



(12) 发明专利

(10) 授权公告号 CN 104378344 B

(45) 授权公告日 2016. 03. 09

(21) 申请号 201410225078. 3

(22) 申请日 2014. 05. 26

(73) 专利权人 腾讯科技(深圳)有限公司

地址 518044 广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室

(72) 发明人 关立群

(74) 专利代理机构 上海波拓知识产权代理有限公司 31264

代理人 杨波

(51) Int. Cl.

H04L 29/06(2006. 01)

(56) 对比文件

CN 103795731 A, 2014. 05. 14,

审查员 王静

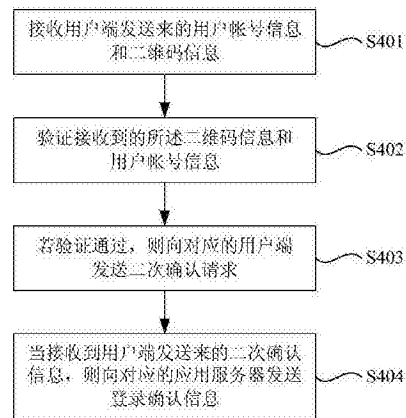
权利要求书4页 说明书10页 附图9页

(54) 发明名称

登录信息传输方法、扫码方法及装置、后台服务器

(57) 摘要

本发明实施例提出一种登录信息传输方法、扫码方法及装置、后台服务器,其登录信息传输方法,包括:接收用户端发送来的用户帐号信息和二维码信息;验证接收到的所述二维码信息和用户帐号信息;若验证通过,则向对应的用户端发送二次确认请求;当接收到用户端发送来的二次确认信息,则向对应的应用服务器发送登录确认信息。本发明可以提高二维码登录技术的安全性。



1. 一种登录信息传输方法,应用于后台服务器,用于至少一用户端和至少一应用服务器之间登录信息的传输,其特征在于,包括:

接收用户端发送来的用户帐号信息和二维码信息,其中,所述二维码信息是由所述后台服务器提供以及显示在登录设备上的二维码被所述用户端拍摄得到的二维码信息,所述用户帐号信息仅包含可以公开的信息,而并不包含密码;

验证接收到的所述二维码信息和用户帐号信息,其中,验证接收到的所述二维码信息是指验证接收到的所述二维码信息与所述后台服务器预存的二维码是否一致,若一致则表示验证通过;验证接收到的所述用户帐号信息是指判断所述后台服务器中是否存有与接收到的所述用户帐号信息中的用户帐号相同的帐号,若存在则表示验证通过;

若验证通过,则向对应的用户端发送二次确认请求;

当接收到用户端发送来的二次确认信息,则向对应的应用服务器发送登录确认信息,以使所述应用服务器向所述登录设备发出通知,并令所述登录设备的应用自动登录,其中,所述登录确认信息包含帐号和密码。

2. 如权利要求 1 所述的登录信息传输方法,其特征在于,所述向对应的应用服务器发送登录确认信息的步骤之后进一步包括:

接收成功登录应用后用户端发送来的长连接请求;

向所述用户端发送长连接响应信息,以建立与相应用户端之间的长连接;

当接收到应用服务器发送来的应用消息,则将所述应用消息通过所述长连接推送给对应的用户端。

3. 如权利要求 2 所述的登录信息传输方法,其特征在于,

所述建立与相应用户端之间的长连接的步骤之后还包括:保存与所述用户端之间的链路信息,所述链路信息是指与用户端之间的连接信息;

所述将所述应用消息推送给对应的用户端的步骤包括:

根据所述用户帐号信息查找预存的用户端标识;

根据查找到的用户端标识查找所述链路信息,并获取具体的长连接物理链路信息;

通过获取的所述长连接物理链路将应用消息推送给对应的用户端。

4. 如权利要求 2 所述的登录信息传输方法,其特征在于,所述当接收到应用服务器发送来的应用消息,则将所述应用消息通过所述长连接推送给对应的用户端的步骤包括:

当接收到应用服务器发送来的应用消息,储存所述应用消息;

定期扫描所述储存的应用消息,判断是否有需要推送的应用消息;

将需要推送的应用消息通过长连接推送给对应的用户端。

5. 如权利要求 4 所述的登录信息传输方法,其特征在于,所述定期扫描所述储存的应用消息,判断是否有需要推送的应用消息的步骤包括:

定期扫描所述储存的应用消息,获取未推送的应用消息;

获取与未推送的应用消息对应的用户端信息;

判断向与未推送的应用消息对应的用户端发送的历史已推送消息是否有对应的回复信息;

若有回复信息,则确定对应的未推送的应用消息为需要推送的应用消息。

6. 一种扫码方法,应用于用户端,用于在二维码登录时通过后台服务器对登录信息进

行确认,其特征在于,包括:

扫描二维码,并获取二维码信息,其中,所述二维码是由所述后台服务器提供并显示在登录设备上的;

获取预设的用户帐号信息,其中,所述用户帐号信息仅包含可以公开的信息,而并不包含密码;

将二维码信息及用户帐号信息发送给所述后台服务器;

接收所述后台服务器对所述二维码信息和用户帐号信息验证通过后发送来的二次确认请求,其中,对所述二维码信息的验证是指验证所述二维码信息与所述后台服务器预存的二维码是否一致,若一致则表示验证通过;对所述用户帐号信息的验证是指判断所述后台服务器中是否存有与所述用户帐号相同的帐号,若存在则表示验证通过;

显示所述二次确认请求的提示信息;

将用户输入的二次确认信息发送给所述后台服务器,由所述后台服务器向对应的应用服务器发送登录确认信息,以使所述应用服务器向所述登录设备发出通知,并令所述登录设备的应用自动登录,其中,所述登录确认信息包含帐号和密码。

7. 如权利要求6所述的扫码方法,其特征在於,所述获取预设的用户帐号信息的步骤包括:

显示预存的帐号;

根据用户选择的帐号,获取对应的用户帐号信息。

8. 如权利要求6所述的扫码方法,其特征在於,所述将用户输入的二次确认信息发送给所述后台服务器的步骤之后进一步包括:

当应用登录成功,则向后台服务器发送长连接请求;

接收后台服务器返回的长连接响应信息,以建立与相应用户端之间的长连接;

实时接收所述后台服务器通过所述长连接推送来的应用消息。

9. 一种后台服务器,用于至少一用户端和至少一应用服务器之间登录信息的传输,其特征在於,包括:

验证信息接收模块,用于接收用户端发送来的用户帐号信息和二维码信息,其中,所述二维码信息是由所述后台服务器提供以及显示在登录设备上的二维码被所述用户端拍摄得到的二维码信息,所述用户帐号信息仅包含可以公开的信息,而并不包含密码;

验证模块,用于验证接收到的所述二维码信息和用户帐号信息,其中,验证接收到的所述二维码信息是指验证接收到的所述二维码信息与所述后台服务器预存的二维码是否一致,若一致则表示验证通过;验证接收到的所述用户帐号信息是指判断所述后台服务器中是否存有与接收到的所述用户帐号信息中的用户帐号相同的帐号,若存在则表示验证通过;

二次确认请求发送模块,用于当所述验证模块对所述二维码信息和用户帐号信息验证通过,则向对应的用户端发送二次确认请求;

二次确认信息接收模块,用于接收用户端发送来的二次确认信息;

登录确认信息发送模块,用于当所述二次确认信息接收模块接收到二次确认信息,则向对应的应用服务器发送登录确认信息,以使所述应用服务器向所述登录设备发出通知,并令所述登录设备的应用自动登录,其中,所述登录确认信息包含帐号和密码。

10. 如权利要求 9 所述的后台服务器,其特征在于,所述后台服务器还包括:
长连接请求接收模块,用于接收成功登录应用后用户端发送来的长连接请求;
长连接响应模块,用于向所述用户端发送长连接响应信息,以建立与相应用户端之间的长连接;

应用消息接收模块,用于接收应用服务器发送来的应用消息;
推送模块,用于当所述应用消息接收模块接收到应用消息,则将所述应用消息通过所述长连接推送给对应的用户端。

11. 如权利要求 10 所述的后台服务器,其特征在于,所述后台服务器还包括:
链路信息保存模块,用于在所述长连接响应模块响应了用户端发送来的长连接请求后,保存与所述用户端之间的链路信息,所述链路信息是指与用户端之间的连接信息;

所述推送模块进一步包括:
标识查找单元,用于根据所述用户帐号信息查找预存的用户端标识;
链路信息查找单元,用于根据查找到的用户端标识查找所述链路信息,并获取具体的长连接物理链路信息;

应用消息推送单元,用于通过获取的所述长连接物理链路将应用消息推送给对应的用户端。

12. 如权利要求 10 所述的后台服务器,其特征在于,
当所述应用消息接收模块接收到应用服务器发送来的应用消息时,储存所述应用消息;

所述推送模块进一步包括:
扫描单元,用于定期扫描所述储存的应用消息,判断是否有需要推送的应用消息;
应用消息推送单元,用于将需要推送的应用消息通过长连接推送给对应的用户端。

13. 如权利要求 12 所述的后台服务器,其特征在于,所述扫描单元进一步包括:
未推送消息获取子单元,用于定期扫描所述储存的应用消息,获取未推送的应用消息;

