



(12) 发明专利申请

(10) 申请公布号 CN 103491084 A

(43) 申请公布日 2014. 01. 01

(21) 申请号 201310425568. 3

(22) 申请日 2013. 09. 17

(71) 申请人 天脉聚源(北京)传媒科技有限公司

地址 100007 北京市东城区安定门东大街
28号雍和大厦E座808室

(72) 发明人 郭建辉

(51) Int. Cl.

H04L 29/06 (2006. 01)

H04L 9/32 (2006. 01)

H04L 9/08 (2006. 01)

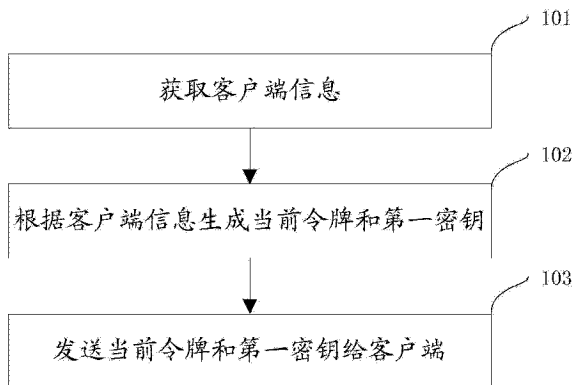
权利要求书2页 说明书6页 附图1页

(54) 发明名称

一种客户端的认证处理方法及装置

(57) 摘要

本发明公开了一种客户端的认证处理方法及装置。所述方法包括:获取客户端信息;根据所述客户端信息生成当前令牌和第一密钥;发送所述当前令牌和第一密钥给客户端。用于实现根据令牌的时间及密钥的使用次数生成新的令牌及新的密钥,可以增加客户使用服务器的安全性。本发明还公开了用于实现所述方法的装置。



1. 一种客户端的认证处理方法,其特征在于,包括以下步骤:

获取客户端信息;

根据所述客户端信息生成当前令牌和第一密钥;

发送所述当前令牌和第一密钥给客户端。

2. 如权利要求 1 所述的方法,其特征在于,所述客户端信息包括:客户端帐号、客户端 IP 地址、所述客户端帐号第一次生成令牌的时间和所述客户端帐号最近一次获取令牌的时间。

3. 如权利要求 1 所述的方法,其特征在于,发送所述当前令牌及第一密钥给客户端后,还包括:

接收客户端发送的登录请求信息,所述登录请求信息包括所述客户端信息、令牌和密钥;

判断登录请求信息与所述获取的客户端信息、所述生成的当前令牌和第一密钥是否匹配,并判断所述登录请求信息的发送时间与所述当前令牌的生成时间之间的时间间隔是否小于预设令牌使用时长;

当登录请求信息与所述获取的客户端信息、所述生成的当前令牌和第一密钥匹配,且所述时间间隔小于预设令牌使用时长时,允许所述客户端登录。

4. 如权利要求 3 所述的方法,其特征在于,所述判断所述登录请求信息的发送时间与所述当前令牌的生成时间之间的时间间隔是否小于预设令牌使用时长之后,还包括:

当所述时间间隔等于或大于预设令牌使用时长时,根据所述客户端信息重新生成令牌;

将所述重新生成的令牌发送给所述客户端。

5. 如权利要求 3 或 4 所述的方法,其特征在于,所述允许所述客户端登录之后,还包括:

判断所述第一密钥的使用次数是否大于预设使用次数;

当所述第一密钥的使用次数大于预设使用次数时,根据所述客户端信息重新生成密钥;

将所述重新生成的密钥发送给所述客户端。

6. 一种客户端的认证处理装置,其特征在于,包括:

获取模块,用于获取客户端信息;

生成模块,用于根据所述客户端信息生成当前令牌和第一密钥;

发送模块,用于发送所述当前令牌和第一密钥给客户端。

7. 如权利要求 6 所述的装置,其特征在于,该装置还包括:

接收模块,用于接收客户端发送的登录请求信息,所述登录请求信息包括所述客户端信息、令牌和密钥;

第一判断模块,用于判断登录请求信息与所述获取的客户端信息、所述生成的当前令牌和第一密钥是否匹配,并判断所述登录请求信息的发送时间与所述当前令牌的生成时间之间的时间间隔是否小于预设令牌使用时长;

