(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104486326 B
(45)授权公告日 2017.08.11

(21)申请号 201410758204.1

(22)申请日 2014.12.11

(65)同一申请的已公布的文献号
申请公布号 CN 104486326 A

(43)申请公布日 2015.04.01

(73)专利权人 深圳市银河风云网络系统股份有限公司
地址 518055 广东省深圳市南山区高新技术产业园区北区新西路5号银河风云大厦

(72)发明人 黄涛 陈世伟

(74)专利代理机构 深圳市中知专利商标代理有限公司 44101
代理人 吕晓蕾

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 201846351 U,2011.05.25,
CN 102845085 A,2012.12.26,
CN 104158808 A,2014.11.19,
US 2014/0258361 A1,2014.09.11,

审查员 张小倩

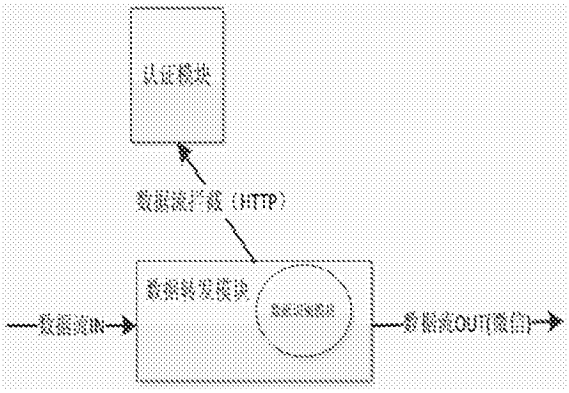
权利要求书1页 说明书4页 附图3页

(54)发明名称

采用微信识别接入网络的认证方法

(57)摘要

一种无地域限制、实用性强且方便用户接入网络的采用微信识别接入网络的认证方法。包括移动通信网第二终端设备和互联网接入端设备，在互联网接入设备端设置数据识别模块；所述数据识别模块对所有接入该网络的数据流进行拦截判断并通过其中的数据转发模块将该数据流中的HTTP数据送至认证模块，其它数据输送至网络服务器。用户通过微信接入网络，完成认证授权，访问网络。同时为营销方提供了快键方便的推送手段，增加客户的使用体验。本发明会紧密关联用户微信帐号，增强推广手段，其具有认证过程简单，方便用户操作；避免蹭网行为，所有在网客户都是有效的客户；通过用户的广告浏览行为，收集推营销推广有用的信息等优点。



CN 104486326 B

1.一种采用微信识别接入网络的认证方法，包括移动通信网第二终端设备和互联网的接入端设备，其特征在于：在互联网的接入端设备设置数据识别模块；所述数据识别模块对所有接入该网络的数据流进行拦截判断并通过其中的数据转发模块将该数据流中的HTTP数据送至认证模块，其它数据输送至网络服务器；所述数据识别模块对所述数据流按以下步骤拦截判断：

1)针对所述数据流的所有报文流进行特征提取；

2)再根据数据特征和行为特征来识别数据流的类型；

3)对接收到的属于未认证网络用户的微信数据，允许其通过该接入端设备上传至上一级网络层，拦截涉及该未认证网络用户的HTTP数据执行特定的提示页面，涉及其的其他数据禁止通过该接入端设备上传到上一级网络层；