用户端信息获取子单元,用于获取与未推送的应用消息对应的用户端信息;
回复信息判断子单元,用于判断向与未推送的应用消息对应的用户端发送的历史已推送消息是否有对应的回复信息;

应用消息确定子单元,用于当所述回复信息判断子单元判断出有回复信息,则确定对应的未推送的应用消息为需要推送的应用消息。

14. 一种扫码装置,应用于用户端,用于在二维码登录时通过后台服务器对登录信息进行确认,其特征在于,包括:

扫码模块,用于扫描二维码,并获取二维码信息,其中,所述二维码是由所述后台服务器提供并显示在登录设备上的;

用户帐号信息获取模块,用于获取预设的用户帐号信息,其中,所述用户帐号信息仅包含可以公开的信息,而并不包含密码;

验证信息发送模块,用于将二维码信息及用户帐号信息发送给所述后台服务器;
二次确认请求接收模块,用于接收所述后台服务器对所述二维码信息和用户帐号信息验证通过后发送来的二次确认请求,其中,对所述二维码信息的验证是指验证所述二维码

信息与所述后台服务器预存的二维码是否一致,若一致则表示验证通过;对所述用户帐号信息的验证是指判断所述后台服务器中是否存有与所述用户帐号相同的帐号,若存在则表示验证通过;

提示信息显示模块,用于显示所述二次确认请求的提示信息;

二次确认信息发送模块,用于将用户输入的二次确认信息发送给所述后台服务器,由所述后台服务器向对应的应用服务器发送登录确认信息,以使所述应用服务器向所述登录设备发出通知,并令所述登录设备的应用自动登录,其中,所述登录确认信息包含帐号和密码。

15. 如权利要求 14 所述的扫码装置,其特征在于,所述用户帐号信息获取模块进一步包括:

帐号显示单元,用于显示预存的帐号;

账户获取单元,用于根据用户选择的帐号,获取对应的用户帐号信息。

16. 如权利要求 14 所述的扫码装置,其特征在于,所述扫码装置还包括:

长连接请求发送模块,用于当应用登录成功,则向后台服务器发送长连接请求;

响应信息接收模块,用于接收后台服务器返回的长连接响应信息,以建立与相应用户端之间的长连接;

推送消息监测模块,用于实时接收所述后台服务器通过所述长连接推送来的应用消息。

登录信息传输方法、扫码方法及装置、后台服务器

技术领域

[0001] 本发明涉及通信技术领域,特别涉及一种登录信息传输方法、扫码方法及装置、后台服务器。

背景技术

[0002] 二维码 (two-dimension code),又称二维条码,它是在一维条码的基础上扩展出另一维具有可读性的条码,二维码用特定的几何图形按一定规律在平面(二维方向)上分布的黑白相间的图形,是所有信息数据的一把钥匙。目前,二维码因其具有的信息存储量大、保密性高、成本低等特点,在工商业、交通运输、金融、医疗等领域逐渐应用推广。而近年来,移动通信领域蓬勃发展起来的移动终端二维码业务,使移动终端用户进入信息随手可得的时代,由此带来的巨大商机在国内外日益显现。

[0003] 目前,许多远端服务器提供了二维码登录的功能,当用户使用远端服务器提供的有权限要求的应用程序时,可以首先利用移动终端自带的摄像头拍摄下应用程序提供二维码的图片,并解析出二维码图片中的验证信息,然后将二维码验证信息和移动终端中预置的登录信息发送给远端服务器,当远端服务器对二维码验证信息验证通过后,直接利用登录信息令应用程序登录成功。

[0004] 这种使用二维码登录的方式,既可以免除传统的输入帐号、密码等一系列繁琐操作,方便快捷,又可以有效防止木马病毒监控键盘窃取输入的密码,一定程度上可以避免移动终端上用户信息的泄露。但是,二维码登录的方式仍然存在一定的安全隐患,如果应用程序提供的二维码图片被木马程序替换成恶意的二维码图片,仍然会造成个人信息的泄露。例如,当移动终端扫描了被替换后的二维码图片,会根据二维码图片中的信息访问恶意的网站服务器,并将移动终端中的帐号、密码等个人信息发送给恶意服务器,从而造成用户信息的泄露甚至私有财产的损失。

发明内容

[0005] 本发明实施例的目的是提供一种登录信息传输方法、扫码方法及装置、后台服务器,以解决二维码登录的安全隐患。

[0006] 本发明实施例提出一种登录信息传输方法,用于至少一用户端和至少一应用服务器之间登录信息的传输,包括:

[0007] 接收用户端发送来的用户帐号信息和二维码信息;

[0008] 验证接收到的所述二维码信息和用户帐号信息;

[0009] 若验证通过,则向对应的用户端发送二次确认请求;

[0010] 当接收到用户端发送来的二次确认信息,则向对应的应用服务器发送登录确认信息。

[0011] 本发明实施例还提出一种扫码方法,用于在二维码登录时通过后台服务器对登录信息进行确认,包括:

- [0012] 扫描二维码,并获取二维码信息;
- [0013] 获取预设的用户帐号信息;
- [0014] 将二维码信息及用户帐号信息发送给后台服务器;
- [0015] 接收后台服务器对所述二维码信息和用户帐号信息验证通过后发送来的二次确认请求;
- [0016] 显示所述二次确认请求的提示信息;
- [0017] 将用户输入的二次确认信息发送给所述后台服务器。
- [0018] 本发明实施例还提出一种后台服务器,用于至少一用户端和至少一应用服务器之间登录信息的传输,包括:
- [0019] 验证信息接收模块,用于接收用户端发送来的用户帐号信息和二维码信息;
- [0020] 验证模块,用于验证接收到的所述二维码信息和用户帐号信息;
- [0021] 二次确认请求发送模块,用于当所述验证模块对所述二维码信息和用户帐号信息验证通过,则向对应的用户端发送二次确认请求;
- [0022] 二次确认信息接收模块,用于接收用户端发送来的二次确认信息;
- [0023] 登录确认信息发送模块,用于当所述二次确认信息接收模块接收到二次确认信息,则向对应的应用服务器发送登录确认信息。
- [0024] 本发明实施例还提出一种扫码装置,用于在二维码登录时通过后台服务器对登录信息进行确认,包括:
- [0025] 扫码模块,用于扫描二维码,并获取二维码信息;
- [0026] 用户帐号信息获取模块,用于获取预设的用户帐号信息;
- [0027] 验证信息发送模块,用于将二维码信息及用户帐号信息发送给后台服务器;
- [0028] 二次确认请求接收模块,用于接收后台服务器对所述二维码信息和用户帐号信息验证通过后发送来的二次确认请求;
- [0029] 提示信息显示模块,用于显示所述二次确认请求的提示信息;
- [0030] 二次确认信息发送模块,用于将用户输入的二次确认信息发送给所述后台服务器。
- [0031] 相对于现有技术,本发明的有益效果是:
- [0032] 通过本实施例的登录信息传输方法、扫码方法及装置、后台服务器,用户端在扫描了二维码信息后,只需提供用户帐号进行验证,而只有在二次确认通过后,才会由后台服务器将含有私密信息的登录确认信息发送给应用服务器,因此即使在登录过程中二维码图片被替换,用户端也不会将用户的个人私密信息泄露给恶意的服务器,有效提高了二维码登录技术的安全性。

附图说明

- [0033] 图1为本发明实施例的一种登录信息传输方法、扫码方法及装置、后台服务器的运行环境示意图;
- [0034] 图2为图1中后台服务器的常用部件的示意图;
- [0035] 图3为图1中用户端的常用部件的示意图;
- [0036] 图4为本发明实施例的一种登录信息传输方法的流程图;

- [0037] 图 5 为本发明实施例的另一种登录信息传输方法的流程图；
- [0038] 图 6 为本发明实施例的一种后台服务器的存储器中的信息存储示意图；
- [0039] 图 7 为本发明实施例的一种扫码方法的流程图；
- [0040] 图 8 为本发明实施例的另一种扫码方法的流程图；
- [0041] 图 9 为本发明实施例的一种用户帐号选择界面的示意图；
- [0042] 图 10 为本发明实施例的一种二次确认提示界面的示意图；
- [0043] 图 11 为本发明实施例的一种推送消息的显示界面示意图；
- [0044] 图 12 为本发明实施例的一种后台服务器的结构图；
- [0045] 图 13 为本发明实施例的另一种后台服务器的结构图；
- [0046] 图 14 为图 13 中推送模块的一种实施例结构图；
- [0047] 图 15 为图 14 中扫描单元 1403 的一种实施例结构图；
- [0048] 图 16 为本发明实施例的一种扫码装置的结构图；
- [0049] 图 17 图 16 中用户帐号信息获取模块的一种实施例结构图；
- [0050] 图 18 为本发明实施例的另一种扫码装置的结构图。

具体实施方式

[0051] 有关本发明的前述及其他技术内容、特点及功效,在以下配合参考图式的较佳实施例详细说明中将可清楚的呈现。通过具体实施方式的说明,当可对本发明为达成预定目的所采取的技术手段及功效得以更加深入且具体的了解,然而所附图式仅是提供参考与说明之用,并非用来对本发明加以限制。

