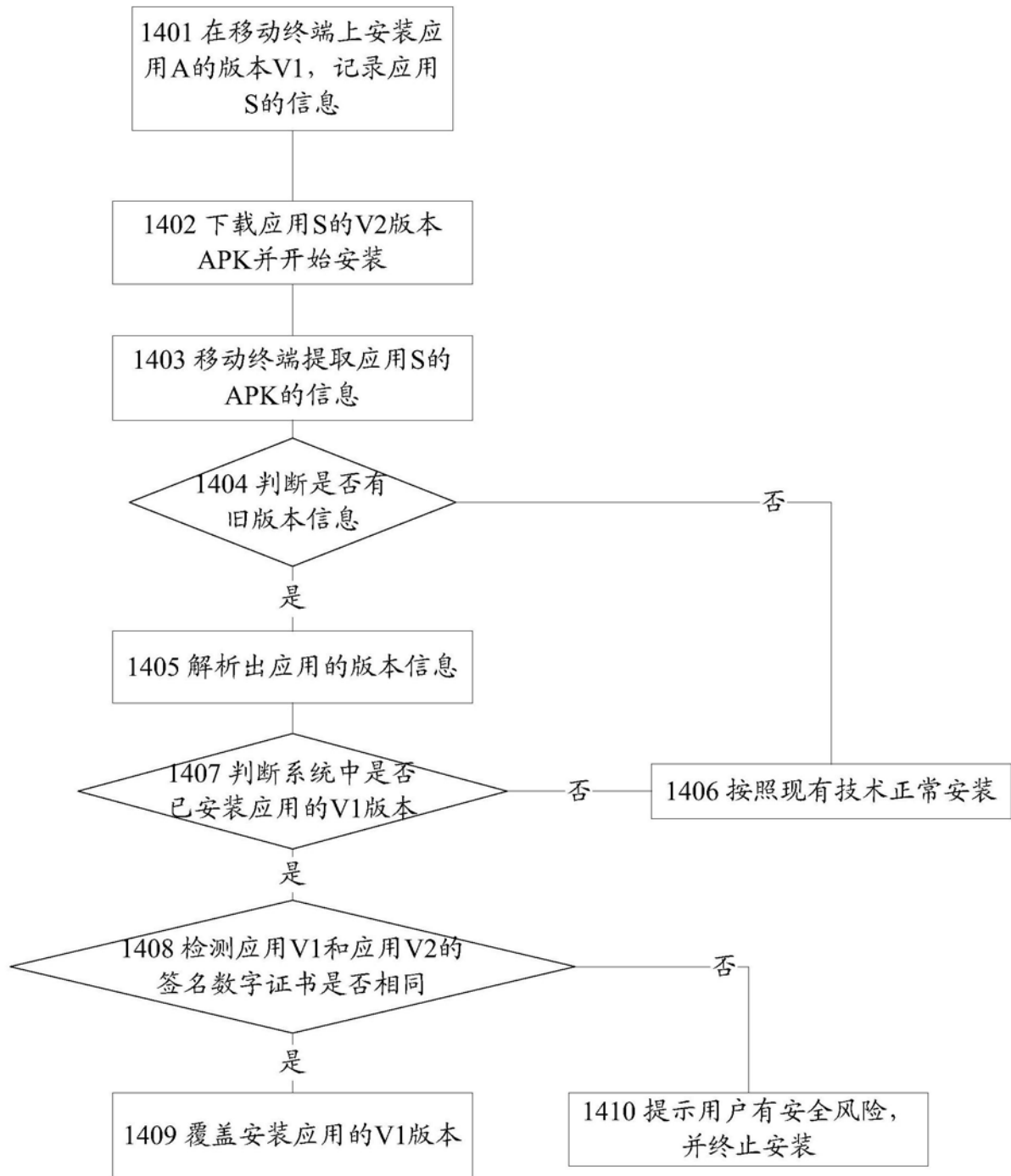


图14

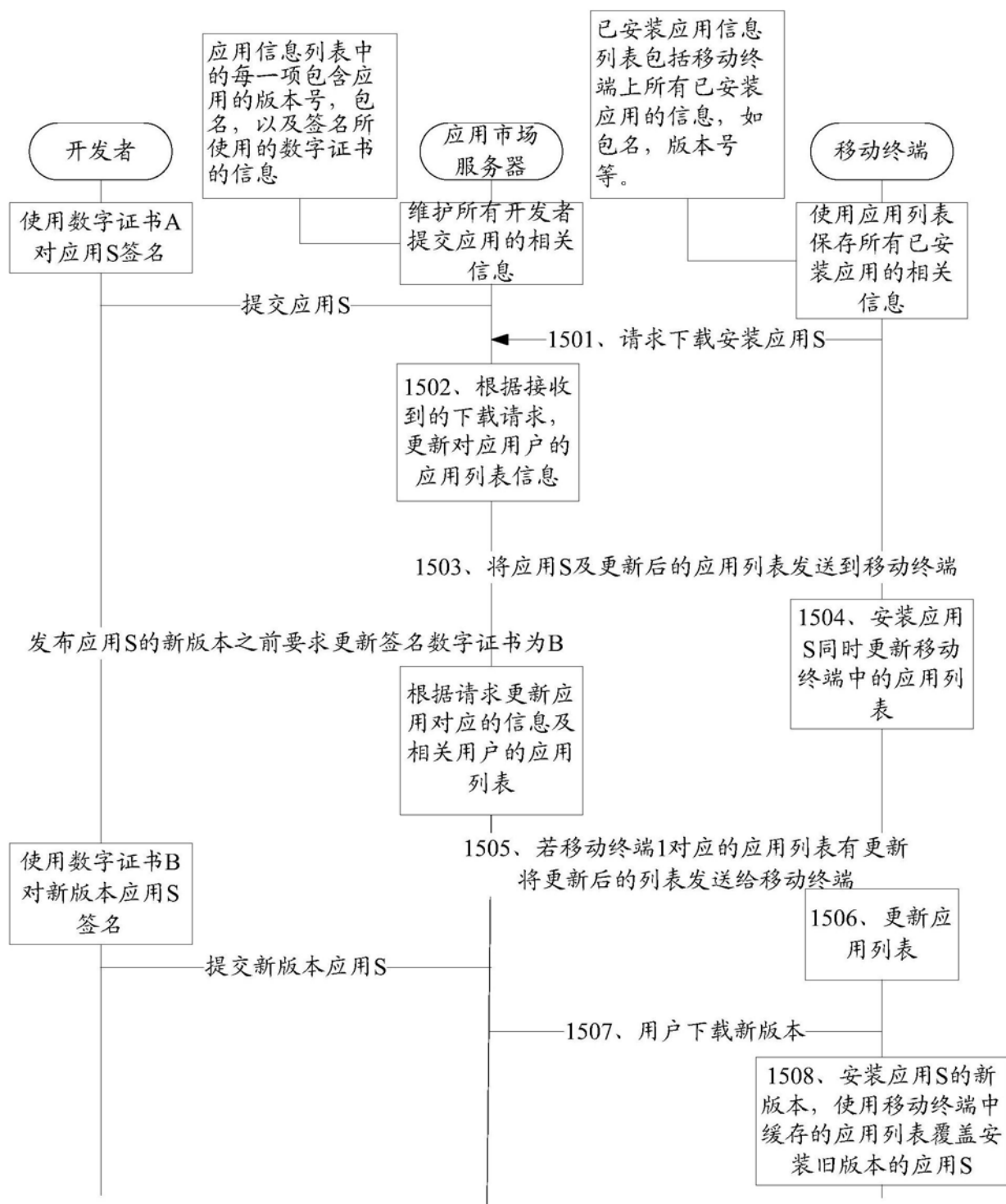


图15