4)对接收到的属于已经通过认证的网络用户的全部数据，允许其通过该接入端设备上传到上一级网络层；

5)将待认证网络用户的HTTP请求重定向到特定的页面，在页面提示下，要求关注该网络用户的微信开通网络；

6)待认证网络用户获得网络的使用认证链接，点击该认证链接后开通网络，该网络用户将正常访问网络。

2.根据权利要求1所述的认证方法，其特征在于：所述特征为BASE、FTS、HTTP、Expect、DNS、DPI和PLC特征。

3.根据权利要求1所述的认证方法，其特征在于：当待认证的网络用户的HTTP请求被重定向到特定的页面后，该页面的提示为“提示+广告”，其提示流程如下：

1)访问设置于所述接入端设备的提示页面；

2)发送CGI获取该接入端设备的IP、MAC或路由器地址；

3)点击页面广告；

4)携获取的IP、MAC或路由器地址信息进入网络后台服务器访问目标URL。

4.根据权利要求1所述的认证方法，其特征在于：所述点击认证链接的认证流程如下：

1)获取设置于所述接入端设备的认证页面；

2)发送认证请求CGI；

3)若显示“失败”，则重新发送认证请求CGI；

4)若提示“成功”，则会获取该接入端设备的IP、MAC或路由器地址信息；

5)主动携所述的IP、MAC或路由器地址信息进入网络后台服务器访问相关广告URL。

采用微信识别接入网络的认证方法

技术领域

[0001] 本发明涉及一种移动智能终端接入网络的方法，特别涉及一种采用微信识别接入网络的认证方法。

背景技术

[0002] 移动互联网是将移动通信和互联网二者结合起来，成为一体。在最近几年里，移动通信和互联网成为当今世界发展最快、市场潜力最大、前景最诱人的两大业务，它们的增长速度都是任何预测家未曾预料到的，所以移动互联网可以预见将会创造怎样的经济神话。

[0003] 随着移动互联网发展和智能手机的不断普及，微信推广是网络经济时代企业面临的营销模式的创新，是伴随着微信的火热产生的一种网络营销方式，微信不存在距离的限制，用户注册微信后，可与周围同样注册的“朋友”形成一种联系，用户订阅自己所需的信息，商家通过提供用户需要的信息，推广自己的产品的点对点的营销方式。

[0004] 微信(英文名:wechat)是腾讯公司于2011年1月21日推出的一个为智能终端提供即时通讯服务的免费应用程序，微信支持跨通信运营商、跨操作系统平台通过网络快速发送免费(需消耗少量网络流量)语音短信、视频、图片和文字，同时，也可以使用通过共享流媒体内容的资料和基于位置的社交插件“摇一摇”、“漂流瓶”、“朋友圈”、”公众平台“、”语音记事本“等服务插件。

[0005] 由于软件本身是免费的，使用任何功能都不会收取费用，使用微信时产生的上网流量费比较低廉，同时用户可以通过微信与好友进行文字，语音，图片等形式上更加丰富的方式沟通，为广大用户所喜爱，以至于在距其推出仅仅400余天的2012年3月29日用户数就突破了一亿，此后，微信先后推出的微信开放平台，微信公众平台更进一步推动了用户数量的快速增长，终于，2012年9月17日，微信用户数突破2亿人，从0到突破2亿用户，距离推出只用了14个月时间。大量的微信用户的背后是巨大的营销市场，微信也成为众多商家和企业潜在客户的聚集地，而微信的用户数量还在不断地攀升中，可以预见，在不久的将来，微信用户群体会越来越壮大，越来越壮观，如此庞大数量的潜在客户，哪个企业不为之心动呢?

[0006] 现有技术中移动终端接入网络，通常有以下几种上网认证方法：

[0007] 1)最常用是无线加密:即要求用户输入密码才能接入网络，如WIFI密码、局域网密码等；

[0008] 2)MAC地址限制:要求用户的MAC地址是特定地址时才可通过无线路由器访问网络；

[0009] 3)页面认证:要求用户登录网站后，在主页面上输入特定的用户名和密码才能真正访问网络；

[0010] 4)手机短信认证:要求用户接入网络之后，通过手机号码获取特定密码后，才能真正访问网络。

[0011] 上述的方法或多或少存在如下不足：

[0012] 1)对于上述方法1)而言，需要将密码通告给待接入网络的用户，尤其是新用户会

一次又一次的询问密码是多少，因此，从推广和使用的角度讲很不方便。

[0013] 2)对于上述方法2)而言，在公共场所无法使用。公共场所的特点是用户的流动性较大，不可能做到用户来一次添加一下MAC地址，离开的时候又要删除该MAC地址，因此，对用户而言便利性也较差。

[0014] 3)对于上述方法3)而言，其与和方法1)的不足一样，从推广和使用的角度讲很不方便。

[0015] 4)对于上述方法4)而言，其问题是待接入网络终端设备的使用者需要支付额外的手机短信费用。

发明内容

[0016] 本发明要解决的技术问题是提供一种无地域限制、实用性强且方便用户接入网络的采用微信识别接入网络的认证方法。

[0017] 为了解决上述技术问题，本发明采用的技术方案为：

[0018] 本发明的采用微信识别接入网络的认证方法，包括移动通信网第二终端设备和互联网的接入端设备，在互联网的接入端设备设置数据识别模块；所述数据识别模块对所有接入该网络的数据流进行拦截判断并通过其中的数据转发模块将该数据流中的HTTP数据送至认证模块，其它数据输送至网络服务器；所述数据识别模块对所述数据流按以下步骤拦截判断：