允许登录模块,用于当登录请求信息与所述获取的客户端信息、所述生成的当前令牌和第一密钥匹配,且所述时间间隔小于预设令牌使用时长时,允许所述客户端登录。

8. 如权利要求 6 所述的装置,其特征在于,所述装置还包括:

第一重新生成模块,用于当所述时间间隔等于或大于预设令牌使用时长时,根据所述客户端信息重新生成令牌;

第一重新发送模块,用于将所述重新生成的令牌发送给所述客户端。

9. 如权利要求 7 或 8 所述的装置,其特征在于,该装置还包括:

第二判断模块,用于在所述允许登录模块允许所述客户端登录之后,判断所述第一密钥的使用次数是否大于预设使用次数;

第二重新生成模块,用于当所述第一密钥的使用次数大于预设使用次数时,根据所述客户端信息重新生成密钥;

第二重新发送模块,用于将所述重新生成的密钥发送给所述客户端。

一种客户端的认证处理方法及装置

技术领域

[0001] 本发明涉及服务器控制客户端技术领域,尤其涉及一种客户端的认证处理方法及装置。

背景技术

[0002] 如今,随着互联网的扩大及在各领域的广泛应用,许多伴生产业应运而生。其中,还有很多需要对用户发送的信息及服务器保密性高的产业,如网银、用户定制服务器、网络游戏等,这些产业中服务商要对用户的帐号信息保有绝对的安全性,由于服务商为客户提供

了令牌。
[0003] 令牌在古代是军队传达命令的一种凭证,近年来,随着网络技术的发展,一些公司、机构为了更好的保护使用者的账号、密码安全,推出了一种被称为动态口令的技术。即每隔固定时间,自动依照特别的算法生成一组新的随机密码(又称动态口令),而生成、表现这些密码的载体工具,往往就也被称为“令牌”,如手机令牌、硬件令牌等。其中,硬件令牌往往是一个钥匙扣大小的轻巧器具,上有显示屏可以显示随机密码。这种技术如今已被广泛运用于网络游戏、网上银行、大型企业内部网络管理等场合。

[0004] 传统的令牌是为了管理通信,生成标识用户身份的唯一串作为通信令牌,在连续请求中重新标识用户身份。而如今的令牌生成时仅仅是通过一定的算法自动生成出令牌并发送给服务器,这样会使令牌的安全性下降。

发明内容

[0005] 本发明实施例提供一种客户端的认证处理方法及装置,用于实现根据令牌的时间及密钥的使用次数生成新的令牌及新的密钥,以增加客户使用服务器的安全性。

[0006] 一种客户端的认证处理方法,包括以下步骤:获取客户端信息;根据所述客户端信息生成当前令牌和第一密钥;发送所述当前令牌和第一密钥给客户端。服务器根据获得的客户端信息生成令牌和密钥并发送给客户端,实现令牌是唯一存在的,提高了用户在使用客户端时的安全性。

[0007] 优选地,所述客户端信息包括:客户端帐号、客户端 IP 地址、所述客户端帐号第一次生成令牌的时间和所述客户端帐号最近一次获取令牌的时间。客户端信息包括客户端帐号第一次生成令牌的时间和客户端帐号最近一次获取令牌的时间可以使提供的客户端信息是唯一存在的。

[0008] 优选地,发送所述当前令牌及第一密钥给客户端后,还包括:接收客户端发送的登录请求信息,所述登录请求信息包括所述客户端信息、令牌和密钥;判断登录请求信息与所述获取的客户端信息、所述生成的当前令牌和第一密钥是否匹配,并判断所述登录请求信息的发送时间与所述当前令牌的生成时间之间的时间间隔是否小于预设令牌使用时长;当登录请求信息与所述获取的客户端信息、所述生成的当前令牌和第一密钥匹配,且所述时间间隔小于预设令牌使用时长时,允许所述客户端登录。服务器通过判断客户端请求登录

时,发送的登录请求信息是否与获取的客户端信息是否匹配,并且判断当前令牌的生成时间是否超时,来确定请求登录的客户端是否有权限登录服务器。通过唯一的令牌及密钥同时确认客户端的身份,增加了客户端登录服务器时,服务器的安全性,进而增加了服务器对其他客户端的安全性。

