(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 104468552 B
(45)授权公告日 2018.10.19

(21)申请号 201410712872.0

(22)申请日 2014.11.28

(65)同一申请的已公布的文献号
申请公布号 CN 104468552 A

(43)申请公布日 2015.03.25

(73)专利权人 迈普通信技术股份有限公司
地址 610041 四川省成都市高新技术开发区九兴大道16号

(72)发明人 陈睿 黄山

(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
代理人 申健

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/06(2009.01)

(56)对比文件
CN 102215597 A,2011.10.12,
CN 103313343 A,2013.09.18,

审查员 程杰

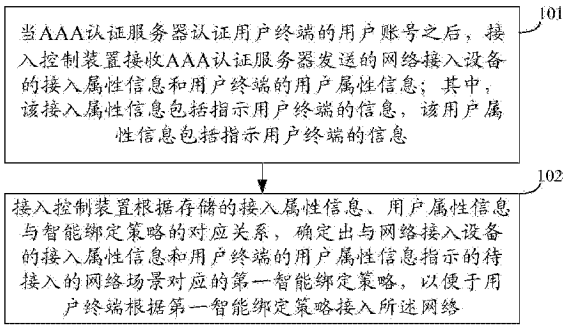
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种接入控制方法和装置

(57)摘要

本发明实施例提供一种接入控制方法和装置，涉及通信领域，能够在多种网络场景中实现接入控制，包括：当AAA认证服务器认证用户终端的用户账号之后，接入控制装置接收所述AAA认证服务器发送的网络接入设备的接入属性信息和用户终端的用户属性信息；其中，所述接入属性信息包括指示所述用户终端待接入的网络场景的信息，所述用户属性信息包括指示所述用户终端的信息；根据存储的接入属性信息、用户属性信息与智能绑定策略的对应关系，确定出与所述网络接入设备的接入属性信息和所述用户终端的用户属性信息指示的待接入的网络场景对应的第一智能绑定策略。本发明应用于网络接入。



CN 104468552 B

1.一种接入控制方法,其特征在于,包括:

当AAA认证服务器认证用户终端的用户账号之后,接入控制装置接收所述AAA认证服务器发送的网络接入设备的接入属性信息和用户终端的用户属性信息;其中,所述接入属性信息包括指示所述用户终端待接入的网络场景的信息,所述用户属性信息包括指示所述用户终端的信息;

根据存储的用户账号和用户组的对应关系,确定出所述用户账号对应的用户组;

根据存储的用户组、接入属性信息、用户属性信息与智能绑定策略的对应关系,确定出与所述用户账号对应的用户组、所述网络接入设备的接入属性信息和所述用户终端的用户属性信息指示的待接入的网络场景对应的第一智能绑定策略,以便于所述用户终端根据所述第一智能绑定策略接入所述网络。

2.根据权利要求1所述的方法,其特征在于,

所述第一智能绑定策略包括绑定实例阈值;

所述根据存储的接入属性信息、用户属性信息与智能绑定策略的对应关系,确定出与所述网络接入设备的接入属性信息和所述用户终端的用户属性信息指示的待接入的网络场景对应的第一智能绑定策略之后,所述方法包括:

统计所述第一智能绑定策略对应的当前绑定实例的数量;

若确定所述绑定实例的数量小于所述绑定实例阈值,则生成一个所述第一智能绑定策略对应的绑定实例。

3.根据权利要求1或2所述的方法,其特征在于,所述用户属性信息包括:所述用户账号和所述用户终端的属性,所述接入属性信息:包括所述网络接入设备的属性。

4.根据权利要求3所述的方法,其特征在于,对于第三代移动通信技术3G网络接入,所述网络接入设备的属性包括所述网络接入设备的介质访问控制MAC地址;所述用户终端的属性包括所述终端设备的系统标识和所述终端设备的系统MAC地址。

5.根据权利要求3所述的方法,其特征在于,对于有线网接入,所述网络接入设备的属性包括所述网络接入设备的MAC地址、所述网络接入设备的端口号;所述用户终端的属性包括用户终端的MAC地址、用户终端的网络之间互连的协议IP地址。

