(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 103677935 A
(43)申请公布日 2014.03.26

(21)申请号 201310717720.5

(22)申请日 2013.12.23

(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 王鹏程 李旋 王力 张瑞博

(74)专利代理机构 北京中强智尚知识产权代理有限公司 11448
代理人 姜精斌

(51)Int.Cl.
G06F 9/445(2006.01)
H04L 29/08(2006.01)

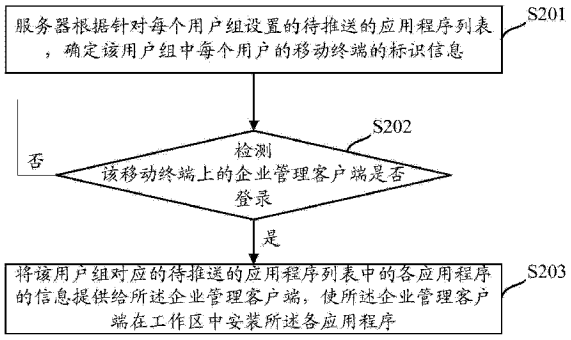
权利要求书2页 说明书13页 附图4页

(54)发明名称

一种应用程序的安装控制方法、系统及装置

(57)摘要

本发明提供一种应用程序的安装控制方法、系统及装置，解决用户下载应用程序浪费时间，效率低的问题。该方法中服务器针对每个用户组对应的移动终端，在检测到移动终端上的企业管理客户端登陆时，向其提供待推送的应用程序列表，使企业管理客户端在工作区中安装该应用程序列表中的各应用程序。由于在本发明实施例中服务器针对每个用户组设置了其对应的待推送的应用程序列表，可以将该用户组所需的应用程序的信息包含在该应用程序列表中，并向该用户组提供，减少了该用户组中每个用户搜索并下载该应用程序列表中相应应用程序的工作量，节省了用户的时间，提高了其工作效率。



CN 103677935 A

1. 一种应用程序的安装控制方法，其特征在于，该方法包括：

服务器根据针对每个用户组设置的待推送的应用程序列表，确定该用户组中每个用户的移动终端的标识信息；

针对该用户组中每个用户的移动终端，检测该移动终端上的企业管理客户端是否登录；

当检测到该移动终端上的企业管理客户端登录时，将该用户组对应的待推送的应用程序列表中的各应用程序的信息提供给所述企业管理客户端，使所述企业管理客户端在工作区中安装所述各应用程序。

2. 如权利要求 1 所述的方法，其特征在于，所述方法还包括：

所述服务器根据向所述移动终端提供的应用程序的信息，将该应用程序的信息保存到针对该移动终端保存的已经推送的应用程序列表中；

所述将该用户组对应的待推送的应用程序列表中的各应用程序的信息提供给所述企业管理客户端之前，还包括：

所述服务器根据针对该移动终端保存的已经推送的应用程序列表，判断是否向该移动终端推送过所述信息的应用程序；

当判断未向该移动终端推送过该信息的应用程序时，进行后续提供步骤。

3. 如权利要求 1 或 2 所述的方法，其特征在于，将该用户组对应的待推送的应用程序列表中的各应用程序的信息提供给所述企业管理客户端，包括：

所述服务器针对每个应用程序，获取所述待推送的应用程序列表中包含的该应用程序的下载地址信息；

将所述下载地址信息携带在控制信令中提供给所述企业管理客户端。

4. 如权利要求 1 ～ 3 任一所述的方法，其特征在于，所述企业管理客户端在工作区中安装所述各应用程序，包括：

所述企业管理客户端根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，使用提取的超级用户 root 权限，在所述工作区安装所述应用程序的安装包；或，

所述企业管理客户端根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，并向用户提供是否安装所述应用程序的安装包的提示信息，在接收到用户安装所述安装包的确认信息后，在所述工作区安装所述应用程序的安装包。

5. 一种应用程序的安装控制系统，其特征在于，所述系统包括服务器和至少一个移动终端上的企业管理客户端：

服务器，用于据针对每个用户组设置的待推送的应用程序列表，确定该用户组中每个用户的移动终端的标识信息；针对该用户组中每个用户的移动终端，检测该移动终端上的企业管理客户端是否登录；当检测到该移动终端上的企业管理客户端登录时，将该用户组对应的待推送的应用程序列表中的各应用程序的信息提供给所述企业管理客户端；

企业管理客户端，用于接收服务器发送的应用程序列表中的各应用程序的信息，并在工作区中安装所述各应用程序。

6. 如权利要求 5 所述的系统，其特征在于，所述服务器，还用于根据向所述移动终端提

供的应用程序的信息，将该应用程序的信息保存到针对该移动终端保存的已经推送的应用程序列表中；

所述服务器，还用于根据针对该移动终端保存的已经推送的应用程序列表，判断是否向该移动终端推送过所述信息的应用程序；当判断未向该移动终端推送过该信息的应用程序时，进行后续提供步骤。

7. 如权利要求 5 或 6 所述的系统，其特征在于，所述服务器，具体用于针对每个应用程序，获取所述待推送的应用程序列表中包含的该应用程序的下载地址信息；将所述下载地址信息携带在控制信令中提供给所述企业管理客户端。

8. 如权利要求 5 ～ 7 任一所述的系统，其特征在于，所述企业管理客户端，具体用于根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，使用提取的超级用户 root 权限，安装所述应用程序的安装包；或，根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，并向用户提供是否安装所述应用程序的安装包的提示信息，在接收到用户安装所述安装包的确认信息后，安装所述应用程序的安装包。

9. 一种企业管理客户端，其特征在于，包括：

接收模块，用于接收服务器提供的待推送的应用程序列表中的各应用程序的信息；

安装模块，用于在工作区中安装所述各应用程序。

10. 如权利要求 9 所述的企业管理客户端，其特征在于，所述安装模块，具体用于根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，使用提取的超级用户 root 权限，在工作区安装所述应用程序的安装包；或，根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，并向用户提供是否安装所述应用程序的安装包的提示信息，在接收到用户安装所述安装包的确认信息后，在工作区安装所述应用程序的安装包。

一种应用程序的安装控制方法、系统及装置

技术领域

[0001] 本发明涉及信息安全技术领域，尤其涉及一种应用程序的安装控制方法、系统及装置。

背景技术

[0002] 随着移动终端的成熟与普及，以智能手机、平板电脑为代表的个人移动终端设备逐渐进入企业领域。据国际权威咨询公司 Gartner 预测，到 2014 年 90% 的企业将会支持员工在个人移动终端设备上运行企业办公应用程序，员工使用个人移动终端设备办公已经成为一种无法逆转的潮流。

[0003] 在 BYOD 中，同一移动终端上既有个人应用程序和数据，也有企业应用程序和数据，企业应用程序设置在企业管理客户端中，企业应用程序的数据也保存在企业管理客户端中。为了区别，个人应用程序和数据所在的区域被称为个人区，企业应用程序和数据所在的区域，即企业管理客户端创建的区域被称为工作区。

