



(12) 发明专利

(10) 授权公告号 CN 110784872 B

(45) 授权公告日 2021. 08. 10

(21) 申请号 201911046793.X

(22) 申请日 2019.10.30

(65) 同一申请的已公布的文献号
申请公布号 CN 110784872 A

(43) 申请公布日 2020.02.11

(73) 专利权人 华南理工大学
地址 510640 广东省广州市天河区五山路
381号

(72) 发明人 陆以勤 王君君 覃健诚 程喆

(74) 专利代理机构 广州粤高专利商标代理有限公司 44102

代理人 何淑珍 陈伟斌

(51) Int.Cl.

H04W 12/06 (2021.01)

H04W 36/08 (2009.01)

(56) 对比文件

孙延鹏.《基于Flash P2P的物流监控视频传输协议及应用研究》.《中国优秀硕士学位论文全文数据库》.2019,

殷攀.《基于 WiFi 的超密集软件定义网络的设计与实现》.《中国优秀硕士学位论文全文数据库》.2019,

Janfizza Bukhari.《Multicasting in Next-Generation Software-Defined》.《IEEE》.2018,

审查员 黄素真

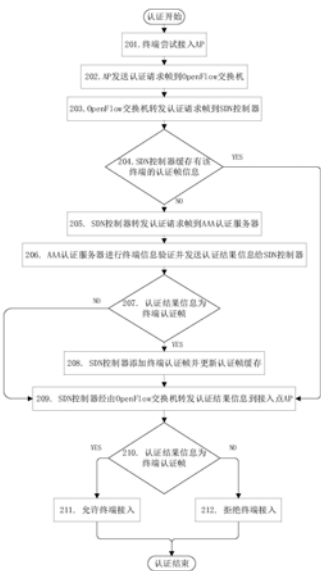
权利要求书2页 说明书7页 附图2页

(54) 发明名称

基于SDN的校园网WLAN漫游接入认证系统及方法

(57) 摘要

本发明公开了基于SDN的校园网WLAN漫游接入认证系统及方法,该系统包括接入和数据转发装置和控制认证装置,接入和数据转发装置包括:接入点AP、OpenFlow交换机、无线接入网关;控制认证装置包括SDN控制器、AAA认证服务器。所述方法包括终端的认证请求帧发送给OpenFlow交换机,所述交换机转发到SDN控制器进行认证,若SDN控制器认证失败,则SDN控制器与AAA认证服务器进行交互,把认证请求帧转发给AAA认证服务器进行认证,并把认证结果信息经由SDN控制器和OpenFlow服务器转发给接入点AP。本发明的认证接入方式缩短漫游接入的时间,提高漫游服务质量。



1. 基于SDN的校园网WLAN漫游接入认证系统,其特征在于,该系统包括接入和数据转发装置和控制认证装置,接入和数据转发装置包括接入点AP(无线访问接入点, WirelessAccessPoint)、OpenFlow交换机、无线接入网关;控制认证装置包括SDN控制器、AAA认证服务器;

OpenFlow交换机用于将认证结果帧发送到SDN控制器,并转发数据到无线接入网关;

无线接入网关用于接受来自OpenFlow交换机发来的数据,由无线接入网关接入Internet;

接入点AP与终端连接,并把终端的认证请求帧发送给OpenFlow交换机,由OpenFlow交换机把认证请求帧转发到SDN 控制器进行认证,若认证成功,则允许终端接入;若认证不成功,则SDN控制器与AAA认证服务器进行交互,把认证请求帧给AAA认证服务器进行认证,并把认证结果信息经由SDN控制器和OpenFlow服务器转发给接入点AP,若认证成功则允许终端接入,若认证不成功,则拒绝终端接入;

控制认证装置的工作过程具体为:当SDN控制器收到来自OpenFlow交换机转发的认证请求帧时,提取其中的终端信息,并将该终端信息与本地缓存的认证帧进行认证匹配,若认证匹配即认证成功,则直接发送终端认证帧到OpenFlow交换机,由OpenFlow交换机把终端认证帧转发给接入点AP,接入点AP允许终端接入,若认证匹配不成功,SDN控制器与AAA认证服务器进行交互,把认证请求帧转发给AAA认证服务器,AAA认证服务器对认证请求帧认证,认证通过后把终端认证帧发送到SDN控制器,再经由OpenFlow交换机转发到接入点AP,接入点AP对终端进行接入,同时SDN控制器把该终端认证帧更新到认证帧缓存中,若AAA认证服务器对认证请求帧认证不成功,则AAA认证服务器将拒绝接入的信息发送到SDN控制器再经由OpenFlow交换机转发到接入点AP,接入点AP拒绝该终端接入。