6.一种接入控制装置,其特征在于,包括:

接收单元,用于接收AAA认证服务器发送的网络接入设备的接入属性信息和用户终端的用户属性信息;其中,所述接入属性信息包括指示所述用户终端待接入的网络场景的信息,所述用户属性信息包括指示所述用户终端的信息;

确定单元,用于根据存储的用户账号和用户组的对应关系,确定出所述用户账号对应的用户组;以及根据存储的用户组、接入属性信息、用户属性信息与智能绑定策略的对应关系,确定出与所述用户账号对应的用户组、所述网络接入设备的接入属性信息和所述用户终端的用户属性信息指示的待接入的网络场景对应的第一智能绑定策略,以便于所述用户终端根据所述第一智能绑定策略接入所述网络。

7.根据权利要求6所述的装置,其特征在于,所述第一智能绑定策略包括绑定实例阈值,所述装置包括:

统计单元,用于统计所述第一智能绑定策略对应的当前绑定实例的数量;

生成单元,用于当确定所述绑定实例的数量小于所述绑定实例阈值时,生成一个所述

第一智能绑定策略对应的绑定实例。

8.根据权利要求6或7所述的装置，其特征在于，所述用户属性信息包括：所述用户账号和所述用户终端的属性，所述接入属性信息包括：所述网络接入设备的属性。

9.根据权利要求8所述的装置，其特征在于，对于3G网络接入，所述网络接入设备的属性包括所述网络接入设备的MAC地址；所述用户终端的属性包括所述终端设备的系统标识和所述终端设备的系统MAC地址。

10.根据权利要求8所述的装置，其特征在于，对于有线网接入，所述网络接入设备的属性包括所述网络接入设备的MAC地址、所述网络接入设备的端口号；所述用户终端的属性包括用户终端的MAC地址、用户终端的IP地址。

一种接入控制方法和装置

技术领域

[0001] 本发明涉及通信领域，尤其涉及一种接入控制方法和装置。

背景技术

[0002] 随着计算机及互联网技术的飞速发展，政府、银行、企业等单位都需要接入互联网进行办公及数据的共享，这样难免会吸引来自世界各地的各种人为攻击，例如信息泄露、信息窃取、数据篡改、数据删除、计算机病毒等。因此，网络的接入控制就显得尤为重要。

[0003] 现有的接入控制方法只针对无线终端WLAN(Wireless Local Area Networks，无线局域网络)接入。具体的，如图1所示，用户终端接入网络接入设备，用户终端向网络接入设备发送账号和密码，网络接入设备再向AAA(Authentication、Authorization、Accounting，验证、授权、记账)认证服务器发送账号和密码，AAA认证服务器对账号和密码进行认证，认证之后，绑定装置根据存储的WLAN的智能绑定策略接入WLAN网络。但是上述接入控制方法只针对WLAN网络，并不支持接入3G网络、有线接入网络等网络场景。

发明内容

[0004] 本发明的实施例提供一种接入控制方法和装置，能够在多种网络场景中实现接入控制。

[0005] 为达到上述目的，本发明的实施例采用如下技术方案：

[0006] 第一方面，提供一种接入控制方法，包括：

[0007] 当AAA认证服务器认证用户终端的用户账号之后，接入控制装置接收所述AAA认证服务器发送的网络接入设备的接入属性信息和用户终端的用户属性信息；其中，所述接入属性信息包括指示所述用户终端待接入的网络场景的信息，所述用户属性信息包括指示所述用户终端的信息；

[0008] 根据存储的接入属性信息、用户属性信息与智能绑定策略的对应关系，确定出与所述网络接入设备的接入属性信息和所述用户终端的用户属性信息指示的待接入的网络场景对应的第一智能绑定策略，以便于所述用户终端根据所述第一智能绑定策略接入所述网络。