[0004] 随着BYOD现象的普及，越来越多的企业用户将使用移动终端办公。现有BYOD现象中，每个企业用户根据自身的需求，下载并安装相应的应用程序。企业用户对本身工作了解的不同，可能会导致企业用户下载的应用程序也不同，例如企业用户工作中需要使用某一应用程序，但其由于其对本身工作了解的不够清楚并没有下载该应用程序，在后续工作时，将会影响其工作效率。

[0005] 另外办公性质相同的企业，每个企业用户可能需要的应用程序基本都是相同的，每个企业用户都采用上述方式下载并安装相应的应用程序，无法保证每个企业用户下载的相同应用程序的版本一致，从而可能会出现后期数据不兼容的问题；另外，每个企业用户针对每个应用程序都要进行搜索、下载的操作，将会耗费企业用户大量的时间，应用程序下载后是否能够与自身的移动终端兼容也是未知的，因此该方式浪费了大量的人力资源，不利于提高企业的工作效率。

发明内容

[0006] 鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决或者减缓上述问题的一种应用程序的安装控制方法、系统及装置。

[0007] 本发明实施例提供了一种应用程序的安装控制方法，该方法包括：

[0008] 服务器根据针对每个用户组设置的待推送的应用程序列表，确定该用户组中每个用户的移动终端的标识信息；

[0009] 针对该用户组中每个用户的移动终端，检测该移动终端上的企业管理客户端是否登录；

[0010] 当检测到该移动终端上的企业管理客户端登录时，将该用户组对应的待推送的应用程序列表中的各应用程序的信息提供给所述企业管理客户端，使所述企业管理客户端在工作区中安装所述各应用程序。

[0011] 较佳地，为了减少重复推送相同应用程序的工作量，所述方法还包括：

[0012] 所述服务器根据向所述移动终端提供的应用程序的信息，将该应用程序的信息保存到针对该移动终端保存的已经推送的应用程序列表中。

[0013] 所述将该用户组对应的待推送的应用程序列表中的各应用程序的信息提供给所述企业管理客户端之前，还包括：

[0014] 所述服务器根据针对该移动终端保存的已经推送的应用程序列表，判断是否向该移动终端推送过所述信息的应用程序；

[0015] 当判断未向该移动终端推送过该信息的应用程序时，进行后续提供步骤。

[0016] 较佳地，为了减少重复推送相同应用程序的工作量，将该用户组对应的待推送的应用程序列表中的各应用程序的信息提供给所述企业管理客户端，包括：

[0017] 所述服务器针对每个应用程序，获取所述待推送的应用程序列表中包含的该应用程序的下载地址信息；

[0018] 将所述下载地址信息携带在控制信令中提供给所述企业管理客户端。

[0019] 较佳地，为了进一步减少企业用户进行应用程序下载的工作量，提高其工作效率，所述企业管理客户端在工作区中安装所述各应用程序，包括：

[0020] 所述企业管理客户端根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，使用提取的超级用户 root 权限，在所述工作区安装所述应用程序的安装包；或，

[0021] 所述企业管理客户端根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，并向用户提供是否安装所述应用程序的安装包的提示信息，在接收到用户安装所述安装包的确认信息后，在所述工作区安装所述应用程序的安装包。

[0022] 本发明实施例提供了一种应用程序的安装控制系统，该系统包括服务器和至少一个移动终端上的企业管理客户端：

[0023] 服务器，用于据针对每个用户组设置的待推送的应用程序列表，确定该用户组中每个用户的移动终端的标识信息；针对该用户组中每个用户的移动终端，检测该移动终端上的企业管理客户端是否登录；当检测到该移动终端上的企业管理客户端登录时，将该用户组对应的待推送的应用程序列表中的各应用程序的信息提供给所述企业管理客户端；

[0024] 至少一个企业管理客户端，用于接收服务器发送的应用程序列表中的各应用程序的信息，并在工作区中安装所述各应用程序。

[0025] 较佳地，为了减少重复推送相同应用程序的工作量，所述服务器，还用于根据向所述移动终端提供的应用程序的信息，将该应用程序的信息保存到针对该移动终端保存的已经推送的应用程序列表中。

[0026] 所述服务器，还用于根据针对该移动终端保存的已经推送的应用程序列表，判断是否向该移动终端推送过所述信息的应用程序；当判断未向该移动终端推送过该信息的应用程序时，进行后续提供步骤。

[0027] 较佳地，为了减少重复推送相同应用程序的工作量，所述服务器，具体用于针对每个应用程序，获取所述待推送的应用程序列表中包含的该应用程序的下载地址信息；将所述下载地址信息携带在控制信令中提供给所述企业管理客户端。

[0028] 较佳地，为了进一步减少企业用户进行应用程序下载的工作量，提高其工作效率，所述企业管理客户端，具体用于根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，使用提取的超级用户 root 权限，安装所述应用程序的安装包；或，根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，并向用户提供是否安装所述应用程序的安装包的提示信息，在接收到用户安装所述安装包的确认信息后，安装所述应用程序的安装包。

[0029] 本发明实施例提供了一种企业管理客户端，包括：

[0030] 接收模块，用于接收服务器提供的待推送的应用程序列表中的各应用程序的信息；

[0031] 安装模块，用于在工作区中安装所述各应用程序。

[0032] 较佳地，为了进一步减少企业用户进行应用程序下载的工作量，提高其工作效率，所述安装模块，具体用于根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，使用提取的超级用户 root 权限，在工作区安装所述应用程序的安装包；或，根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，并向用户提供是否安装所述应用程序的安装包的提示信息，在接收到用户安装所述安装包的确认信息后，在工作区安装所述应用程序的安装包。

[0033] 本发明实施例提供了一种应用程序的安装控制方法、系统及装置，该方法中服务器针对每个用户组对应的移动终端，在检测到移动终端上的企业管理客户端登陆时，向其提供待推送的应用程序列表，使企业管理客户端在工作区中安装该应用程序列表中的各应用程序。由于在本发明实施例中服务器针对每个用户组设置了其对应的待推送的应用程序列表，可以将该用户组所需的应用程序的信息包含在该应用程序列表中，并向该用户组提供，从而可以避免用户对自身工作了解不清楚，没有下载或下载错误应用程序影响工作效率的问题，并且减少了该用户组中每个用户搜索并下载该应用程序列表中相应应用程序的工作量，节省了用户的时间，提高了其工作效率。

[0034] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0035] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0036] 图 1 为本发明实施例中移动终端的企业管理系统的系统架构示意图；

[0037] 图 2 为本发明实施例提供了一种应用程序的安装控制过程图；

[0038] 图 3 为本发明实施例一提供的应用程序的安装控制过程图；

[0039] 图 4 为本发明实施例二提供的一种应用程序的安装控制过程图；

[0040] 图 5 为本发明实施例提供的一种应用程序的安装控制系统结构图。

[0041] 图 6 为本发明实施例提供的一种企业管理客户端结构图。

具体实施方式

[0042] 为了减少 BYOD 场景中企业用户进行应用程序搜索及下载的工作量，减少其进行应用程序搜索及下载的时间，提高其工作效率，本发明实施例提供了一种应用程序的安装控制方法、系统及装置。