2. 根据权利要求1所述的认证系统,其特征在于,若认证成功时,接入点AP与终端的通信采用802.1x认证的方式接入。

3. 根据权利要求1所述的认证系统,其特征在于,所述AAA认证服务器利用802.1X认证方式对终端进行认证。

4. 根据权利要求1所述的认证系统,其特征在于,所述SDN控制器能够缓存认证帧。

5. 根据权利要求1所述的认证系统,其特征在于,所述的接入和数据转发装置,其工作过程具体为:终端发送的请求探测帧给接入点AP,接入点AP发送探测回复帧给终端,之后终端发送网络信息请求帧给接入点AP请求网络信息,接入点AP发送对应的网络信息回复帧回复终端,接着由终端发送连接请求帧给接入点AP请求与接入点AP建立连接,接入点AP回复连接回复帧与终端建立连接,最后终端发送认证请求帧给接入点AP进行认证请求,接入点AP将认证请求帧发送到OpenFlow交换机,由OpenFlow交换机把认证请求帧转发到SDN 控制器,接入点AP根据收到来自OpenFlow交换机的认证结果信息,若认证成功则允许终端接入,若认证不成功,则拒绝终端接入。

6. 用于权利要求1所述的基于SDN的校园网WLAN漫游接入认证系统,其特征在于,若SDN控制器中没有缓存该终端的终端认证帧,则SDN控制器与AAA认证服务器进行一次交互,SDN控制器把终端认证请求帧转发给AAA认证服务器,由AAA认证服务器对认证请求帧认证,把认证结果发送到SDN控制器再经由OpenFlow交换机转发到接入点AP对终端进行接入,同时SDN控制器把该终端的认证帧更新到认证帧缓存中。

7. 用于权利要求1所述的基于SDN的校园网WLAN漫游接入认证系统的认证方法,其特征在于,包括以下步骤:

步骤1、终端发送的请求探测帧给接入点AP;

步骤2、接入点AP发送探测回复帧给终端;

步骤3、终端发送网络信息请求帧给接入点AP请求网络信息;

步骤4、接入点AP发送对应的网络信息回复帧给终端进行回复;

步骤5、终端发送连接请求帧请求与接入点AP建立连接;

步骤6、接入点AP发送连接回复帧与终端建立连接;

步骤7、终端发送认证请求帧给接入点AP进行认证请求,接入点AP将认证请求帧发送到OpenFlow交换机,OpenFlow交换机转发认证请求帧到SDN控制器;

步骤8、若SDN控制器缓存有该终端认证帧,则转到步骤12,否则接着步骤9;

步骤9、SDN 控制器将认证请求帧转发给AAA 服务器进行认证;

步骤10、若AAA服务器认证通过,则发送终端认证帧给SDN 控制器,反之发送认证失败信息给SDN控制器;SDN 控制器下发认证失败信息给OpenFlow交换机;

步骤11、若SDN 控制器收到是终端认证帧,则将该终端认证帧更新到认证帧缓存中;

步骤12、SDN 控制器下发终端认证帧信息给OpenFlow交换机;

步骤13、OpenFlow将来自SDN控制器的认证结果下发到对应接入点AP上;

步骤14、当接入点AP收到来自OpenFlow转发的认证信息时,若收到的是终端认证帧,则允许终端接入,若是认证失败信息,则拒绝终端接入。

基于SDN的校园网WLAN漫游接入认证系统及方法

技术领域

[0001] 本发明涉及校园网WLAN漫游接入认证技术,特别涉及基于SDN的校园网WLAN漫游接入认证系统及方法。

背景技术

[0002] 随着移动智能终端设备的飞速发展,用户使用移动智能设备终端越来越广泛,无线网络接入已经成为互联网接入的最广泛的接入标准。如今,基于IEEE802.11标准的无线局域网(Wireless Local Area Network,WLAN)的部署也随处可见。移动终端要想接入WLAN连接互联网得首先完成接入认证,接入认证在WLAN中占据着重要的地位,WLAN接入认证的基本原理是:网络管理服务端维护着注册用户的基本信息,基本信息包括:用户账户,用户密码,用户年龄,用户性别等。当用户发起请求接入WLAN时,由网络管理服务端对请求用户进行身份信息认证,认证一般包括对用户账户,用户密码的认证,认证通过时,用户就可以接入WLAN进行上网,否则用户则被拒绝接入WLAN,这种认证方式适合于用户初始化认证,安全性较高,然而对于短时间,比如几个小时内,移动终端在一个接入点AP完成了初始化认证后,在短时间内移动(漫游)到了另外一个接入点AP的覆盖范围内,这时用户又要手动输入信息完成和初始化认证流程一样的认证,影响了用户短期内的上网体验,给用户带来了不便。传统的WLAN漫游接入认证方法认证时延较长并不具备全网视图,缺乏灵活性。