[0009] 第二方面，提供一种接入控制装置，包括：

[0010] 接收单元，用于接收AAA认证服务器发送的网络接入设备的接入属性信息和用户终端的用户属性信息；其中，所述接入属性信息包括指示所述用户终端待接入的网络场景的信息，所述用户属性信息包括指示所述用户终端的信息；

[0011] 确定单元，用于根据存储的接入属性信息、用户属性信息与智能绑定策略的对应关系，确定出与所述网络接入设备的接入属性信息和所述用户终端的用户属性信息指示的待接入的网络场景对应的第一智能绑定策略，以便于所述用户终端根据所述第一智能绑定策略接入所述网络。

[0012] 相较于现有技术，本发明实提供的方法和装置不再只能够根据WLAN的设备属性信

息和WLAN对应的唯一的智能绑定策略接入WLAN，而是能够根据不同接入网络场景下的绑定属性信息，从针对多种网络场景的绑定策略中选择一种合适的待绑定智能绑定策略，从而使得用户终端可以接入该网络，不再只限制于一种WLAN网，还能在其他网络中进行如接入WLAN网的控制。

附图说明

[0013] 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一些实施例，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，还可以根据这些附图获得其他的附图。

[0014] 图1为一种网络接入系统的结构示意图；

[0015] 图2为本发明实施例提供的一种接入控制方法的流程图；

[0016] 图3为本发明实施例提供的另一种接入控制方法的流程图；

[0017] 图4为本发明实施例提供的一种接入控制装置的结构示意图；

[0018] 图5为本发明实施例提供的另一种接入控制装置的结构示意图。

具体实施方式

[0019] 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。

[0020] 为了满足国内政府部门、公安、军队、保密、金融、证券及科研院所等重要网络系统的网络安全需求。网络接入系统可以保护整个企业内部网络，包括可管理的(企业台式机、手提电脑、服务器)以及不可管理的(外部访客、合作伙伴、客户)终端。能够强制提升企业网络终端的安全，保证企业网络保护机制不被间断，配置正确无误，以及补丁拥有最新的时效性，使网络安全得到更有效提升。与此同时基于设备接入控制网关，还可以对于远程接入企业内部网络的计算机进行身份、唯一性及安全认证。

[0021] 实施例一

[0022] 本发明实施例提供一种接入控制方法，应用于网络接入系统，该网络接入系统可以包括AAA认证服务器、网络接入设备、用户终端和接入控制装置，如图2所示，可以包括：

[0023] 步骤101、当AAA认证服务器认证用户终端的用户账号之后，接入控制装置接收AAA认证服务器发送的网络接入设备的接入属性信息和用户终端的用户属性信息；其中，该接入属性信息包括指示用户终端待接入的网络场景的信息，该用户属性信息包括指示所述用户终端的信息。

[0024] 步骤102、接入控制装置根据存储的接入属性信息、用户属性信息与智能绑定策略的对应关系，确定出与网络接入设备的接入属性信息和用户终端的用户属性信息指示的待接入的网络场景对应的第一智能绑定策略，以便于用户终端根据第一智能绑定策略接入所述网络。

[0025] 相较于现有技术，本发明实提供的方法不再只能够根据WLAN的设备属性信息和

WLAN对应的唯一的智能绑定策略来接入WLAN，而是能够根据不同接入网络场景下的绑定属性信息，从针对多种网络场景的绑定策略中选择一种合适的待绑定智能绑定策略，从而使得用户终端可以接入该网络，不再只限制于一种WLAN网，还能在其他网络中进行如接入WLAN网的控制。

[0026] 进一步的，步骤102之后，所述方法还可以包括：接入控制装置统计第一智能绑定策略对应的当前绑定实例的数量；若确定绑定实例的数量小于绑定实例阈值，则生成一个第一智能绑定策略对应的绑定实例。