[0009] 优选地,所述判断所述登录请求信息的发送时间与所述当前令牌的生成时间之间的时间间隔是否小于预设令牌使用时长之后,还包括:当所述时间间隔等于或大于预设令牌使用时长时,根据所述客户端信息重新生成令牌;将所述重新生成的令牌发送给所述客户端。通过判断登录请求信息的发送时间与当前令牌的生成时间间隔是否超过预设的令牌使用时长,判断当前的令牌是否有效。实现了当前令牌在使用时间的唯一性,进一步地提高了用户的安全性。

[0010] 优选地,所述允许所述客户端登录之后,还包括:判断所述第一密钥的使用次数是否大于预设使用次数;当所述第一密钥的使用次数大于预设使用次数时,根据所述客户端信息重新生成密钥;将所述重新生成的密钥发送给所述客户端。根据第一密钥的使用次数判断第一密钥是否过期,若过其则生成新的密钥发给客户,达到同一密钥不会使用过长时间,并且密钥不会经常改变,有利于对密钥的控制及密钥的安全性。

[0011] 一种客户端的认证处理装置,包括:获取模块,用于获取客户端信息;生成模块,用于根据所述客户端信息生成当前令牌和第一密钥;发送模块,用于发送所述当前令牌和第一密钥给客户端。

[0012] 优选地,该装置还包括:接收模块,用于接收客户端发送的登录请求信息,所述登录请求信息包括所述客户端信息、令牌和密钥;第一判断模块,用于判断登录请求信息与所述获取的客户端信息、所述生成的当前令牌和第一密钥是否匹配,并判断所述登录请求信息的发送时间与所述当前令牌的生成时间之间的时间间隔是否小于预设令牌使用时长;允许登录模块,用于当登录请求信息与所述获取的客户端信息、所述生成的当前令牌和第一密钥匹配,且所述时间间隔小于预设令牌使用时长时,允许所述客户端登录。

[0013] 优选地,所述装置还包括:第一重新生成模块,用于当所述时间间隔等于或大于预设令牌使用时长时,根据所述客户端信息重新生成令牌;第一重新发送模块,用于将所述重新生成的令牌发送给所述客户端。

[0014] 优选地,该装置还包括:第二判断模块,用于在所述允许登录模块允许所述客户端登录之后,判断所述第一密钥的使用次数是否大于预设使用次数;第二重新生成模块,用于当所述第一密钥的使用次数大于预设使用次数时,根据所述客户端信息重新生成密钥;第二重新发送模块,用于将所述重新生成的密钥发送给所述客户端。

[0015] 本发明的其它特征和优点将在随后的说明书中阐述,并且,部分地从说明书中变得显而易见,或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

[0016] 下面通过附图和实施例,对本发明的技术方案做进一步的详细描述。

附图说明

[0017] 附图用来提供对本发明的进一步理解,并且构成说明书的一部分,与本发明的实施例一起用于解释本发明,并不构成对本发明的限制。在附图中:

[0018] 图 1 为本发明实施例中一种客户端的认证处理方法的流程图。

[0019] 图 2 为本发明实施例中一种客户端的认证处理装置的结构示意图。

具体实施方式

[0020] 以下结合附图对本发明的优选实施例进行说明,应当理解,此处所描述的优选实施例仅用于说明和解释本发明,并不用于限定本发明。

[0021] 如图 1 所示,本发明实施例提供了一种客户端的认证处理方法,用于服务器侧,包括以下步骤:

[0022] 步骤 101,获取客户端信息。

[0023] 步骤 102,根据客户端信息生成当前令牌和第一密钥。

[0024] 步骤 103,发送当前令牌和第一密钥给客户端。

[0025] 服务器根据获得的客户端信息生成当前令牌和密钥并发送给客户端,实现令牌是唯一存在,提高了用户在使用客户端时的安全性。由于服务器是根据客户端信息生成的当前令牌,而每个客户端的信息并不相同,所以当前令牌是唯一存在的,不会出现有与之相同的令牌。

[0026] 较佳地,客户端信息包括:客户端帐号、客户端 IP 地址、客户端帐号第一次生成令牌的时间和客户端帐号最近一次获取令牌的时间。

[0027] 较佳地,发送当前令牌及第一密钥给客户端后,客户端通过令牌及密钥登录服务器侧时,服务器侧执行以下步骤 S1-S3:

[0028] 步骤 S1、接收客户端发送的登录请求信息,登录请求信息包括客户端信息、令牌和密钥;

[0029] 步骤 S2、判断登录请求信息与所述获取的客户端信息、生成的当前令牌和第一密钥是否匹配,并判断登录请求信息的发送时间与当前令牌的生成时间之间的时间间隔是否小于预设令牌使用时长;

[0030] 步骤 S3、当登录请求信息与获取的客户端信息、生成的当前令牌和第一密钥匹配,且时间间隔小于预设令牌使用时长时,允许客户端登录。

[0031] 服务器通过判断客户端请求登录时,发送的登录请求信息是否与获取的客户端信息是否匹配,并且判断当前令牌的生成时间是否超时,来确定请求登录的客户端是否有权登录服务器。通过唯一的令牌及密钥同时确认客户端的身份,增加了客户端登录服务器时,服务器的安全性,进而增加了服务器对其他客户端的安全性。

[0032] 较佳地,当执行上述步骤 S2 时,若判断时间间隔等于或大于预设令牌使用时长时:则重新根据客户端信息生成令牌;并重新生成的令牌发送给客户端。通过判断登录请求信息的发送时间与当前令牌的生成时间间隔是否超过预设的令牌使用时长,判断当前的令牌是否有效。实现了当前令牌在使用时间的唯一性,进一步地提高了用户的安全性。

[0033] 较佳地,当执行完上述步骤 S3 之后,需要判断密钥的使用次数,若密钥的使用次数大于预设使用次数时,服务器根据客户端信息重新生成密钥;将重新生成的密钥发送给客户端。并且生成当前令牌时,还会生成第一密钥,第一密钥并不是每次生成令牌时都同时生成,而是根据第一密钥的使用次数来判断第一密钥是否需要生成,如果第一密钥的使用次数过高,则第一密钥的安全性有所下降,这时就需要重新生成密钥来更新密钥,使客户端

及服务器保持着较的安全性。根据第一密钥的使用次数判断第一密钥是否过期,若过其则生成新的密钥发给客户,达到同一密钥不会使用过长时间,并且密钥不会经常改变,有利于对密钥的控制及密钥的安全性。

[0034] 下面通过几个典型实施例来详细介绍本发明实施例提供的技术方案。

[0035] 实施例一

[0036] 本实施例一利用上述客户端的认证处理方法进行通过令牌的管理,服务器和客户端的具体操作如下:

[0037] 步骤A,服务器获取客户端信息,其中,客户端信息包括:客户端帐号、客户端 IP 地址、客户端帐号第一次生成令牌的时间和客户端帐号最近一次获取令牌的时间。

[0038] 步骤B,服务器根据客户端信息生成当前令牌和第一密钥。

[0039] 步骤C,服务器发送当前令牌和第一密钥给客户端。

[0040] 步骤D、客户端向服务器发送登录请求信息,登录请求信息包括所述客户端信息、令牌和密钥。

[0041] 步骤E,服务器接收客户端发送的登录请求信息。

[0042] 步骤F,服务器判断登录请求信息与获取的客户端信息、生成的当前令牌和第一密钥是否匹配,并判断登录请求信息的发送时间与当前令牌的生成时间之间的时间间隔是否小于预设令牌使用时长。

[0043] 当上述判断的结果全部为是时,继续执行步骤G;

[0044] 当上述判断的结果全部为否,则不允许客户端登录,结束流程;或者,当服务器判断出上述时间间隔等于或大于预设令牌使用时长时,继续执行步骤H。

[0045] 步骤G,服务器当登录请求信息与获取的客户端信息、生成的当前令牌和第一密钥匹配,且上述时间间隔小于预设令牌使用时长时,允许客户端登录,继续执行步骤I。

[0046] 步骤H,服务器判断出上述时间间隔等于或大于预设令牌使用时长时:则重新根据客户端信息生成令牌;并重新生成的令牌发送给客户端。

[0047] 步骤I,服务器需要判断密钥的使用次数,若密钥的使用次数大于预设使用次数时,服务器根据客户端信息重新生成密钥;将重新生成的密钥发送给所述客户端。

[0048] 本发明实施例一提供一种客户端的认证处理方法,服务器根据客户端发来的客户端信息生成令牌和密钥,并将生成的令牌和密钥发送给客户端,客户端再用获得的令牌登录服务器进行其他操作。