[0052] 本发明实施例涉及一种登录信息传输方法、扫码方法及装置、后台服务器,请参见图 1,其为该方法、装置、服务器的应用环境示意图。至少一个用户端 100、后台服务器 200、至少一个应用服务器 300 以及至少一个登录设备 400 与网络 500 连接。所述登录设备 400 可以是 PC、笔记本电脑等具有显示和通讯功能的智能设备,登录设备 400 上安装有应用服务器 300 提供的应用程序,用户可以通过登录设备 400 登录该应用。所述用户端 100 可以是平板电脑、手机等具有拍摄和通讯功能的智能设备,用户可以利用用户端 100 令登录设备 400 上的应用快速登录,具体来说,用户可以通过用户端 100 自带的拍摄功能对登录设备 400 上显示的二维码进行扫码,并将带有二维码信息的验证信息传输给后台服务器 200 进行验证,以及在验证通过后由应用服务器 300 通知登录设备 400 登录相应的应用程序。特别的,所述应用服务器 300 和后台服务器 200 的功能也可以集成在同一服务器中,或者所述应用服务器 300 和后台服务器 200 的集群可以设置在同一机房中。

[0053] 进一步参见图 2,为上述后台服务器 200 可能会使用到的常用部件的示意图。

[0054] 后台服务器 200 包括:存储器 102、存储控制器 104、一个或多个(图中仅示出一个)处理器 106、外设接口 108 以及网络控制器 112。可以理解,图 2 所示的结构仅为示意,其并不对后台服务器 200 的结构造成限定。例如,后台服务器 200 还可包括比图 2 中所示更多或者更少的组件,或者具有与图 2 所示不同的配置。

[0055] 存储器 102 可用于存储软件程序以及模块,如本发明实施例中的登录信息传输方法对应的程序指令/模块,处理器 106 通过运行存储在存储器 102 内的软件程序以及模块,从而执行各种功能应用以及数据处理,即实现上述的方法。

[0056] 存储器 102 可包括高速随机存储器,还可包括非易失性存储器,如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中,存储器 102 可进一步包括相对于处理器 106 远程设置的存储器,这些远程存储器可以通过网络连接至后台服务器 200。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。处理器 106 以及其他可能的组件对存储器 102 的访问可在存储控制器 104 的控制下进行。

[0057] 外设接口 108 将各种输入/输出装置耦合至处理器 106。处理器 106 运行存储器 102 内的各种软件、指令,以及进行数据处理。在一些实施例中,外设接口 108、处理器 106 以及存储控制器 104 可以在单个芯片中实现。在其他一些实例中,他们可以分别由独立的芯片实现。

[0058] 网络控制器 112 用于接收以及发送网络信号。上述网络信号可包括无线信号或者有线信号。在一个实例中,上述网络信号为有线网络信号。此时,网络控制器 112 可包括处理器、随机存储器、转换器、晶体振荡器等元件。

[0059] 存储于存储器 102 的软件程序以及模块可以包括:操作系统 122。操作系统 122 例如可为 LINUX, UNIX, WINDOWS, 其可包括各种用于管理系统任务(例如内存管理、存储设备控制、电源管理等)的软件组件和/或驱动,并可与各种硬件或软件组件相互通讯,从而提供其他软件组件的运行环境。

[0060] 进一步参阅图 3,其为图 1 中用户端 100 的常用部件示意图,可以看到,用户端 100 与后台服务器 200 的结构相似,其不同之处在于,用户端 100 还可以包括摄像模块 110。摄像模块 110 用于拍摄照片或者视频。拍摄的照片或者视频可以存储至存储器 102 内,并可通过网络控制器 112 发送。摄像模块 110 具体可包括镜头模组、影像感测器以及闪光灯等组件。镜头模组用于对被拍摄的目标成像,并将所成的像映射至影像感测器中。影像感测器用于接收来自镜头模组的光线,实现感光,以记录图像信息。具体地,影像感测器可基于互补金属氧化物半导体(Complementary Metal Oxide Semiconductor, CMOS)、电荷耦合元件(Charge-coupled Device, CCD)或者其他影像感测原理实现。闪光灯用于在拍摄时进行曝光补偿。一般来说,用于用户端 100 的闪光灯可为发光二极管(Light Emitting Diode, LED)闪光灯。

[0061] 本发明实施例提出一种登录信息传输方法,应用于后台服务器,用于至少一用户端和至少一应用服务器之间登录信息的传输,请参见图 4,本实施例的方法包括以下步骤:

[0062] S401,接收用户端发送来的用户帐号信息和二维码信息。

[0063] 所述的用户帐号信息中仅包含可以公开的信息,例如后台服务器提供给用户用于验证的帐号,而并不包含密码等私密信息,所述的用户帐号信息主要是用来确认后台服务器与用户端之间的对应关系,以建立与用户端的通讯通道。

[0064] S402,验证接收到的所述二维码信息和用户帐号信息。验证所述二维码信息是指验证用户端拍摄到的二维码与后台服务器预存的二维码是否一致,若一致则验证通过。验证所述用户帐号信息是指判断后台服务器中是否存有与接收到的用户帐号相同的帐号,若存在则验证通过。

[0065] S403,若验证通过,则向对应的用户端发送二次确认请求。若验证失败,则流程结束或向对应用户端返回验证失败的信息。

[0066] S404,当接收到用户端发送来的二次确认信息,则向对应的应用服务器发送登录

确认信息。

[0067] 后台服务器中预存有与用户帐号对应的应用程序的信息，例如假设应用为一个游戏客户端，则后台可以预存与用户帐号对应的游戏帐号、密码、游戏角色、游戏服务器的地址等信息。所述的二次确认请求用于让用户对所登录的应用作进一步的确认，只有当二次确认通过后，后台服务器才会将登录确认信息（其中可能包含应用的帐号、密码等私密信息）发送给相应的应用服务器，从而让应用服务器通知对应的登录设备登录应用。这样，即使用户端扫码获得的二维码被木马程序替换，也不会泄露用户端中的私密信息，而只有当二次确认通过后，才会由后台服务器将相应的登录确认信息发送给应用服务器，因此在现有的二维码登录技术的基础上，进一步地提高了用户端的使用安全性。

[0068] 请参见图 5，其为本发明实施例的另一种登录信息传输方法的流程图，该登录信息传输方法应用于后台服务器，包括以下步骤：

[0069] S501，接收用户端发送来的用户帐号信息和二维码信息。

[0070] S502，验证接收到的所述二维码信息和用户帐号信息。

[0071] S503，若验证通过，则向对应的用户端发送二次确认请求。若验证失败，则流程结束或向对应用户端返回验证失败的信息。

[0072] S504，当接收到用户端发送来的二次确认信息，则向对应的应用服务器发送登录确认信息。所述登录确认信息中包含登录应用需要的信息，应用服务器接收到登录确认信息后，通过网络向对应的登录设备发出通知，并令登录设备端的应用自动登录。

[0073] S505，接收成功登录应用后用户端发送来的长连接请求。

[0074] S506，向所述用户端发送长连接响应信息，以建立与相应用户端之间的长连接。所述的长连接可以在一个连接上连续发送多个数据包，并且在发包完毕后，会在一定的时间内保持连接。

[0075] S507，保存与所述用户端之间的链路信息。所述链路信息是指与用户端之间的连接信息，通过链路信息可以方便快捷地找出后台服务器与各个用户端之间的长连接链路。链路信息可以包括帐号信息、用户端标识、接入层 IP 地址、时间戳等。

[0076] S508，当接收到应用服务器发送来的应用消息，储存所述应用消息。

[0077] 由于很多时候网络环境较为复杂（带宽限制、无线信号强度等），如果由应用服务器直接通过网络向用户端发送应用消息，信号传输成本较高，且容易造成数据丢包，导致用户错过重要的应用消息。因此本实施例通过后台服务器统一接收应用服务器发出的应用消息并储存，以及后续再利用与用户端之间建立的长连接，将应用消息推送给对应的用户端，可以有效保证应用消息的送达。

[0078] 藉于信息的传输和定向需要，后台服务器的存储器中存储的信息需要包括几个部分，请参见图 6，其为本发明实施例的一种后台服务器的存储器中的信息存储示意图，其中存储的信息包括：链路信息部分、发送队列缓存部分、应用登录信息部分以及备份数据部分。链路信息中保存用户端的连接信息，用于查找后台服务器与各个用户端之间长连接的物理连接链路，包括用户端的标识、用户帐号信息、接入层 IP 地址等。发送队列缓存保存待推送的数据，包括具体待推送的应用消息、时间标签、目的应用帐号等。应用登录信息保存应用与用户端之间的对应关系，用于找出发送给用户端的信息传输方向，包括用户帐号、应用服务器编号、用户帐号和应用对应的相关数据（如用户帐号曾经登录过的应用的名称、

应用帐号)等。备份数据部分类似于发送队列缓存部分,只是该部分是持久化保存,以避免机器重启或故障后数据丢失。

[0079] 值得注意的是,所述的用户端标识可以是指用户端设备的标识,也可以是后台服务器提供给用户端的一个应用程序的标识。如果用户固定使用同一台用户端进行二维码登录,那么用户端标识就可以是指用户端设备的标识。而如果用户可能会使用不同的用户端进行二维码登录,那么为了便于通过用户帐号找出后台服务器与用户端之间的连接链路,那么用户端标识就可以是后台服务器提供给用户端的一个应用程序的标识。