[0027] 进一步的，所述用户属性信息包括：所述用户账号和所述用户终端的属性，所述接入属性信息包括：所述网络接入设备的属性，步骤102具体可以包括：接入控制装置根据存储的账号和用户组的对应关系，确定出所述用户账号对应的用户组；根据存储的用户组、属性与智能绑定策略的对应关系，确定出与所述用户账号对应的用户组、所述用户终端的属性和所述网络接入设备的属性对应的所述待绑定智能绑定策略。

[0028] 进一步的，对于3G(3rd-Generation，第三代移动通信技术)网络接入，所述网络接入设备的属性包括所述网络接入设备的MAC(Media Access Control，介质访问控制)地址；所述用户终端的属性包括所述终端设备的系统标识和所述终端设备的系统MAC地址。

[0029] 进一步的，对于有线网接入，所述网络接入设备的属性包括所述网络接入设备的MAC地址、所述网络接入设备的端口号；所述用户终端的属性包括用户终端的MAC地址、用户终端的IP(Internet Protocol，网络之间互连的协议)地址。

[0030] 实施例二

[0031] 本发明实施例提供一种接入控制方法，假设应用于银行的网络接入系统，该银行的网络接入系统可以包括AAA认证服务器、网络接入设备、用户终端和接入控制装置。本发明以手机接入3G网为例，该方法可以包括：

[0032] 步骤201、手机根据用户选的网络向网络接入设备发送访问请求，该请求包括手机的用户属性、用户账号和用户密码。

[0033] 用户可以根据实际情况选择有线网、3G、4G(4th-Generation，第四代移动通信技术)、WLAN等等。当用户使用有线连接的台式电脑时，用户可以选择有线网，当用户使用手机时，用户可以根据当前无线网情况选择WLAN、3G或4G。访问请求包括用户终端的用户属性，例如，终端设备的系统标识、终端设备的系统MAC地址。系统标识用于指示当前的系统，可以是手机Android(安卓)系统、手机塞班系统、手机苹果系统、手机Windows系统等等。此处的用户账号和用户密码可以是用户手动输入的，也可以是自动保存的。

[0034] 步骤202、网络接入设备向AAA认证服务器通过RADIUS(Remote Authentication Dial In User Service，远程用户拨号认证服务)协议发送手机的用户属性、用户账号和用户密码。

[0035] 步骤203、AAA认证服务器判断用户账号和用户密码进行匹配。若是，则执行步骤204；若否，则执行步骤210。

[0036] 具体的，AAA认证服务器判断该用户账号是否是已保存的账号，若否，则执行210；若是，则根据已保存的账号和密码的对应关系，获取与该用户账号对应的密码，判断用户密码和对应的密码是否相同。若相同，则执行步骤204，若不同，则执行步骤210。

[0037] 步骤204、AAA认证服务器向接入控制装置发送属性信息，该属性信息包括手机的

用户属性、用户账号和用户密码、网络接入设备的接入属性。

[0038] 用户绑定该接入属性可以包括网络接入设备的MAC地址，该MAC地址表示该网络接入设备所在网络是3G网络，该属性信息是实施例一中的接入属性信息和用户属性信息的总称。

[0039] 步骤205、接入控制装置根据存储的账号和用户组的对应关系，确定出用户账号对应的用户组。

[0040] 具体的，银行的用户组可以分为企业用户组、个人用户组和管理员用户组。接入控制装置可以预先将账号按照用户组分类，保存账号和用户组的对应关系。用户组的分类是根据不同用户的操作权利进行分配的。例如，个人用户组的用户只能进行小额金额交易，企业用户组可以进行大额金额交易，管理组能够对各个用户进行管理，同样不具有交易的权利等等。因此即使只针对不同的用户组的不同操作，智能绑定策略也是有差别的(具体可以如表1)。

[0041] 步骤206、接入控制装置根据用户组、属性与智能绑定策略的对应关系，确定出与用户账号对应的用户组、手机的属性和网络接入设备的属性对应的待绑定智能绑定策略。