[0049] 其中,客户端发来的客户端信息包括:客户端帐号、客户端 IP 地址、客户端帐号第一次生成令牌的时间和客户端帐号最近一次获取令牌的时间。由于上述客户端信息所组合之后是唯一的,所以根据唯一的客户端信息所生成的令牌及密钥也必然唯一。

[0050] 当客户端向服务器发送登录请求时,服务器根据获得的客户端信息、发送的令牌及密钥确定客户端是否有权限进入服务,判断客户端是否有权限时还需要判断客户端所发送的令牌是否还在使用时间内,具体的判断方法是判断登录请求信息的发送时间与当前令牌的生成时间之间的时间间隔是否小于预设令牌使用时长,若登录请求信息的发送时间与当前令牌的生成时间之间的时间间隔小于预设令牌使用时长,则可以继续使用该当前令牌登录服务器;若登录请求信息的发送时间与当前令牌的生成时间之间的时间间隔是等于或大于预设令牌使用时长时,则服务器重新根据客户端信息生成令牌并发送给客户端,客户

端通过新的令牌登录服务器。

[0051] 当客户端登录进入服务器后,密钥被使用一次,这时还需要判断密钥被使用的次数确定密钥是否需要更新。

[0052] 本发明实施例一通过以上多重方法同时进行,使令牌及密钥是唯一存在的,提高客户端及服务器的安全性。

[0053] 以上描述了一种处理通讯录的方法实现过程,该过程可由装置实现,下面对装置的内部功能和结构进行介绍。

[0054] 如图 2 所示,一种客户端的认证处理装置,包括:

[0055] 获取模块 201,用于获取客户端信息;

[0056] 生成模块 202,用于根据客户端信息生成当前令牌和第一密钥;

[0057] 发送模块 203,用于发送当前令牌和第一密钥给客户端。

[0058] 该装置还包括:接收模块,用于接收客户端发送的登录请求信息,登录请求信息包括客户端信息、令牌和密钥;

[0059] 第一判断模块,用于判断登录请求信息与获取的客户端信息、生成的当前令牌和第一密钥是否匹配,并判断登录请求信息的发送时间与当前令牌的生成时间之间的时间间隔是否小于预设令牌使用时长;

[0060] 允许登录模块,用于当登录请求信息与获取的客户端信息、生成的当前令牌和第一密钥匹配,且时间间隔小于预设令牌使用时长时,允许客户端登录。

[0061] 该装置还包括:第一重新生成模块,用于当时间间隔等于或大于预设令牌使用时长时,根据客户端信息重新生成令牌;

[0062] 第一重新发送模块,用于将重新生成的令牌发送给客户端。

[0063] 该装置还包括:第二判断模块,用于判断第一密钥的使用次数是否大于预设使用次数;

[0064] 第二重新生成模块,用于当第一密钥的使用次数大于预设使用次数时,根据客户端信息重新生成密钥;

[0065] 第二重新发送模块,用于将重新生成的密钥发送给客户端。

[0066] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器和光学存储器等)上实施的计算机程序产品的形式。

[0067] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0068] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特

定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制品,该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

