(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103826226 A
(43)申请公布日 2014.05.28

(21)申请号 201410059119.6

(22)申请日 2014.02.20

(71)申请人 深信服网络科技(深圳)有限公司
地址 518000 广东省深圳市南山区麒麟路1号南山科技创业服务中心418、419

(72)发明人 王诚 张兴彦 王金红

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国

(51)Int.Cl.
H04W 12/06(2009.01)

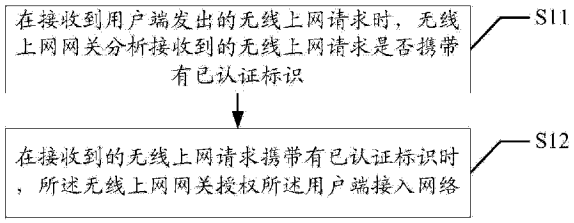
权利要求书2页 说明书7页 附图1页

(54)发明名称

无线上网的控制方法及装置

(57)摘要

本发明公开了一种无线上网的控制方法，该方法包括：在接收到用户端发出的无线上网请求时，无线上网网关分析接收到的无线上网请求是否携带有已认证标识；在接收到的无线上网请求携带有已认证标识时，所述无线上网网关授权所述用户端接入网络。本发明还公开了一种无线上网的控制装置，旨在实现有效避免对用户端再次发出无线上网请求时，还需通过短信验证的方式实现访问互联网产生的短信费用的问题，实现快速、有效的完成用户身份验证，提高用户身份验证的效率，降低用户身份验证成本。



CN 103826226 A

1. 一种无线上网的控制方法，其特征在于，该方法包括步骤：

在接收到用户端发出的无线上网请求时，无线上网网关分析接收到的无线上网请求是否携带有已认证标识；

在接收到的无线上网请求携带有已认证标识时，所述无线上网网关授权所述用户端接入网络。

2. 根据权利要求 1 所述的无线上网的控制方法，其特征在于，在所述无线上网网关分析接收到的无线上网请求是否携带有已认证标识的步骤之后，该方法还包括：

在接收到的无线上网请求未携带有已认证标识时，所述无线上网网关提示用户输入手机号码，并在接收到用户输入的手机号码时，向所述手机号码发送短信验证码；

在接收到用户端发出的所述短信验证码时，所述无线上网网关授权所述用户端接入网络。

3. 根据权利要求 2 所述的无线上网的控制方法，其特征在于，所述在接收到的无线上网请求未携带有已认证标识时，所述无线上网网关提示用户输入手机号码，并在接收到用户输入的手机号码时，向所述手机号码发送短信验证码的步骤之后，该方法还包括：

在未接收到用户端发出的所述短信验证码时，所述无线上网网关提示用户在第一预设时间内发出所述短信验证码，或者，提示用户重新获取短信验证码。

4. 根据权利要求 1 所述的无线上网的控制方法，其特征在于，该方法还包括：

所述无线上网网关分析在第二预设时间内是否接收到携带有已认证标识用户端的无线上网请求；

在第二预设时间内未接收到携带有已认证标识用户端的无线上网请求时，所述无线上网网关将所述未接收到无线上网请求用户端的相关信息进行删除。

5. 根据权利要求 4 所述的无线上网的控制方法，其特征在于，所述无线上网网关分析在第二预设时间内是否接收到携带有已认证标识用户端的无线上网请求的步骤之后，该方法还包括：