[0043] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0044] 下面结合说明书附图，本发明实施例进行详细说明。

[0045] 首先，对本发明实施例提供的移动终端的企业管理系统的系统架构进行说明。如图 1 所示，本发明实施例提供的移动终端的企业管理系统是面向企业的移动终端管理平台，包括部署在企业内网的服务端和安装在需要被管理的移动终端上的客户端，本发明实施例中，将部署在企业内网的服务端称为服务器，安装在需要被管理的移动终端上的客户端称为企业管理客户端。其中：

[0046] 服务器的主要功能包括：管理、下发企业内网的应用，以及管理、下发安全策略等；服务器还提供丰富的移动终端统计与管理工具，企业管理员可以通过服务器查看每个需要被管理的移动终端的详细信息，包括：终端型号、系统版本、IMEI（International Mobile Equipment Identification Number，国际移动设备识别码）、序列号、MSISDN（移动台识别号码，俗称手机号码）、是否离线、是否 Root（超级用户）、更换密码时间、是否安装安全软件、电源信息、无线网络信息等。

[0047] 企业管理客户端的主要功能包括：数据防泄密，执行安全策略等，数据防泄密包括数据加密、数据隔离等，加密的数据可以是涉及系统文件内的数据；或者是用户选定的财务文件、生产文件、销售文件、市场文件、人力资源文件等内的数据；还可以是用户个人文件的数据，例如：照片、视频、日志等。以在 Android（安卓）系统上实现为例对数据加密进行简要说明。数据加密是通过 .so（动态链接库）文件实现，主要是在应用程序中注入代码，使得 apk（Android Package，安卓安装包）初始化时去调用该 .so 文件，要保证 .so 文件运行的时机比应用程序的读写文件的时间早，如果晚了文件就会变成“一半加密的状态”，导致文件损坏。通过数据加密，.so 文件会拦截该应用程序的所有文件操作，实现加密。

[0048] 本发明实施例提供的移动终端的企业管理系统，基于企业管理客户端的数据防泄密机制，在不影响企业员工对个人应用使用感受的基础上，在移动终端上建立了一个安全、独立的工作区内存空间，工作区内存空间（简称工作区）是指分配给企业管理客户端的内存空间，所有的企业应用和数据存储在受保护的工作区内。相应的，移动终端的内存空间中工作区内存空间之外的内存空间称为个人区内存空间（简称个人区），所有的个人应用和数据存储在个人区内，个人应用无法访问企业数据，从而避免企业数据被个人应用非法访问、存取。本发明实施例提供的移动终端的企业管理系统，不仅将企业数据和个人数据完全隔离，更好地保护企业应用和数据，也为企业员工提供了无差别的个人应用体验，达到了“一机两用”的效果。

[0049] 企业管理服务器提供两种应用程序下发方式：自由安装和强制安装。通过自由安装方式下发的应用程序，供企业用户自由选择下载安装；通过强制安装方式下发的应用程

序，企业用户需安装该应用程序后才能正常使用工作区。具体实施中，针对工作区内的企业应用，一般采用强制安装方式；针对个人区内的个人应用，一般采用自由安装方式。当然也可以对工作区内的企业应用采用自由安装方式。通过自由安装方式下发的应用程序，将显示在工作区企业应用市场的应用列表中，客户端用户可自由选择下载安装；通过强制安装方式下发的应用，客户端用户需安装此应用才能正常使用工作区。

[0050] 由于移动终端一般是企业配发给企业员工的，采用应用黑白名单，可以对个人区内的个人应用提供的安全管理机制。应用黑名单中会列出禁止安装的应用程序的名称及版本号，应用白名单中会列出仅允许安装的应用程序的名称及版本号。

[0051] 应用黑名单或应用白名单的设置都是企业管理员可以配置的。企业管理员对应用黑名单或者应用白名单的设置包括如下场景：

[0052] 场景一、企业所有移动终端设备，仅允许企业员工办公使用，因此会限制仅允许安装办公使用的应用程序，即可以采用应用白名单的方式限定仅允许安装工作相关的应用程序。

[0053] 场景二、禁止被曝出有安全漏洞或恶意行为的应用程序的安装。例如一些特定的应用程序，或者是安全软件查出有恶意行为的应用程序，或者是漏洞扫描功能扫描出的有安全漏洞的应用程序等，即可以采用应用黑名单的方式禁止有安全漏洞或恶意行为的应用程序的安装。

[0054] 场景三、禁止某些文件分享类应用程序的安装，例如网盘等应用程序的安装，因为文件分享类应用程序会导致企业内部的资源被上传到云端，从而破坏了企业信息的私密性，即可以采用应用黑名单的方式禁止文件分享类应用程序的安装。

[0055] 其他具体场景不再一一列举，总之，企业可以按照本企业的实际需求，采用应用黑名单或者应用白名单的方式，灵活的控制每一个用户组中应用程序的安装。

[0056] 企业应用一般是企业强制下发并安装在企业员工的移动终端上的应用程序，一般情况下，企业应用具有较高的安全可靠性，企业员工可以放心使用；本发明实施例通过强制安装方式下发的应用程序，提供了一种应用程序的安装控制方法。针对工作区中的企业应用采用企业强制安装的方式。下面提供具体的实施方式说明企业应用的下发过程。

[0057] 图 2 为本发明实施例提供了一种应用程序的安装控制过程图，该过程包括以下步骤：

[0058] S201：服务器根据针对每个用户组设置的待推送的应用程序列表，确定该用户组中每个用户的移动终端的标识信息。

[0059] 具体的，在服务器中建立了一个专用空间，用于存储上传到服务器的应用程序的安装包，本发明实施例中将该专用空间称为企业应用库。服务器中维护有所有已上传到服务器安装包的应用程序的名称及版本号，当然也可以包括该应用程序的其他信息，例如上传时间、安装包大小、安装量等。企业管理员可以查看、编辑应用管理列表，查看各应用程序的安装量等统计信息。

[0060] 一般情况下，应用程序的安装包是由企业上传给企业管理服务器的，为了保证移动终端上所使用应用程序的安全可靠性，企业管理服务器在保存应用程序的安装包之前，对应用程序的安装包进行病毒检测和加固处理。

[0061] 对应用程序的安装包进行加固处理，可以防止应用程序被轻易逆向从而获取密钥

体系等关键信息，同时给应用程序增加了数据加密的功能，增加安全系数。以在Android(安卓)系统上实现为例对应用程序的安装包进行加固处理进行简要说明。对应用程序的安装包进行加固处理主要就是改变应用程序的class.dex文件的内容，对其内容进行一些算法加密，在apk（Android Package，安卓安装包）运行时再动态的去解密，还原内容；在修改class.dex文件的时候要保证其符合dex文件的固有格式。所有上传的应用程序的安装包均经过病毒检测和加固处理，从而杜绝恶意篡改、代码注入、内存修改、窃取数据、反编译等威胁。