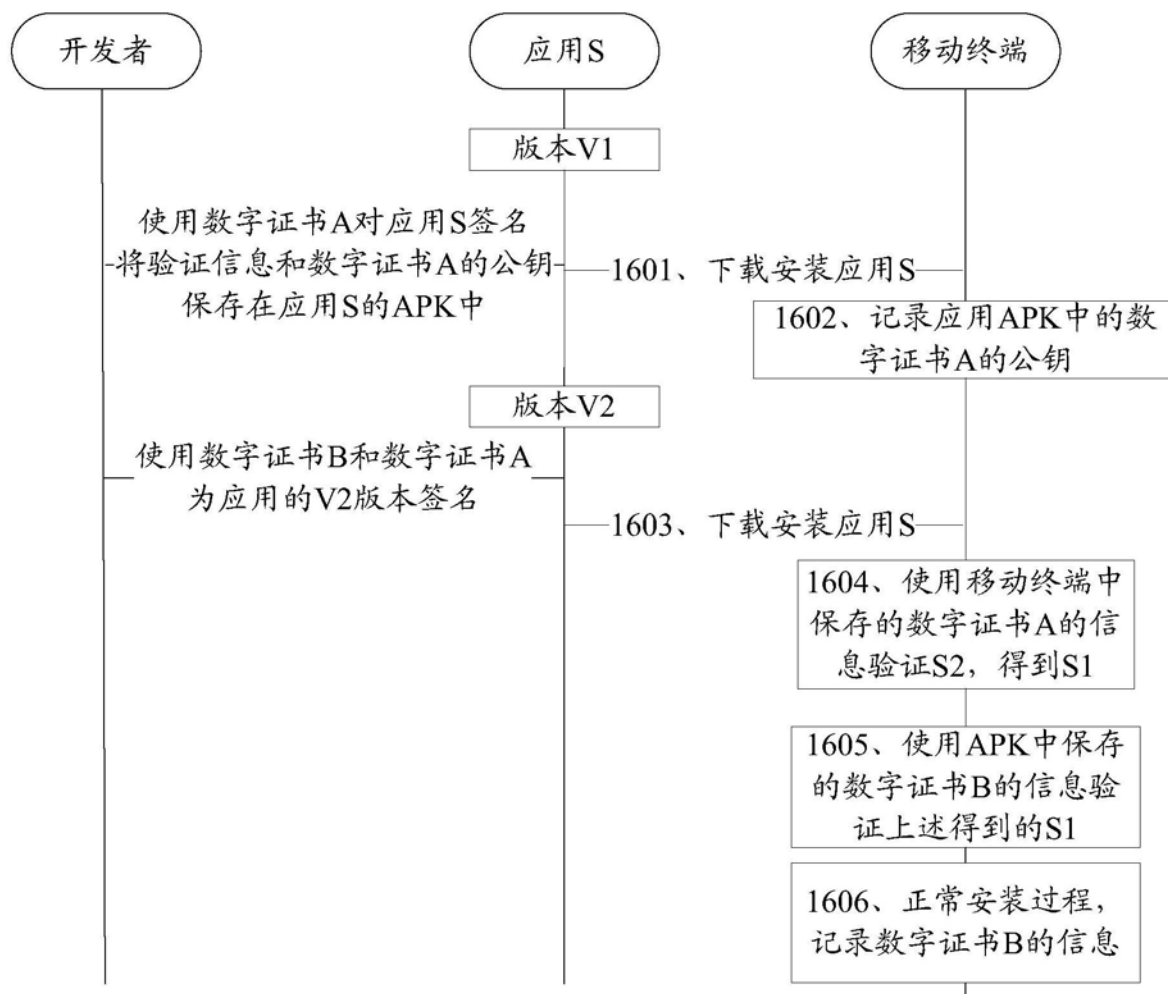


图16

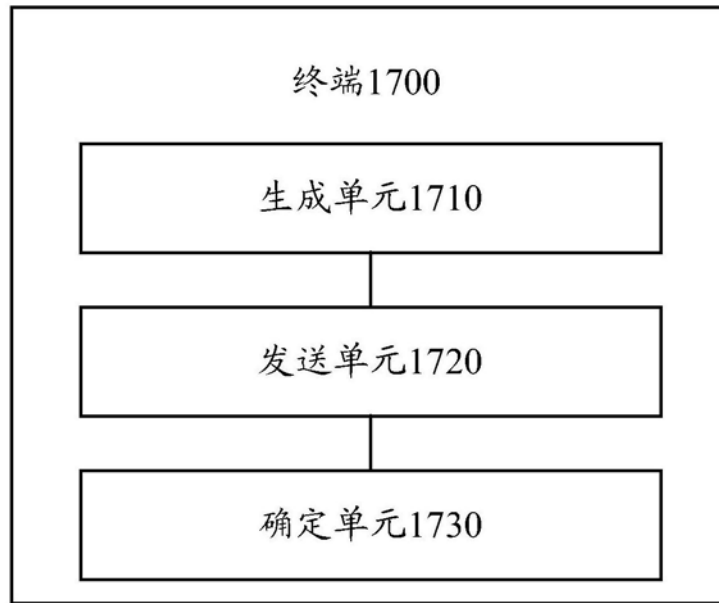


图17



图18