[0080] S509,定期扫描所述储存的应用消息,获取未推送的应用消息。具体来说,即定期扫描前述发送队列缓存,获取其中储存的应用消息。其中,已经推送的应用消息,以及根据时间标签超过一定期限的应用消息会从发送队列缓存删除。

[0081] S510,获取与未推送的应用消息对应的用户帐号。具体来说,查找发送队列缓存时,在获得应用消息的同时,也可以获得接收该应用消息对应的应用帐号。如果应用帐号采用用户帐号,则在查找发送队列缓存的过程中就可以获得用户帐号。如果应用帐号和用户帐号不同,则可以根据应用帐号查找应用登录信息,从而获得用户帐号。

[0082] S511,根据所述用户帐号信息查找预存的用户端标识。具体来说,即通过用户帐号查找应用登录信息,获取对应的用户端标识。

[0083] S512,根据查找到的用户端标识查找所述链路信息,并获取具体的长连接物理链路信息。具体来说,即根据用户端标识查找链路信息,找出具体的长连接物理链路。

[0084] S513,判断向与未推送的应用消息对应的用户端发送的历史已推送消息是否有对应的回复信息。具体来说,步骤 S512 找出的长连接链路即为未推送消息要使用的通信链路,根据获得的链路信息,可以查找这条长连接链路上曾经推送过的应用消息是否有对应的回复信息,即历史记录中发送给某一个用户端应用消息之后,该用户端是否反馈过信息回包,如果存在没有收到回复信息的已推送消息,则说明这条长连接链路有可能断路了,则要在这一条长连接链路上推送的应用消息停止处理。反之,如果长连接链路连接正常,则进入步骤 S514,将要推送的应用消息推送给相应的用户端。

[0085] S514,通过获取的所述长连接物理链路将要推送的应用消息推送给对应的用户端。

[0086] 请参见图 7,其为本发明实施例的一种扫码方法的流程图,其应用于用户端,用于在二维码登录时通过后台服务器对登录信息进行确认,本实施例的方法包括以下步骤:

[0087] S701,扫描二维码,并获取二维码信息。所述的二维码是由后台服务器提供并显示在登录设备上的。

[0088] S702,获取预设的用户帐号信息。所述的用户帐号信息是由后台服务器提供,并用于验证用户端的身份,以建立后台服务器与用户端之间的通信链路。

[0089] S703,将二维码信息及用户帐号信息发送给后台服务器。后台服务器接收到二维码信息和用户帐号信息后,会对二维码信息和用户帐号信息进行验证。

[0090] S704,接收后台服务器对所述二维码信息和用户帐号信息验证通过后发送来的二次确认请求。

[0091] S705,显示所述二次确认请求的提示信息。

[0092] S706,将用户输入的二次确认信息发送给所述后台服务器。

[0093] 所述的二次确认请求用于让用户对所要登录的应用作进一步的确认,只有当二次确认通过后,后台服务器才会将登录确认信息(其中可能包含应用的帐号、密码等私密信息)发送给相应的应用服务器,从而让应用服务器通知对应的登录设备登录应用。这样,即使用户端扫码获得的二维码被木马程序替换,也不会泄露用户端中的私密信息,而只有当二次确认通过后,才会由后台服务器将相应的登录确认信息发送给应用服务器,因此在现有的二维码登录技术的基础上,进一步地提高了用户端的使用安全性。

[0094] 请参见图 8,其为本发明实施例的另一种扫码方法的流程图,其包括以下步骤:

[0095] S801,扫描二维码,并获取二维码信息。

[0096] S802,显示预存的帐号。

[0097] S803,根据用户选择的帐号,获取对应的用户帐号信息。

[0098] S804,将二维码信息及用户帐号信息发送给后台服务器。

[0099] S805,接收后台服务器对所述二维码信息和用户帐号信息验证通过后发送来的二次确认请求。

[0100] S806,显示所述二次确认请求的提示信息。

[0101] S807,将用户输入的二次确认信息发送给所述后台服务器。

[0102] S808,当应用登录成功,则向后台服务器发送长连接请求。

[0103] S809,接收后台服务器返回的长连接响应信息,以建立与相应用户端之间的长连接。

[0104] S810,实时接收所述后台服务器通过所述长连接推送来的应用消息。

[0105] 为进一步理解本实施例,现以登录一个游戏的过程为例进行说明:

[0106] 扫描二维码图片成功后,在用户端显示屏上会显示出用户帐号信息,如图 9 所示,这里的用户帐号即为游戏帐号,显示的帐号为用户端中存储的曾经登录过的帐号。用户端中可能存有多个用户帐号,因而通过步骤 S802 和步骤 S803 可以让用户选择相应的帐号,并同二维码信息一起发送给后台服务器。

[0107] 后台服务器对二维码信息和用户帐号验证通过后,会返回二次确认请求,如图 10 所示,二次确认请求的显示界面上会提示用户帐号和所要登录的游戏的信息,当用户选择确认后,用户端将二次确认信息发送给后台服务器,然后后台服务器将登录确认信息发送给对应的游戏服务器。最后游戏服务器通知登录设备登录游戏。

[0108] 游戏登录成功后,后台服务器会和用户端建立长连接,并定时将游戏服务器发送来的消息推送给相应的用户端。例如,当游戏下线时,游戏服务器会将下线确认信息发送给后台服务器,由后台服务器推送给对应的用户端,如图 11 所示,只有当用户在用户端侧确认下线后,游戏服务器才会接收游戏下线操作。除此之外,游戏中的虚拟资产交易、系统消息、聊天信息等均可以通过后台服务器推送给对应的用户端,不仅可以保证信息的送达,防止数据丢包,也可以确保游戏中的各种操作是经由用户本人确认的,提高了游戏操作的安全性。

[0109] 本发明实施例还提出一种后台服务器,用于至少一用户端和至少一应用服务器之间登录信息的传输。请参见图 12,其为本发明实施例的一种后台服务器的结构图,该后台服务器包括:验证信息接收模块 1201、验证模块 1202、二次确认请求发送模块 1203、二次确认信息接收模块 1204 以及登录确认信息发送模块 1205。

- [0110] 验证信息接收模块 1201 用于接收用户端发送来的用户帐号信息和二维码信息。
- [0111] 验证模块 1202 用于对验证信息接收模块 1201 接收到的二维码信息和用户帐号信息进行验证。
- [0112] 二次确认请求发送模块 1203 用于当验证模块 1202 对二维码信息和用户帐号信息验证通过后,向对应的用户端发送二次确认请求。
- [0113] 二次确认信息接收模块 1204 用于接收用户端发送来的二次确认信息。
- [0114] 登录确认信息发送模块 1205 用于当二次确认信息接收模块 1204 接收到二次确认信息后,向对应的应用服务器发送登录确认信息。
- [0115] 通过本实施例的后台服务器,用户端在扫描了二维码信息后,只需提供用户帐号进行验证,而只有在二次确认通过后,才会由后台服务器将含有私密信息的登录确认信息发送给应用服务器,因此即使在登录过程中二维码图片被替换,用户端也不会将用户的个人私密信息泄露给恶意的服务器,有效提高了二维码登录技术的安全性。
- [0116] 请参见图 13,其为本发明实施例的另一种后台服务器的结构图,与图 12 的实施例相比,本实施例的后台服务器不仅包括:验证信息接收模块 1201、验证模块 1202、二次确认请求发送模块 1203、二次确认信息接收模块 1204 以及登录确认信息发送模块 1205,还包括:长连接请求接收模块 1206、长连接响应模块 1207、应用消息接收模块 1208、推送模块 1209 以及链路信息保存模块 1210。
- [0117] 长连接请求接收模块 1206 用于接收成功登录应用后用户端发送来的长连接请求。
- [0118] 长连接响应模块 1207 用于在长连接请求接收模块 1206 接收到长连接请求后,向相应的用户端发送长连接响应信息,以建立与相应用户端之间的长连接。
- [0119] 链路信息保存模块 1210 用于在长连接响应模块 1207 响应了用户端发送来的长连接请求后,保存与用户端之间的链路信息。所述链路信息是指与用户端之间的连接信息。
- [0120] 应用消息接收模块 1208 用于接收并保存应用服务器发送来的应用消息。
- [0121] 推送模块 1209 用于当所述应用消息接收模块接收到应用消息,则将所述应用消息通过所述长连接推送给对应的用户端。
- [0122] 请参见图 14,其为图 13 中推送模块的一种实施例结构图,其中,推送模块 1209 又进一步包括:标识查找单元 1401、链路信息查找单元 1402、扫描单元 1403 以及应用消息推送单元 1404。
- [0123] 标识查找单元 1401 用于根据用户帐号信息查找预存的用户端标识。
- [0124] 链路信息查找单元 1402 用于根据标识查找单元 1401 查找到的用户端标识查找储存的链路信息,并获取具体的长连接物理链路信息。
- [0125] 扫描单元 1403 用于定期扫描所述储存的应用消息,判断是否有需要推送的应用消息。
- [0126] 应用消息推送单元 1404 用于将需要推送的应用消息通过长连接推送给对应的用户端。
- [0127] 请参见图 15,其为图 14 中扫描单元的一种实施例结构图,该扫描单元包括:未推送消息获取子单元 1501、用户端信息获取子单元 1502、回复信息判断子单元 1503 以及应用消息确定子单元 1504。