[0062] BYOD场景中很多用户使用的应用程序可能都是相同，可以根据用户之间使用的应用程序的相似度，将用户划分为不同的用户组，每个用户组中包含至少一个用户。一般情况下，同一职能部门的用户使用的应用程序的相似比较高，例如财务部的各用户会使用相同的财务软件，研发部的各用户会使用相同的开发软件，行政部的各用户会使用相同的office办公软件，市场部的各用户会使用即时聊天工具，例如飞信、微信、QQ等等。因此具体的，在将用户划分到不同的用户组时，可以根据用户所在的职能部分进行划分。另外，对移动终端的工作区的安全状态进行监控的杀毒软件、防火墙等，针对无论哪个用户组都进行推送，并安装在对应用户移动终端的工作区中。

[0063] 将用户划分到不同的用户组后，为了便于应用程序的推送及安装，在服务器中保存有每个用户组中包含的每个用户的移动终端的标识信息。从而可以确定将应用程序列表中的各应用程序的信息推送给哪些移动终端。

[0064] 为了减少BYOD场景中每个用户在工作区下载应用程序的工作量及时间，在本发明实施例中可以在服务器中针对不同的用户组，根据其使用的各应用程序，确定该用户组对应的待推送的应用程序列表，将至少一个应用程序的信息包含在该应用程序列表中。

[0065] 服务器中针对每个用户组维护有待推送的应用程序列表，该应用程序列表中包括待推送给每个企业管理客户端的应用程序的名称及版本号，当然也可以包括该应用程序的其他信息，例如上传时间、安装包大小、安装量等。

[0066] S202：针对该用户组中每个用户的移动终端，检测该移动终端上的企业管理客户端是否登录，当检测结果为是时进行步骤S203，否则，进行步骤S202。

[0067] 检测移动终端上的企业管理客户端是否登录包括很多方法，例如企业管理客户端在每次登录时，向服务器发送登录信息，以便服务器将最新的策略下发到企业管理客户端，因此服务器可以根据是否接收到企业管理客户端的登录信息进行检测；或者，服务器向企业管理客户端发送询问请求，根据企业管理客户端是否回复进行检测。检测方法还包括多种，在本发明实施例中就不进行赘述，相信本领域技术人员能够根据本发明实施例的描述，确定相应的检测方法。

[0068] S203：将该用户组对应的待推送的应用程序列表中的各应用程序的信息提供给所述企业管理客户端，使所述企业管理客户端在工作区中安装所述各应用程序。

[0069] 该待推送的应用程序列表中包含至少一个应用程序的信息，该应用程序的信息可以是该应用程序的标识信息，例如该应用程序的名称，或者该应用程序的代码等等。该应用程序的信息还可以包括应用程序的版本号信息，和应用程序的下载地址信息中的一种或几种。

[0070] 服务器在向企业管理客户端提供应用程序的信息时，可以将应用程序的信息携带

在控制信令中。当该应用程序列表中包含2个或者2个以上的应用程序的信息时，服务器在向企业管理客户端提供各应用程序的信息时，可以将各应用程序的信息包含在一条控制信令中，一并提供给企业管理客户端；或者，也可以一条控制信令包含一个应用程序的信息，将每个应用程序的信息分别提供给企业管理客户端。当应用程序的信息提供给企业管理客户端后，企业管理客户端可以根据服务器提供的应用程序的信息，在工作区进行相应应用程序的下载安装。

[0071] 由于在本发明实施例中服务器针对每个用户组设置了其对应的待推送的应用程序列表，可以将该用户组所需的应用程序的信息包含在该应用程序列表中，并向该用户组提供，从而可以避免用户对自身工作了解不清楚，没有下载或下载错误应用程序影响工作效率的问题，并且减少了该用户组中每个用户搜索并下载该应用程序列表中相应应用程序的工作量，节省了用户的时间，提高了其工作效率。

[0072] 待推送的应用程序列表中的每个应用程序的信息可以是管理员设置的，管理员在针对每个用户组设置其对应的应用程序列表时，将每个应用程序的名称、版本号及下载地址信息设置到该应用程序列表中，以便后续向对应的用户推送。待推送的应用程序列表中的每个应用程序的信息也可以是服务器根据相应的规则，在应用商店中提取的。此时上传到服务器的应用程序的安装包保存在应用商店中，应用商店维护有所有已上传到服务器安装包的应用程序的名称及版本号，当然也可以包括该应用程序的其他信息，例如上传时间、安装包大小、安装量等。企业管理员可以设置服务器待推送的应用程序列表中的每个应用程序的名称及版本号信息。服务器根据设置的该信息，到应用商店中查找相应名称及版本号的应用程序的安装包，并将该应用程序的安装包的下载地址信息添加到该应用程序列表中。

[0073] 服务器中针对每个用户组维护有该用户组对应的应用程序列表，该应用程序列表中保存有个应用程序的标识信息、版本号信息及下载地址信息等等。具体的，当用户组是针对用户所在职能部门进行的划分时，服务器中针对每个用户组设置的应用程序列表中都保存有对工作进行监控的应用程序，例如杀毒软件，安全卫士等。

[0074] 针对研发部对应的用户组设置的应用程序列表中保存有各编程软件的名称、版本号及下载地址信息等，针对财务部对应的用户组设置的应用程序列表中保存有各财务软件的名称、版本号及下载地址信息等，针对行政部对应的用户组设置的应用程序列表中保存有各办公软件的名称、版本号及下载地址信息等，针对市场部对应的用户组设置的应用程序列表中保存有各即时聊天工具的名称、版本号及下载地址信息等。

[0075] 当服务器确定了每个用户组对应的待推送的应用程序列表后，为了保证向每个用户的企业管理服务器推送的应用程序不存在重复，减少服务器重复推送相同应用程序的工作量，本发明实施例中还包括：

[0076] 所述服务器根据向所述移动终端提供的应用程序的信息，将该应用程序的信息保存到针对该移动终端保存的已经推送的应用程序列表中。

[0077] 所述将该用户组对应的待推送的应用程序列表中的各应用程序的信息提供给所述企业管理客户端之前，还包括：

[0078] 所述服务器根据针对该移动终端保存的已经推送的应用程序列表，判断是否向该移动终端推送过所述信息的应用程序；

[0079] 当判断未向该移动终端推送过该信息的应用程序时，进行后续提供步骤。

[0080] 为了减少服务器重复推送相同应用程序的工作量，服务器针对每个移动终端，在本地保存有已经推送的应用程序列表，在该应用程序列表中保存有已经向该移动终端推送的应用程序的信息。该应用程序的信息可以是应用程序的标识信息，在该应用程序的信息中还包括应用程序的版本号信息。

[0081] 服务器可以将应用程序的信息携带在控制信令中，将该控制信令发送到企业管理客户端。为了便于企业管理客户端安装该应用程序，控制信令中携带的应用程序的信息可以包含应用程序的下载地址信息。具体的服务器在获取该应用程序的下载地址信息时，当应用程序列表中包含该应用程序的下载地址信息时，服务器直接从该应用程序列表中获取该下载地址信息，当该应用程序列表中未包含该应用程序的下载地址信息时，服务器根据自身应用市场提供的各应用程序的信息，获取相应应用程序的下载地址信息。