[0019] 1)针对所述数据流的所有报文流进行特征提取；

[0020] 2)再根据数据特征和行为特征来识别数据流的类型；

[0021] 3)对接收到的属于未认证网络用户的微信数据，允许其通过该接入端设备上传至上一级网络层，拦截涉及该未认证网络用户的HTTP数据执行特定的提示页面，涉及其的其他数据禁止通过该接入端设备上传到上一级网络层；

[0022] 4)对接收到的属于已经通过认证的网络用户的全部数据，允许其通过该接入端设备上传到上一级网络层；

[0023] 5)将待认证网络用户的HTTP请求重定向到特定的页面，在页面提示下，要求关注该网络用户的微信开通网络；

[0024] 6)待认证网络用户获得网络的使用认证链接，点击该认证链接后开通网络，该网络用户将正常访问网络。

[0025] 所述特征为BASE、FTS、HTTP、Expect、DNS、DPI和PLC特征。

[0026] 当待认证的网络用户的HTTP请求被重定向到特定的页面后，该页面的提示为“提示+广告”，其提示流程如下：

[0027] 1)访问设置于所述接入端设备的提示页面；

[0028] 2)发送CGI获取该接入端设备的IP、MAC或路由器地址；

[0029] 3)点击页面广告；

[0030] 4)携获取的IP、MAC或路由器地址信息进入网络后台服务器访问目标URL。

[0031] 所述点击认证链接的认证流程如下：

[0032] 1)获取设置于所述接入端设备的认证页面；

[0033] 2)发送认证请求CGI；

[0034] 3)若显示“失败”,则重新发送认证请求CGI;

[0035] 4)若提示“成功”,则会获取该接入端设备的IP、MAC或路由器地址信息;

[0036] 5)主动携所述的IP、MAC或路由器地址信息进入网络后台服务器访问相关广告URL。

[0037] 与现有技术相比,本发明克服了现有技术中的不足,提供了一种方便快捷的基于微信的网络认证方案,用户可以通过微信接入网络,完成认证授权,访问网络。同时为营销方提供了快键方便的推送手段,增加客户的使用体验,增强易用性,提高推广效果。本发明基于微信帐号认证的互联网的接入端设备方案,基于微信帐号,推广微信互联网营销业务。本发明会紧密关联用户微信帐号,增强推广手段,其具有认证过程简单,方便用户操作;避免蹭网行为,所有在网客户都是有效的客户;通过用户的广告浏览行为,收集推营销推广有用的信息等优点。

附图说明

[0038] 图1为本发明的方法中数据转发模块处理数据示意图。

[0039] 图2为本发明的方法中数据转发模块提示流程图。

[0040] 图3为本发明的方法中设备认证流程图。

具体实施方式

[0041] 以下结合附图对本发明作进一步说明。

[0042] 1、微信识别

[0043] 设备(指互联网的接入端设备)针对所有的报文流(具有相同基本特征的一类报文,比如具有相同的源目的IP,源目的端口,协议类型的报文)进行特征的提取。

[0044] 所述特征包括如下部分:

[0045] BASE特征:即基本特征,包含基本协议,ip端口,方向,包序,长度等。

[0046] FTS特征:即关键字特征。表述报文中若干偏移量(L7载荷)的位置可使用某个正则表达式进行匹配。

[0047] HTTP特征:基于HTTP协议的应用比较多而且报文具有固定的格式。我们可采用HTTP的常见字域作为特征,采用正则表达式进行描述。值得一提的是我们自己引入的seq字域,它表示特征中字域的顺序特征。

[0048] Expect特征:及期望连接特征。首先发送一个探测或广播包,该报文特征比较明显。后面的数据报文源端口均采用之前的报文所采用的端口。基于这个基本事实,我们可以在识别那个探测或广播包后做一个期望。

[0049] DNS特征:由于在应用的识别过程中需要循环的针对哈希类型进行哈希计算,并且有一些哈希链表比较长,如DGET,因此引入DNS特征来加速识别应用。基本原理是这样的:识别框架建立一个域名数据库,域名和IP有一个对应的关系,当一个新连接进入识别框架时通过IP就能找到对应的域名,进而就能定位那种应用。

