



(12) 发明专利

(10) 授权公告号 CN 110764807 B

(45) 授权公告日 2021.10.29

(21) 申请号 201911038192.4

(22) 申请日 2019.10.29

(65) 同一申请的已公布的文献号  
申请公布号 CN 110764807 A

(43) 申请公布日 2020.02.07

(73) 专利权人 京东方科技集团股份有限公司  
地址 100015 北京市朝阳区酒仙桥路10号

(72) 发明人 杜洪军

(74) 专利代理机构 北京风雅颂专利代理有限公司 11403

代理人 张聪聪

(51) Int. Cl.

G06F 8/65 (2018.01)

G06F 8/71 (2018.01)

(56) 对比文件

CN 1578307 A, 2005.02.09

CN 109560931 A, 2019.04.02

审查员 林方清

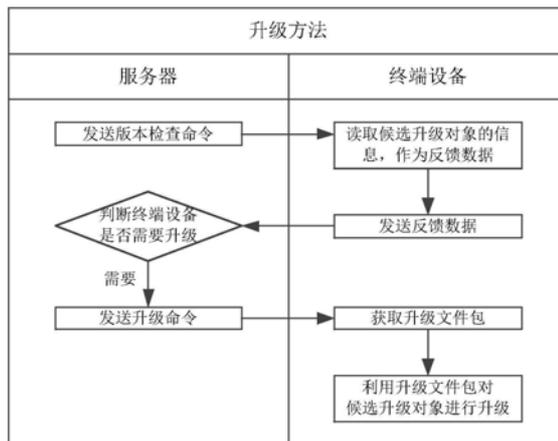
权利要求书3页 说明书15页 附图4页

(54) 发明名称

一种升级方法、系统、服务器及终端设备

(57) 摘要

本发明实施例公开了一种升级方法、系统、服务器及终端设备,方法包括:服务器向终端设备发送版本检查命令;接收终端设备基于版本检查命令发送的反馈数据;基于反馈数据,判断终端设备是否需要升级;如果需要,向终端设备发送升级命令;也就是说,由服务器主动检查终端设备中的版本,仅在版本需要升级的情况下,对终端设备进行升级,这样,可以由服务器确定升级时机,减少了同时对多台设备进行升级的情况,降低了服务器的升级压力。



1. 一种升级方法,其特征在于,应用于服务器,所述方法包括:

向终端设备发送版本检查命令;

接收所述终端设备基于所述版本检查命令发送的反馈数据;

基于所述反馈数据,判断所述终端设备是否需要升级;

如果需要,向终端设备发送升级命令;

所述向终端设备发送版本检查命令,包括:基于第一命令参数和终端设备的标识信息,生成第一命令体;基于预先约定的第一私钥和所述第一命令体,生成第一签名信息;向终端设备发送版本检查命令,所述版本检查命令中包括第一命令名、所述第一命令体和所述第一签名信息;

所述向终端设备发送升级命令,包括:基于第二命令参数和终端设备的标识信息,生成第二命令体;基于预先约定的第二私钥和所述第二命令体,生成第二签名信息;向终端设备发送升级命令,所述升级命令中包括第二命令名、所述第二命令体和所述第二签名信息。

2. 根据权利要求1所述的方法,其特征在于,所述向终端设备发送版本检查命令,包括:

获取升级任务;

基于所述升级任务,确定候选升级终端设备;

在检测到候选升级终端设备上线的情况下,向上线的候选升级终端设备发送版本检查命令。

3. 根据权利要求2所述的方法,其特征在于,所述基于所述反馈数据,判断所述终端设备是否需要升级,包括:

读取所述升级任务中包括的升级版本号信息;

判断所述升级版本号信息与所述反馈数据是否相匹配;

如果不相匹配,表示所述终端设备需要升级。

4. 根据权利要求2所述的方法,其特征在于,所述基于所述反馈数据,判断所述终端设备是否需要升级,包括:

读取所述升级任务中包括的升级对象的摘要值;

判断所述升级对象的摘要值与所述反馈数据是否相匹配;

如果不相匹配,表示所述终端设备需要升级。

5. 根据权利要求2所述的方法,其特征在于,所述向终端设备发送升级命令,包括:

读取所述升级任务中包括的升级文件包的存储地址;

向终端设备发送包括所述存储地址的升级命令。

6. 一种升级方法,其特征在于,应用于终端设备,所述方法包括:

接收服务器发送的版本检查命令;

基于所述版本检查命令,读取候选升级对象的信息,作为反馈数据;

将所述反馈数据发送至所述服务器;

接收所述服务器发送的升级命令,所述升级命令为所述服务器基于所述反馈数据判定所述终端设备需要升级的情况下发送的;

基于所述升级命令,获取升级文件包,并利用所述升级文件包对所述候选升级对象进行升级;

所述版本检查命令中包括第一命令体和第一签名信息;在所述接收服务器发送的版本

检查命令之后,还包括:基于预先约定的第一公钥,验证所述第一命令体与所述第一签名信息是否匹配;如果匹配,执行所述基于所述版本检查命令,读取候选升级对象的信息,作为反馈数据的步骤;

所述升级命令中包括第二命令体和第二签名信息;在所述接收所述服务器发送的升级命令之后,还包括:基于预先约定的第二公钥,验证所述第二命令体与所述第二签名信息是否匹配;如果匹配,执行所述基于所述升级命令,获取升级文件包的步骤。

7. 根据权利要求6所述的方法,其特征在于,所述基于所述版本检查命令,读取候选升级对象的信息,作为反馈数据,包括:

读取候选升级对象的版本号信息,作为反馈数据;

或者,读取候选升级对象的摘要值,作为反馈数据。

8. 根据权利要求6所述的方法,其特征在于,所述基于所述升级命令,获取升级文件包,包括:

读取所述升级命令中包括的升级文件包的存储地址;

基于所述存储地址获取升级文件包;

所述利用所述升级文件包对所述候选升级对象进行升级,包括:

解压所述升级文件包,得到升级脚本;

通过执行所述升级脚本,进行升级操作。

9. 一种升级系统,其特征在于,包括:服务器和终端设备;其中,

所述服务器,用于向终端设备发送版本检查命令;包括:基于第一命令参数和终端设备的标识信息,生成第一命令体;基于预先约定的第一私钥和所述第一命令体,生成第一签名信息;向终端设备发送版本检查命令,所述版本检查命令中包括第一命令名、所述第一命令体和所述第一签名信息;

所述终端设备,用于接收所述版本检查命令;基于所述版本检查命令,读取候选升级对象的信息,作为反馈数据;将所述反馈数据发送至所述服务器;在所述接收服务器发送的版本检查命令之后,还包括:基于预先约定的第一公钥,验证所述第一命令体与所述第一签名信息是否匹配;如果匹配,执行所述基于所述版本检查命令,读取候选升级对象的信息,作为反馈数据的步骤;

所述服务器,还用于接收所述反馈数据;基于所述反馈数据,判断所述终端设备是否需要升级;如果需要,向所述终端设备发送升级命令;所述向终端设备发送升级命令,包括:基于第二命令参数和终端设备的标识信息,生成第二命令体;基于预先约定的第二私钥和所述第二命令体,生成第二签名信息;向终端设备发送升级命令,所述升级命令中包括第二命令名、所述第二命令体和所述第二签名信息;

所述终端设备,还用于在接收到所述升级命令的情况下,基于所述升级命令,获取升级文件包,并利用所述升级文件包对所述候选升级对象进行升级;在所述接收所述服务器发送的升级命令之后,还包括:基于预先约定的第二公钥,验证所述第二命令体与所述第二签名信息是否匹配;如果匹配,执行所述基于所述升级命令,获取升级文件包的步骤。

10. 一种服务器,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时实现如权利要求1至5任意一项所述的方法。