[0082] 在每个下载地址信息保存的应用程序的安装包是进行了病毒检测、加固处理和加密处理的。一般情况下，应用程序的安装包是由第三方上传给服务器的，为了保证移动终端上所使用应用程序的安全可靠性，服务器在保存应用程序的安装包之前，对应用程序的安装包进行病毒检测、加固处理和加密处理。所有上传的应用程序的安装包均经过病毒检测和加固保护，从而杜绝恶意篡改、代码注入、内存修改、窃取数据、反编译等威胁，从而可以保证企业管理客户端中工作区的安全性。

[0083] 例如，该应用程序的信息包含：应用程序的标识信息、应用程序的版本号信息及应用程序的下载地址信息。待推送的应用程序列表中包含一个应用程序。基于上述描述，图3为本发明实施例一提供的应用程序的安装控制过程图，该过程包括以下步骤：

[0084] S301：服务器根据针对每个用户组设置的待推送的应用程序列表，确定该用户组中每个用户的移动终端的标识信息。

[0085] 其中，该应用程序列表中包含至少一个应用程序的信息。

[0086] S302：根据针对每个移动终端保存的已经推送的应用程序程序列表，判断是否向该移动终端提供过该标识信息的应用程序，当判断结果为是时，进行步骤S303，否则，进行步骤S305。

[0087] S303：判断向该移动终端已经推送的应用程序的版本号是否与该应用程序的版本号一致，当判断结果为是时，进行步骤S304，否则，进行步骤S305。

[0088] S304：不向该移动终端上的企业管理客户端推送该应用程序的信息。

[0089] S305：针对该用户组中每个用户的移动终端，检测该移动终端上的企业管理客户端是否登录，当检测结果为是时进行步骤S306，否则，进行步骤S305。

[0090] S306：将该应用程序的下载地址信息携带在控制信令中，提供给该移动终端上的企业管理客户端。

[0091] 服务器在获取该应用程序的下载地址信息时，根据自身应用市场提供的各应用程序的信息，获取该应用程序的下载地址信息。

[0092] S307：在针对该移动终端保存的已经推送的应用程序列表中添加该应用程序的信息。

[0093] 上述是以该应用程序列表中包含的应用程序的信息为应用程序的标识信息，应用程序的版本号信息为例进行的说明，当该应用程序列表中只包含应用程序的标识信息时，

在进行上述判断时只需要进行上述 S302 的判断，并在判断结果为是时，进行步骤 S304，否则进行步骤 S305。当该应用程序列表中包含的应用程序的信息为应用程序的标识信息，应用程序的版本号信息，和应用程序的下载地址信息时，在步骤 S306 中，服务器将该应用程序列表中该应用程序的下载地址信息携带在控制信令中，提供给该移动终端上的企业管理客户端。

[0094] 该应用程序列表中包含的该应用程序的信息较多，例如包含应用程序的标识信息及应用程序的版本号信息，可以降低应用程序重复推送的概率，当该应用程序列表中包含的应用程序的信息较少时，例如包含该应用程序的标识信息，可以提高服务器向企业管理客户端推送应用程序的效率。

[0095] 在本发明实施例中为了进一步减少企业用户进行应用程序下载的工作量，提高其工作效率，所述企业管理客户端在工作区中安装所述各应用程序，包括：

[0096] 所述企业管理客户端根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，使用提取的超级用户 root 权限，在所述工作区安装所述应用程序的安装包；或，

[0097] 所述企业管理客户端根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，并向用户提供是否安装所述应用程序的安装包的提示信息，在接收到用户安装所述安装包的确认信息后，在所述工作区安装所述应用程序的安装包。

[0098] 企业管理客户端在安装该应用程序的安装包时，以在安卓（Android）系统上实现为例进行说明。企业管理客户端首先通过一段 Root 代码提取 Root 权限，使用 Root 权限启动一个具有 Root 权限的 Service(服务)。具有 Root 权限的 Service 启动之后，预留本地的 Socket（套接字)接口供调用。企业管理客户端调用该 Socket 接口，使得具有 Root 权限的 Service Hook 在安卓系统的一个核心进程 System Service（系统服务）上，从而具有 Root 权限的 Service 可以监控与 Binder（安卓系统中进程间通信的机制）相关的 IOCTL（输入输出控制）函数，如果监控到与 Package Manager（安卓系统中对安装包进行管理的服务）相关的内容，即需要启动 Package Manager，在工作区中安装该应用程序的安装包。

[0099] 企业管理客户端没有 root 权限时，企业管理客户端在根据该控制信令中的下载地址信息，将相应的应用程序的安装包下载到工作区中后，向用户提供是否安装该应用程序的安装包的提示信息，并根据接收到的用户的指示，进行后续操作，接收到用户安装所述安装包的确认信息时，在工作区中安装该应用程序的安装包；接收到用户不安装该安装包的信息时，该应用程序的安装过程结束。

[0100] Root 权限可以访问和修改用户移动终端中几乎所有的文件（Android 系统文件及用户文件，不包括 ROM）。Root 权限是系统中唯一的超级管理员，具有等同于操作系统的权限，当移动终端具有 root 权限时，即可直接安装下载的应用程序的安装包。

[0101] 企业管理客户端在判断移动终端是否具有 root 权限时，企业管理客户端可以到移动终端的常见目录下检测是否存在 root 权限标识文件，从而检测移动终端是否具有 root 权限。例如针对安卓系统的移动终端，企业管理客户端可以到 /system/bin/system/sbin/system/xbin 等目录下检测是否存在 SU 文件，当检测到存在 SU 文件时，确定该移动终端具有 root 权限，否则，确定该移动终端不具有 root 权限；针对 IOS 系统的移动终端，企业

管理客户端可以到 /Applications 目录下检测是否存在通常没有权限访问的文件，当检测到存在通常没有权限访问的文件时，确定该移动终端具有 root 权限，否则，确定该移动终端不具有 root 权限。

[0102] 图 4 为本发明实施例二提供的一种应用程序的安装控制过程图，该过程包括以下步骤：

[0103] S401：服务器根据针对每个用户组设置的待推送的应用程序列表，确定该用户组中每个用户的移动终端的标识信息。

[0104] 其中，该应用程序列表中包含至少一个应用程序的信息。

[0105] S402：根据针对每个移动终端保存的已经推送的应用程序程序列表，判断是否向该移动终端提供过该标识信息的应用程序，当判断结果为是时，进行步骤 S403，否则，进行步骤 S405。

[0106] S403：判断向该移动终端已经推送的应用程序的版本号是否与该应用程序的版本号一致，当判断结果为是时，进行步骤 S404，否则，进行步骤 S405。

[0107] S404：不向该移动终端上的企业管理客户端推送该应用程序的信息。

[0108] S405：针对该用户组中每个用户的移动终端，检测该移动终端上的企业管理客户端是否登录，当检测结果为是时进行步骤 S406，否则，进行步骤 S405。