在第二预设时间内接收到携带有已认证标识用户端的无线上网请求时，所述无线上网网关为所述接收到无线上网请求用户端的相关信息设置特定标识。

6. 一种无线上网的控制装置，其特征在于，该装置包括：

分析模块，用于在接收到用户端发出的无线上网请求时，分析接收到的无线上网请求是否携带有已认证标识；

控制模块，用于在接收到的无线上网请求携带有已认证标识时，授权所述用户端接入网络。

7. 根据权利要求 6 所述的无线上网的控制装置，其特征在于，该装置还包括：

提醒模块，用于在接收到的无线上网请求未携带有已认证标识时，提示用户输入手机号码，并在接收到用户输入的手机号码时，向所述手机号码发送短信验证码；

所述控制模块，用于在接收到用户端发出的所述短信验证码时，授权所述用户端接入网络。

8. 根据权利要求 7 所述的无线上网的控制装置，其特征在于，

所述提醒模块，用于在未接收到用户端发出的所述短信验证码时，提示用户在第一预设时间内发出所述短信验证码，或者，提示用户重新获取短信验证码。

9. 根据权利要求 6 所述的无线上网的控制装置，其特征在于，该装置还包括处理模块，

所述分析模块，用于分析在第二预设时间内是否接收到携带有已认证标识用户端的无线上网请求；

所述处理模块，用于在第二预设时间内未接收到携带有已认证标识用户端的无线上网请求时，将所述未接收到无线上网请求用户端的相关信息进行删除。

10. 根据权利要求 9 所述的无线上网的控制装置，其特征在于，

所述处理模块，还用于在第二预设时间内接收到携带有已认证标识用户端的无线上网请求时，为所述接收到无线上网请求用户端的相关信息设置特定标识。

无线上网的控制方法及装置

技术领域

[0001] 本发明涉及无线上网领域，尤其涉及无线上网的控制方法及装置。

背景技术

[0002] 随着互联网的普及，使得人们的工作与生活越来越离不开网络。伴随着移动互联网与移动终端的发展，人们期待能随时随地的通过移动互联网来完成工作或进行娱乐。例如，人们在商场购物、餐厅吃饭、银行办理业务或是入住酒店等都期待能通过移动终端上网。

[0003] 目前，使用国内的 3G（The3rd Generation Telecommunication，第 3 代移动通信技术）网络上网会产生非常高的流量费用，基于此原因，为了吸引顾客光临，商场、餐厅、银行、酒店等地往往都提供了免费的 wifi 网络给客户使用。客户可通过连接商家提供的 Wifi 网络上网、看电影、与朋友互动，随时或实时的了解各种信息等。

[0004] 然而，为了满足商家自身营销需要和满足国家上网法律法规，商家提供的 Wifi 网络需要认证用户身份信息。目前，认证用户身份信息的方式主要是使用短信认证的方式。通过短信认证，商家可以得到用户手机号码，方便进行一些营销策略的发布，也可以对用户的上网行为进行审计，防止用户使用网络进行非法活动。

[0005] 但短信认证的用户身份信息的认证方式存在以下缺陷：

[0006] 1、因商家人流量大，使用短信认证将产生高昂的短信费用；

[0007] 2、部分客户是经常到某些固定商家光顾的，他们每次光临都需要重新进行身份认证，这样导致用户身份验证过程繁琐、低效。

[0008] 上述内容仅用于辅助理解本发明的技术方案，并不代表承认上述内容是现有技术。

发明内容

[0009] 本发明的主要目的为提供无线上网的控制方法及装置，旨在实现快速、有效的完成用户身份验证，提高用户身份验证的效率，降低用户身份验证成本。

[0010] 为实现上述目的，本发明提供一种无线上网的控制方法，该方法包括步骤：

[0011] 在接收到用户端发出的无线上网请求时，无线上网网关分析接收到的无线上网请求是否携带有已认证标识；

[0012] 在接收到的无线上网请求携带有已认证标识时，所述无线上网网关授权所述用户端接入网络。

[0013] 优选地，在所述无线上网网关分析接收到的无线上网请求是否携带有已认证标识的步骤之后，该方法还包括：

[0014] 在接收到的无线上网请求未携带有已认证标识时，所述无线上网网关提示用户输入手机号码，并在接收到用户输入的手机号码时，向所述手机号码发送短信验证码；

[0015] 在接收到用户端发出的所述短信验证码时，所述无线上网网关授权所述用户端接

入网络。

[0016] 优选地，所述在接收到的无线上网请求未携带有已认证标识时，所述无线上网网关提示用户输入手机号码，并在接收到用户输入的手机号码时，向所述手机号码发送短信验证码的步骤之后，该方法还包括：