[0042] 表1显示了3G网络中属性信息与智能绑定策略的对应关系。可以看出个人用户组的用户可以使用手机3G接入，但企业用户组和企业用户组禁止手机3G接入，但可以通过笔记本3G接入，因此，本发明实施例提供的智能绑定策略是根据实际情况人为设计的，在此就不多做介绍了。假设用户组是个人用户组，根据表1中用户属性和接入属性就可以确定出待绑定策略(实施例一中的第一智能绑定策略)是3G策略1。

[0043] 表1

[0044]

用户组	用户属性	接入属性	智能绑定策略
个人用户组	手机的系统标识；手机的系统MAC地址	网络接入设备的MAC地址	3G策略1
企业用户组	手机的系统标识；手机的系统MAC地址	网络接入设备的MAC地址	禁止策略
管理员组	手机的系统标识；手机的系统MAC地址	网络接入设备的MAC地址	禁止策略
个人用户组	笔记本的系统标识；笔记本的系统MAC地址	网络接入设备的MAC地址	3G策略1
企业用户组	笔记本的系统标识；笔记本的系统MAC地址	网络接入设备的MAC地址	3G策略2
管理员组	笔记本的系统标识；笔记本的系统MAC地址	网络接入设备的MAC地址	3G策略3

[0045] 智能绑定策略可以配置一个或多个手机(用户终端)及接入设备属性绑定规则，包括：指定属性绑定值、不限属性绑定值、绑定实例阈值中的一个或多个。本实施例以绑定实例阈值为规则。

[0046] 步骤207、接入控制装置统计已存在的待绑定策略对应的绑定实例的数量。

[0047] 该待绑定策略可以对应多个绑定实例，不同的绑定实例可以针对不同的用户。

[0048] 步骤208、接入控制装置判断已存在的绑定实例的数量是否小于预设的实例阈值。若是，则执行步骤209；若否，则执行步骤210。

[0049] 步骤209、当已存在的绑定实例的数量小于预设的实例阈值时，接入控制装置生成一个待绑定策略对应的实例，使得手机可以接入银行的网络。

[0050] 步骤210、当已存在的绑定实例的数量大于或等于预设的实例阈值时，接入控制装置拒绝手机接入。

[0051] 相较于现有技术，本发明实提提供的方法和装置不再只能够根据WLAN的设备属性信息和WLAN对应的唯一的智能绑定策略来接入WLAN，而是能够根据不同接入网络场景下的绑定属性信息，从针对多种网络场景的绑定策略中选择一种合适的待绑定智能绑定策略，从而使得用户终端可以接入该网络，不再只限制于一种WLAN网，还能在其他网络中进行如接入WLAN网的控制。

[0052] 实施例三

[0053] 本发明实施例提供一种接入控制装置30，包括：

[0054] 接收单元301，用于接收AAA认证服务器发送的网络接入设备的接入属性信息和用户终端的用户属性信息；其中，所述接入属性信息包括指示所述用户终端待接入的网络场景的信息，所述用户属性信息包括指示所述用户终端的信息。

[0055] 确定单元302，用于根据存储的接入属性信息、用户属性信息与智能绑定策略的对应关系，确定出与所述网络接入设备的接入属性信息和所述用户终端的用户属性信息指示的待接入的网络场景对应的第一智能绑定策略，以便于所述用户终端根据所述第一智能绑定策略接入所述网络。

[0056] 相较于现有技术，本发明实提供的装置不再只能够根据WLAN的设备属性信息和WLAN对应的唯一的智能绑定策略接入WLAN，而是能够根据不同接入网络场景下的绑定属性信息，从针对多种网络场景的绑定策略中选择一种合适的待绑定智能绑定策略，从而使得用户终端可以接入该网络，不再只限制于一种WLAN网，还能在其他网络中进行如接入WLAN网的控制。