[0109] S406：将该应用程序的下载地址信息携带在控制信令中，提供给该移动终端上的企业管理客户端。

[0110] S407：企业管理客户端接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包。

[0111] S408：企业管理客户端使用提取的超级用户 root 权限，在所述工作区安装所述应用程序的安装包。

[0112] 企业管理客户端安装了对应的应用程序安装包后，可以在工作区的桌面上看到该应用的图标和名称，点击该应用的图标即可使用。

[0113] 或者，企业管理客户端向用户提供是否安装所述应用程序的安装包的提示信息，在接收到用户安装所述安装包的确认信息后，在所述工作区安装所述应用程序的安装包；在接收到用户不安装该安装包的信息时，该应用程序的安装过程结束。

[0114] 由于在本发明实施例中服务器针对每个用户组设置了其对应的待推送的应用程序列表，可以将该用户组所需的应用程序的信息包含在该应用程序列表中，并向该用户组提供，从而可以避免用户对自身工作了解不清楚，没有下载或下载错误应用程序影响工作效率的问题，并且减少了该用户组中每个用户搜索并下载该应用程序列表中相应应用程序的工作量，节省了用户的时间，提高了其工作效率。

[0115] 图 5 为本发明实施例提供的一种应用程序的安装控制系统结构图，所述系统包括服务器 51 和至少一个移动终端上的企业管理客户端 52：

[0116] 服务器 51，用于据针对每个用户组设置的待推送的应用程序列表，确定该用户组中每个用户的移动终端的标识信息；针对该用户组中每个用户的移动终端，检测该移动终端上的企业管理客户端 52 是否登录；当检测到该移动终端上的企业管理客户端 52 登录时，将该用户组对应的待推送的应用程序列表中的各应用程序的信息提供给所述企业管理客户端 52；

[0117] 至少一个企业管理客户端 52，用于接收服务器发送的应用程序列表中的各应用程序的信息，并在工作区中安装所述各应用程序。

[0118] 所述服务器 51，还用于根据向所述移动终端提供的应用程序的信息，将该应用程序的信息保存到针对该移动终端保存的已经推送的应用程序列表中。

[0119] 所述服务器 51，还用于根据针对该移动终端保存的已经推送的应用程序列表，判断是否向该移动终端推送过所述信息的应用程序；当判断未向该移动终端推送过该信息的应用程序时，进行后续提供步骤。

[0120] 所述服务器 51，具体用于针对每个应用程序，获取所述待推送的应用程序列表中包含的该应用程序的下载地址信息；将所述下载地址信息携带在控制信令中提供给所述企业管理客户端。

[0121] 至少一个所述企业管理客户端 52，具体用于根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，使用提取的超级用户 root 权限，安装所述应用程序的安装包。

[0122] 至少一个所述企业管理客户端 52，具体用于根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，并向用户提供是否安装所述应用程序的安装包的提示信息，在接收到用户安装所述安装包的确认信息后，安装所述应用程序的安装包。

[0123] 所述服务器 51，还用于对该应用程序列表中包含的各应用程序的安装包进行病毒检测、加固处理和加密处理。

[0124] 图 6 为本发明实施例提供的一种企业管理客户端结构图，包括：

[0125] 接收模块 61，用于接收服务器提供的待推送的应用程序列表中的各应用程序的信息；

[0126] 安装模块 62，用于在工作区中安装所述各应用程序。

[0127] 所述安装模块 62，具体用于根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，使用提取的超级用户 root 权限，在工作区安装所述应用程序的安装包。

[0128] 所述安装模块 62，具体用于根据接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包，并向用户提供是否安装所述应用程序的安装包的提示信息，在接收到用户安装所述安装包的确认信息后，在工作区安装所述应用程序的安装包。

[0129] 本发明实施例提供了一种应用程序的安装控制方法、系统及装置，该方法中服务器针对每个用户组对应的移动终端，在检测到移动终端上的企业管理客户端登陆时，向其提供待推送的应用程序列表，使企业管理客户端在工作区中安装该应用程序列表中的各应用程序。由于在本发明实施例中服务器针对每个用户组设置了其对应的待推送的应用程序列表，可以将该用户组所需的应用程序的信息包含在该应用程序列表中，并向该用户组提供，从而可以避免用户对自身工作了解不清楚，没有下载或下载错误应用程序影响工作效率的问题，并且减少了该用户组中每个用户搜索并下载该应用程序列表中相应应用程序的工作量，节省了用户的时间，提高了其工作效率。

[0130] 需要说明的是，本发明实施例中的设备可以包括计算机设备、移动设备等各种设

备。其中，移动设备可以为游戏控制台、膝上型计算机、便携式媒体播放器、板式计算机、平板计算机、PDA、移动计算机以及移动电话等各种移动设备，本发明实施例对此不作限制。

[0131] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0132] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0133] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0134] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0135] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0136] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的应用程序的安装控制服务器、企业管理客户端及系统中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0137] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，

不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0138] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