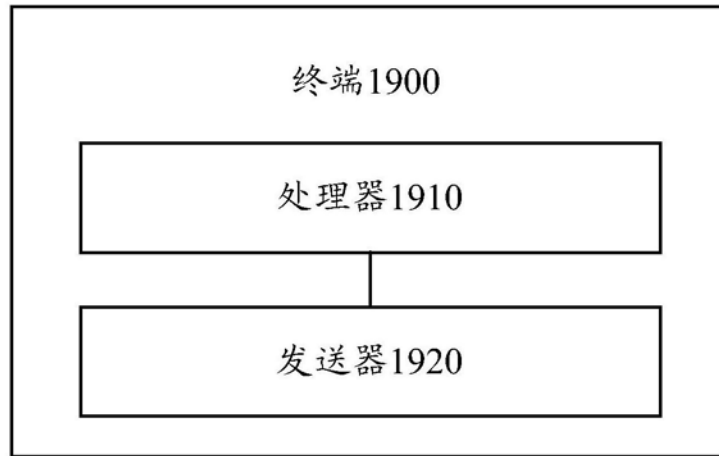


图19



图20

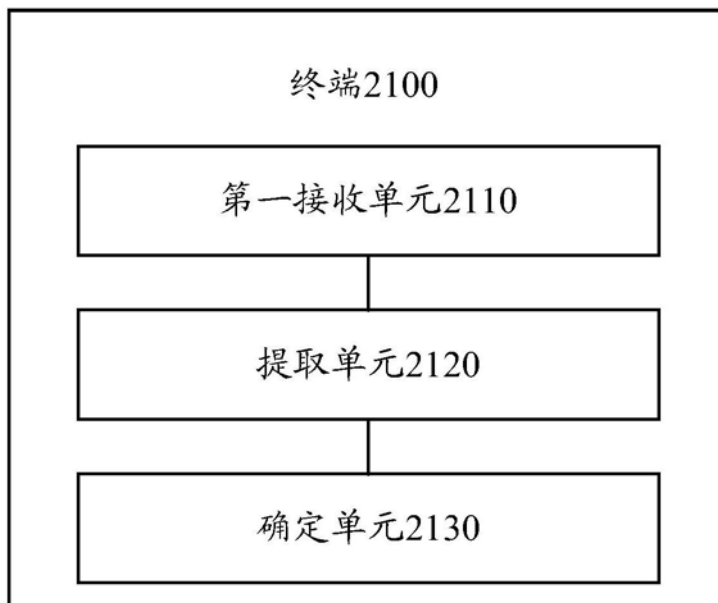


图21