[0128] 未推送消息获取子单元 1501 用于定期扫描储存的应用消息, 获取未推送的应用消息。

[0129] 用户端信息获取子单元 1502 用于当未推送消息获取子单元 1501 扫描到为推送的应用消息时, 获取与未推送的应用消息对应的用户端信息。

[0130] 回复信息判断子单元 1503 用于判断向用户端信息获取子单元 1502 获取的用户端发送的历史已推送消息是否有对应的回复信息。

[0131] 应用消息确定子单元 1504 用于当回复信息判断子单元 1503 判断出有回复信息, 则确定对应的未推送的应用消息为需要推送的应用消息。

[0132] 通过本实施的后台服务器, 不仅进一步地提高了二维码登录技术的安全性, 同时还利用与用户端之间的长连接将应用服务器发送来的应用消息推送给对应的用户端, 确保了复杂网络的情况下应用消息的送达。

[0133] 本发明实施例还提出一种扫码装置, 其应用于用户端, 用于在二维码登录时通过后台服务器对登录信息进行确认, 请参见图 16, 其为本发明实施例的一种扫码装置的结构图, 该扫码装置包括: 扫码模块 1601、用户帐号信息获取模块 1602、验证信息发送模块 1603、二次确认请求接收模块 1604、提示信息显示模块 1605 以及二次确认信息发送模块 1606。

[0134] 扫码模块 1601 用于扫描二维码, 并获取二维码信息。

[0135] 用户帐号信息获取模块 1602 用于获取预设的用户帐号信息。

[0136] 验证信息发送模块 1603 用于将二维码信息及用户帐号信息发送给后台服务器。

[0137] 二次确认请求接收模块 1604 用于接收后台服务器对所述二维码信息和用户帐号信息验证通过后发送来的二次确认请求。

[0138] 提示信息显示模块 1605 用于显示所述二次确认请求的提示信息。

[0139] 二次确认信息发送模块 1606 用于将用户输入的二次确认信息发送给所述后台服务器。

[0140] 请参见图 17, 其为图 16 中用户帐号信息获取模块的一种实施例结构图, 该用户帐号信息获取模块包括: 帐号显示单元 1701 和账户获取单元 1702。帐号显示单元 1701 用于显示预存的帐号。账户获取单元 1702 用于根据用户选择的帐号, 获取对应的用户帐号信息。

[0141] 请参见图 18, 其为本发明实施例的另一种扫码装置的结构图, 与图 16 的实施例相比, 本实施例的扫码装置除了包括: 扫码模块 1601、用户帐号信息获取模块 1602、验证信息发送模块 1603、二次确认请求接收模块 1604、提示信息显示模块 1605 和二次确认信息发送模块 1606, 还包括: 长连接请求发送模块 1607、响应信息接收模块 1608 以及推送消息监测模块 1609。

[0142] 长连接请求发送模块 1607 用于当应用登录成功, 则向后台服务器发送长连接请求。

[0143] 响应信息接收模块 1608 用于接收后台服务器返回的长连接响应信息, 以建立与相应用户端之间的长连接。

[0144] 推送消息监测模块 1609 用于实时接收所述后台服务器通过所述长连接推送来的应用消息。

[0145] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到本发明实施例可以通过硬件实现,也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解,本发明实施例的技术方案可以以软件产品的形式体现出来,该软件产品可以存储在一个非易失性存储介质(可以是 CD-ROM, U 盘, 移动硬盘等)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,或网络设备等)执行本发明实施例各个实施场景所述的方法。

[0146] 以上所述,仅是本发明的较佳实施例而已,并非对本发明作任何形式上的限制,虽然本发明已以较佳实施例揭露如上,然而并非用以限定本发明,任何熟悉本专业的技术人员,在不脱离本申请技术方案范围内,当可利用上述揭示的技术内容作出些许更动或修饰为等同变化的等效实施例,但凡是未脱离本申请技术方案内容,依据本发明的技术实质对以上实施例所作的任何简单修改、等同变化与修饰,均仍属于本发明技术方案的范围。