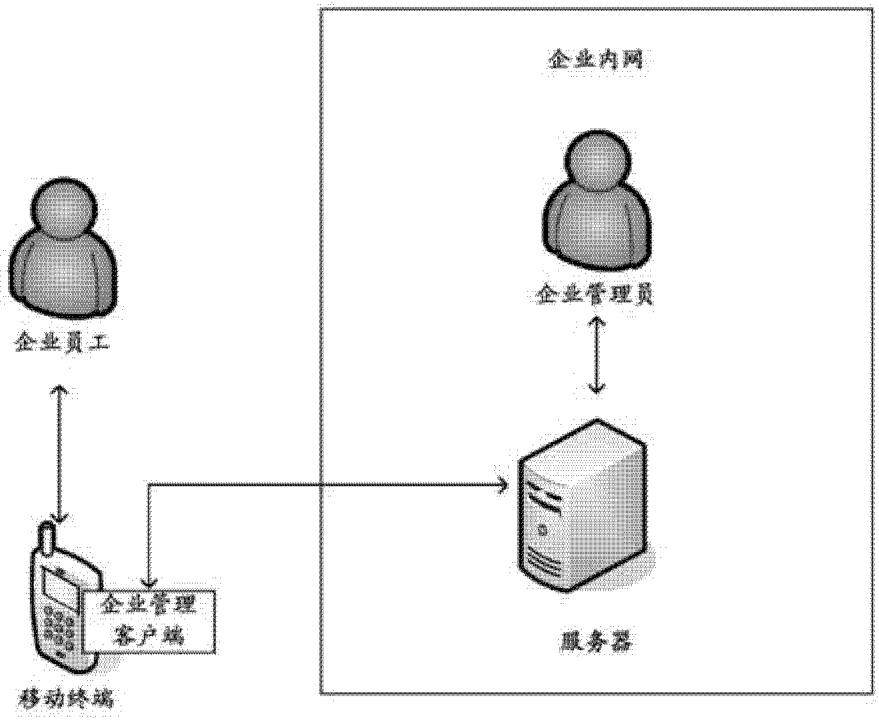

企业内网
企业管理员
企业员工
企业管理
客户端
移动终端
服务器

图 1

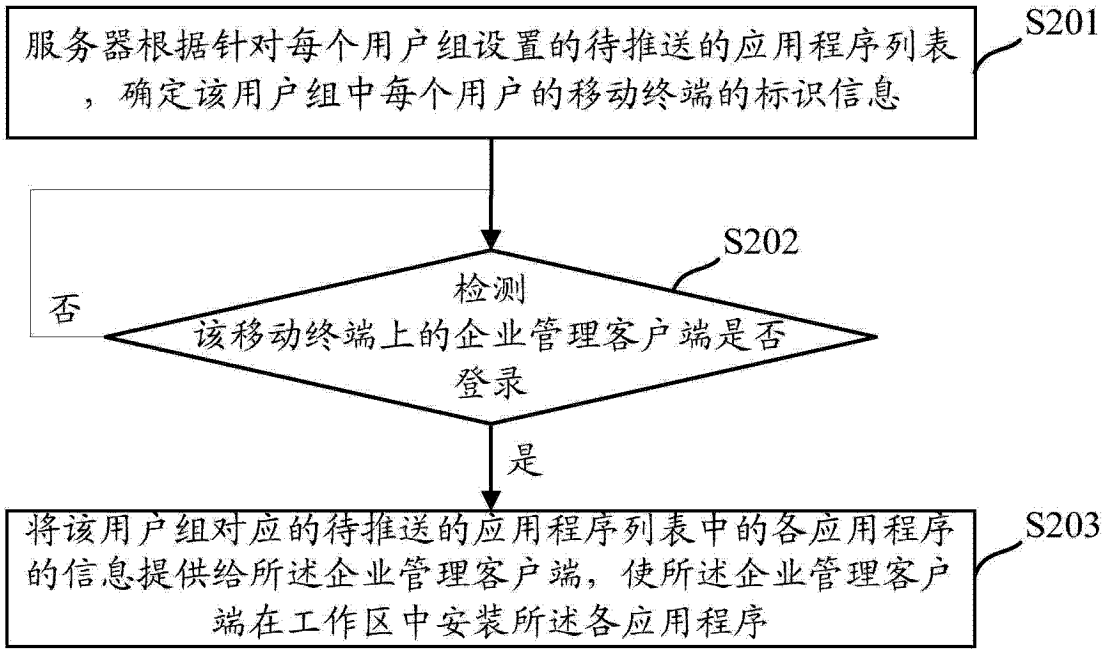

服务器根据针对每个用户组设置的待推送的应用程序列表，确定该用户组中每个用户的移动终端的标识信息
S201
检测
该移动终端上的企业管理客户端是否登录
S202
否
是
将该用户组对应的待推送的应用程序列表中的各应用程序的信息提供给所述企业管理客户端，使所述企业管理客户端在工作区中安装所述各应用程序
S203

图 2

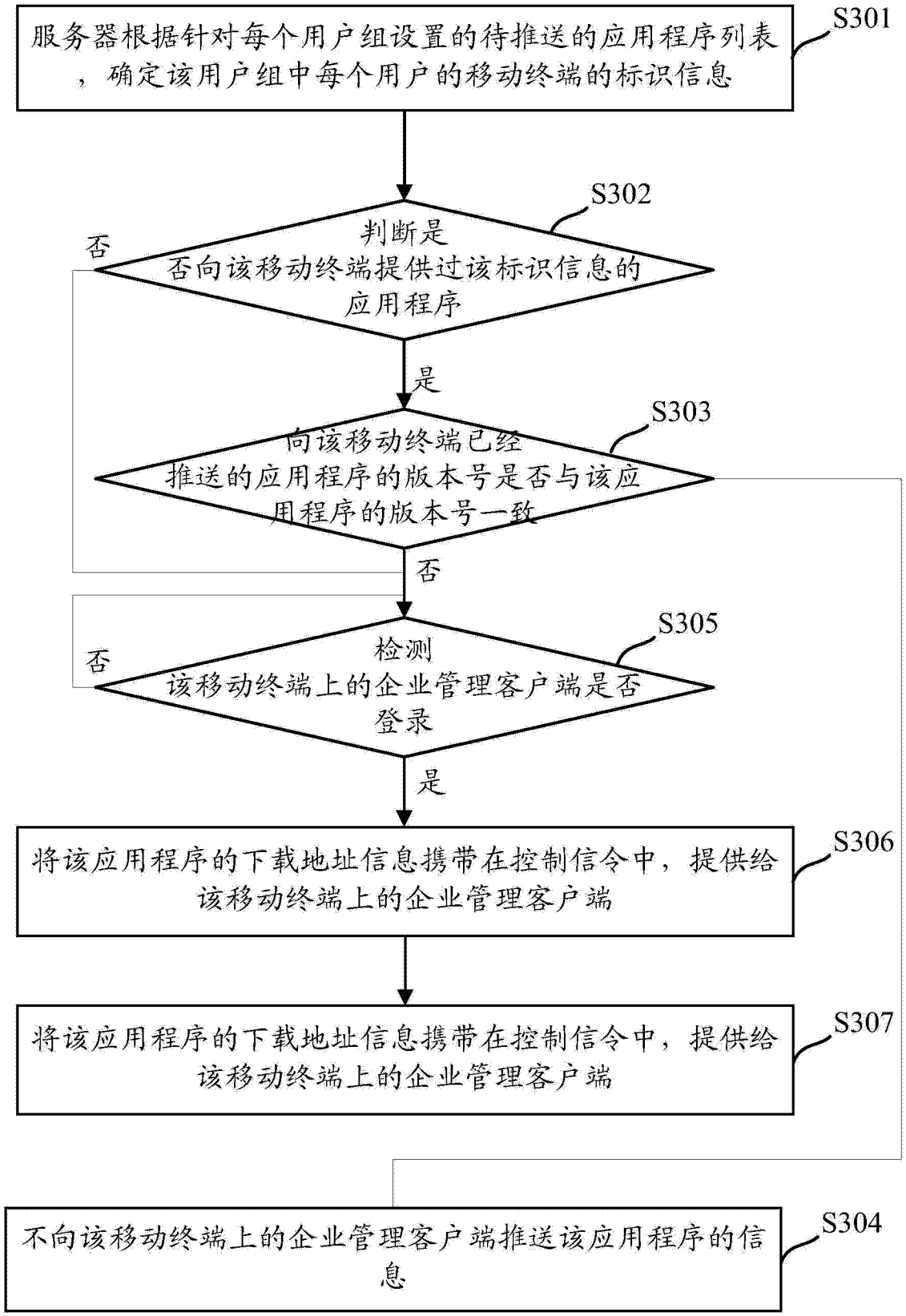

服务器根据针对每个用户组设置的待推送的应用程序列表，确定该用户组中每个用户的移动终端的标识信息
S301
判断是否向该移动终端提供过该标识信息的应用程序
S302
否
是
向该移动终端已经推送的应用程序的版本号是否与该应用程序的版本号一致
S303
否
检测该移动终端上的企业管理客户端是否登录
S305
否
是
将该应用程序的下载地址信息携带在控制信令中，提供给该移动终端上的企业管理客户端
S306
将该应用程序的下载地址信息携带在控制信令中，提供给该移动终端上的企业管理客户端
S307
不向该移动终端上的企业管理客户端推送该应用程序的信息
S304