[0017] 在未接收到用户端发出的所述短信验证码时，所述无线上网网关提示用户在第一预设时间内发出所述短信验证码，或者，提示用户重新获取短信验证码。

[0018] 优选地，该方法还包括：

[0019] 所述无线上网网关分析在第二预设时间内是否接收到携带有已认证标识用户端的无线上网请求；

[0020] 在第二预设时间内未接收到携带有已认证标识用户端的无线上网请求时，所述无线上网网关将所述未接收到无线上网请求用户端的相关信息进行删除。

[0021] 优选地，所述无线上网网关分析在第二预设时间内是否接收到携带有已认证标识用户端的无线上网请求的步骤之后，该方法还包括：

[0022] 在第二预设时间内接收到携带有已认证标识用户端的无线上网请求时，所述无线上网网关为所述接收到无线上网请求用户端的相关信息设置特定标识。

[0023] 本发明进一步提供一种无线上网的控制装置，该装置包括：

[0024] 分析模块，用于在接收到用户端发出的无线上网请求时，分析接收到的无线上网请求是否携带有已认证标识；

[0025] 控制模块，用于在接收到的无线上网请求携带有已认证标识时，授权所述用户端接入网络。

[0026] 优选地，该装置还包括：

[0027] 提醒模块，用于在接收到的无线上网请求未携带有已认证标识时，提示用户输入手机号码，并在接收到用户输入的手机号码时，向所述手机号码发送短信验证码；

[0028] 所述控制模块，用于在接收到用户端发出的所述短信验证码时，授权所述用户端接入网络。

[0029] 优选地，所述提醒模块，用于在未接收到用户端发出的所述短信验证码时，提示用户在第一预设时间内发出所述短信验证码，或者，提示用户重新获取短信验证码。

[0030] 优选地，该装置还包括处理模块，

[0031] 所述分析模块，用于分析在第二预设时间内是否接收到携带有已认证标识用户端的无线上网请求；

[0032] 所述处理模块，用于在第二预设时间内未接收到携带有已认证标识用户端的无线上网请求时，将所述未接收到无线上网请求用户端的相关信息进行删除。

[0033] 优选地，所述处理模块，还用于在第二预设时间内接收到携带有已认证标识用户端的无线上网请求时，为所述接收到无线上网请求用户端的相关信息设置特定标识。

[0034] 相对现有技术，本发明在接收到用户端发出的无线上网请求时，分析接收到的无线上网请求是否携带有已认证标识；在接收到的无线上网请求携带有已认证标识时，控制用户端的显示界面跳转至所述无线上网请求对应的访问页面。有效避免对用户端再次发出无线上网请求时，还需通过短信验证的方式实现访问互联网产生的短信费用的问题，实现快速、有效的完成用户身份验证，提高用户身份验证的效率，降低用户身份验证成本。

附图说明

[0035] 图 1 为本发明无线上网的控制方法第一实施例的流程示意图；

[0036] 图 2 为本发明无线上网的控制方法第二实施例的流程示意图；

[0037] 图 3 为本发明无线上网的控制装置第一实施例的功能模块示意图；

[0038] 图 4 为本发明无线上网的控制装置第二实施例的功能模块示意图。

[0039] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0040] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0041] 如图 1 所示，为本发明无线上网的控制方法第一实施例的流程示意图。

[0042] 需要强调的是：图 1 所示流程图仅为一个较佳实施例，本领域的技术人员当知，任何围绕本发明思想构建的实施例都不应脱离于如下技术方案涵盖的范围：

[0043] 在接收到用户端发出的无线上网请求时，无线上网网关分析接收到的无线上网请求是否携带有已认证标识；在接收到的无线上网请求携带有已认证标识时，所述无线上网网关授权所述用户端接入网络。

[0044] 以下是本实施例逐步实现无线上网控制的具体步骤：

[0045] 步骤 S11，在接收到用户端发出的无线上网请求时，无线上网网关分析接收到的无线上网请求是否携带有已认证标识。

[0046] 在本实施例中，所述无线上网的方式优选为 Wifi 上网，用户端通过连接建立的 Wifi 热点实现访问互联网；Wifi 热点经安全网关与互联网服务器连接，安全网关起到对各个用户端的上网连接及上网内容进行控制及监控。各个用户端在通过安全网关的认证之后，即，在安全网关授权接入网络之后，可以访问互联网服务器的内容。所述无线上网网关优选为部署在网络中的安全网关。

[0047] 安全网关在接收到用户端发出的无线上网请求时，分析接收到的无线上网请求是否携带有已验证标识，所述已验证标识可以是用户端的 Mac 地址，及 / 或用户端访问互联网的浏览器中设置的 Cookie。

