



(12) 发明专利申请

(10) 申请公布号 CN 104780176 A

(43) 申请公布日 2015.07.15

(21) 申请号 201510208327.2

(22) 申请日 2015.04.28

(71) 申请人 中国科学院微电子研究所

地址 100029 北京市朝阳区北土城西路3号
中科院微电子所

(72) 发明人 陈岚 肖京 雷君

(74) 专利代理机构 北京集佳知识产权代理有限公司 11227

代理人 王宝筠

(51) Int. Cl.

H04L 29/06(2006.01)

H04L 9/32(2006.01)

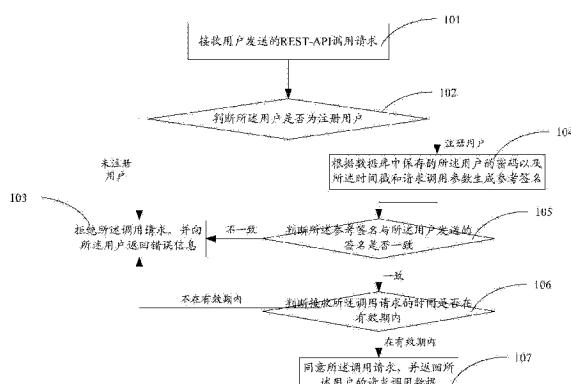
权利要求书2页 说明书6页 附图1页

(54) 发明名称

安全调用表述性状态转移应用编程接口的方法和系统

(57) 摘要

本发明提供的一种安全调用表述性状态转移应用编程接口的方法和系统，包括：接收用户发送的表述性状态转移应用编程接口调用请求；判断用户是否为注册用户；若为未注册用户，则拒绝调用请求，并向用户返回错误信息；若为注册用户，则根据数据库中保存的用户的密码以及时间戳和请求调用参数生成参考签名，并判断参考签名与用户发送的签名是否一致；若不一致，拒绝调用请求，并向用户返回错误信息；若一致，判断接收调用请求的时间是否在有效期内，若在有效期内，同意调用请求，并向用户返回请求调用数据，若不在，则拒绝调用请求，并向用户返回错误信息，以提高调用物联网表述性状态转移应用编程接口的安全性。



1. 一种安全调用表述性状态转移应用编程接口的方法,其特征在于,包括:

接收用户发送的表述性状态转移应用编程接口调用请求,所述调用请求包括所述用户的用户名、请求调用参数、时间戳和签名;

判断所述用户是否为注册用户;

若为未注册用户,则拒绝所述调用请求,并向所述用户返回错误信息;

若为注册用户,则根据数据库中保存的所述用户的密码以及所述时间戳和请求调用参数生成参考签名,并判断所述参考签名与所述用户发送的签名是否一致;

若不一致,拒绝所述调用请求,并向所述用户返回错误信息;

若一致,判断接收所述调用请求的时间是否在有效期内,若在有效期内,同意所述调用请求,并向所述用户返回请求调用数据,若不在,则拒绝所述调用请求,并向所述用户返回错误信息。

2. 根据权利要求 1 所述的方法,其特征在于,所述签名是根据所述请求调用参数、时间戳和所述用户的密码生成并加密的,所述参考签名与所述签名的生成和加密方式相同。

3. 根据权利要求 2 所述的方法,其特征在于,所述接收用户发送的表述性状态转移应用编程接口调用请求之前,还包括:

接收所述用户的注册请求,并对所述用户进行认证,认证通过后,向所述用户发送授权的用户名和对应的密码,所述用户名和密码与所述用户一一对应。

4. 根据权利要求 2 所述的方法,其特征在于,所述判断接收所述调用请求的时间是否在有效期内包括:

判断接收所述调用请求的时间与当前时间是否相差不超过 10s;

若不超过,则在有效期内,若超过,则不在有效期内。

5. 根据权利要求 2 所述的方法,其特征在于,所述向所述用户返回的错误信息是指提示所述用户拒绝所述调用请求的原因的信息。

6. 一种安全调用表述性状态转移应用编程接口的系统,其特征在于,包括:

接收模块,用于接收用户发送的表述性状态转移应用编程接口调用请求,所述调用请求包括所述用户的用户名、请求调用参数、时间戳和签名;

第一判断模块,用于判断所述用户是否为注册用户,若为未注册用户,则拒绝所述调用请求,并发送第一控制指令至发送模块,若为注册用户,则发送第二控制指令至加密模块;