11. 一种终端设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算

机程序,其特征在于,所述处理器执行所述程序时实现如权利要求6至8任意一项所述的方法。

## 一种升级方法、系统、服务器及终端设备

### 技术领域

[0001] 本发明涉及通信技术领域,特别是指一种升级方法、系统、服务器及终端设备。

### 背景技术

[0002] 目前,各种场景中设置有各式各样的电子设备来执行相应的任务。比如,公共场所中设置的路由器可以提供无线网络,显示终端可以进行内容展示,摄像头可以进行监控,等等。

[0003] 一般来说,如果这些电子设备需要进行升级,则这些电子设备可以向服务器发送升级请求,服务器获取升级文件,基于这些升级文件对这些电子设备进行升级操作。

[0004] 上述方案中,如果需要升级的电子设备数量较多,则服务器的升级压力较大。

### 发明内容

[0005] 有鉴于此,本发明的目的在于提出一种升级方法、系统、服务器及终端设备,以降低服务器的升级压力。

[0006] 基于上述目的,本发明实施例提供了一种升级方法,应用于服务器,所述方法包括:

[0007] 向终端设备发送版本检查命令;

[0008] 接收所述终端设备基于所述版本检查命令发送的反馈数据;

[0009] 基于所述反馈数据,判断所述终端设备是否需要升级;

[0010] 如果需要,向终端设备发送升级命令。

[0011] 可选的,所述向终端设备发送版本检查命令,包括:

[0012] 获取升级任务;

[0013] 基于所述升级任务,确定候选升级终端设备;

[0014] 在检测到候选升级终端设备上线的情况下,向上线的候选升级终端设备发送版本检查命令。

[0015] 可选的,所述基于所述反馈数据,判断所述终端设备是否需要升级,包括:

[0016] 读取所述升级任务中包括的升级版本号信息;

[0017] 判断所述升级版本号信息与所述反馈数据是否相匹配;

[0018] 如果不相匹配,表示所述终端设备需要升级。

[0019] 可选的,所述基于所述反馈数据,判断所述终端设备是否需要升级,包括:

[0020] 读取所述升级任务中包括的升级对象的摘要值;

[0021] 判断所述升级对象的摘要值与所述反馈数据是否相匹配;

[0022] 如果不相匹配,表示所述终端设备需要升级。

[0023] 可选的,所述向终端设备发送升级命令,包括:

[0024] 读取所述升级任务中包括的升级文件包的存储地址;

[0025] 向终端设备发送包括所述存储地址的升级命令。

- [0026] 可选的,所述向终端设备发送版本检查命令,包括:
- [0027] 基于第一命令参数和终端设备的标识信息,生成第一命令体;
- [0028] 基于预先约定的第一私钥和所述第一命令体,生成第一签名信息;
- [0029] 向终端设备发送版本检查命令,所述版本检查命令中包括第一命令名、所述第一命令体和所述第一签名信息;
- [0030] 所述向终端设备发送升级命令,包括:
- [0031] 基于第二命令参数和终端设备的标识信息,生成第二命令体;
- [0032] 基于预先约定的第二私钥和所述第二命令体,生成第二签名信息;
- [0033] 向终端设备发送升级命令,所述升级命令中包括第二命令名、所述第二命令体和所述第二签名信息。
- [0034] 基于上述目的,本发明实施例还提供了一种升级方法,应用于终端设备,所述方法包括:
- [0035] 接收服务器发送的版本检查命令;
- [0036] 基于所述版本检查命令,读取候选升级对象的信息,作为反馈数据;
- [0037] 将所述反馈数据发送至所述服务器;
- [0038] 接收所述服务器发送的升级命令,所述升级命令为所述服务器基于所述反馈数据判定所述终端设备需要升级的情况下发送的;
- [0039] 基于所述升级命令,获取升级文件包,并利用所述升级文件包对所述候选升级对象进行升级。
- [0040] 可选的,所述基于所述版本检查命令,读取候选升级对象的信息,作为反馈数据,包括:
- [0041] 读取候选升级对象的版本号信息,作为反馈数据;
- [0042] 或者,读取候选升级对象的摘要值,作为反馈数据。
- [0043] 可选的,所述基于所述升级命令,获取升级文件包,包括:
- [0044] 读取所述升级命令中包括的升级文件包的存储地址;
- [0045] 基于所述存储地址获取升级文件包;
- [0046] 所述利用所述升级文件包对所述候选升级对象进行升级,包括:
- [0047] 解压所述升级文件包,得到升级脚本;
- [0048] 通过执行所述升级脚本,进行升级操作。
- [0049] 可选的,所述版本检查命令中包括第一命令体和第一签名信息;在所述接收服务器发送的版本检查命令之后,还包括:
- [0050] 基于预先约定的第一公钥,验证所述第一命令体与所述第一签名信息是否匹配;如果匹配,执行所述基于所述版本检查命令,读取候选升级对象的信息,作为反馈数据的步骤;
- [0051] 所述升级命令中包括第二命令体和第二签名信息;在所述接收所述服务器发送的升级命令之后,还包括:
- [0052] 基于预先约定的第二公钥,验证所述第二命令体与所述第二签名信息是否匹配;如果匹配,执行所述基于所述升级命令,获取升级文件包的步骤。
- [0053] 基于上述目的,本发明实施例还提供了一种升级系统,包括:服务器和终端设备;

其中，

[0054] 所述服务器，用于向终端设备发送版本检查命令；

[0055] 所述终端设备，用于接收所述版本检查命令；基于所述版本检查命令，读取候选升级对象的信息，作为反馈数据；将所述反馈数据发送至所述服务器；

[0056] 所述服务器，还用于接收所述反馈数据；基于所述反馈数据，判断所述终端设备是否需要升级；如果需要，向所述终端设备发送升级命令；

[0057] 所述终端设备，还用于在接收到所述升级命令的情况下，基于所述升级命令，获取升级文件包，并利用所述升级文件包对所述候选升级对象进行升级。

[0058] 基于上述目的，本发明实施例还提供了一种服务器，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述任一种应用于服务器的升级方法。

[0059] 基于上述目的，本发明实施例还提供了一种终端设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述任一种应用于终端设备的升级方法。

[0060] 应用本发明所示实施例，服务器向终端设备发送版本检查命令；接收终端设备基于版本检查命令发送的反馈数据；基于反馈数据，判断终端设备是否需要升级；如果需要，向终端设备发送升级命令；也就是说，由服务器主动检查终端设备中的版本，仅在版本需要升级的情况下，对终端设备进行升级，这样，可以由服务器确定升级时机，减少了同时对多台设备进行升级的情况，降低了服务器的升级压力。

## 附图说明

[0061] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术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。

[0062] 图1为本发明实施例提供的一种升级系统的结构示意图；

[0063] 图2为本发明实施例提供的一种服务器与终端设备的交互示意图；

[0064] 图3为本发明实施例提供的另一种服务器与终端设备的交互示意图；

[0065] 图4为本发明实施例提供的一种应用于服务器的升级方法的流程示意图；

[0066] 图5为本发明实施例提供的一种应用于终端设备的升级方法的流程示意图；

[0067] 图6为本发明实施例提供的一种服务器的结构示意图；

[0068] 图7为本发明实施例提供的一种终端设备的结构示意图。

## 具体实施方式

[0069] 为使本发明的目的、技术方案和优点更加清楚明白，以下结合具体实施例，并参照附图，对本发明进一步详细说明。

[0070] 需要说明的是，本发明实施例中所有使用“第一”和“第二”的表述均是为了区分两个相同名称非相同的实体或者非相同的参量，可见“第一”“第二”仅为了表述的方便，不应理解为对本发明实施例的限定，后续实施例对此不再一一说明。

[0071] 为了达到上述目的,本发明实施例提供了一种应用于服务器的升级方法、一种应用于终端设备的升级方法、一种服务器、一种终端设备以及一种升级系统。该终端设备可以为各种需要进行升级的设备,比如,路由器、显示终端的控制设备、摄像头等等,具体不做限定。下面首先对该升级系统进行详细介绍。

[0072] 图1为本发明实施例提供的一种升级系统的结构示意图,包括:服务器100和终端设备200,服务器100与终端设备200的交互过程可以如图2所示:

[0073] 服务器100,用于向终端设备200发送版本检查命令;

[0074] 终端设备200,用于接收服务器100发送的版本检查命令;基于所述版本检查命令,读取候选升级对象的信息,作为反馈数据;将所述反馈数据发送至服务器100;

[0075] 服务器100,还用于接收所述反馈数据;基于所述反馈数据,判断终端设备200是否需要升级;如果需要,向终端设备200发送升级命令;

[0076] 终端设备200,还用于在接收到所述升级命令的情况下,基于所述升级命令,获取升级文件包,并利用所述升级文件包对所述候选升级对象进行升级。

[0077] 一种实施方式中,终端设备200和服务器100之间基于MQTT(Message Queuing Telemetry Transport,消息队列遥测传输)协议进行数据传输。或者,另一种实施方式中,终端设备200和服务器100之间可以基于MQTTS(MQTT+TLS;TLS:Transport Layer Security,安全传输层)协议进行数据传输,这样,对传输通道进行了加密,提高了数据传输的安全性。或者,终端设备200与服务器100之间也可以基于TCP(Transmission Control Protocol,传输控制协议)、或者CoAP(Constrained Application Protocol,约束应用协议,一种在物联网协议)、或者其他能够进行长连接的协议进行数据传输,不再一一列举。

[0078] 一种实施方式中,终端设备200中配置有第一代理进程;服务器100接入第二代理进程;所述第一代理进程与所述第二代理进程之间基于MQTT协议、或者MQTTS协议、或者TCP、或者CoAP进行数据传输。以MQTT协议为例来说,可以在终端设备200中配置基于POSIX C(Portable Operating System Interface,可移植操作系统接口)实现的跨平台应用程序,该应用程序以daemon(守护进程)的方式在后台运行,该应用程序即为第一代理进程。

[0079] 举例来说,第二代理进程可以为Broker(一种消息代理)。服务器100和终端设备中配置的第一代理进程均接入Broker。Broker可以配置在服务器100中,或者,Broker可以配置在其他设备中,服务器100接入配置有Broker的设备。终端设备200中配置的应用程序通过Broker接收服务器发送的命令,比如上述版本检查命令和升级命令。

[0080] 举例来说,上述候选升级对象为可能需要升级的软件、或者配置文件、或者其他文件等等,具体的升级对象不做限定。

[0081] 举例来说,版本检查命令和升级命令中均可以包括命令名和命令体,命令名即为需要执行的命令的名称,命令体中可以包括执行该命令所需要的参数。举例来说,服务器可以将命令名和命令体组装为JSON(JavaScript Object Notation,JS对象简谱)格式的命令,命令的具体格式不做限定。

[0082] 一种实施方式中,服务器生成命令(版本检查命令或者升级命令)的过程可以包括:获取待执行命令的命令名、命令参数、以及指向的终端设备的标识信息;基于所述命令参数和所述终端设备的标识信息,生成命令体;生成包括所述命令名和所述命令体的命令。

[0083] 举例来说,终端设备的标识信息可以为设备序列号,或者也可以为其他能够标识

终端设备的信息,具体不做限定。服务器和终端设备接入Broker后,终端设备订阅主题,然后服务器便可以通过Publish(发布)将命令发送至终端设备。

[0084] 另一种实施方式中,服务器生成版本检查命令的过程可以包括:基于第一命令参数和终端设备的标识信息,生成第一命令体;基于预先约定的第一私钥和所述第一命令体,生成第一签名信息;生成包括第一命令名、所述第一命令体和所述第一签名信息的命令。

[0085] 服务器生成升级命令的过程可以包括:基于第二命令参数和终端设备的标识信息,生成第二命令体;基于预先约定的第二私钥和所述第二命令体,生成第二签名信息;生成包括第二命令名、所述第二命令体和所述第二签名信息的命令。

[0086] 为了区分描述,将版本检查命令中的命令参数称为第一命令参数,将升级命令中的命令参数称为第二命令参数;将版本检查命令中的命令体称为第一命令体,将升级命令中的命令体称为第二命令体;将版本检查命令中的签名信息称为第一签名信息,将升级命令中的签名信息称为第二签名信息;将生成第一签名信息时涉及的私钥称为第一私钥,将生成第二签名信息时涉及的私钥称为第二私钥;将第一私钥对应的公钥称为第一公钥,将第二私钥对应的公钥称为第二公钥。

[0087] 如果版本检查命令中包括第一命令体和第一签名信息,终端设备在接收到服务器发送的版本检查命令之后,可以基于预先约定的第一公钥,验证所述第一命令体与所述第一签名信息是否匹配;如果匹配,再执行后续步骤。如果升级命令中包括第二命令体和第二签名信息,终端设备在接收到服务器发送的升级命令之后,可以基于预先约定的第二公钥,验证所述第二命令体与所述第二签名信息是否匹配;如果匹配,再执行后续步骤。

[0088] 举例来说,命令中可以包括:命令的ID(Identity,身份标识号)、发送该命令的设备类型、命令名、命令体和签名信息,该命令体中可以包括执行该命令所需要的参数、终端设备的设备标识信息等等。

[0089] 一种情况下,版本检查命令可以为shell命令,假设候选升级对象为软件程序文件“myapp”,版本检查命令的格式可以为:

```
{
  "id":20190730002,           /命令的 ID
  "from":"upgrade_server",   //发送该命令的服务器
                              的标识信息, 这里为升级服务器
  "command":"shell",        /命令名: shell
```

[0090] "body":{"cmd":"/usr/bin/myapp --version","sn":"A0BB3ED2BF3D"}, /命令体: 其中, cmd 表示要执行的 shell 命令, /usr/bin 表示软件的安装目录, 通过/usr/bin/myapp --version 命令, 可以获得软件版本号, sn 表示终端设备的设备标识信息,

```
  "sig": "签名信息"       /签名信息
}
```

[0091] 上述“/usr/bin/myapp--version”中的参数都可以理解为执行版本检查命令所需要的参数,或者称为第一命令参数。

[0092] 一种情况下,升级命令可以为另一种格式的命令(非shell命令),仍假设候选升级

对象为软件程序文件“myapp”，升级命令的格式可以为：

```

{
  "id":20190730003,           //命令的 ID
  "from":"upgrade_server",   //发送该命令的服务
                              //器的标识信息，这里为升级服务器
  "command":"upgrade",       //命令名：upgrade
  "body":{
    "downloadCmd":"wget
http://fileservr.boe.com.cn/publicFile/M00/00/07/Cvxdg910ufBSANe-
[0093] bAAk2jVjzCE08302.gz", //升级包下载命令，其中：wget 表示下载工具，
                              //wget 后面的内容表示下载地址，
    "upgradeScript": "upgrade.sh", //默认值 upgrade.sh，可
                              //省略
    "md5": "36fe52b1f17326f64b5c625361818045", //升级包的 md5 值
    "sn":"A0BB3ED2BF3D" //终端设备的设备标识信息
  }, //命令体
  "sig": "签名信息" //签名信息
}

```

[0094] 上述下载工具、下载地址等都可以理解为执行升级命令所需要的参数，或者称为第二命令参数。升级包的md5值为：利用md5摘要算法，对升级包进行计算得到的值。升级包的md5值可以用于验证升级包是否被篡改。

[0095] 一种实施方式中，服务器生成签名信息的过程可以包括：

[0096] 利用第一编码算法对命令体进行编码处理，得到第一编码后的命令体；基于预先约定的私钥和第一编码后的命令体，生成签名信息；利用第二编码算法对签名信息进行编码处理，得到编码后的签名信息；这样，命令（版本检查命令或者升级命令）中包括的签名信息为编码后的签名信息。

[0097] 举例来说，第一编码算法可以为sha256算法，第二编码算法可以为base64编码算法，命令中包括的签名信息可以为base64编码字符串。或者，也可以采用其他编码算法，具体算法不做限定。