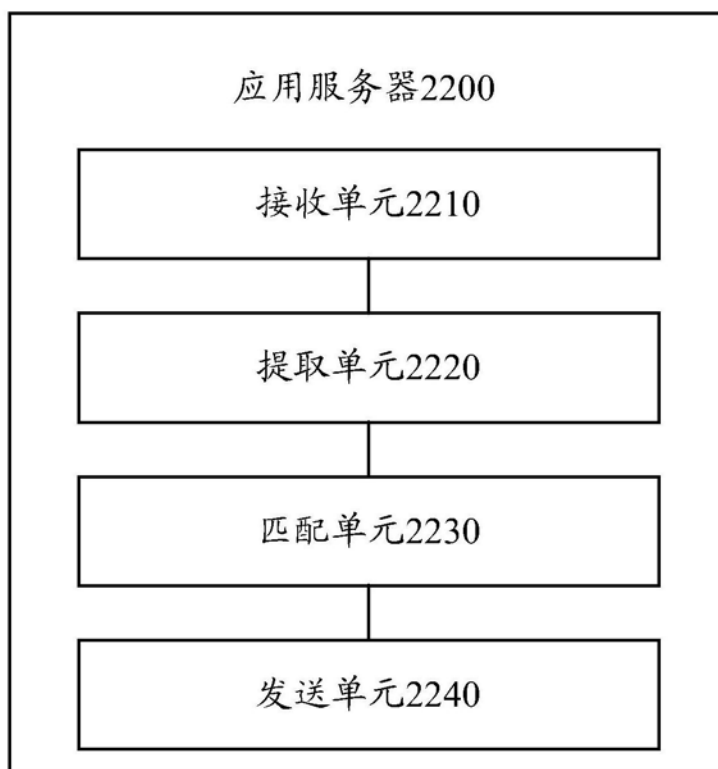


图22



图23

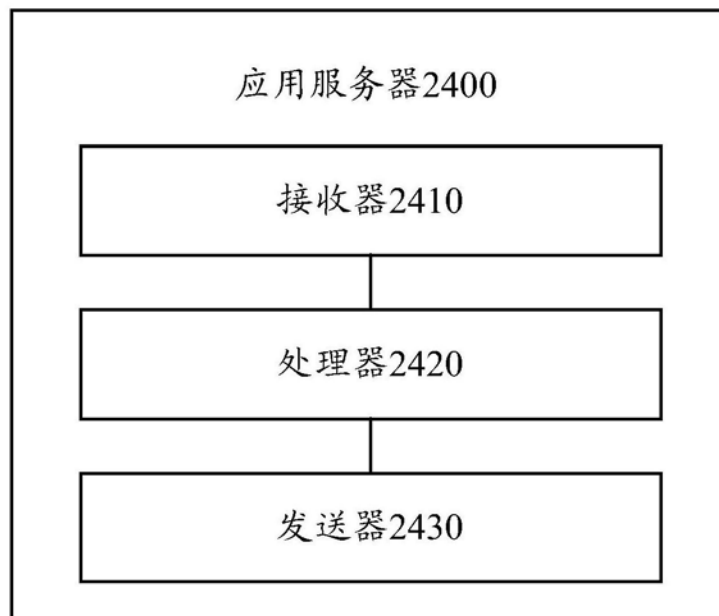


图24



图25



图26