[0048] 步骤 S12，在接收到的无线上网请求携带有已认证标识时，所述无线上网网关授权所述用户端接入网络。

[0049] 在本实施例中，所述安全网关在接收到的无线上网请求携带有已认证标识时，授权所述用户端接入网络。例如，所述已验证标识为用户端的 Mac 地址，所述安全网关预存有各个已验证用户端的 Mac 地址，在接收到无线上网请求，获取无线上网请求包括的用户端的 Mac 地址，并分析是否有预存 Mac 地址与获取的用户端的 Mac 地址一致，在有预存 Mac 地址与获取的用户端的 Mac 地址一致时，确定接收到的无线上网请求携带有已认证标识，授权所述用户端接入网络，即，所述用户端用户可以进行无线上网访问互联网服务器上的内容。例如，所述已验证标识为用户端访问互联网的浏览器中设置的 Cookie，所述安全网关预存有各个用户端访问互联网的浏览器中设置的 Cookie，在接收到无线上网请求，获取无线上网请求包括的用户端访问互联网的浏览器中设置的 Cookie，并分析是否有预存 Cookie 与获取的用户端访问互联网的浏览器中设置的 Cookie 一致，在有预存 Cookie 与获取的用

户端访问互联网的浏览器中设置的 Cookie 一致时，确定接收到的无线上网请求携带有已认证标识，授权所述用户端接入网络，即，所述用户端用户可以进行无线上网访问互联网服务器上的内容。

[0050] 在接收到的无线上网请求未携带有已认证标识时，所述安全网关提示用户输入手机号码，并在接收到用户输入的手机号码时，向所述手机号码发送短信验证码；在接收到用户端发出的所述短信验证码时，所述安全网关授权所述用户端接入网络。例如，在没有预存 Mac 地址与获取的用户端的 Mac 地址一致，或者，在没有预存 Cookie 与获取的用户端访问互联网的浏览器中设置的 Cookie 一致时，所述安全网关确定接收到的无线上网请求未携带有已认证标识，通过短信验证的方式实现访问互联网服务器上的内容。在未接收到用户端发出的所述短信验证码时，即，在一定时间后(例如，在需要短信验证的方式实现访问互联网服务器上的内容起开始计时，0 秒、1 秒或者 1 分钟后)未接收到用户端发出的所述短信验证码时，所述安全网关提示用户在第一预设时间内发出所述短信验证码，或者，提示用户重新获取短信验证码，以便及时通过发出上述短信验证码，通过用户身份认证，访问互联网。在成功通过安全网关的用户身份认证之后，所述安全网关将无线上网请求包括的用户端的 Mac 地址或者用户端访问互联网的浏览器中设置的 Cookie 进行预存，以在该用户端再次发出无线上网请求时，无需再次通过短信验证的方式实现访问互联网服务器上的内容。所述第一预设时间可以是 30s 或 1 分钟等时间间隔。

[0051] 在本实施例在接收到用户端发出的无线上网请求时，无线上网网关分析接收到的无线上网请求是否携带有已认证标识；在接收到的无线上网请求携带有已认证标识时，所述无线上网网关授权所述用户端接入网络。有效避免对用户端再次发出无线上网请求时，还需通过短信验证的方式实现访问互联网产生的短信费用的问题，实现快速、有效的完成用户身份验证，提高用户身份验证的效率，降低用户身份验证成本。

[0052] 如图 2 所示，为本发明无线上网的控制方法第二实施例的流程示意图。

[0053] 基于上述第一实施例，该方法还包括：

[0054] 步骤 S13，无线上网网关分析在第二预设时间内是否接收到携带有已认证标识用户端的无线上网请求；

[0055] 步骤 S14，在第二预设时间内未接收到携带有已认证标识用户端的无线上网请求时，所述无线上网网关将所述未接收到无线上网请求用户端的相关信息进行删除。

[0056] 在本实施例中，所述已认证标识以用户端的 Mac 地址为例，安全网关预存有所有通过用户身份验证用户端的 Mac 地址。在某个用户端通过用户身份验证访问互联网，结束互联网访问之时起开始计时，分析在第二预设时间内是否接收到该用户端发出的无线上网请求，在第二预设时间内未接收到该用户端发出的无线上网请求时，将存有的该用户端的相关信息进行删除。所述第二预设时间可以是 30 天或 2 个月等时间间隔；所述该用户端的相关信息包括但不限于该用户端的 Mac 地址及 / 或该用户端访问互联网的浏览器中设置的 Cookie。在本发明其他实施例，也还可以是所述安全网关在某个用户端通过用户身份验证访问互联网起开始计时，分析在第二预设时间内是否接收到该用户端发出的无线上网请求。

[0057] 在第二预设时间内接收到携带有已认证标识用户端的无线上网请求时，所述安全网关为所述接收到无线上网请求用户端的相关信息设置特定标识，以防止所述接收到无线