[0098] 这种实施方式中，终端设备接收到命令（版本检查命令或者升级命令）之后，可以先利用第一编码算法对命令体进行编码处理，得到第一编码后的命令体；以及利用第二编码算法对应的解码算法对签名信息进行解码处理，得到第二解码后的签名信息；基于预先约定的公钥，验证所述第一编码后的命令体与所述第二解码后的签名信息是否匹配；如果匹配，再执行后续步骤。

[0099] 延续上述例子，可以利用base64编码算法对应的解码算法对命令中的签名信息进行解码处理，为了区分描述，将这里解码得到的数据称为“第二解码后的签名信息”；以及利用sha256算法对命令体进行编码处理，为了区分描述，将这里编码得到的数据称为“第一编

码后的命令体”。

[0100] 服务器与终端设备预先约定公私钥,举例来说,公钥可以为RSA(一种非对称加密算法)公钥,私钥可以为RSA私钥。服务器基于RSA私钥生成签名信息;终端设备基于RSA公钥,验证第一编码后的命令体与第二解码后的签名信息是否匹配,如果匹配,表示该命令(版本检查命令或者升级命令)未被篡改,也不是伪造的命令,终端设备再执行后续步骤。这可以理解为对命令(版本检查命令或者升级命令)进行安全验证,可以过滤掉被篡改的命令,也可以识别出伪造的命令,提高了升级的安全性。

[0101] 一种实施方式中,如果验证第一编码后的命令体与第二解码后的签名信息匹配,可以进一步验证命令体中的设备标识信息与终端设备的标识信息是否相同;如果相同,表示该命令(版本检查命令或者升级命令)未被篡改,也不是伪造的命令,终端设备再执行后续步骤。这可以理解为对命令(版本检查命令或者升级命令)进行安全验证,可以进一步过滤掉被篡改的命令,也可以进一步识别出伪造的命令,进一步提高了升级的安全性。

[0102] 一种实施方式中,终端设备在验证命令的安全性的过程中,可以将验证结果反馈给服务器。命令中还可以包括命令标识,终端设备可以基于该命令标识向服务器反馈安全验证结果,使得服务器确定该安全验证结果针对哪条命令。

[0103] 比如,若第一编码后的命令体与第二解码后的签名信息未匹配成功,则终端设备向服务器发送包括相应命令标识的第一提示信息。

[0104] 再比如,若命令体中的设备标识信息与终端设备的标识信息不相同,则终端设备向服务器发送包括相应命令标识的第二提示信息。

[0105] 再比如,终端设备执行升级命令的情况下,可以向服务器发送包括升级命令标识的第三提示信息,使得服务器获取到升级命令的执行情况。

[0106] 一种实施方式中,服务器可以获取升级任务,基于所述升级任务,确定候选升级终端设备;在检测到候选升级终端设备上线的情况下,向上线的候选升级终端设备发送版本检查命令。

[0107] 举例来说,相关人员可以在服务器中配置升级任务,升级任务中包括可能需要升级的终端设备的标识信息、升级文件包的下载地址等等。一种情况下,升级任务中还可以包括升级版本号信息,也就是升级后的文件或者软件版本号信息。或者,另一种情况下,升级任务中还可以包括升级对象的摘要值,也就是对升级后的文件或者软件进行摘要算法后得到的值,比如,摘要算法可以为md5(Message-Digest Algorithm,一种被广泛使用的密码散列函数)摘要算法,摘要值可以为md5值。升级任务的具体内容不做限定。

[0108] 服务器获取到升级任务后,通过读取升级任务,确定候选升级终端设备,也就是可能需要升级的终端设备;然后服务器可以监测候选升级终端设备是否上线,如果上线,则向上线的候选升级终端设备发送版本检查命令。

[0109] 一种情况下,候选升级终端设备接收到该版本检查命令后,可以先对该版本检查命令进行安全验证(可选步骤),上面内容中已经对安全验证的过程进行了介绍,这里不再赘述。该版本检查命令通过安全验证后,候选升级终端设备通过解析该版本检查命令,确定候选升级对象,也就是可能需要升级的文件或者软件。

[0110] 一种情况下,可以读取候选升级对象的版本号信息,作为反馈数据。或者,另一种情况下,可以读取候选升级对象的摘要值,作为反馈数据。摘要值可以为:对候选升级对象

进行摘要算法后得到的值,比如,摘要算法可以为md5摘要算法,摘要值可以为md5值。举例来说,如果候选升级对象没有版本号,则可以将其摘要值作为反馈数据。

[0111] 终端设备将该反馈数据发送至服务器。一种情况下,服务器读取所述升级任务中包括的升级版本号信息;判断所述升级版本号信息与所述反馈数据是否相匹配;如果不相匹配,表示所述终端设备需要升级。另一种情况下,服务器读取所述升级任务中包括的升级对象的摘要值;判断所述升级对象的摘要值与所述反馈数据是否相匹配;如果不相匹配,表示所述终端设备需要升级。

[0112] 举例来说,如果升级任务中包括升级版本号信息,则反馈数据也为候选升级对象的版本号信息;如果二者相匹配,则表示该候选升级对象已是最新版本,不需要升级,如果二者不匹配,则表示该候选升级对象不是最新版本,需要升级。如果升级任务中包括升级对象的摘要值,则反馈数据也为候选升级对象的摘要值;如果二者相匹配,则表示该候选升级对象已是最新版本,不需要升级,如果二者不匹配,则表示该候选升级对象不是最新版本,需要升级。

[0113] 举例来说,如上所述,升级任务中可以包括升级文件包的下载地址,这样,服务器可以读取所述升级任务中包括的升级文件包的存储地址;向终端设备发送包括所述存储地址的升级命令。

[0114] 终端设备可以读取所述升级命令中包括的升级文件包的存储地址;基于所述存储地址获取升级文件包;解压所述升级文件包,得到升级脚本;通过执行所述升级脚本,进行升级操作。

[0115] 举例来说,升级包中可以包括升级脚本upgrade.sh、以及升级所需的其他文件等等,终端设备可以执行升级脚本upgrade.sh,该升级脚本upgrade.sh自动基于升级包中的文件进行升级操作。这样,不需要对终端设备的配置进行修改,便可以通过升级脚本实现升级逻辑的灵活定制。

[0116] 应用本发明所示实施例,第一方面,由服务器主动检查终端设备中的版本,仅在版本需要升级的情况下,对终端设备进行升级,这样,可以由服务器确定升级时机,服务器可以主动分散升级时间段,或者主动分散存储升级文件包的设备,减少了多台设备同时进行升级、同时访问同一设备中的升级文件包的情况,降低了升级压力。

[0117] 第二方面,一些相关方案中,终端设备通过轮询访问服务器,判断是否存在最新版本,以进行版本升级;这样,服务器的访问压力较大。而本方案中,由服务器主动发起版本检查,服务器可以主动分散版本检查时机,降低了访问压力。

[0118] 第三方面,一种实施方式中,升级文件包中包括升级脚本,终端设备通过执行升级脚本进行升级操作,这样,不需要对终端设备的配置进行修改,便可以通过升级脚本实现升级逻辑的灵活定制。

[0119] 下面参考图3,介绍一种具体的实施方式:

[0120] 对终端设备来说:

[0121] 可以在终端设备中配置基于POSIX C实现的跨平台应用程序,该应用程序以daemon的方式在后台运行,该应用程序即为第一代理进程。举例来说,该应用程序可以装载命令处理程序,以执行版本检查命令(shell命令)和升级命令(upgrade命令);该应用程序可以订阅接收服务器发送的命令;该应用程序可以对接收到的命令进行安全验证,并将通

过安全验证的命令发送给相应的命令处理程序。

[0122] 命令处理程序可以包括shell执行程序 and 升级程序;该shell执行程序可以执行版本检查命令,并通过Publish(发布)将执行结果发送至服务器;该升级程序可以执行升级文件包校验、下载、解压、以及执行升级脚本等操作,并通过Publish将执行结果发送至服务器。