[0069] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

[0070] 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。

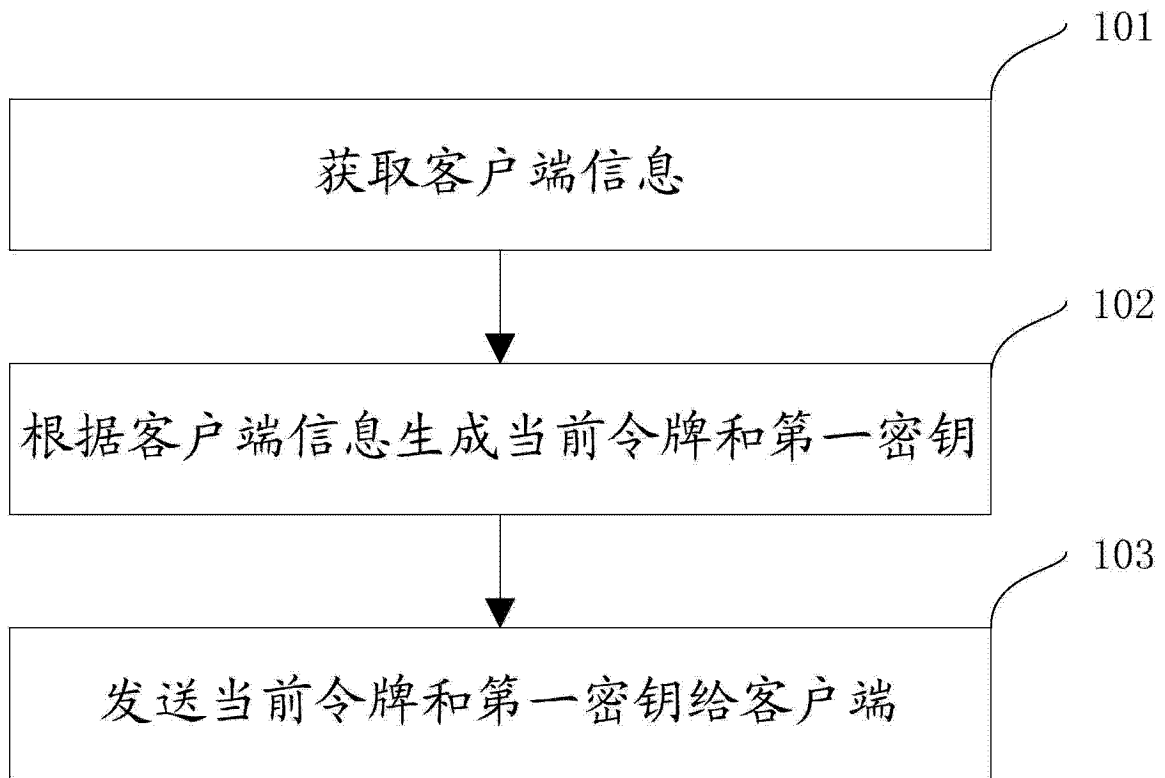


图 1

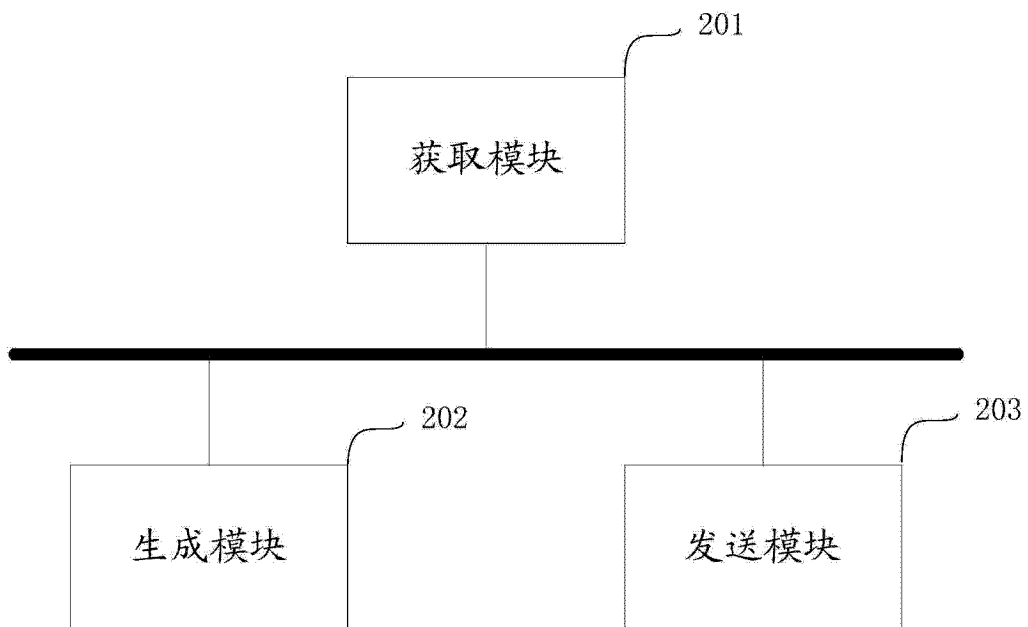


图 2