[0003] 随着软件定义网络(Software Defined Networking,SDN)的面世,如何将网络变得灵活可控成为人们关注的焦点。SDN采用集中式控制与分布式转发思想,实现控制平面全局优化及高性能的网络转发能力,具有全局的网络视图,可以实时掌握网络运行情况,有益于管理整个网络。鉴于SDN的优势,人们将SDN控制与转发分离的思想引入到WLAN中,用以解决WLAN存在的问题。由此,软件定义无线网络(Software Defined Wireless Networks,SDWN)应运而生。SDWN继承了SDN的网络集中控制、网络可编程及虚拟化,灵活性强等优点,为解决传统WLAN中的很多问题提供了新的思路。

[0004] 传统WLAN的认证技术根据认证层次分为链路级认证和网络级认证,在校园网,企业网等中小型网络中普遍采用的是网络级认证方式,对于WLAN漫游过程中接入WLAN目前常见的认证方式包括:1、MAC地址认证;2、Portal认证;3、802.1X认证;简单介绍如下:

[0005] 现有技术一:MAC地址认证。

[0006] 原理:在WLAN网络环境中,MAC地址认证是通过由认证端维护一份注册用户的MAC地址名单,用户请求接入WLAN网时,由认证端对用户的MAC地址进行认证,只有在认证通过后,用户才能接入WLAN网。

[0007] 缺点:由于MAC地址只对用户的MAC地址进行验证,虽然认证时间短,认证流程简单,但是认证的安全性低。

[0008] 现有技术二:Portal认证

[0009] 原理:在WLAN网络环境中,当用户试图申请接入WLAN时,用户端会收到来自Portal认证服务器上提供的WEB认证页面,当用户输入信息,提交WEB页面后,Portal认证服务器获

取到用户信息,并将该数据与后台数据库进行匹配,如果匹配成功则认证成功,匹配失败则认证失败,所以Portal认证也叫做WEB认证。

[0010] 缺点:虽然Portal认证技术提高了验证接入的安全性,但是认证过程相比较MAC地址认证来说比较复杂,认证时延长,并且当用户从WLAN中一个组网移动到另一个组网时,用户需要重新认证信息,认证麻烦。

[0011] 现有技术三:802.1X认证

[0012] 原理:802.1X是通过一系列的连接和认证协议来和ADIUS服务器完成对接入的终端进行认证,其中最重要中的标准是EAP,严格来说它并非一种协议,而是终端和认证服务器之间交互信息所使用的标准,在802.1X认证中必然会使用到EAP,因为基于802.1X的认证系统在终端和认证系统之间需要使用EAPOL格式封装的EAP数据包传送认证信息。

[0013] 缺点:利用802.1X进行漫游认证时,认证时延长,不能满足实时语音,视频业务的需求,且对于漫游过程中可能会导致漫游后接入点的流量拥塞,漫游接入不够灵活。

[0014] 综上所述,现有的传统校园网WLAN漫游接入认证技术要么安全性较低,要么安全性提高了但是认证时延长。

发明内容

[0015] 针对现有的传统校园网WLAN漫游接入认证技术要么安全性较低,要么安全性提高了但是认证时延长等问题,本发明提供基于SDN的校园网WLAN漫游接入认证系统及方法,该系统利用SDN网络的灵活性,通过在SDN控制器上的认证信息缓存功能,来完成用户的漫游切换认证。

[0016] 本发明至少通过如下技术方案之一实现。

[0017] 基于SDN的校园网WLAN漫游接入认证系统,该系统包括接入和数据转发装置和控制认证装置,接入和数据转发装置包括接入点AP(无线访问接入点,WirelessAccessPoint)、OpenFlow交换机、无线接入网关;控制认证装置包括SDN控制器、AAA认证服务器;

[0018] OpenFlow交换机用于将认证请求帧发送的SDN控制器,并转发数据到无线接入网关;

[0019] 无线接入网关用于接受来自OpenFlow交换机发来的数据,由无线接入网关接入Internet;

[0020] 接入点AP与终端的连接,并把终端的认证请求帧发送给OpenFlow交换机,由OpenFlow交换机把认证请求帧转发到SDN控制器进行认证,若认证成功,则允许终端接入;若认证不成功,则SDN控制器与AAA认证服务器进行交互,把认证请求帧给AAA认证服务器进行认证,并把认证结果信息经由SDN控制器和OpenFlow服务器转发给接入点AP,若认证成功则允许终端接入,若认证不成功,则拒绝终端接入。