[0123] 终端设备启动第一代理进程,加载RSA公钥,加载shell执行程序和升级程序。此外,终端设备接入第二代理进程,第一代理进程与第二代理进程之间基于MQTT协议进行通信,终端设备订阅主题。延续上述例子,终端设备的标识信息为序列号A0BB3ED2BF3D,则终端设备可以订阅topic cmd/A0BB3ED2BF3D,topic表示订阅主题,cmd是command的缩写,表示命令提示符。

[0124] 对于服务器来说:

[0125] 服务器接入第二代理进程,加载RSA私钥,获取到升级任务后,基于该升级任务确定候选升级终端设备;接收到终端设备的上线消息后,判断上线的终端设备是否为候选升级终端设备,如果是,则组装第一命令体,对该第一命令体进行RSA私钥签名,生成第一签名信息,组装版本检查命令;向上线的候选升级终端设备发送该版本检查命令。由于终端设备订阅了topic cmd/A0BB3ED2BF3D,服务器便可以通过Publish将该版本检查命令发送至该终端设备。

[0126] 终端设备接收到服务器发送的命令后,先基于RSA公钥验证命令中的签名信息是合法,如果合法,则判断该命令是版本检查命令还是升级命令;如果是版本检查命令,则将该版本检查命令发送给shell执行程序,以执行该版本检查命令,并将执行结果也就是反馈数据发送至服务器。

[0127] 服务器接收到终端设备发送的反馈数据后,基于该反馈数据,判断该终端设备是需要升级,如果不需要升级,则可以记录该终端设备为最新版本,如果需要升级,则组装第二命令体,对该第二命令体进行RSA私钥签名,生成第二签名信息,组装升级命令。由于终端设备订阅了topic cmd/A0BB3ED2BF3D,服务器便可以通过Publish(发布)将该升级命令发送至该终端设备。

[0128] 终端设备接收到服务器发送的命令后,先基于RSA公钥验证命令中的签名信息是合法,如果合法,则判断该命令是版本检查命令还是升级命令;如果是升级命令,则将该升级命令发送给升级程序,以执行该升级命令:下载升级文件包,判断该升级文件包是否合法,如果合法,解压该升级文件包,执行该升级文件包中的升级脚本,并将升级结果发送至服务器。

[0129] 如果升级结果为升级成功,则服务器可以记录该终端设备为最新版本,如果升级结果为升级失败,则服务器可以记录失败次数、失败时间等信息,以便后续处理。

[0130] 一些情况下,如果终端设备接收到其他命令,可以进行其他处理。如果终端设备验证命令不合法、或者升级文件包不合法,可以输出提示信息。

[0131] 应用本发明所示实施例,第一方面,由服务器主动检查终端设备中的版本,仅在版本需要升级的情况下,对终端设备进行升级,这样,可以由服务器确定升级时机,服务器可以主动分散升级时间段,或者主动分散存储升级文件包的设备,减少了多台设备同时进行升级、同时访问同一设备中的升级文件包的情况,降低了升级压力。

[0132] 第二方面,一些相关方案中,终端设备通过轮询访问服务器,判断是否存在最新版本,以进行版本升级;这样,服务器的访问压力较大。而本方案中,由服务器主动发起版本检查,服务器可以主动分散版本检查时机,降低了访问压力。

[0133] 第三方面,一种实施方式中,升级文件包中包括升级脚本,终端设备通过执行升级脚本进行升级操作,这样,不需要对终端设备的配置进行修改,便可以通过升级脚本实现升级逻辑的灵活定制。

[0134] 第四方面,MQTT协议的通信方式的通用性较佳,不需要专门定制的终端设备和服务器,只需要在终端设备中配置第一处理进程,并且将服务器接入第二处理进程即可。

[0135] 第五方面,终端设备对命令进行签名验证和/或设备标识信息验证,可以过滤掉被篡改的命令,也可以识别出伪造的命令,提高了升级的安全性。

[0136] 下面对应用于服务器的升级方法进行介绍,如图4所示,图4为一种应用于服务器的升级方法的流程示意图,包括:

[0137] S401:向终端设备发送版本检查命令。

[0138] 一种实施方式中,服务器生成版本检查命令的过程可以包括:获取第一命令名、第一命令参数、以及指向的终端设备的标识信息;基于第一命令参数和所述终端设备的标识信息,生成第一命令体;生成包括第一命令名和第一命令体的版本检查命令。

[0139] 命令名即为需要执行的命令的名称,命令参数即为执行命令所需要的参数,比如版本号的存储目录、可能需要升级的对象的标识等等。指向的终端设备也就是需要进行升级的终端设备,终端设备的标识信息可以为设备序列号,或者也可以为其他能够标识终端设备的信息,具体不做限定。

[0140] 为了区分描述,将版本检查命令的命令名称为第一命令名,将升级命令中的命令名称为第二命令名,将版本检查命令中的命令参数称为第一命令参数,将升级命令中的命令参数称为第二命令参数,将版本检查命令中的命令体称为第一命令体,将升级命令中的命令体称为第二命令体。

[0141] 另一种实施方式中,服务器生成版本检查命令的过程可以包括:基于第一命令参数和终端设备的标识信息,生成第一命令体;基于预先约定的第一私钥和所述第一命令体,生成第一签名信息;生成包括第一命令名、所述第一命令体和所述第一签名信息的命令。

[0142] 为了区分描述,将版本检查命令中的签名信息称为第一签名信息,将升级命令中的签名信息称为第二签名信息,将生成第一签名信息时涉及的私钥称为第一私钥,将生成第二签名信息时涉及的私钥称为第二私钥。

[0143] 服务器与终端设备预先约定公私钥,举例来说,公钥可以为RSA公钥,私钥可以为RSA私钥。服务器基于RSA私钥生成签名信息;终端设备基于RSA公钥验证签名信息是否合法。这可以理解为对版本检查命令进行安全验证,可以过滤掉被篡改的命令,也可以识别出伪造的命令,提高了升级的安全性。

[0144] 一种实施方式中,服务器生成第一签名信息的过程可以包括:

[0145] 利用第一编码算法对第一命令体进行编码处理,得到编码后的命令体;基于预先约定的第一私钥和该编码后的命令体,生成第一签名信息;利用第二编码算法对第一签名信息进行编码处理,得到编码后的签名信息;这样,版本检查命令中包括的签名信息为编码后的签名信息。

[0146] 举例来说,第一编码算法可以为sha256算法,第二编码算法可以为base64编码算法,命令中包括的签名信息可以为base64编码字符串。或者,也可以采用其他编码算法,具体算法不做限定。

[0147] 一种情况下,版本检查命令可以为shell命令,假设候选升级对象为软件程序文件“myapp”,版本检查命令的格式可以为:

```

    {
      "id":20190730002,           /命令的 ID
      "from":"upgrade_server",  //发送该命令的服务器
                                的标识信息, 这里为升级服务器
      "command":"shell",        /命令名: shell
[0148]   "body":{"cmd":"/usr/bin/myapp --version","sn":"A0BB3ED2BF3D"}, /命令
        体: 其中, cmd 表示要执行的 shell 命令, /usr/bin 表示软件的安装目录,
        通过/usr/bin/myapp --version 命令, 可以获得软件版本号, sn 表示终端设备的
        设备标识信息,
        "sig":“签名信息”      /签名信息
    }

```

[0149] 上述“/usr/bin/myapp--version”中的参数都可以理解为执行版本检查命令所需要的参数,或者称为第一命令参数。

[0150] 一种实施方式中,S401可以包括:获取升级任务,基于所述升级任务,确定候选升级终端设备;在检测到候选升级终端设备上线的情况下,向上线的候选升级终端设备发送版本检查命令。

[0151] 举例来说,相关人员可以在服务器中配置升级任务,升级任务中包括可能需要升级的终端设备的标识信息、升级文件包的下载地址等等。一种情况下,升级任务中还可以包括升级版本号信息,也就是升级后的文件或者软件版本号信息。或者,另一种情况下,升级任务中还可以包括升级对象的摘要值,也就是对升级后的文件或者软件进行摘要算法后得到的值,比如,摘要算法可以为md5(Message-Digest Algorithm,一种被广泛使用的密码散列函数)摘要算法,摘要值可以为md5值。升级任务的具体内容不做限定。