[0057] 所述待绑定智能绑定策略包括绑定实例阈值，所述装置30包括：

[0058] 统计单元303，用于统计所述第一智能绑定策略对应的当前绑定实例的数量。

[0059] 判断单元304，用于判断所述待绑定智能绑定策略对应的绑定实例的数量是否小于所述绑定实例阈值；

[0060] 生成单元305，用于当确定所述绑定实例的数量小于所述绑定实例阈值时，生成一个所述第一智能绑定策略对应的绑定实例。

[0061] 进一步的，所述用户属性信息包括：用户账号和所述用户终端的属性，所述接入属性信息包括：网络接入设备的属性，所述确定单元302具体用于：

[0062] 根据存储的账号和用户组的对应关系，确定出所述用户账号对应的用户组；

[0063] 根据存储的用户组、属性与智能绑定策略的对应关系，确定出与所述用户账号对应的用户组、所述用户终端的属性和所述网络接入设备的属性对应的所述待绑定智能绑定策略。

[0064] 进一步的，对于3G网络接入，所述网络接入设备的属性包括所述网络接入设备的MAC地址；所述用户终端的属性包括所述终端设备的系统标识和所述终端设备的系统MAC地址。

[0065] 进一步的，对于有线网接入，所述网络接入设备的属性包括所述网络接入设备的MAC地址、所述网络接入设备的端口号；所述用户终端的属性包括用户终端的MAC地址、用户终端的IP地址。

[0066] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0067] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