[0021] 在终端已经接入网络而后从一个接入点漫游到另一个接入点时,通过的SDN控制器认证信息缓存可以不经由AAA认证服务器从而快速对漫游终端进行认证,从而缩短漫游接入的时间,提高漫游服务质量。

[0022] 进一步的,当终端请求接入点AP时,接入点AP与终端的通信采用802.1x认证方式中的接入。终端成功接入点AP后,由OpenFlow交换机转发数据包到无线接入网关访问互联

网资源。

[0023] 进一步的,若认证成功时,接入点AP与终端的通信采用802.1x认证的方式接入。

[0024] 进一步的,所述AAA认证服务器利用802.1X认证方式对终端进行认证。

[0025] 进一步的,所述SDN控制器能够缓存认证帧。

[0026] 进一步的,所述的接入和数据转发装置,其工作过程具体为:所述的接入和数据转发装置,其工作过程具体为:终端发送的Probe Request帧(请求探测帧)给接入点AP,接入点AP发送Probe Response帧(探测回复帧)给终端,之后终端发送GAS Request帧(网络信息请求帧)给接入点AP请求网络信息,接入点AP发送对应的GAS Response帧(网络信息回复帧)回复终端,接着由终端发送Association Request帧(连接请求帧)给接入点AP请求与接入点AP建立连接,接入点AP回复Association Response帧(连接回复帧)与终端建立连接,最后终端发送认证请求帧给接入点AP进行认证请求,接入点AP将认证请求帧发送到OpenFlow交换机,由OpenFlow交换机把认证请求帧转发到SDN控制器,接入点AP根据收到来自OpenFlow交换机的认证结果信息,若认证成功则允许终端接入,若认证不成功,则拒绝终端接入。

[0027] 进一步的,控制认证装置的工作过程具体为:当SDN控制器收到来自OpenFlow交换机转发的认证请求帧时,提取其中的终端信息,并将该终端信息与本地的认证帧缓存进行认证匹配,若认证匹配即认证成功,则直接发送终端认证帧到OpenFlow交换机,由OpenFlow交换机把终端认证帧转发给接入点AP,接入点AP允许终端接入,若认证匹配不成功,SDN控制器与AAA认证服务器进行交互,把认证请求帧转发给AAA认证服务器,AAA认证服务器对认证请求帧认证,认证通过后把终端认证帧发送到SDN控制器,再经由OpenFlow交换机转发到接入点AP,接入点AP对终端进行接入,同时SDN控制器把该终端认证帧更新到认证帧缓存中,若AAA认证服务器对认证请求帧认证不成功,则AAA认证服务器将拒绝接入的信息发送到SDN控制器再经由OpenFlow交换机转发到接入点AP,接入点AP拒绝该终端接入。

[0028] 进一步的,若SDN控制器中没有缓存该终端的终端认证帧,则SDN控制器与AAA认证服务器进行一次交互,SDN控制器把终端认证请求帧转发给AAA认证服务器,当AAA认证服务器对认证请求帧认证,把认证结果发送到SDN控制器再经由OpenFlow交换机转发到接入点AP对终端进行接入,同时SDN控制器把该终端的认证帧更新到认证帧缓存中。

[0029] 在终端已经接入网络而后发生漫游时,由于SDN控制器中有认证帧缓存功能,SDN控制器认证帧缓存可以不经由AAA认证服务器从而快速对漫游终端进行认证,这种认证接入方式相比现有WLAN漫游接入方式具有更快的接入速度,从而缩短漫游接入的时间,提高漫游服务质量,从而解决上述问题。

[0030] 在SDN控制器中含有信息缓存函数,从而SDN控制器能够缓存认证帧。

[0031] 本发明中,SDN控制器每次接收到认证请求帧后,将认证请求帧与认证帧缓存信息进行对比,对比成功后直接,SDN控制器将认证成功的结果信息发送给OpenFlow交换机,接着由OpenFlow交换机转发给接入点AP,若对比失败,则SDN控制发送认证请求帧给AAA认证服务器进行认证,SDN控制接收来自AAA服务器的认证结果信息,若认证结果信息为认证通过的终端认证帧,SDN控制把终端认证帧存入认证帧缓存中,最后同时SDN控制器把认证结果信息发送给OpenFlow交换机,接着由OpenFlow交换机转发给接入点AP。

[0032] 用于所述的基于SDN的校园网WLAN漫游接入认证系统的认证方法,包括以下步骤:

- [0033] 步骤1、终端发送的Probe Request帧(请求探测帧)给接入点AP;
- [0034] 步骤2、接入点AP发送Probe Response帧(探测回复帧)给终端;
- [0035] 步骤3、终端发送GAS Request帧(网络信息请求帧)给接入点AP请求网络信息;
- [0036] 步骤4、接入点AP发送对应的GAS Response帧(网络信息回复帧)给终端进行回复;
- [0037] 步骤5、终端发送Association Request帧(连接请求帧)请求与接入点AP建立连接;
- [0038] 步骤6、接入点AP回复Association Response帧(连接回复帧)与终端建立连接;
- [0039] 步骤7、终端发送认证请求帧给接入点AP进行认证请求,接入点AP将认证请求帧发送到OpenFlow交换机,OpenFlow交换机转发认证请求帧到SDN控制器;
- [0040] 步骤8、若SDN控制器缓存有该终端认证帧,则转到步骤12,否则接着步骤9;
- [0041] 步骤9、SDN控制器将认证请求帧转发给AAA服务器进行认证;
- [0042] 步骤10、若AAA服务器认证通过,则发送终端认证帧给SDN控制器,反之发送认证失败信息给SDN控制器;
- [0043] 步骤11、若SDN控制器收到是终端认证帧,则将该终端认证帧更新到认证帧缓存中;
- [0044] 步骤12、SDN控制器下发终端认证帧或认证失败信息给OpenFlow交换机;
- [0045] 步骤13、OpenFlow将来自SDN控制器的认证结果下发到对应接入点AP上;
- [0046] 步骤14、当接入点AP收到来自OpenFlow转发的认证信息时,若收到的是终端认证帧,则允许终端接入,若是认证失败信息,则拒绝终端接入。
- [0047] 与现有的技术相比,本发明的有益效果为:该系统利用SDN网络的灵活性,通过在SDN控制器上的认证帧缓存功能,来完成用户的漫游切换认证。在该系统中,当SDN控制器的认证帧缓存中缓存有该接入终端的终端认证帧时,SDN控制器直接下发该终端的终端认证帧给OpenFlow交换机,再转发到接入点AP对终端进行接入。在终端已经接入网络而后发生漫游时,通过开发的SDN控制器认证信息缓存可以不经由AAA认证服务器从而快速对漫游终端进行认证,这种认证接入方式相比现有WLAN漫游接入方式具有更快的接入速度,从而缩短漫游接入的时间,提高漫游服务质量,本发明解决了WLAN漫游中时延较长的问题,与现有的WLAN漫游接入认证技术相比具有认证时延短的优点。

附图说明

- [0048] 图1为本实施例提供的基于SDN的校园网WLAN漫游接入认证系统结构示意图;
- [0049] 图2为本实施例提供的基于SDN的校园网WLAN漫游接入认证方法的认证流程图。

具体实施方式

- [0050] 下面结合附图和具体实施例对发明做出进一步说明,需指出的是,以下若有未特别说明之过程或符号如代码等,均是本领域技术人员可参照现有技术理解或实现的。
- [0051] 如图1所示的基于SDN的校园网WLAN漫游接入认证系统,该系统包括接入和数据转发装置、控制认证装置,接入和数据转发装置包括:接入点AP(无线访问接入点, WirelessAccessPoint)、OpenFlow交换机、无线接入网关;控制认证装置包括:SDN控制器、AAA认证服务器;