加密模块,用于在接收到所述第二控制指令后,根据数据库中保存的所述用户的密码以及所述时间戳和请求调用参数生成参考签名,并将所述签名发送至第二判断模块;

第二判断模块,用于判断所述参考签名与所述用户发送的签名是否一致,若不一致,则拒绝所述调用请求,并发送所述第一控制指令至发送模块,若一致,进一步判断接收所述调用请求的时间是否在有效期内,若在有效期内,则同意所述调用请求,并发送第三控制指令至发送模块,若不在,则拒绝所述调用请求,并发送所述第一控制指令至发送模块;

发送模块,用于在接收到所述第一控制指令后,向所述用户返回错误信息;在接收到所述第三控制指令后,向所述用户返回请求调用数据。

7. 根据权利要求 6 所述的系统,其特征在于,所述签名是根据所述请求调用参数、时间戳和所述用户的密码生成并加密的,所述参考签名与所述签名的生成和加密方式相同。

8. 根据权利要求 7 所述的系统,其特征在于,还包括:

注册认证模块，用于接收所述用户的注册请求，并对所述用户进行认证，认证通过后，向所述用户发送授权的用户名和对应的密码，所述用户名和密码与所述用户一一对应。

9. 根据权利要求 7 所述的系统，其特征在于，所述第二判断模块判断接收所述调用请求的时间是否在有效期内包括判断接收所述调用请求的时间与当前时间是否相差不超过 10s，若不超过，则在有效期内，若超过，则不在有效期内。

10. 根据权利要求 7 所述的系统，其特征在于，还包括：

异常处理模块，用于生成所述用户的表达性状态转移应用编程接口调用请求的错误信息，以提示所述用户拒绝所述调用请求的原因。

安全调用表述性状态转移应用编程接口的方法和系统

技术领域

[0001] 本发明涉及计算机网络技术领域,更具体地说,涉及一种安全调用表述性状态转移应用编程接口的方法和系统。

背景技术

[0002] REST(Representational State Transfer,表述性状态转移)是一种针对网络应用的设计和开发方式。当前,REST的流行使得越来越多的框架开始支持REST,为我们构建下一代高性能、高可伸缩性、简单性、可移植性以及高可靠性的Web程序提供了一个架构风格上的准则。其中,REST风格架构具有如下特点:所有的事物都被抽象为资源,每个资源都对应一个唯一的资源标示符URI,对资源的各类操作并不会改变其资源标示符URI,所有的操作都是无状态的。

[0003] 随着使用者对安全性的要求越来越高,关于REST的安全话题已经成为人们关注的重点之一。由于REST-API(Application Programming Interface,应用编程接口)的无状态性,即下一次的调用请求和这一次的调用请求是完全无关的,因此,每一次调用请求都得做身份认证。但是,由于TLS(Transport Layer Security,安全传输层协议)的服务器端配置相对复杂,且其对客户端的兼容性较差,不适用于这种数据量大、调用频度高的泛在网络的物联网应用,因此,必须依靠开发人员定义自己的安全方法来维护资源的操作,防止调用REST-APT时受到攻击。

发明内容

[0004] 有鉴于此,本发明提供了一种安全调用表述性状态转移应用编程接口的方法和系统,以保证调用REST-API的安全性,防止调用REST-APT时受到攻击。

[0005] 为实现上述目的,本发明提供如下技术方案:

[0006] 一种安全调用表述性状态转移应用编程接口的方法,包括:

[0007] 接收用户发送的表述性状态转移应用编程接口调用请求,所述调用请求包括所述用户的用户名、请求调用参数、时间戳和签名;

[0008] 判断所述用户是否为注册用户;

[0009] 若为未注册用户,则拒绝所述调用请求,并向所述用户返回错误信息;

[0010] 若为注册用户,则根据数据库中保存的所述用户的密码以及所述时间戳和请求调用参数生成参考签名,并判断所述参考签名与所述用户发送的签名是否一致;

[0011] 若不一致,拒绝所述调用请求,并向所述用户返回错误信息;

[0012] 若一致,判断接收所述调用请求的时间是否在有效期内,若在有效期内,同意所述调用请求,并向所述用户返回请求调用数据,若不在,则拒绝所述调用请求,并向所述用户返回错误信息。