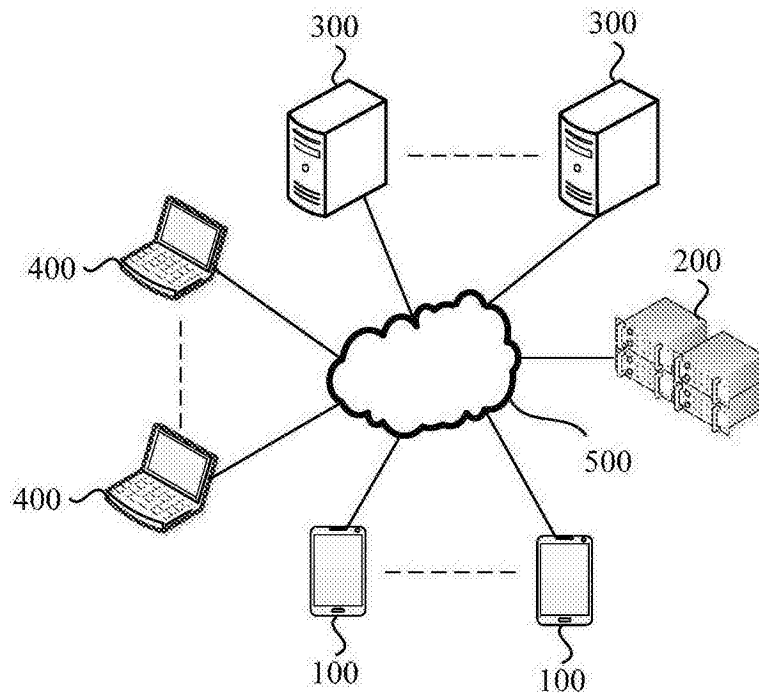


图 1

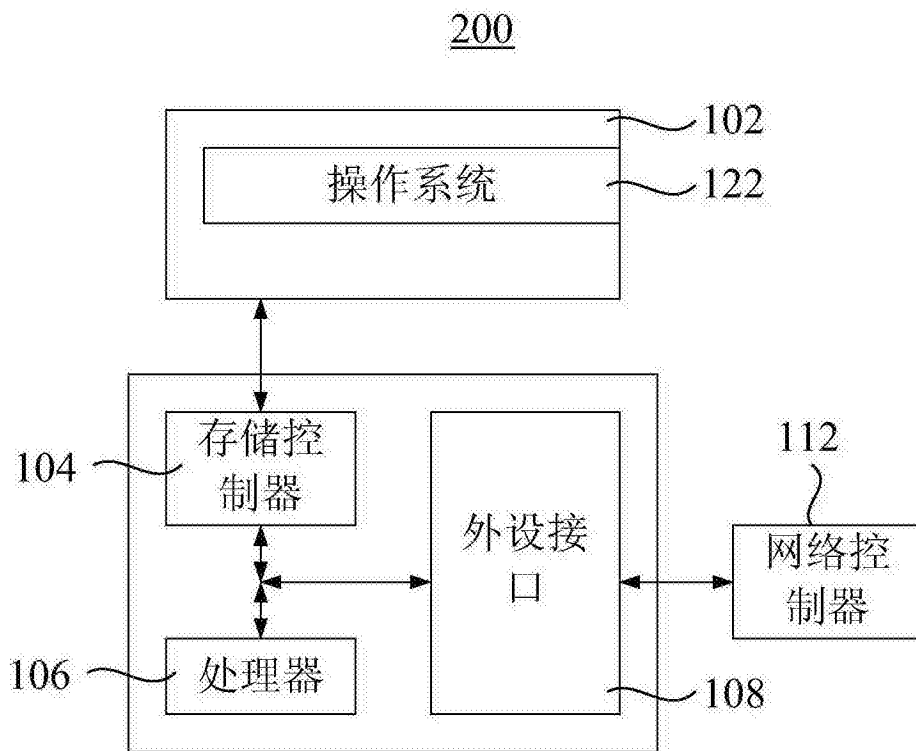


图 2

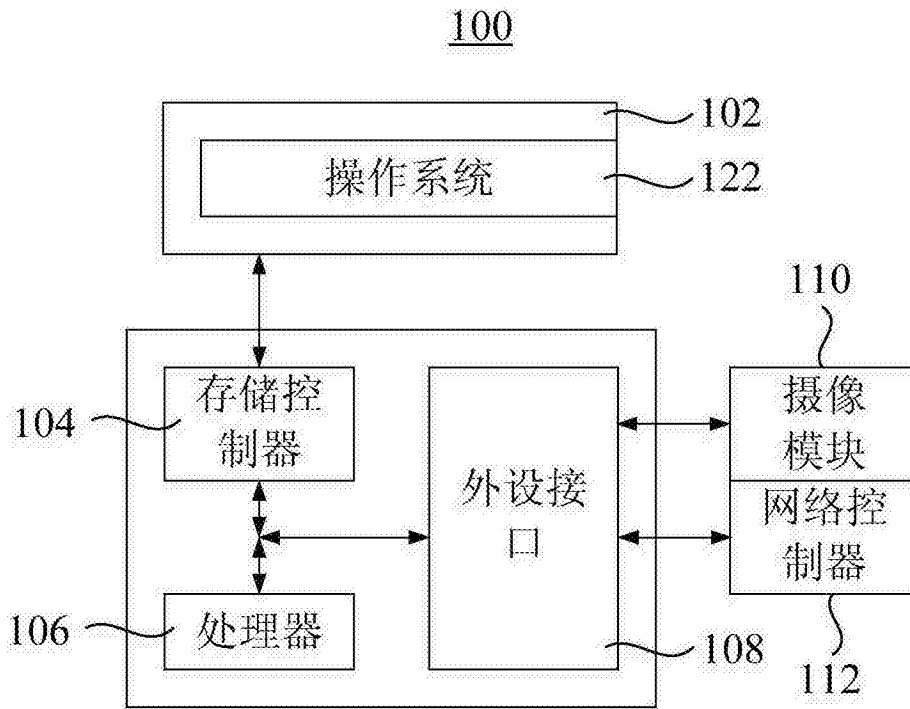


图 3

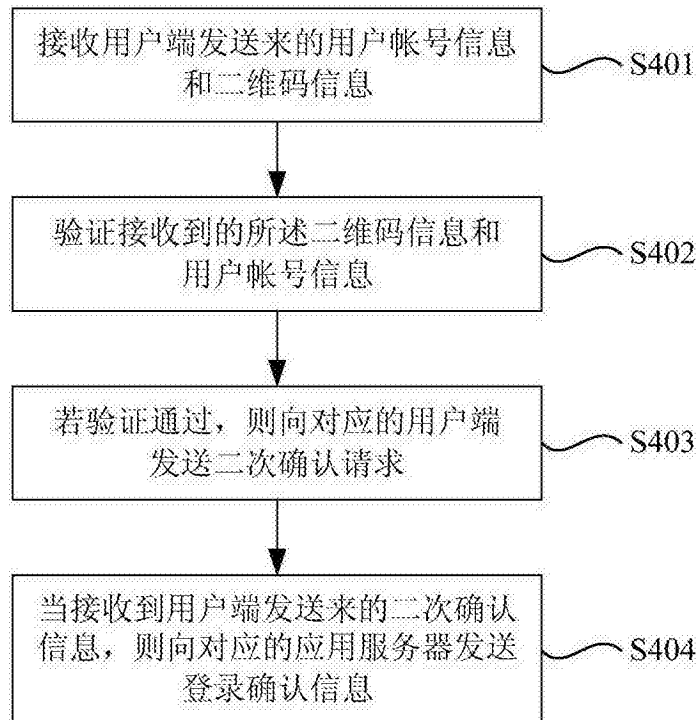


图 4

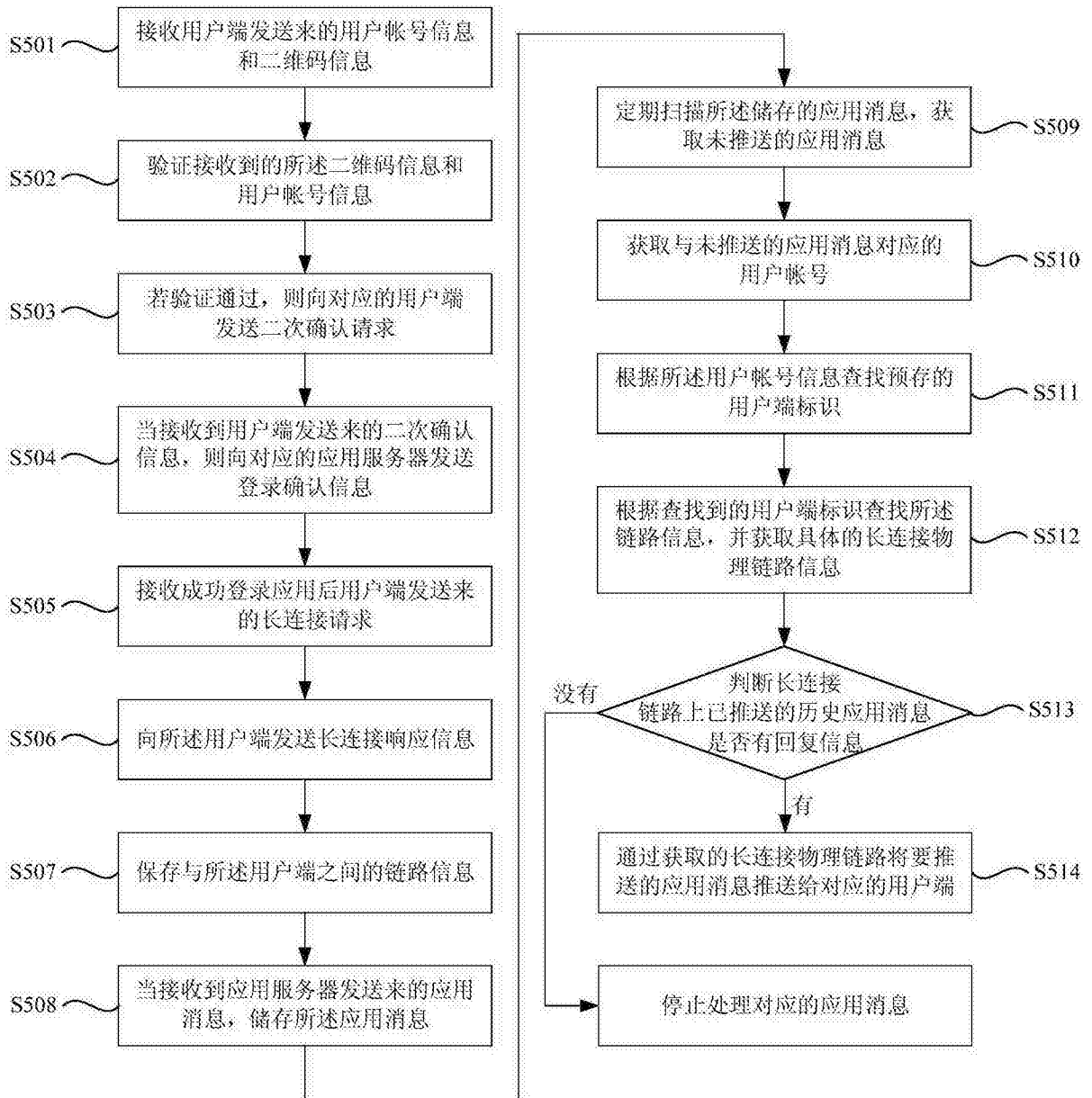


图 5



图 6

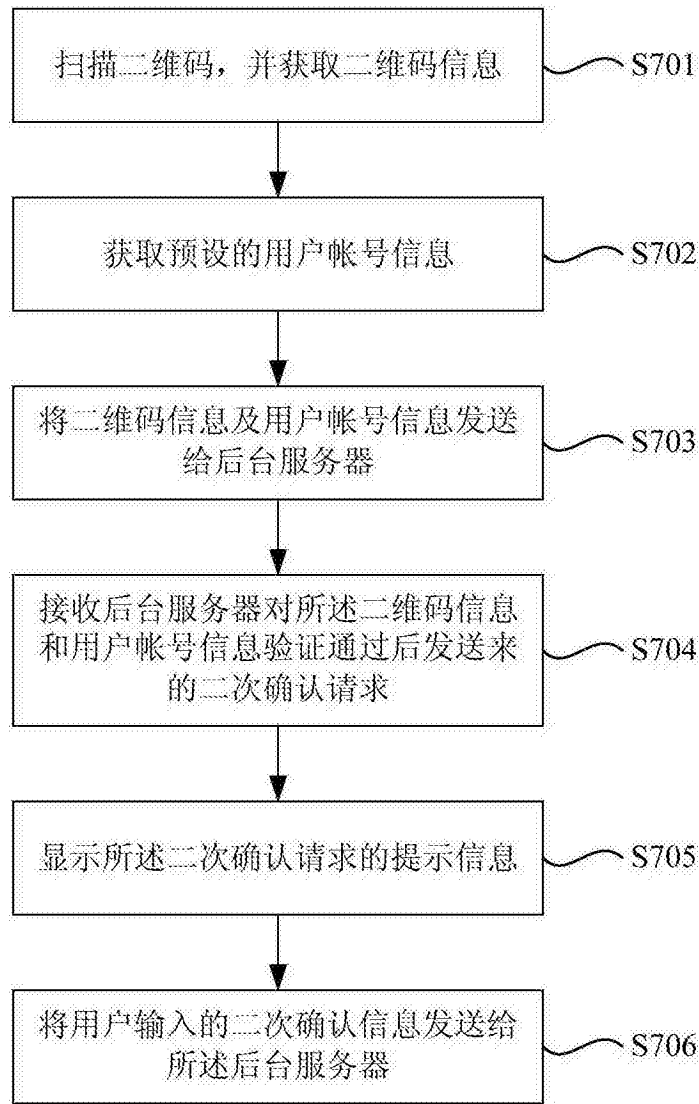