[0152] 服务器获取到升级任务后,通过读取升级任务,确定候选升级终端设备,也就是可能需要升级的终端设备;然后服务器可以监测候选升级终端设备是否上线,如果上线,则向上线的候选升级终端设备发送版本检查命令。

[0153] S402:接收终端设备基于版本检查命令发送的反馈数据。

[0154] 一种情况下,终端设备读取候选升级对象的版本号信息,作为反馈数据;或者,另一种情况下,终端设备读取候选升级对象的摘要值,作为反馈数据。举例来说,如果候选升级对象没有版本号,则可以将其摘要值作为反馈数据。

[0155] 举例来说,上述候选升级对象为可能需要升级的软件、或者配置文件、或者其他文件等等,具体的升级对象不做限定。

[0156] S403:基于该反馈数据,判断终端设备是否需要升级,如果需要,执行S404。

[0157] 一种实施方式中,S403可以包括:读取所述升级任务中包括的升级版本号信息;判

断所述升级版本号信息与所述反馈数据是否相匹配;如果不相匹配,表示所述终端设备需要升级。

[0158] 另一种实施方式中,S403可以包括:读取所述升级任务中包括的升级对象的摘要值;判断所述升级对象的摘要值与所述反馈数据是否相匹配;如果不相匹配,表示所述终端设备需要升级。

[0159] 举例来说,如果升级任务中包括升级版本号信息,则反馈数据也为候选升级对象的版本号信息;如果二者相匹配,则表示该候选升级对象已是最新版本,不需要升级,如果二者不匹配,则表示该候选升级对象不是最新版本,需要升级。如果升级任务中包括升级对象的摘要值,则反馈数据也为候选升级对象的摘要值;如果二者相匹配,则表示该候选升级对象已是最新版本,不需要升级,如果二者不匹配,则表示该候选升级对象不是最新版本,需要升级。

[0160] S404:向终端设备发送升级命令。

[0161] 延续上述例子,升级任务中可以包括升级文件包的下载地址,这样,服务器可以读取所述升级任务中包括的升级文件包的存储地址;向终端设备发送包括所述存储地址的升级命令。

[0162] 或者,另一种情况下,升级命令中可以包括升级文件包,终端设备基于该升级文件包进行升级。

[0163] 一种实施方式中,服务器生成升级命令的过程可以包括:获取第二命令名、第二命令参数、以及指向的终端设备的标识信息;基于第二命令参数和所述终端设备的标识信息,生成第二命令体;生成包括第二命令名和第二命令体的升级命令。

[0164] 另一种实施方式中,服务器生成升级命令的过程可以包括:基于第二命令参数和终端设备的标识信息,生成第二命令体;基于预先约定的第二私钥和所述第二命令体,生成第二签名信息;生成包括第二命令名、所述第二命令体和所述第二签名信息的命令。

[0165] 服务器与终端设备预先约定公私钥,举例来说,公钥可以为RSA公钥,私钥可以为RSA私钥。服务器基于RSA私钥生成签名信息;终端设备基于RSA公钥验证签名信息是否合法。这可以理解为对升级命令进行安全验证,可以过滤掉被篡改的命令,也可以识别出伪造的命令,提高了升级的安全性。

[0166] 一种实施方式中,服务器生成第二签名信息的过程可以包括:

[0167] 利用第一编码算法对命令体进行编码处理,得到编码后的命令体;基于预先约定的私钥和编码后的命令体,生成第二签名信息;利用第二编码算法对签名信息进行编码处理,得到编码后的签名信息;这样,升级命令中包括的签名信息为编码后的签名信息。

[0168] 举例来说,第一编码算法可以为sha256算法,第二编码算法可以为base64编码算法,命令中包括的签名信息可以为base64编码字符串。或者,也可以采用其他编码算法,具体算法不做限定。

[0169] 一种情况下,升级命令可以为另一种格式的命令(非shell命令),仍假设候选升级对象为软件程序文件“myapp”,升级命令的格式可以为:

```

    {
      "id":20190730003, //命令的 ID
      "from":"upgrade_server", //发送该命令的服务
器的标识信息，这里为升级服务器
      "command":"upgrade", //命令名：upgrade
      "body":{
        "downloadCmd":"wget
[0170] http://fileserver.boe.com.cn/publicFile/M00/00/07/Cvxg910ufBSANe-
bAAk2jVjzCE08302.gz", //升级包下载命令，其中：wget 表示下载工具，
wget 后面的内容表示下载地址，
        "upgradeScript": "upgrade.sh", //默认值 upgrade.sh，可
省略
        "md5": "36fe52b1f17326f64b5c625361818045", //升级包的 md5 值
        "sn": "A0BB3ED2BF3D" //终端设备的设备标识信息
      }, //命令体
[0171] "sig": "签名信息" //签名信息
    }

```

[0172] 上述下载工具、下载地址等都可以理解为执行升级命令所需要的参数，或者称为第二命令参数。升级包的md5值为：利用md5 (Message-Digest Algorithm, 一种被广泛使用的密码散列函数) 摘要算法，对升级包进行计算得到的值。升级包的md5值可以用于验证升级包是否被篡改。

[0173] 应用本发明所示实施例，第一方面，由服务器主动检查终端设备中的版本，仅在版本需要升级的情况下，对终端设备进行升级，这样，可以由服务器确定升级时机，服务器可以主动分散升级时间段，或者主动分散存储升级文件包的设备，减少了多台设备同时进行升级、同时访问同一设备中的升级文件包的情况，降低了升级压力。第二方面，由服务器主动发起版本检查，服务器可以主动分散版本检查时机，降低了访问压力。

[0174] 下面对应用于终端设备的升级方法进行介绍，该终端设备可以为各种需要进行升级的设备，比如，路由器、显示终端的控制设备、摄像头等等，具体不做限定。如图5所示，图5为一种应用于终端设备的升级方法的流程示意图，包括：

[0175] S501：接收服务器发送的版本检查命令。

[0176] S502：基于版本检查命令，读取候选升级对象的信息，作为反馈数据。

[0177] 一些情况下，终端设备可以先对接收到的版本检查命令进行安全验证，通过安全验证后，再执行S402。

[0178] 一种实施方式中，版本检查命令中包括第一命令体和第一签名信息；S401之后还包括：基于预先约定的第一公钥，验证所述第一命令体与所述第一签名信息是否匹配；如果匹配，再执行S402。

[0179] 为了区分描述，将第一私钥对应的公钥称为第一公钥，将第二私钥对应的公钥称

为第二公钥。

[0180] 服务器与终端设备预先约定公私钥,举例来说,公钥可以为RSA公钥,私钥可以为RSA私钥。服务器基于RSA私钥生成签名信息;终端设备基于RSA公钥,验证编码后的命令体与解码后的签名信息是否匹配,如果匹配,表示版本检查命令未被篡改,也不是伪造的命令,终端设备再执行后续步骤。这可以理解为对命令(版本检查命令或者升级命令)进行安全验证,可以过滤掉被篡改的命令,也可以识别出伪造的命令,提高了升级的安全性。

[0181] 终端设备接收到版本检查命令之后,可以先利用第一编码算法对第一命令体进行编码处理,得到编码后的命令体;以及利用第二编码算法对应的解码算法对签名信息进行解码处理,得到解码后的签名信息;基于预先约定的公钥,验证编码后的命令体与解码后的签名信息是否匹配;如果匹配,再执行后续步骤。

[0182] 举例来说,第一编码算法可以为sha256算法,第二编码算法可以为base64编码算法。

[0183] 一种实施方式中,如果验证编码后的命令体与解码后的签名信息匹配,可以进一步验证命令体中的设备标识信息与终端设备的标识信息是否相同;如果相同,表示该版本检查命令未被篡改,也不是伪造的命令,终端设备再执行后续步骤。这可以理解为对版本检查命令进行安全验证,可以进一步过滤掉被篡改的命令,也可以进一步识别出伪造的命令,进一步提高了升级的安全性。