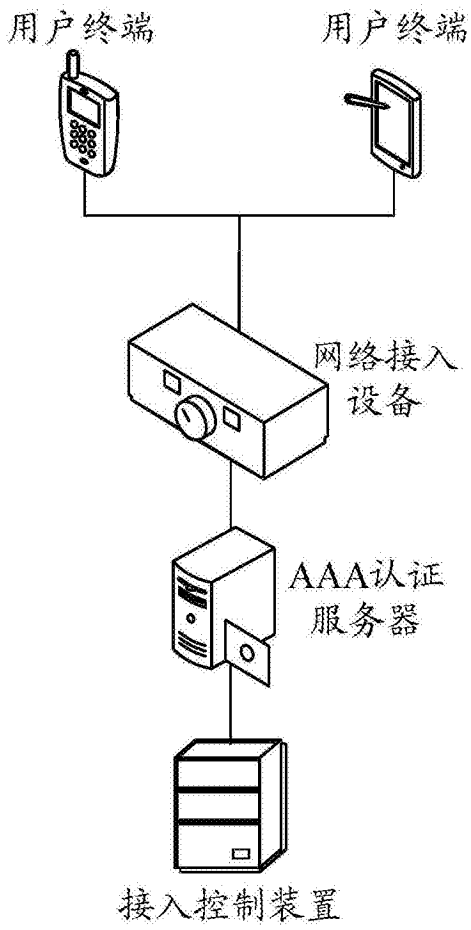

用户终端
用户终端
网络接入设备
AAA认证服务器
接入控制装置

图1

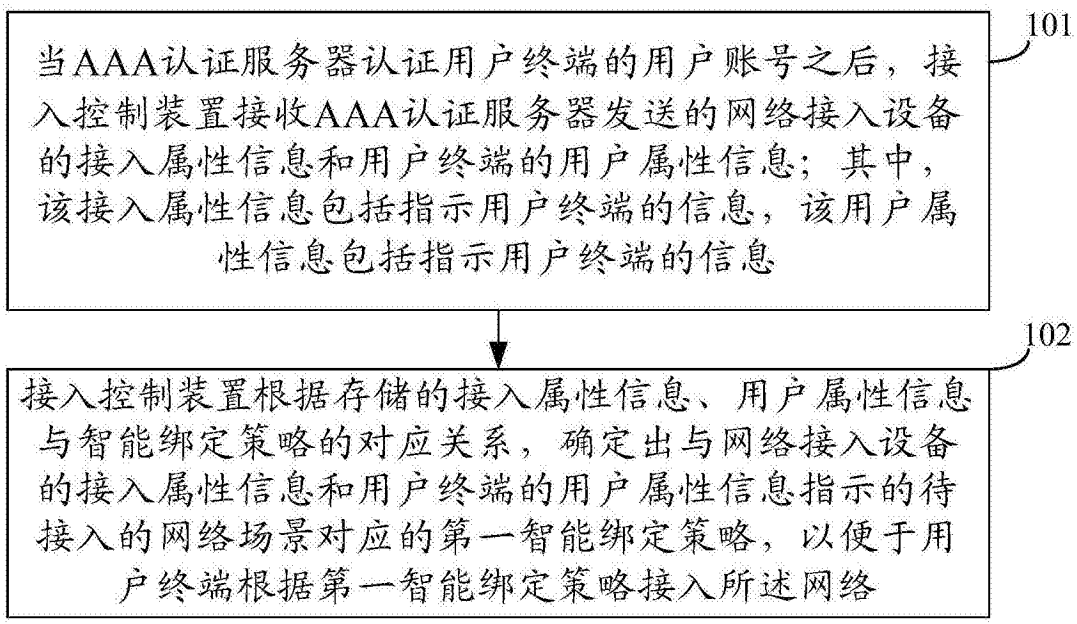

101
当AAA认证服务器认证用户终端的用户账号之后，接入控制装置接收AAA认证服务器发送的网络接入设备的接入属性信息和用户终端的用户属性信息；其中，该接入属性信息包括指示用户终端的信息，该用户属性信息包括指示用户终端的信息
102
接入控制装置根据存储的接入属性信息、用户属性信息与智能绑定策略的对应关系，确定出与网络接入设备的接入属性信息和用户终端的用户属性信息指示的待接入的网络场景对应的第一智能绑定策略，以便于用户终端根据第一智能绑定策略接入所述网络