图 7

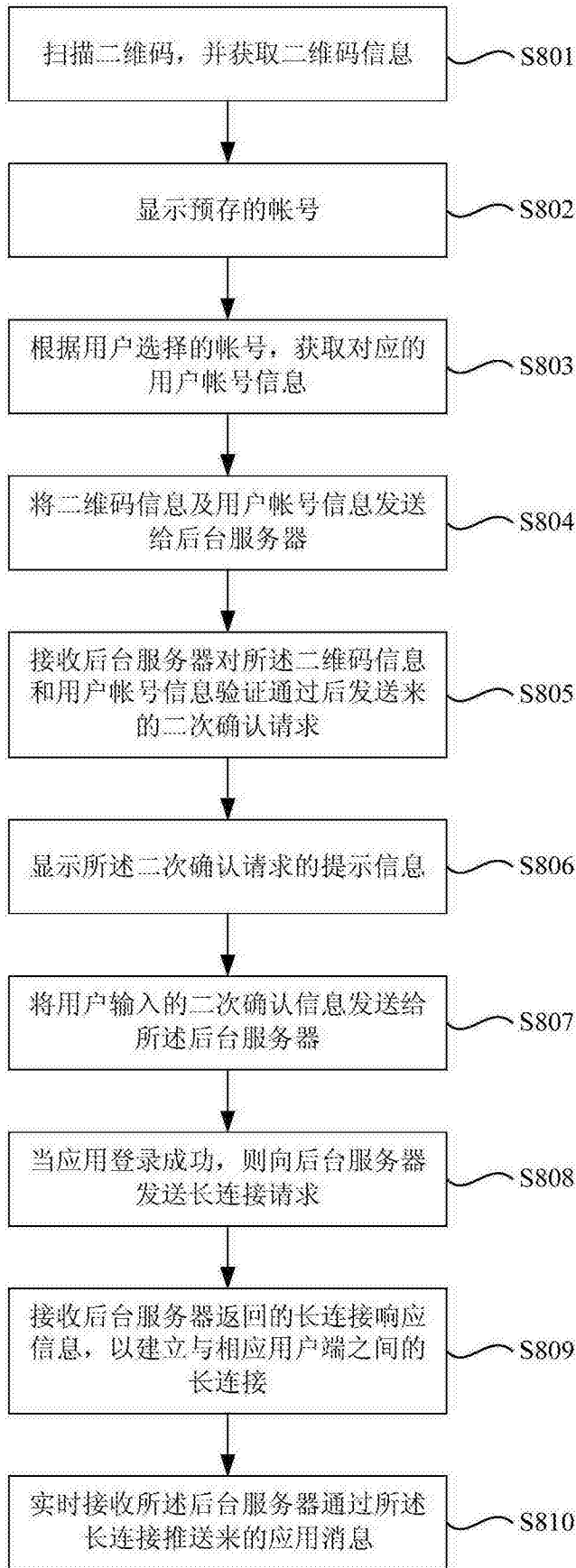


图 8

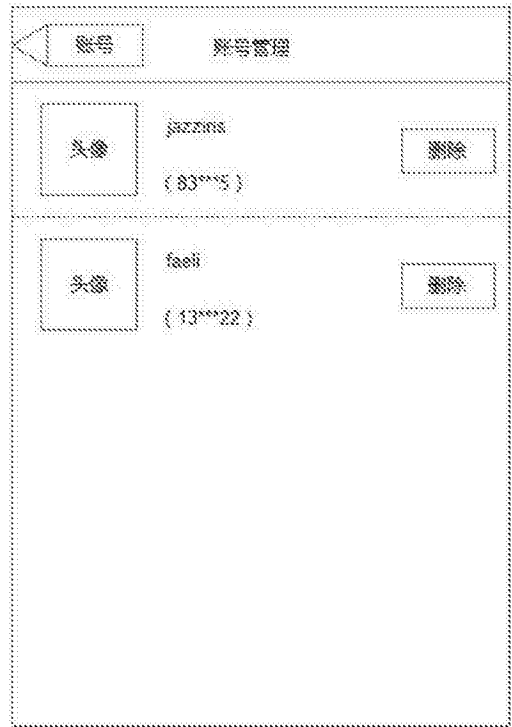


图 9

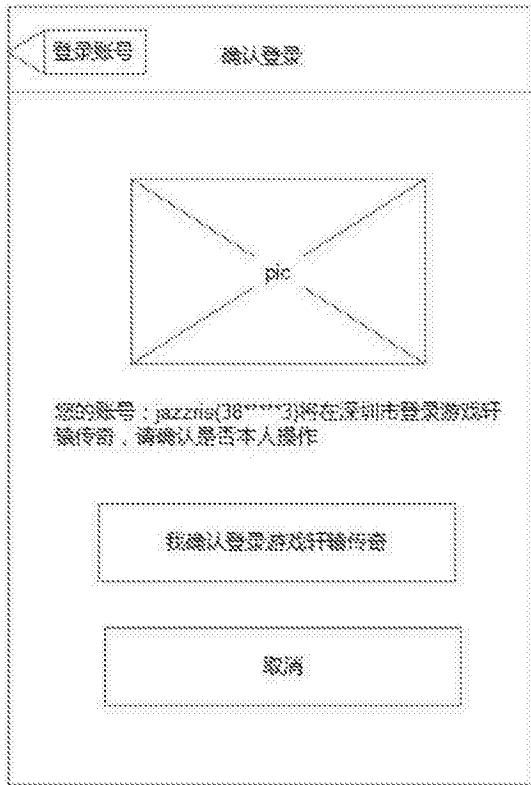


图 10

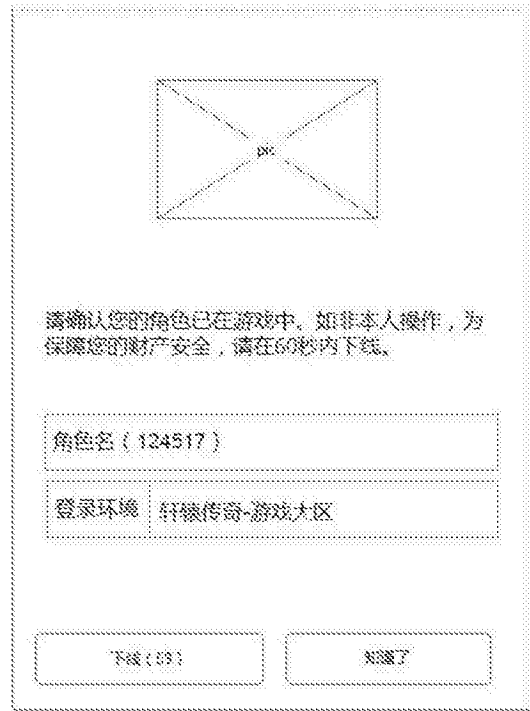


图 11

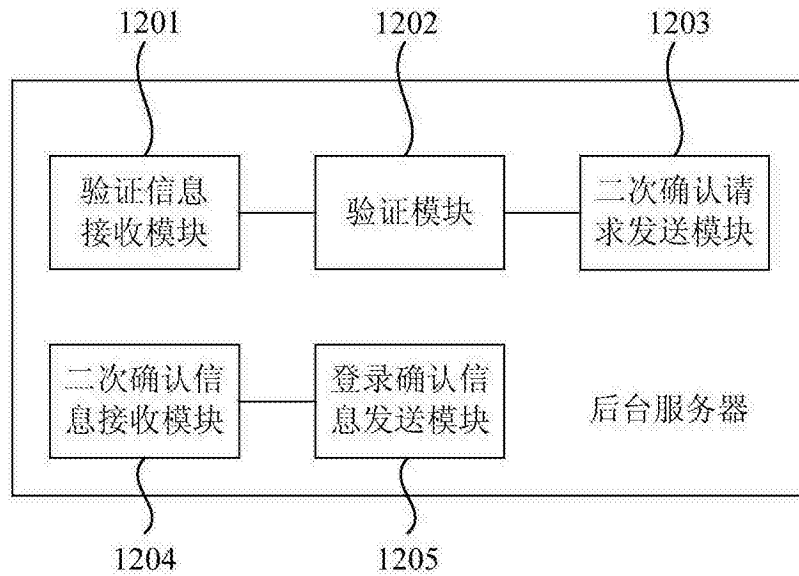


图 12