[0184] 候选升级对象为可能需要升级的软件、或者配置文件、或者其他文件等等,具体的升级对象不做限定。一种情况下,可以读取候选升级对象的版本号信息,作为反馈数据。或者,另一种情况下,可以读取候选升级对象的摘要值,作为反馈数据。摘要值可以为:对候选升级对象进行摘要算法后得到的值,比如,摘要算法可以为md5摘要算法,摘要值可以为md5值。举例来说,如果候选升级对象没有版本号,则可以将其摘要值作为反馈数据。

[0185] S503:将该反馈数据发送至服务器。

[0186] S504:接收服务器发送的升级命令,所述升级命令为所述服务器基于所述反馈数据判定所述终端设备需要升级的情况下发送的。

[0187] 一些情况下,终端设备可以先对接收到的升级命令进行安全验证,通过安全验证后,再执行S505。

[0188] 一种实施方式中,升级命令中包括第二命令体和第二签名信息;在S504之后还包括:基于预先约定的第二公钥,验证所述第二命令体与所述第二签名信息是否匹配;如果匹配,再执行S505。

[0189] 对升级命令进行安全验证的过程与对版本检查命令进行安全验证的过程类似,不再赘述。

[0190] S505:基于升级命令,获取升级文件包,并利用升级文件包对候选升级对象进行升级。

[0191] 一种实施方式中,S505可以包括:读取所述升级命令中包括的升级文件包的存储地址;基于所述存储地址获取升级文件包;解压所述升级文件包,得到升级脚本;通过执行所述升级脚本,进行升级操作。

[0192] 举例来说,升级包中可以包括升级脚本upgrade.sh、以及升级所需的其他文件等等,终端设备可以执行升级脚本upgrade.sh,该升级脚本upgrade.sh自动基于升级包中的

文件进行升级操作。这样,不需要对终端设备的配置进行修改,便可以通过升级脚本实现升级逻辑的灵活定制。

[0193] 应用本发明所示实施例,第一方面,一种实施方式中,升级文件包中包括升级脚本,终端设备通过执行升级脚本进行升级操作,这样,不需要对终端设备的配置进行修改,便可以通过升级脚本实现升级逻辑的灵活定制。第二方面,终端设备对命令进行签名验证和/或设备标识信息验证,可以过滤掉被篡改的命令,也可以识别出伪造的命令,提高了升级的安全性。

[0194] 与上述方法实施例相对应,本发明实施例还提供了一种服务器,如图6所示,包括:存储器602、处理器601及存储在存储器602上并可在处理器601上运行的计算机程序,处理器601执行所述程序时实现上述任一种应用于服务器的升级方法。

[0195] 与上述方法实施例相对应,本发明实施例还提供了一种终端设备,如图7所示,包括:存储器702、处理器701及存储在存储器702上并可在处理器701上运行的计算机程序,处理器701执行所述程序时实现上述任一种应用于终端设备的升级方法。

[0196] 本发明实施例还提供一种非暂态计算机可读存储介质,所述非暂态计算机可读存储介质存储计算机指令,所述计算机指令用于使所述计算机执行上述任一种升级方法。

[0197] 所属领域的普通技术人员应当理解:以上任何实施例的讨论仅为示例性的,并非旨在暗示本公开的范围(包括权利要求)被限于这些例子;在本发明的思路下,以上实施例或者不同实施例中的技术特征之间也可以进行组合,步骤可以以任意顺序实现,并存在如上所述的本发明的不同方面的许多其它变化,为了简明它们没有在细节中提供。

[0198] 另外,为简化说明和讨论,并且为了不会使本发明难以理解,在所提供的附图中可以示出或不示出与集成电路(IC)芯片和其它部件的公知的电源/接地连接。此外,可以以框图的形式示出装置,以便避免使本发明难以理解,并且这也考虑了以下事实,即关于这些框图装置的实施方式的细节是高度取决于将要实施本发明的平台的(即,这些细节应当完全处于本领域技术人员的理解范围内)。在阐述了具体细节(例如,电路)以描述本发明的示例性实施例的情况下,对本领域技术人员来说显而易见的是,可以在没有这些具体细节的情况下或者这些具体细节有变化的情况下实施本发明。因此,这些描述应被认为是说明性的而不是限制性的。

[0199] 尽管已经结合了本发明的具体实施例对本发明进行了描述,但是根据前面的描述,这些实施例的很多替换、修改和变型对本领域普通技术人员来说将是显而易见的。例如,其它存储器架构(例如,动态RAM(DRAM))可以使用所讨论的实施例。

[0200] 本发明的实施例旨在涵盖落入所附权利要求的宽泛范围之内的所有这样的替换、修改和变型。因此,凡在本发明的精神和原则之内,所做的任何省略、修改、等同替换、改进等,均应包含在本发明的保护范围之内。