[0013] 优选的,所述签名是根据所述请求调用参数、时间戳和所述用户的密码生成并加密的,所述参考签名与所述签名的生成和加密方式相同。

[0014] 优选的，所述接收用户发送的表述性状态转移应用编程接口调用请求之前，还包括：

[0015] 接收所述用户的注册请求，并对所述用户进行认证，认证通过后，向所述用户发送授权的用户名和对应的密码，所述用户名和密码与所述用户一一对应。

[0016] 优选的，所述判断接收所述调用请求的时间是否在有效期内包括：

[0017] 判断接收所述调用请求的时间与当前时间是否相差不超过 10s；

[0018] 若不超过，则在有效期内，若超过，则不在有效期内。

[0019] 优选的，所述向所述用户返回的错误信息是指提示所述用户拒绝所述调用请求的原因的信息。

[0020] 一种安全调用表述性状态转移应用编程接口的系统，包括：

[0021] 接收模块，用于接收用户发送的表述性状态转移应用编程接口调用请求，所述调用请求包括所述用户的用户名、请求调用参数、时间戳和签名；

[0022] 第一判断模块，用于判断所述用户是否为注册用户，若为未注册用户，则拒绝所述调用请求，并发送第一控制指令至发送模块，若为注册用户，则发送第二控制指令至加密模块；

[0023] 加密模块，用于在接收到所述第二控制指令后，根据数据库中保存的所述用户的密码以及所述时间戳和请求调用参数生成参考签名，并将所述签名发送至第二判断模块；

[0024] 第二判断模块，用于判断所述参考签名与所述用户发送的签名是否一致，若不一致，则拒绝所述调用请求，并发送所述第一控制指令至发送模块，若一致，进一步判断接收所述调用请求的时间是否在有效期内，若在有效期内，则同意所述调用请求，并发送第三控制指令至发送模块，若不在，则拒绝所述调用请求，并发送所述第一控制指令至发送模块；

[0025] 发送模块，用于在接收到所述第一控制指令后，向所述用户返回错误信息；在接收到所述第三控制指令后，向所述用户返回请求调用数据。

[0026] 优选的，所述签名是根据所述请求调用参数、时间戳和所述用户的密码生成并加密的，所述参考签名与所述签名的生成和加密方式相同。

[0027] 优选的，还包括：

[0028] 注册认证模块，用于接收所述用户的注册请求，并对所述用户进行认证，认证通过后，向所述用户发送授权的用户名和对应的密码，所述用户名和密码与所述用户一一对应。

[0029] 优选的，所述第二判断模块判断接收所述调用请求的时间是否在有效期内包括判断接收所述调用请求的时间与当前时间是否相差不超过 10s，若不超过，则在有效期内，若超过，则不在有效期内。

[0030] 优选的，还包括：

[0031] 异常处理模块，用于生成所述用户的表述性状态转移应用编程接口调用请求的错误信息，以提示所述用户拒绝所述调用请求的原因。

[0032] 与现有技术相比，本发明所提供的技术方案具有以下优点：

[0033] 本发明所提供的安全调用表述性状态转移应用编程接口的方法和系统，通过在调用表述性状态转移应用编程接口的过程中检验用户身份的方法来保证调用数据的安全，由于用户的密码通过加密为签名的形式传输，因此，用户的密码从未出现在网络传输中，从而保护了用户的隐私信息；此外，本发明通过时间戳来判断调用请求的时间是否在有效期内，

以应对黑客在传输中的拦截、窃取数据或进行重发攻击等恶意行为。本发明提供的方法和系统大大提高了调用物联网表述性状态转移应用编程接口的安全性，既保证了 REST 风格架构无状态的特点，又满足了表述性状态转移应用编程接口安全调用的要求，提高了服务的安全性和可靠性。

附图说明

[0034] 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，还可以根据提供的附图获得其他的附图。

[0035] 图 1 本发明的第一个实施例提供的一种安全调用 REST-API 的方法的流程图；

[0036] 图 2 为本发明的第二个实施例提供的一种安全调用 REST-API 的系统的结构示意图。

具体实施方式

[0037] 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，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。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前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0038] 本发明的第一个实施例提供了一种安全调用 REST-API 的方法，该方法的流程图如图 1 所示，包括：