上网请求用户端的相关信息被删除。例如，在某个用户端通过用户身份验证访问互联网，结束互联网访问之时起开始计时，所述安全网关分析在第二预设时间内是否接收到该用户端发出的无线上网请求，在第二预设时间内接收到该用户端发出的无线上网请求时，将该用户端的相关信息设置特定标识，以防止该用户端的相关信息被删除，即为该用户端的相关信息设置一个不被删除的标识，默认将该用户端的相关信息永久保存（该用户端为常用用户端），或者，直至接收到删除该用户端的相关信息的指令时，才将该用户端的相关信息进行删除。所述标识可以是“0”或“1”等用以区分其他未再次发出无线上网请求终端的标识。

[0058] 在本实施例无线上网网关分析在第二预设时间内是否接收到携带有已认证标识用户端的无线上网请求；在第二预设时间内未接收到携带有已认证标识用户端的无线上网请求时，所述无线上网网关将所述未接收到无线上网请求用户端的相关信息进行删除。即，在第二预设时间内未接收到同一用户端发出的无线上网请求时，所述无线上网网关将保存的该用户端的相关信息进行删除，以节约安全网关的内存空间，进而提高安全网关的性能。

[0059] 如图 3 所示，为本发明无线上网的控制装置第一实施例的功能模块示意图。该装置包括：分析模块 10，控制模块 20 及提醒模块 30。

[0060] 所述分析模块 10，用于在接收到用户端发出的无线上网请求时，分析接收到的无线上网请求是否携带有已认证标识。

[0061] 在本实施例中，所述无线上网的方式优选为 Wifi 上网，用户端通过连接建立的 Wifi 热点实现访问互联网；Wifi 热点经安全网关与互联网服务器连接，安全网关起到对各个用户端的上网连接及上网内容进行控制及监控。各个用户端在通过安全网关的认证之后，可以访问互联网服务器的内容。所述无线上网的控制装置优选为安全网关。

[0062] 所述安全网关在接收到用户端发出的无线上网请求时，分析接收到的无线上网请求是否携带有已验证标识，所述已验证标识可以是用户端的 Mac 地址，及 / 或用户端访问互联网的浏览器中设置的 Cookie。

[0063] 所述控制模块 20，用于在接收到的无线上网请求携带有已认证标识时，授权所述用户端接入网络。

[0064] 在本实施例中，所述安全网关在接收到的无线上网请求携带有已认证标识时，授权所述用户端接入网络。例如，所述已验证标识为用户端的 Mac 地址，所述安全网关在接收到无线上网请求，获取无线上网请求包括的用户端的 Mac 地址，安全网关预存有各个已验证用户端的 Mac 地址，并分析是否有预存 Mac 地址与获取的用户端的 Mac 地址一致，在有预存 Mac 地址与获取的用户端的 Mac 地址一致时，确定接收到的无线上网请求携带有已认证标识，授权所述用户端接入网络，即，所述用户端用户可以进行无线上网访问互联网服务器上的内容。例如，所述已验证标识为用户端访问互联网的浏览器中设置的 Cookie，所述安全网关预存有各个用户端访问互联网的浏览器中设置的 Cookie，所述安全网关在接收到无线上网请求，获取无线上网请求包括的用户端访问互联网的浏览器中设置的 Cookie，并分析是否有预存 Cookie 与获取的用户端访问互联网的浏览器中设置的 Cookie 一致，在有预存 Cookie 与获取的用户端访问互联网的浏览器中设置的 Cookie 一致时，确定接收到的无线上网请求携带有已认证标识，授权所述用户端接入网络，即，用户端用户可以进行无线上网访问互联网服务器上的内容。

[0065] 在接收到的无线上网请求未携带有已认证标识时，所述安全网关提示用户输入手

机号码，并在接收到用户输入的手机号码时，向所述手机号码发送短信验证码；在接收到用户端发出的所述短信验证码时，所述安全网关授权所述用户端接入网络。例如，在没有预存Mac地址与获取的用户端的Mac地址一致，或者，在没有预存Cookie与获取的用户端访问互联网的浏览器中设置的Cookie一致时，确定接收到的无线上网请求未携带有已认证标识，通过短信验证的方式实现访问互联网服务器上的内容。