- [0052] 所述接入点AP用于终端接入并发送终端的认证请求帧给OpenFlow交换机；
- [0053] OpenFlow交换机用于将认证请求帧发送的SDN控制器，并转发数据到无线接入网关；
- [0054] SDN控制器通过认证帧缓存直接下发终端认证帧给漫游接入点AP实现终端的快速漫游接入认证；所述SDN控制器有认证帧缓存功能。
- [0055] AAA认证服务器利用传统的802.1X认证方式来对终端进行初始化认证，并将认证结果信息发送给SDN控制器；
- [0056] 无线接入网关用于接受来自OpenFlow交换机发来的数据，由无线接入网关接入Internet。
- [0057] 接入点AP与终端的连接，并把终端的认证请求帧发送给OpenFlow交换机，由OpenFlow交换机把认证请求帧转发到SDN控制器进行认证，若认证成功，则允许终端接入；若认证不成功，则SDN控制器与AAA认证服务器进行交互，把认证请求帧给AAA认证服务器进行认证，并把认证结果信息经由SDN控制器和OpenFlow服务器转发给接入点AP，若认证成功则允许终端接入，若认证不成功，则拒绝终端接入。若认证成功时，接入点AP与终端的通信采用802.1x认证方式接入。
- [0058] 所述AAA认证服务器利用802.1X认证方式对终端进行认证。
- [0059] 所述的接入和数据转发装置，其工作过程具体为：终端发送的Probe Request帧（请求探测帧）给接入点AP，接入点AP发送Probe Response帧（探测回复帧）给终端，之后终端发送GAS Request帧（网络信息请求帧）给接入点AP请求网络信息，接入点AP发送对应的GAS Response帧（网络信息回复帧）回复终端，接着由终端发送Association Request帧（连接请求帧）给接入点AP请求与接入点AP建立连接，接入点AP回复Association Response帧（连接回复帧）与终端建立连接，最后终端发送认证请求帧给接入点AP进行认证请求，接入点AP将认证请求帧发送到OpenFlow交换机，由OpenFlow交换机把认证请求帧转发到SDN控制器，接入点AP根据收到来自OpenFlow交换机的认证结果信息，若认证成功则允许终端接入，若认证不成功，则拒绝终端接入。
- [0060] 控制认证装置的工作过程具体为：当SDN控制器收到来自OpenFlow交换机转发的认证请求帧时，提取其中的终端信息，并将该终端信息与本地的认证帧缓存进行认证匹配，若认证匹配即认证成功，则直接发送终端认证帧到OpenFlow交换机，由OpenFlow交换机把终端认证帧转发给接入点AP，接入点AP允许终端接入，若认证匹配不成功，SDN控制器与AAA认证服务器进行交互，把认证请求帧转发给AAA认证服务器，AAA认证服务器对认证请求帧认证，认证通过后把终端认证帧发送到SDN控制器，再经由OpenFlow交换机转发到接入点AP，接入点AP对终端进行接入，同时SDN控制器把该终端认证帧更新到认证帧缓存中，若AAA认证服务器对认证请求帧认证不成功，则AAA认证服务器将拒绝接入的信息发送到SDN控制器再经由OpenFlow交换机转发到接入点AP，接入点AP拒绝该终端接入。
- [0061] 通过选取主流的SDN控制器OpenDaylight来作为控制器，并在其中开发信息缓存函数来保存认证帧缓存，具体如下（仅作为举例）：


```
public class AuthenticationMessageCache {
    private static Map<String, String> AuthenticationCacheMap = new HashMap<String, String>();
    public static synchronized void addAuthenticationMessage(String userInformation, String
[0062] authenticationMessage) {
        if (AuthenticationCacheMap.isEmpty() || !AuthenticationCacheMap.containsKey(userInformation)) {
            AuthenticationCacheMap.put(userInformation, authenticationMessage);
        }
    }
    public static synchronized String getAuthenticationMessgae(String userInformation) {
        if (AuthenticationCacheMap.isEmpty() || !AuthenticationCacheMap.containsKey(userInformation)) {
            return "";
        } else {
            String message = AuthenticationCacheMap.get(userInformation);
[0063] return message;
        }
    }
}
```

[0064] 其中,一个名为AuthenticationMessageCache的类来对认证帧进行存储和获取,其中名为AuthenticationCacheMap的成员属性用来作为认证帧的缓存空间介质;函数addAuthenticationMessage用来添加终端信息和相对应的认证帧,该函数第一个参数userInformation表示终端信息,第二个参数authenticationMessage表示对应的认证帧,在添加终端信息和相对应的认证帧时调用函数方式为:AuthenticationMessageCache.addAuthenticationMessage(终端信息,认证帧);函数getAuthenticationMessgae用来根据终端信息获取对应的认证帧,其中参数参数userInformation表示终端信息,根据终端信息获取对应的认证帧调用函数方式为:String认证帧信息=AuthenticationMessageCache.getAuthenticationMessgae(终端信息)。

[0065] 在图1中终端4从扩展集1漫游到扩展集2的过程中,由扩展集2的漫游接入点AP发送终端4的认证请求帧到OpenFlow交换机再转发到SDN控制中,由于终端4在漫游之前已经接入过无线网络,所以SDN控制器认证帧缓存里面存有终端4的终端认证帧,由SDN控制器直接下发终端4的终端认证帧到OpenFlow交换机,再转发给扩展集2的漫游接入点AP,允许终端4接入漫游接入点AP,从而终端4从扩展集1漫游到扩展集2。所述扩展集1和扩展集2分别包括若干个终端。

[0066] 如图2所示,用于所述的基于SDN的校园网WLAN漫游接入认证系统的认证方法,包括以下步骤:

[0067] 步骤201、终端尝试接入AP并发送认证请求帧进行认证请求;

[0068] 步骤202、接入点AP将认证请求帧发送到OpenFlow交换机;

[0069] 步骤203、OpenFlow交换机转发认证请求帧到SDN控制器;

[0070] 步骤204、若SDN控制器缓存有该终端认证帧,转到步骤209,否则接着步骤205;

[0071] 步骤205、SDN控制器将认证请求帧转发给AAA服务器进行认证;

[0072] 步骤206、若AAA服务器认证通过,则发送终端认证帧给SDN控制器,反之发送认证

失败信息给SDN控制器；

[0073] 步骤207、若SDN控制器收到的是终端认证帧，则转步骤208，否则进行步骤步骤209；

[0074] 步骤208、SDN控制器将该终端认证帧更新到认证帧缓存中；

[0075] 步骤209、SDN控制器下发终端认证帧或认证失败信息给OpenFlow交换机；

[0076] 步骤210、OpenFlow将来自SDN控制器的认证结果信息下发到对应接入点AP上；

[0077] 步骤211、当AP收到来自OpenFlow转发的认证结果信息时，若收到的是终端认证帧，则允许终端接入，结束认证流程，否则转步骤212；

[0078] 步骤212、拒绝终端接入，结束认证流程。

[0079] 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本发明可必需的硬件平台的方式来实现。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。