[0050] DPI特征:深度报文特征。描述提取一段敏感内容的通用方法,内容可表示长度,账户等;可作为特征,也可作为非特征(若内容表示长度则作为特征查看和包长是否匹配。

[0051] PLC特征:报文长度特征。若干包的长度统计学特征(平均值;最大值;逐包长度

等)。

[0052] 基于上述方法,我们可以构建数据识别模块将微信相关的数据识别出来。

[0053] 2、数据流区分与重定向

[0054] 如图1所示,设备使用如下的方法处理微信数据和其他数据:

[0055] 即在转发过程中增加数据识别模块,根据数据特征(即所述的BASE、FTP和HTTP特征)和行为特征(即所述的EXPECT、DNS、DPI和PLC特征)来识别数据流的类型(即各种应用的数据,如微信的数据、微博的数据、迅雷数据和QQ数据等)。

[0056] 对还没有认证的用户,放过微信数据,拦截HTTP数据执行特定的提示页面,丢弃其他数据。

[0057] HTTP数据经过处理之后可以用来实现提示流程。

[0058] 对已经通过认证的用户,放过全部的数据。

[0059] 3、点击认证和密码获取

[0060] 用户的HTTP请求被重定向到特定的页面之后,产生的效果是用户会看到一个提示(提示+广告),要求关注网络用户的微信开通网络。

[0061] 通过关注网络用户的微信,网络用户将获得网络的使用认证链接,点击链接之后,网络开通,网络用户将正常访问网络。

[0062] 4、提示流程

[0063] 如图2所示,设备展现的提示流程如下:

[0064] 1)用户请求访问网络(HTTP请求);

[0065] 2)判断用户请求数据地址是否在白名单内;

[0066] 3)用户请求的数据地址在白名单内,允许用户访问数据;

[0067] 4)用户请求的数据不在白名单内,使用302跳转,引导用户访问提示页面;

[0068] 5)展现提示页面。提示页面展现在用户终端时,获取设备的MAC,IP等信息;

[0069] 6)用户可点击提示页面内的广告,带上相关的MAC,IP信息访问广告URL,可提供有效的统计信息。

[0070] 5、认证流程

[0071] 如图3所示,设备展现的认证流程如下:

[0072] 1)用户点击提示页面内的认证按钮,请求认证;

[0073] 2)设备收到请求发送认证页面给用户终端;

[0074] 3)展现认证页面。认证页面展现在用户终端时,自动收集相关的MAC,IP等信息,发送真正的认证请求;

[0075] 4)等待认证结果,认证成功,则开通网络,提示认证成功;

[0076] 5)等待认证结果,认证失败,则提示体失败;