[0066] 所述提醒模块30，用于在未接收到用户端发出的所述短信验证码时，即，在一定时间后（例如，在需要短信验证的方式实现访问互联网服务器上的内容起开始计时，0秒、1秒或者1分钟后）未接收到用户端发出的所述短信验证码时，提示用户在第一预设时间内发出所述短信验证码，或者，提示用户重新获取短信验证码，以便及时通过发出上述短信验证码，通过用户身份认证，访问互联网。在成功通过安全网关的用户身份认证之后，所述安全网关将无线上网请求包括的用户端的Mac地址或者用户端访问互联网的浏览器中设置的Cookie进行预存，以在该用户端再次发出无线上网请求时，无需再次通过短信验证的方式实现访问互联网服务器上的内容。所述第一预设时间可以是30s或1分钟等时间间隔。

[0067] 在本实施例在接收到用户端发出的无线上网请求时，分析模块10分析接收到的无线上网请求是否携带有已认证标识；在接收到的无线上网请求携带有已认证标识时，控制模块20授权所述用户端接入网络。有效避免对用户端再次发出无线上网请求时，还需通过短信验证的方式实现访问互联网产生的短信费用的问题，实现快速、有效的完成用户身份验证，提高用户身份验证的效率，降低用户身份验证成本。

[0068] 如图4所示，为本发明无线上网的控制装置第二实施例的功能模块示意图。该装置还包括：处理模块40，

[0069] 所述分析模块10，用于分析在第二预设时间内是否接收到携带有已认证标识用户端的无线上网请求；

[0070] 所述处理模块40，用于在第二预设时间内未接收到携带有已认证标识用户端的无线上网请求时，将所述未接收到无线上网请求用户端的相关信息进行删除。

[0071] 在本实施例中，所述已认证标识以用户端的Mac地址为例，安全网关预存有所有通过用户身份验证用户端的Mac地址。在某个用户端通过用户身份验证访问互联网，结束互联网访问之时起开始计时，分析在第二预设时间内是否接收到该用户端发出的无线上网请求，在第二预设时间内未接收到该用户端发出的无线上网请求时，将存有的该用户端的相关信息进行删除。所述第二预设时间可以是30天或2个月等时间间隔；所述该用户端的相关信息包括但不限于该用户端的Mac地址及/或该用户端访问互联网的浏览器中设置的Cookie。在本发明其他实施例，也还可以是安全网关在某个用户端通过用户身份验证访问互联网起开始计时，分析在第二预设时间内是否接收到该用户端发出的无线上网请求。

[0072] 在第二预设时间内接收到携带有已认证标识用户端的无线上网请求时，所述安全网关为所述接收到无线上网请求用户端的相关信息设置特定标识，以防止所述接收到无线上网请求用户端的相关信息被删除。例如，在某个用户端通过用户身份验证访问互联网，结束互联网访问之时起开始计时，所述安全网关分析在第二预设时间内是否接收到该用户端发出的无线上网请求，在第二预设时间内接收到该用户端发出的无线上网请求时，为该用户端的相关信息设置特定标识，以防止该用户端的相关信息被删除，即为该用户端的相关信息设置一个不被删除的标识，默认将该用户端的相关信息永久保存（该用户端为常用用

户端)，或者，直至接收到删除该用户端的相关信息的指令时，才将该用户端的相关信息进行删除。所述标识可以是“0”或“1”等用以区分其他终端的标识。

[0073] 在本实施例分析模块 10 分析在第二预设时间内是否接收到携带有已认证标识用户端的无线上网请求；在第二预设时间内未接收到携带有已认证标识用户端的无线上网请求时，处理模块 40 将所述未接收到无线上网请求用户端的相关信息进行删除。即，在第二预设时间内未接收到同一用户端发出的无线上网请求时，安全网关将保存的该用户端的相关信息进行删除，以节约安全网关的内存空间，进而提高安全网关的性能。

[0074] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。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上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如 ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，或者网络设备等)执行本发明各个实施例所述的方法。