[0039] S101：接收用户发送的 REST-API 调用请求；

[0040] 所述调用请求包括所述用户的用户名、请求调用参数、时间戳和签名。

[0041] 由于只有已注册的用户才能调用 REST-API，因此，每个用户都需拥有一个用户名 User ID 以及对应的密码 Password。

[0042] 基于此，客户端向应用服务器发起调用请求之前，即应用服务器在接收用户发送的 REST-API 调用请求之前，还包括：

[0043] 接收所述用户的注册请求，并对所述用户进行认证，认证通过后，向所述用户发送授权的用户名 User ID 和对应的密码 Password，所述用户名 User ID 和密码 Password 与所述用户一一对应。

[0044] 客户端向应用服务器发起 REST-API 调用请求时，在 HTTP 报文中封装用户名 User ID、请求调用参数、时间戳 timestamp 和签名 signature。其中，所述签名 signature 是根据所述请求调用参数、时间戳 timestamp 和所述用户的密码 Password 生成并加密的，具体为：

[0045] 将需要发送的请求调用参数数据以字典序升序排序好，使用 key = value 的形式，每个参数中间用 ‘&’ 连接，尾部加上时间戳 timestamp，最后加上密码 Password 组成一个字符串，其中请求调用参数为空时，字符串只包含时间戳 timestamp 和密码 Password，然后将整个字符串经 MD5 加密后生成签名 signature，之后客户端通过 HTTP 请求将用户名 User ID、请求调用参数、时间戳 timestamp 和签名 signature 发送给应用服务器。

[0046] 例如,已注册的用户身份为 :User ID = user1, Password = 123456789,该用户需要发送的请求调用参数为 k1 = v1,k2 = v2,k3 = v3,时间戳为 2015-01-0617:27:12,则字符串为 k1 = v1&k2 = v2&k3 = v3&2015-01-0617:27:12&123456789,通过 MD5 加密得到的签名为 03D509391F64BF048CC832C7B82A9FF3,则客户端发送的数据即应用服务器接收到的用户发送的 REST-API 调用请求的数据包括 :User ID = user1 ;k1 = v1 ;k2 = v2 ;k3 = v3 ;timestamp = 2015-01-0617:27:12 ;signature = 03D509391F64BF048CC832C7B82A9FF3。

[0047] S102 :判断所述用户是否为注册用户,若为未注册用户,则进入 S103 ;若为注册用户,则进入 S104 ;

[0048] 服务器在接收到 HTTP 报文时,首先提取 HTTP 报文中的用户名 User ID 信息,然后服务器在自身数据库中保存的用户信息表中查询是否存在 ID 为 User ID 的用户,如果不存在,说明该用户为未注册用户,则鉴权失败,进入 S103,即拒绝所述调用请求,并向用户返回错误信息 ;如果存在,则说明该用户为注册用户,则进入 S104。

[0049] S103 :拒绝所述调用请求,并向所述用户返回错误信息 ;

[0050] 拒绝所述调用请求后,还包括 :向所述用户返回错误信息,以提示所述用户拒绝所述调用请求的原因。

[0051] S104 :根据数据库中保存的所述用户的密码以及所述时间戳和请求调用参数生成参考签名,并进入 S105 ;

[0052] 若用户为注册用户,则服务器继续在自身数据库中查找该用户对应的密码,然后根据 HTTP 报文中的时间戳、请求调用参数以及查询到的密码生成参考签名,该参考签名的生成方法和加密方法与客户端发送的签名生成方法和加密方法相同。生成参考签名后,进入 S105。

[0053] S105 :判断所述参考签名与所述用户发送的签名是否一致,若不一致,则进入 S103 ;若一致,进入 S106 ;

[0054] S106 :判断接收所述调用请求的时间是否在有效期内,若在有效期内,则进入 S107,若不在有效期内,则进入 S103。

[0055] 本实施例中,判断接收所述调用请求的时间是否在有效期内包括 :

[0056] 判断接收所述调用请求的时间与当前时间是否相差不超过 10s ;

[0057] 若不超过,则在有效期内,若超过,则不在有效期内。

[0058] 若调用请求的时间在有效期内,则说明数据在网络传输的过程中并未被黑客拦截和窃取,该 REST-API 调用请求是安全有效的 ;若调用请求的时间不在有效期内,则说明数据在网络传输的过程中受到了黑客的拦截、窃取或攻击等,因此,服务器不会响应该调用请求,以免调用的数据被泄露或恶意窃取。