[0077] 6)无论结果成功或失败,认证页面自动带上用户的IP,MAC等信息,主动访问广告URL。

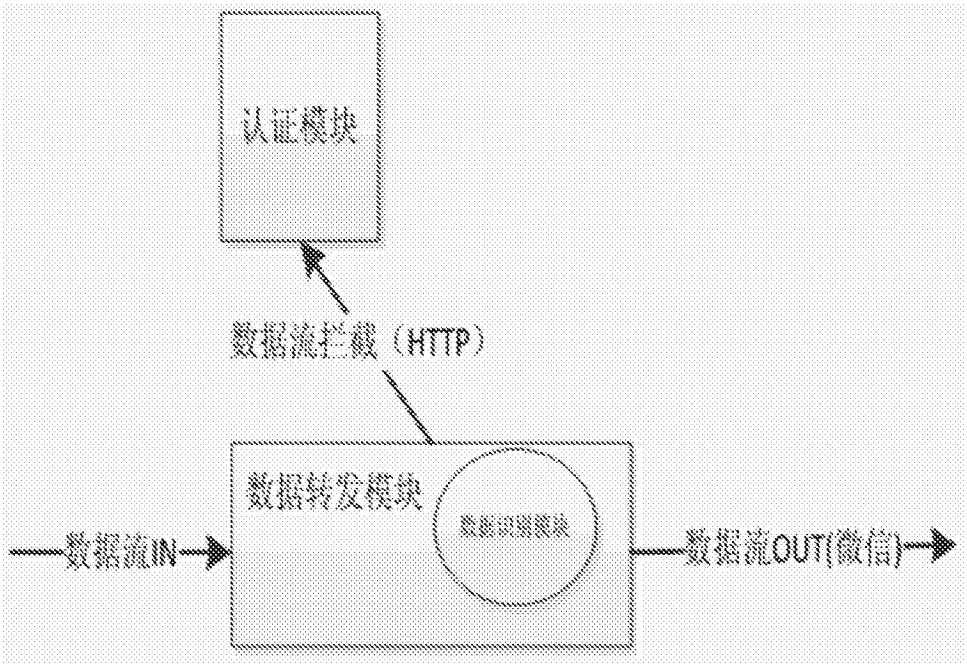