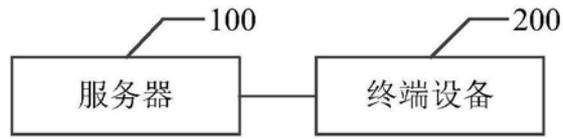


图1

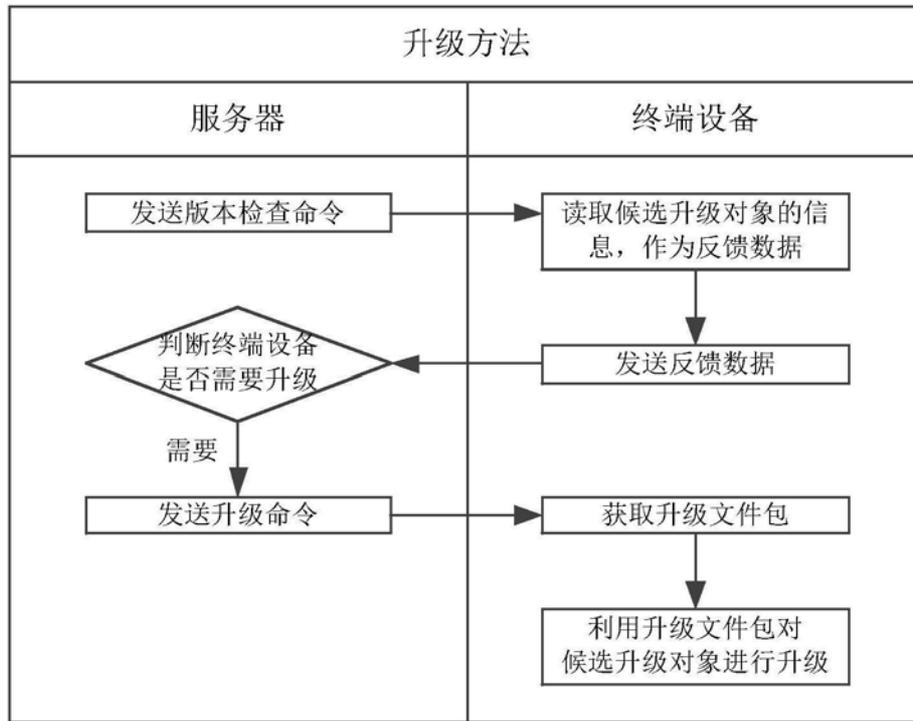


图2

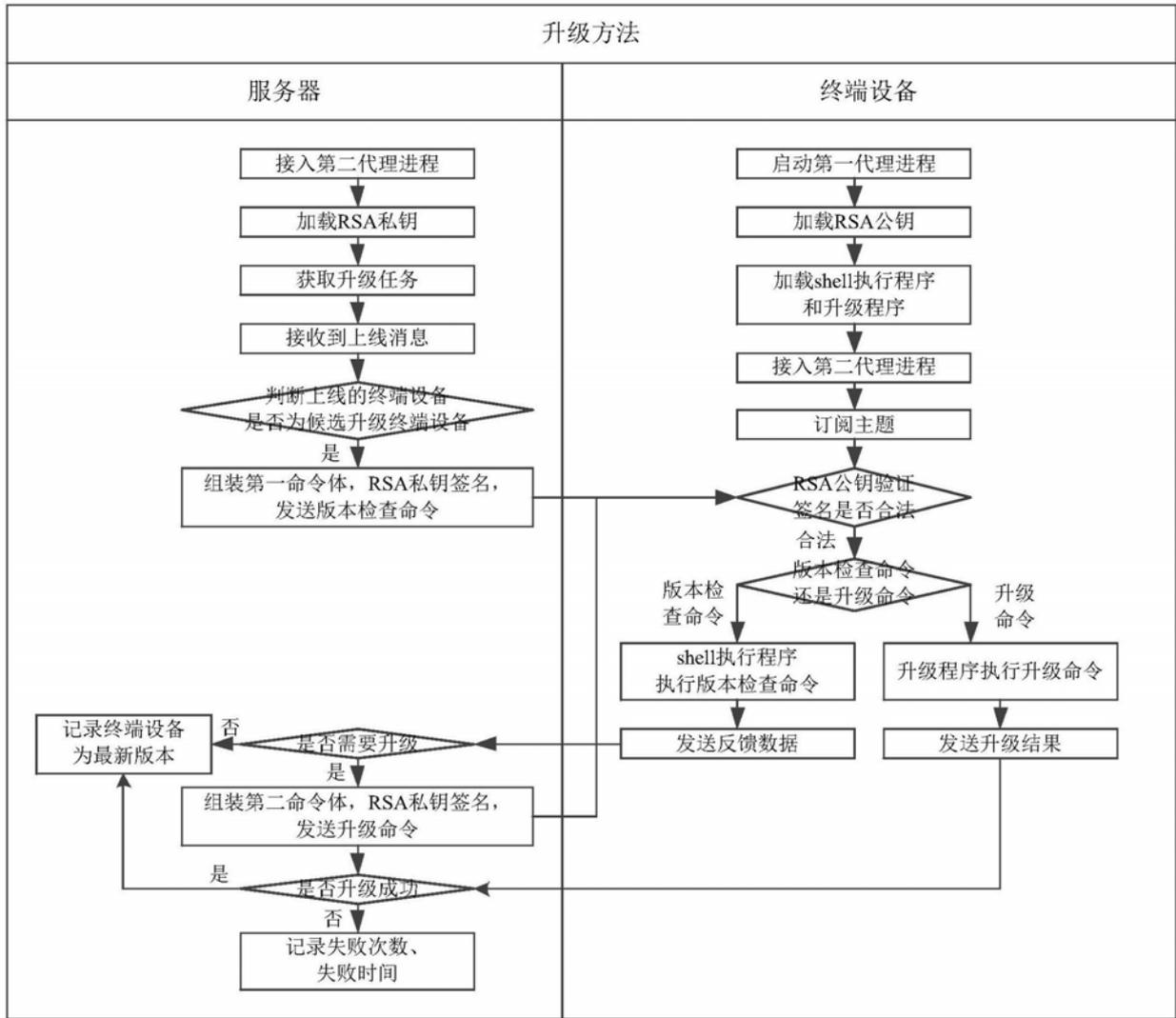


图3

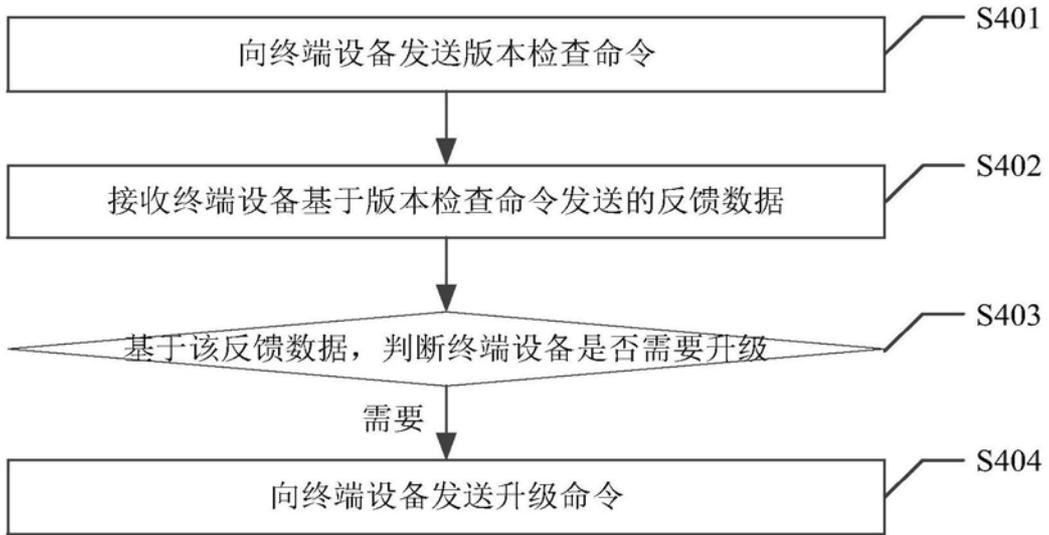


图4

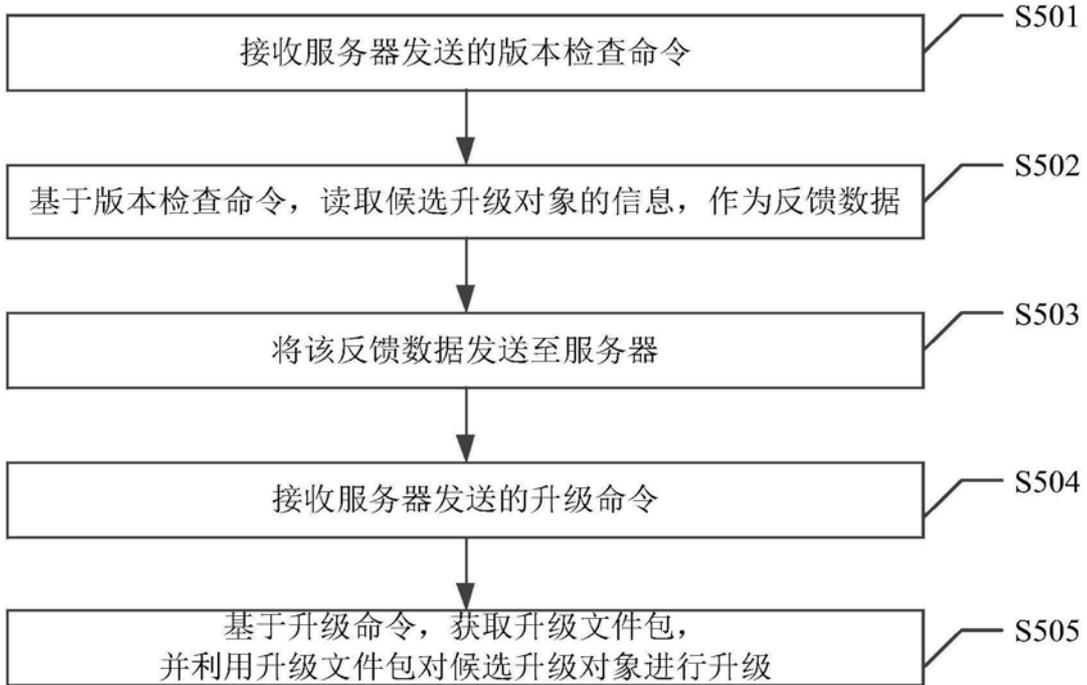


图5

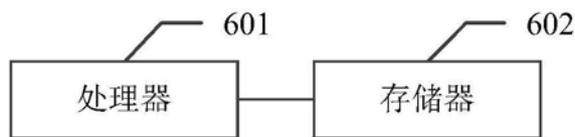


图6

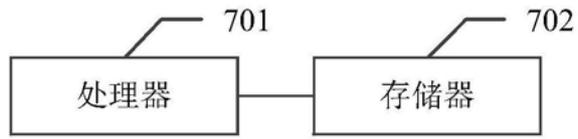


图7