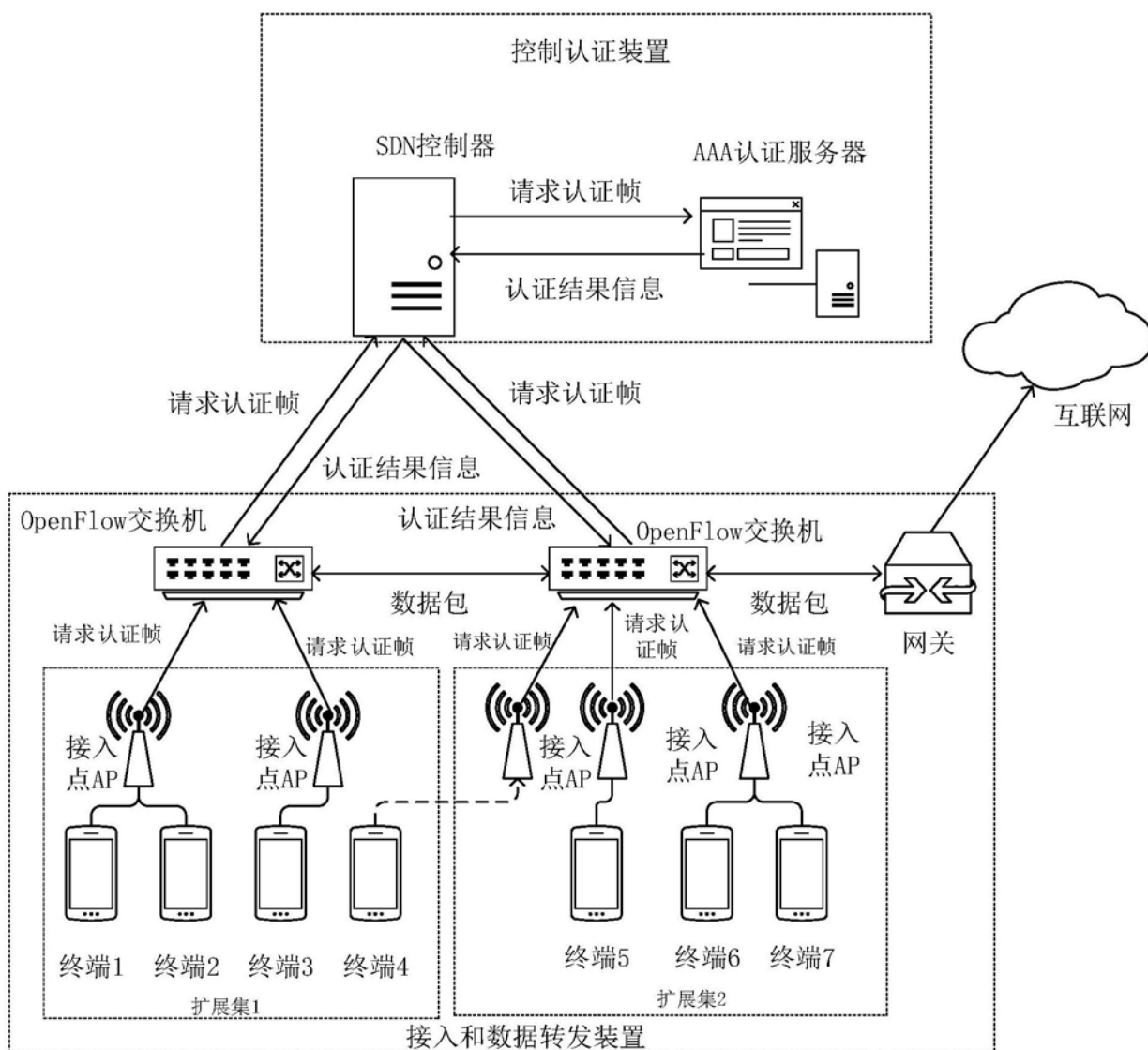


图1

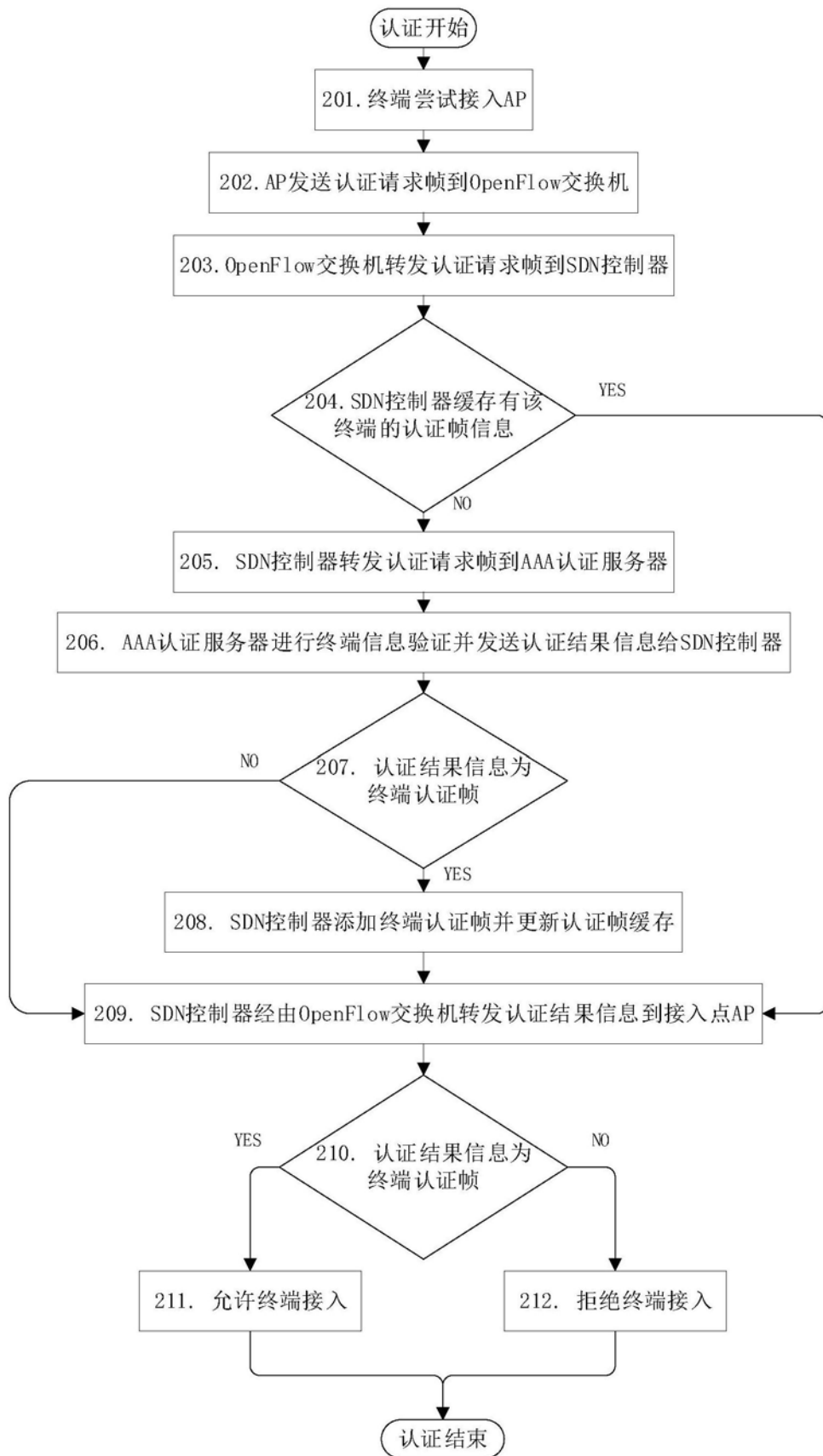


图2