图1

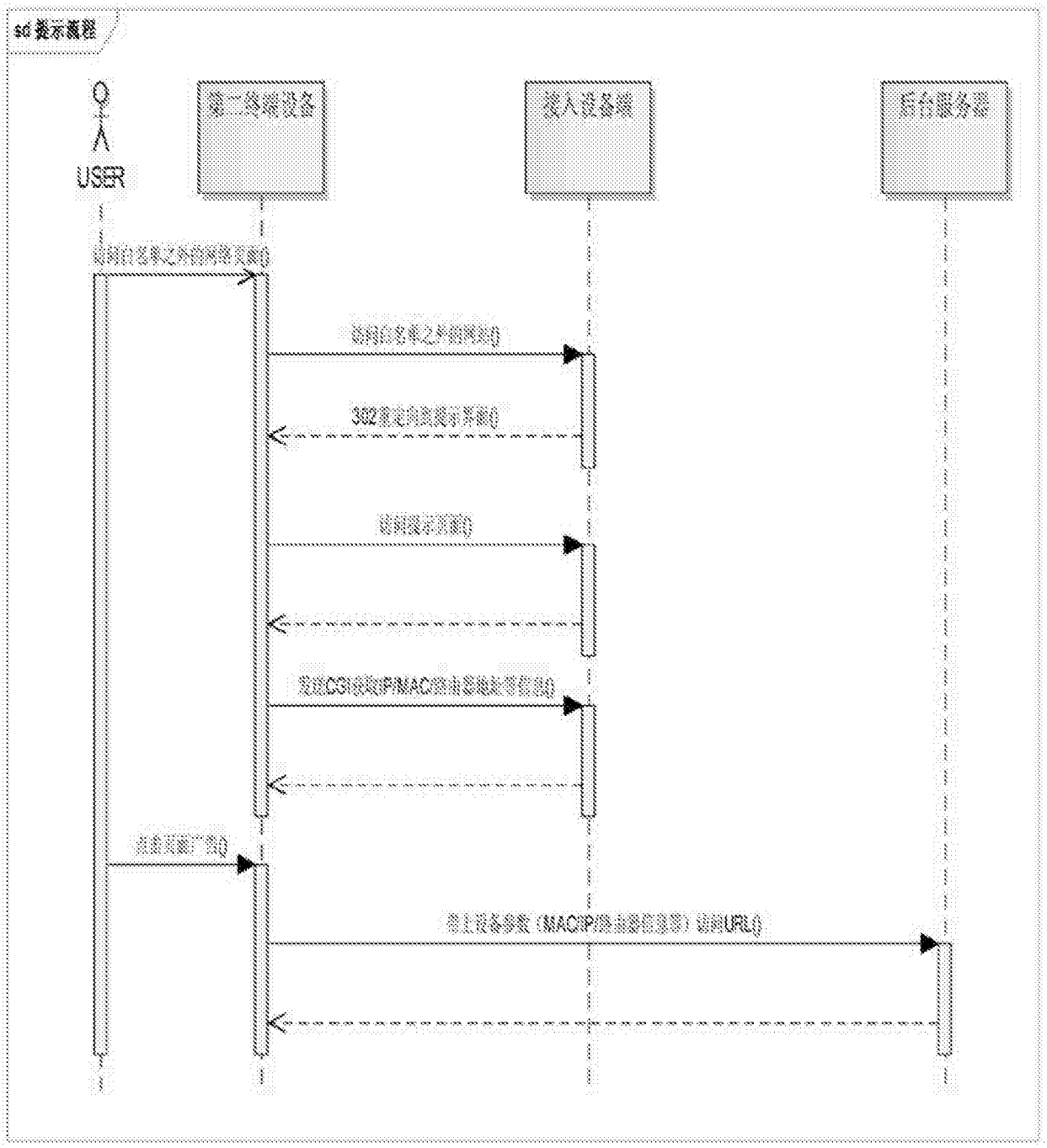


图2

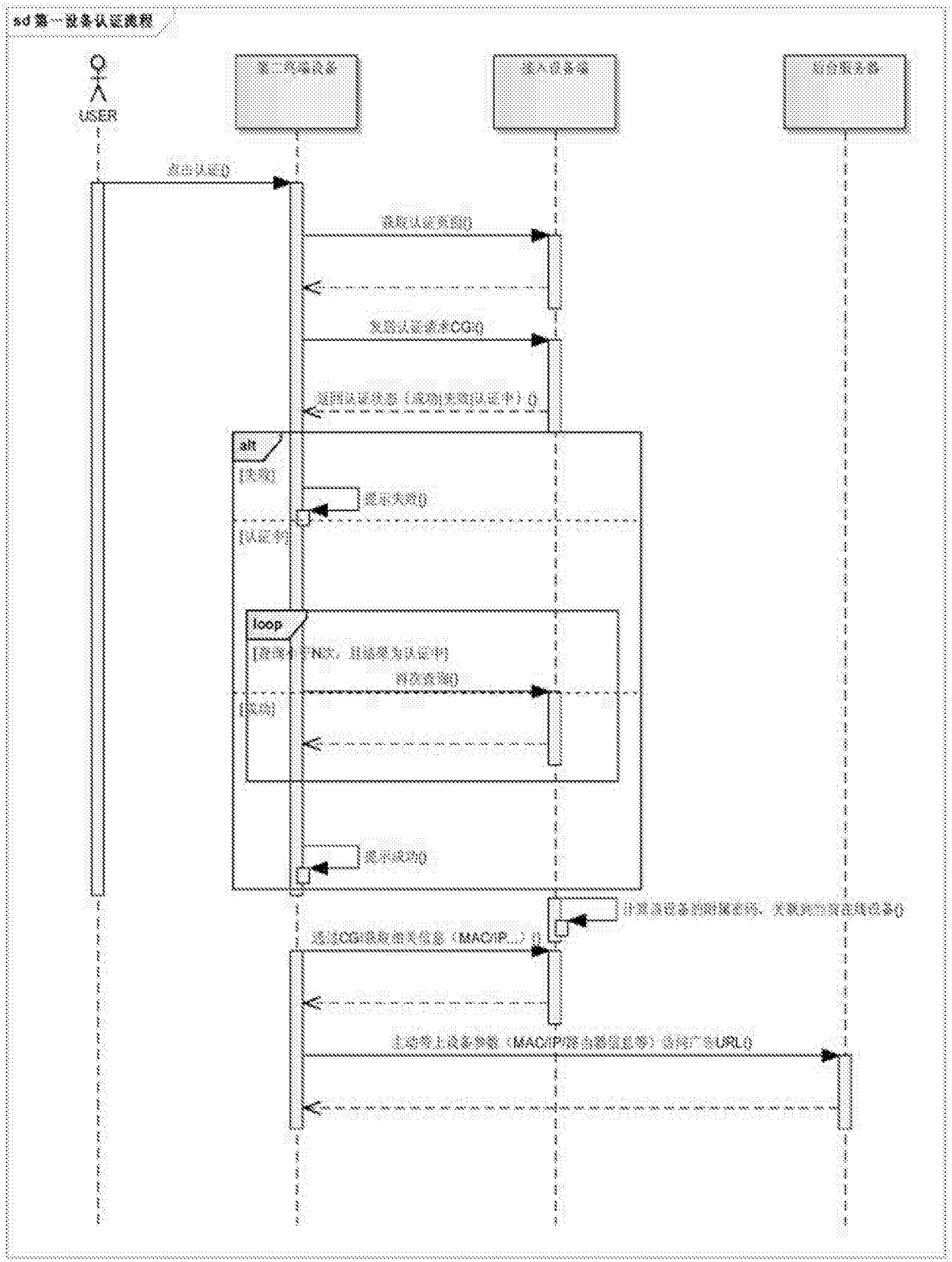


图3