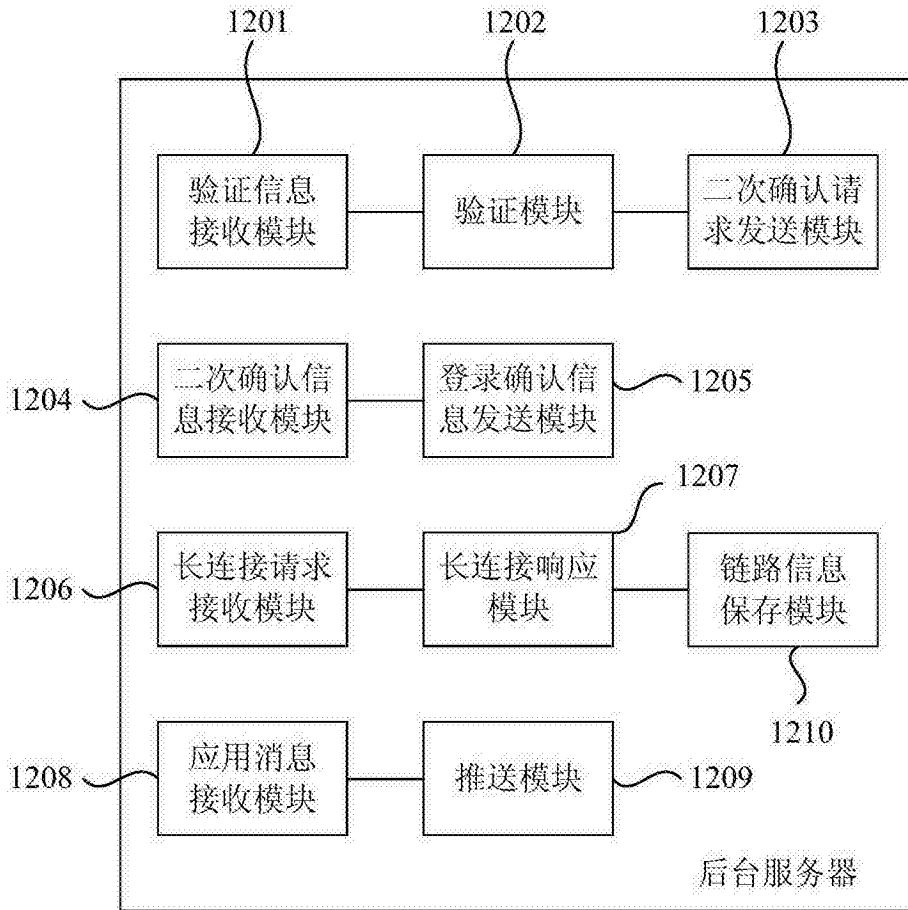


图 13

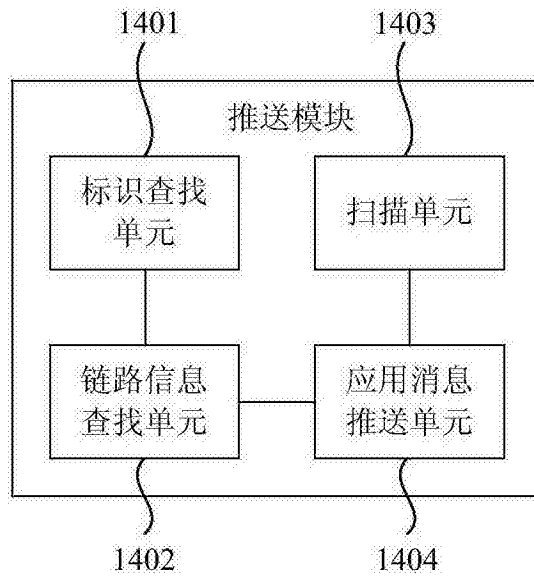


图 14

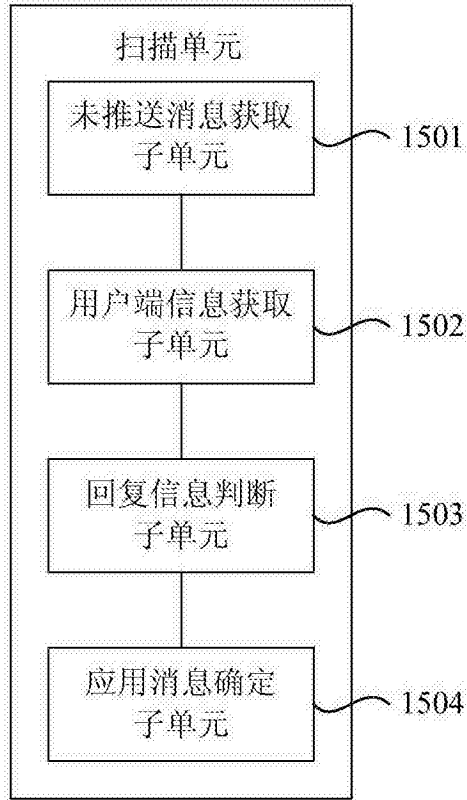


图 15

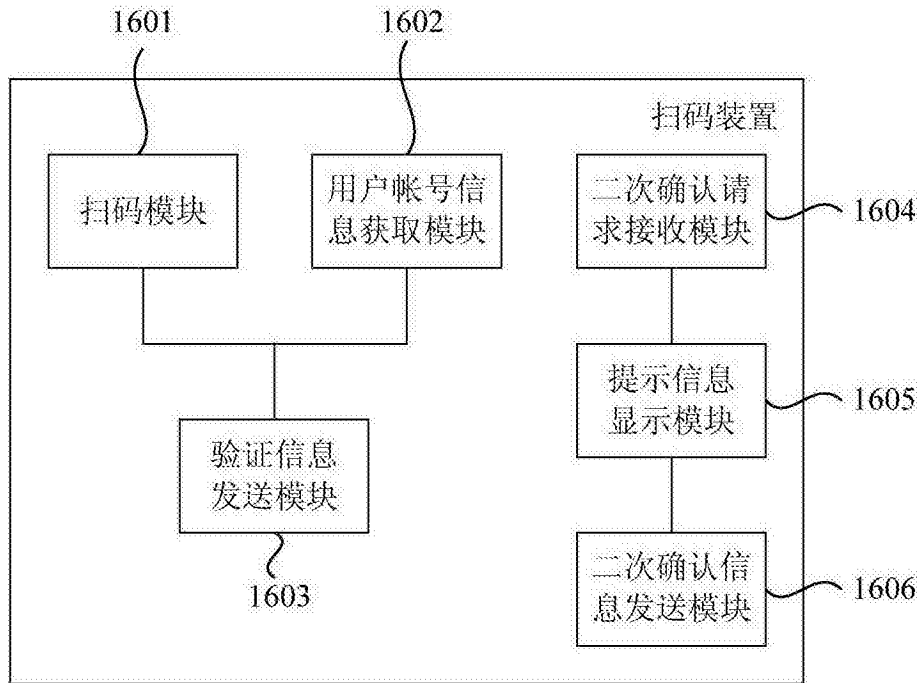


图 16

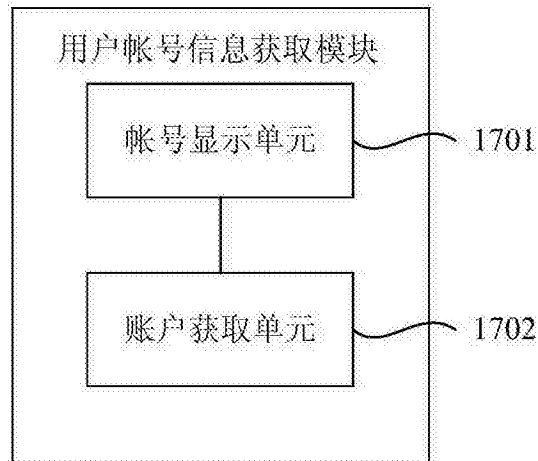


图 17

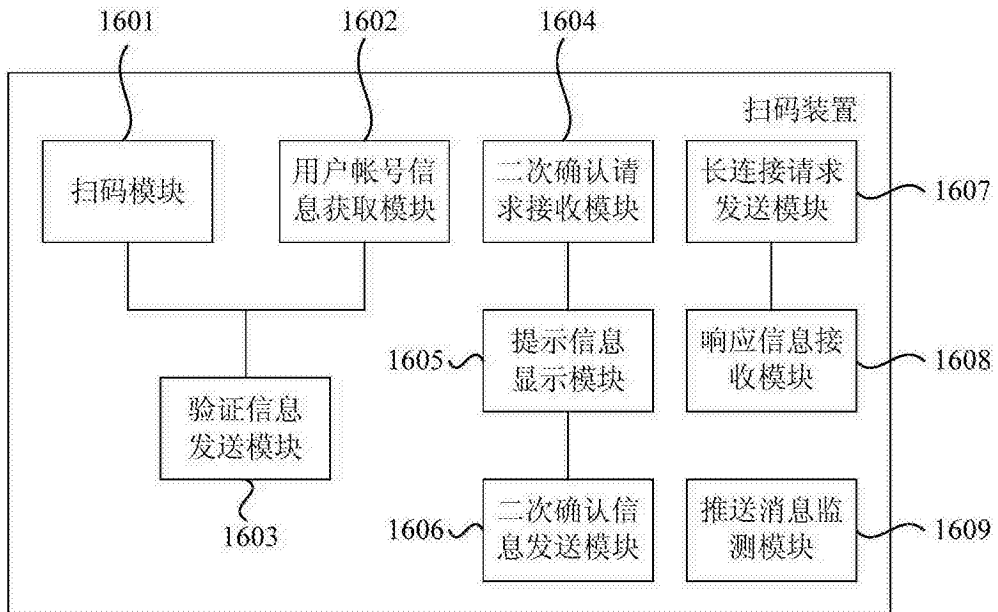


图 18