[0075] 以上所述仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

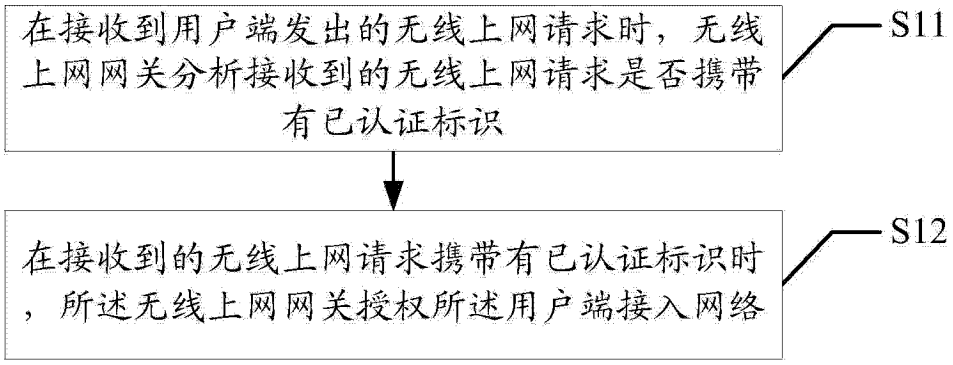

在接收到用户端发出的无线上网请求时，无线上网网关分析接收到的无线上网请求是否携带有已认证标识
S11
在接收到的无线上网请求携带有已认证标识时，所述无线上网网关授权所述用户端接入网络
S12

图 1

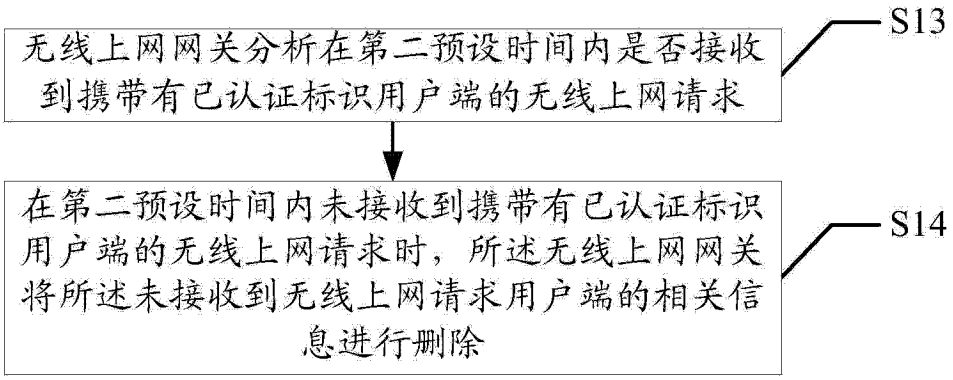

无线上网网关分析在第二预设时间内是否接收到携带有已认证标识用户端的无线上网请求
S13
在第二预设时间内未接收到携带有已认证标识用户端的无线上网请求时，所述无线上网网关将所述未接收到无线上网请求用户端的相关信息进行删除
S14

图 2

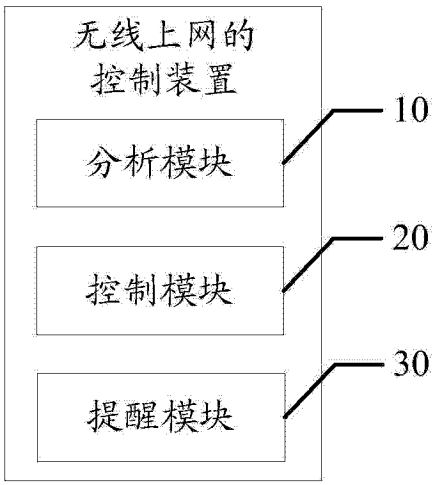

无线上网的控制装置
分析模块
10
控制模块
20
提醒模块
30

图 3

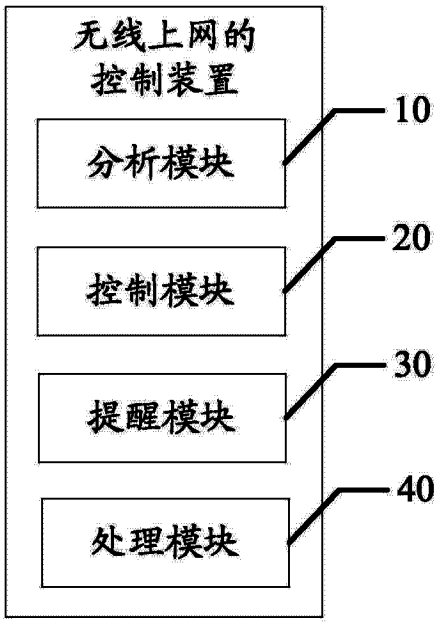

无线上网的控制装置
分析模块
10
控制模块
20
提醒模块
30
处理模块
40

图 4