[0059] S107 :同意所述调用请求,并返回所述用户的请求调用数据。

[0060] 本实施例提供的安全调用 REST-API 的方法,通过在调用 REST-API 的过程中检验用户身份的方法来保证调用数据的安全,由于用户的密码通过加密为签名的形式传输,因此,用户的密码从未出现在网络传输中,从而保护了用户的隐私信息 ;此外,本实施例通过时间戳来判断调用请求的时间是否在有效期内,以应对黑客在传输中的拦截、窃取数据或进行重发攻击等恶意行为。本实施例提供的方法大大提高了调用物联网 REST-API 的安全性,既保证了 REST 风格架构无状态的特点,又满足了 REST-API 安全调用的要求,提高了服

务的安全性和可靠性。

[0061] 本发明的第二个实施例提供了一种安全调用 REST-API 的系统，该系统的结构示意图如图 2 所示，包括接收模块 201、第一判断模块 202、加密模块 203、第二判断模块 204 和发送模块 205。

[0062] 其中，接收模块 201 用于接收用户发送的 REST-API 调用请求，所述调用请求包括所述用户的用户名、请求调用参数、时间戳和签名；

[0063] 第一判断模块 202 用于判断所述用户是否为注册用户，若为未注册用户，则拒绝所述调用请求，并发送第一控制指令至发送模块，若为注册用户，则发送第二控制指令至加密模块；

[0064] 加密模块 203 用于在接收到所述第二控制指令后，根据数据库中保存的所述用户的密码以及所述时间戳和请求调用参数生成参考签名，并将所述签名发送至第二判断模块；

[0065] 第二判断模块 204 用于判断所述参考签名与所述用户发送的签名是否一致，若不一致，则拒绝所述调用请求，并发送所述第一控制指令至发送模块，若一致，进一步判断接收所述调用请求的时间是否在有效期内，若在有效期内，则同意所述调用请求，并发送第三控制指令至发送模块，若不在，则拒绝所述调用请求，并发送所述第一控制指令至发送模块；

[0066] 发送模块 205 用于在接收到所述第一控制指令后，向所述用户返回错误信息；在接收到所述第三控制指令后，向所述用户返回请求调用数据。

[0067] 其中，第二判断模块 204 判断接收所述调用请求的时间是否在有效期内包括判断接收所述调用请求的时间与当前时间是否相差不超过 10s，若不超过，则在有效期内，说明数据在网络传输的过程中并未被黑客拦截和窃取，该 REST-API 调用请求是安全有效的；若超过，则不在有效期内，说明数据在网络传输的过程中受到了黑客的拦截、窃取或攻击等，因此，服务器不会响应该调用请求，以免调用的数据被泄露或恶意窃取。

[0068] 本实施例中，客户端发送的签名是根据所述请求调用参数、时间戳和所述用户的密码生成并加密的，所述参考签名与所述签名的生成方式和加密方式相同。具体的，签名的生成方式和加密方式在第一个实施例中已经说明，在此不再赘述。

[0069] 本实施例中的安全调用 REST-API 的系统还包括：注册认证模块，该注册认证模块用于接收所述用户的注册请求，并对所述用户进行认证，认证通过后，向所述用户发送授权的用户名和对应的密码，所述用户名和密码与所述用户一一对应。

[0070] 此外，该系统还包括异常处理模块，该异常处理模块用于生成所述用户的 REST-API 调用请求的错误信息，以提示所述用户拒绝所述调用请求的原因，便于用户针对性地进行操作。

[0071] 本实施例提供的安全调用 REST-API 的系统，通过在调用 REST-API 的过程中检验用户身份的方法来保证调用数据的安全，由于用户的密码通过加密为签名的形式传输，因此，用户的密码从未出现在网络传输中，从而保护了用户的隐私信息；此外，本实施例通过时间戳来判断调用请求的时间是否在有效期内，以应对黑客在传输中的拦截、窃取数据或进行重发攻击等恶意行为。本实施例提供的系统大大提高了调用物联网 REST-API 的安全性，既保证了 REST 风格架构无状态的特点，又满足了 REST-API 安全调用的要求，提高了服

务的安全性和可靠性。

[0072] 本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。对于实施例公开的装置而言，由于其与实施例公开的方法相对应，所以描述的比较简单，相关之处参见方法部分说明即可。