图2

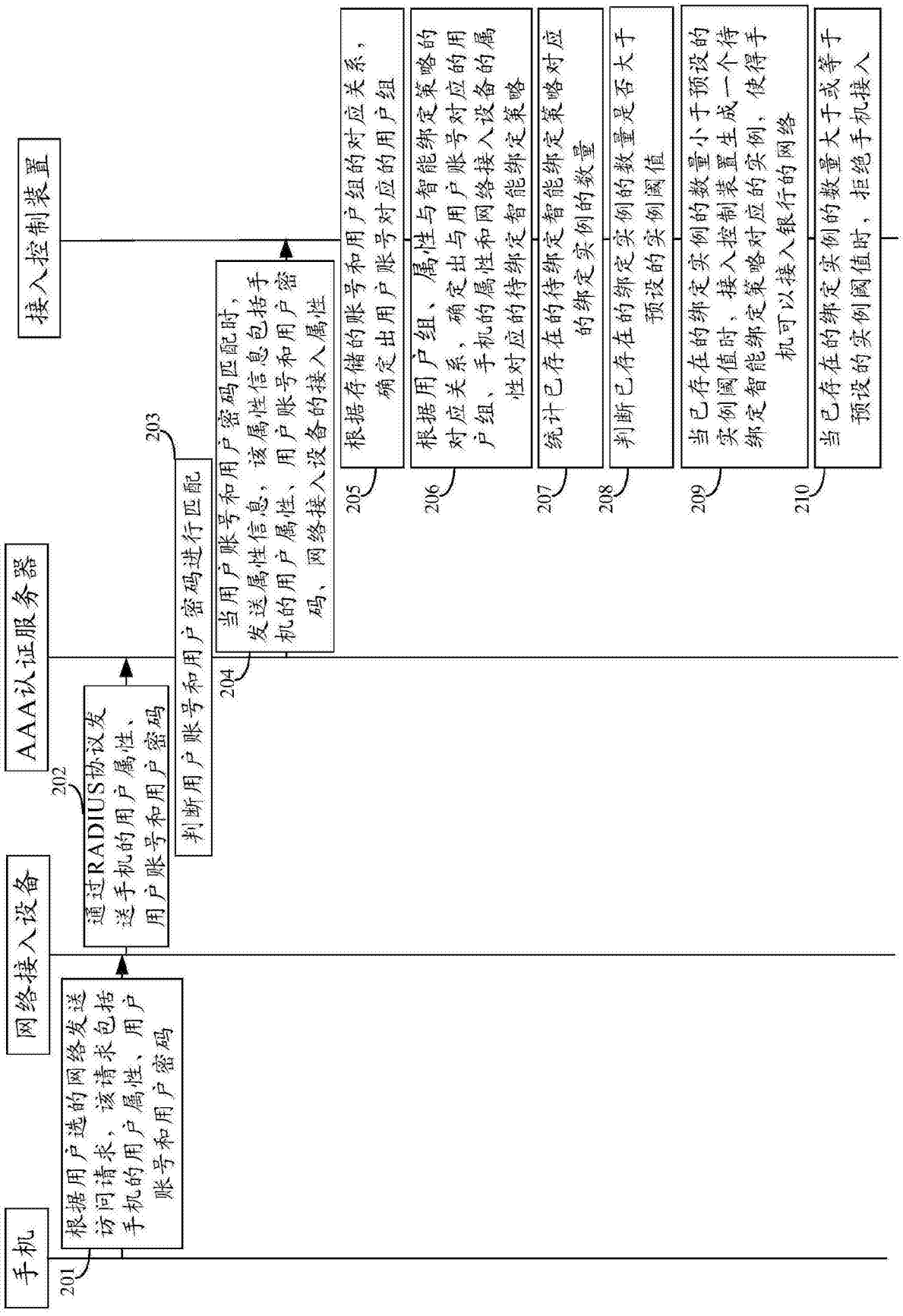

手机
网络接入设备
AAA认证服务器
接入控制装置
201
根据用户选的网络发送访问请求，该请求包括手机的用户属性、用户账号和用户密码
202
通过RADIUS协议发送手机的用户属性、用户账号和用户密码
203
判断用户账号和用户密码进行匹配
204
当用户账号和用户密码匹配时，发送属性信息，该属性信息包括手机的用户属性、用户账号和用户密码、网络接入设备的接入属性
205
根据存储的账号和用户组的对应关系，确定出用户账号对应的用户组
206
根据用户组、属性与智能绑定策略的对应关系，确定出与用户账号对应的用户组、手机的属性和网络接入设备的属性对应的待绑定智能绑定策略
207
统计已存在的待绑定智能绑定策略对应的绑定实例的数量
208
判断已存在的绑定实例的数量是否大于预设的实例阈值
209
当已存在的绑定实例的数量小于预设的实例阈值时，接入控制装置生成一个待绑定智能绑定策略对应的实例，使得手机可以接入银行的网络
210
当已存在的绑定实例的数量大于或等于预设的实例阈值时，拒绝手机接入

图3

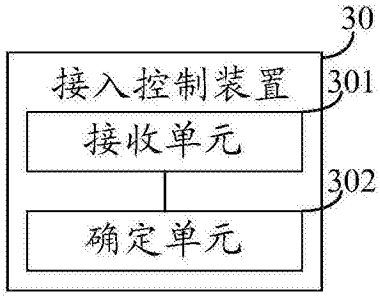

30
接入控制装置
301
接收单元
302
确定单元

图4

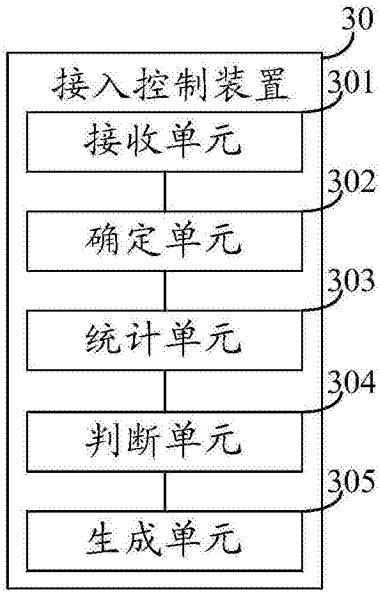

30
接入控制装置
301
接收单元
302
确定单元
303
统计单元
304
判断单元
305
生成单元

图5