图 3

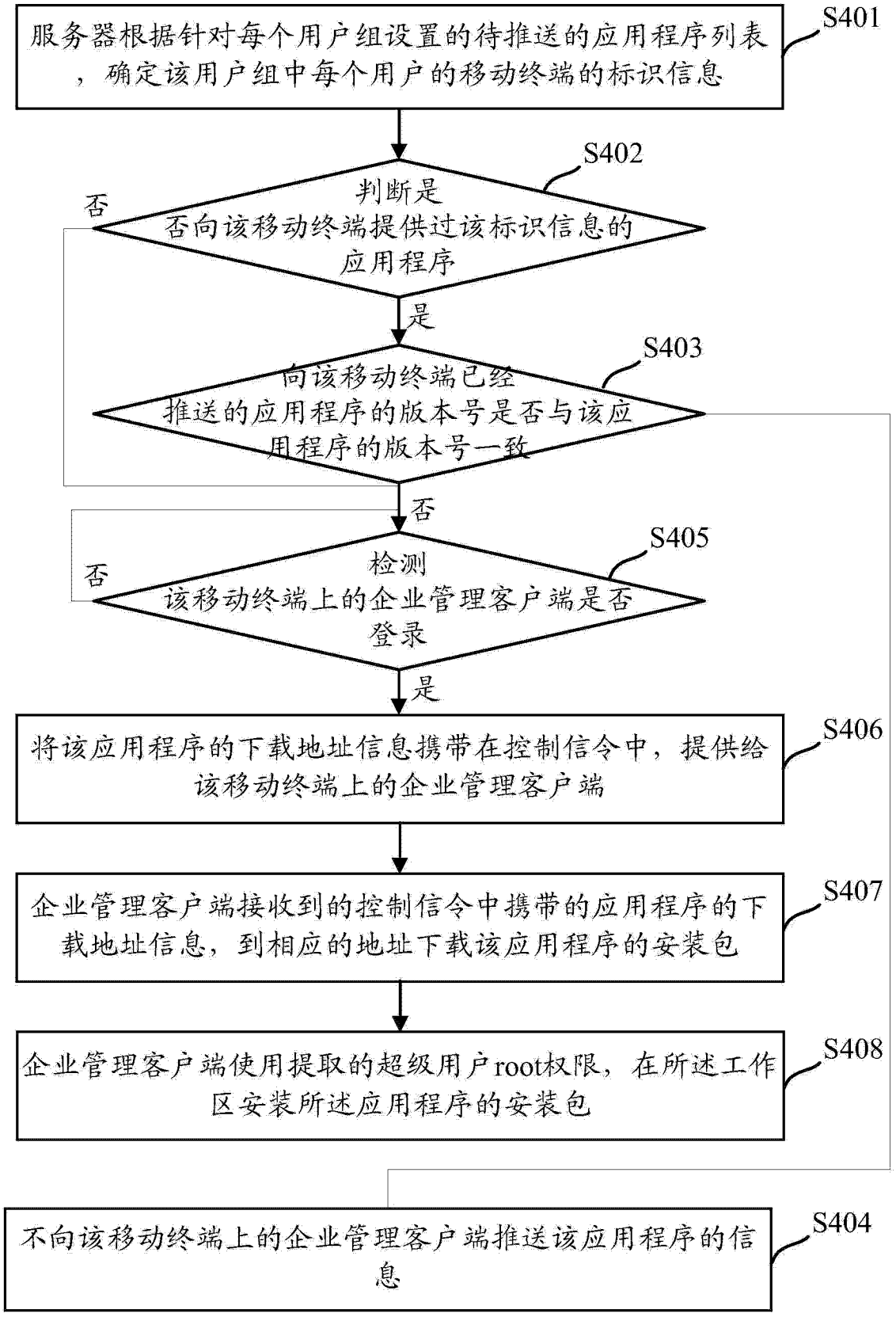

服务器根据针对每个用户组设置的待推送的应用程序列表，确定该用户组中每个用户的移动终端的标识信息
S401
判断是否向该移动终端提供过该标识信息的应用程序
S402
否
是
向该移动终端已经推送的应用程序的版本号是否与该应用程序的版本号一致
S403
否
检测该移动终端上的企业管理客户端是否登录
S405
否
是
将该应用程序的下载地址信息携带在控制信令中，提供给该移动终端上的企业管理客户端
S406
企业管理客户端接收到的控制信令中携带的应用程序的下载地址信息，到相应的地址下载该应用程序的安装包
S407
企业管理客户端使用提取的超级用户root权限，在所述工作区安装所述应用程序的安装包
S408
不向该移动终端上的企业管理客户端推送该应用程序的信息
S404

图 4

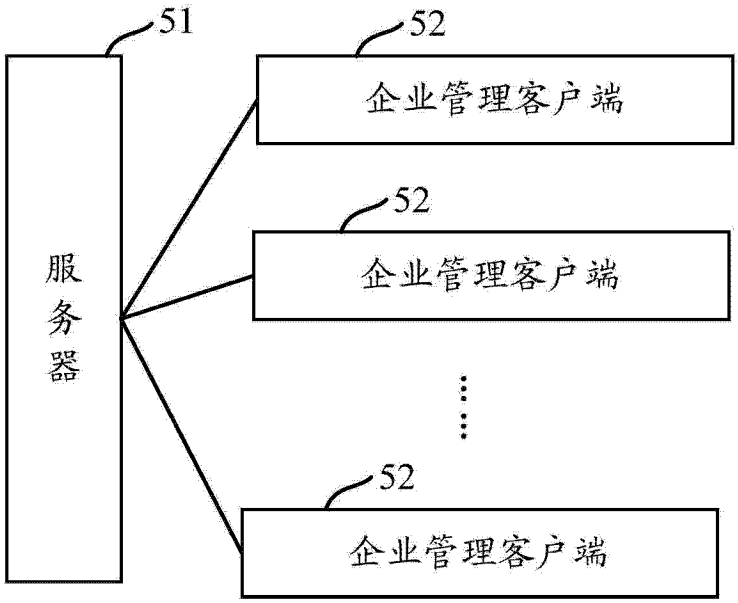


图 5

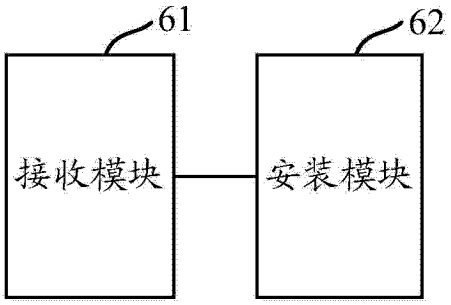


图 6