[0073] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

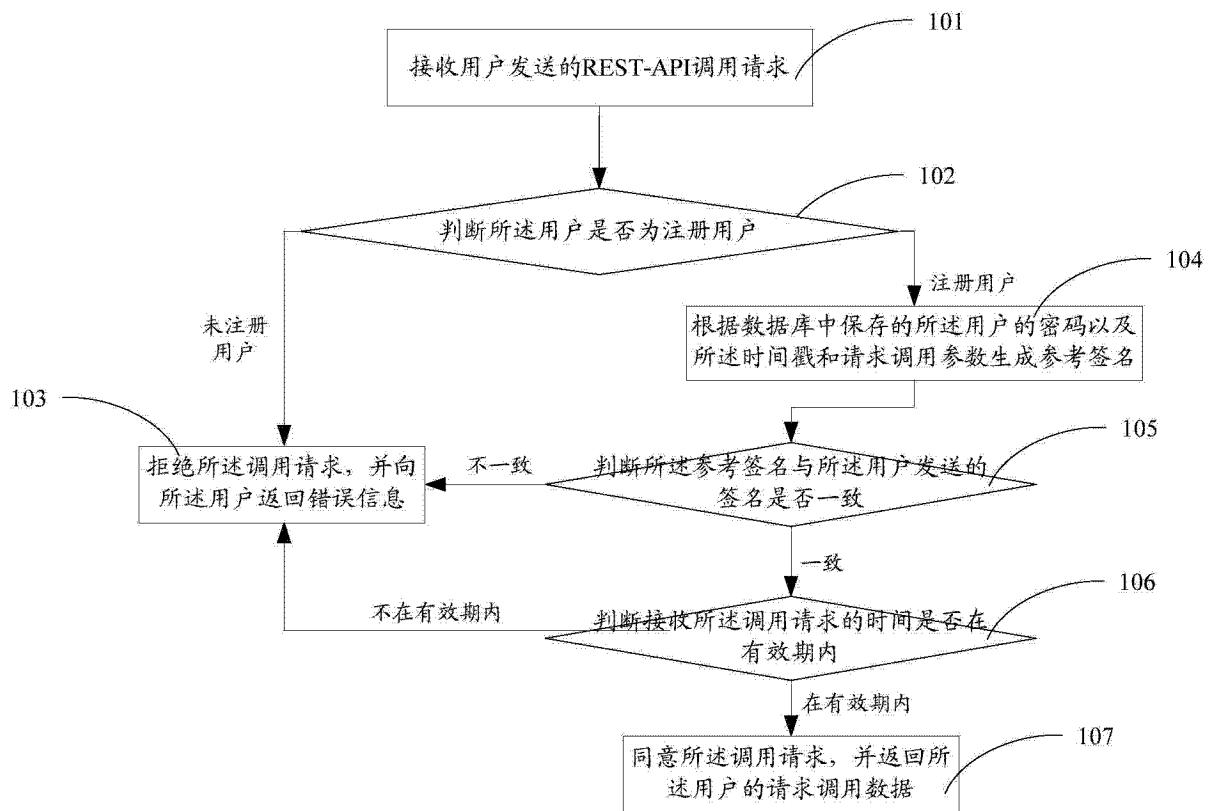


图 1

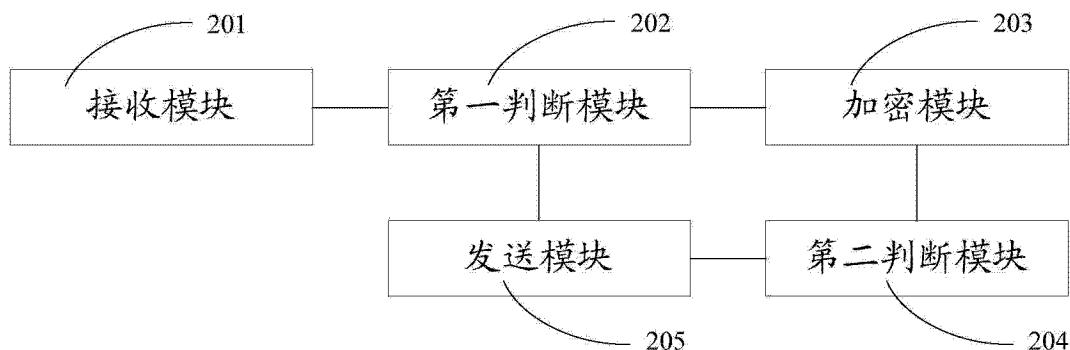


图 2