



(12) 发明专利

(10) 授权公告号 CN 103491540 B

(45) 授权公告日 2016. 05. 25

(21) 申请号 201310429993. X

US 2003056096 A1, 2003. 03. 20,

(22) 申请日 2013. 09. 18

CN 103002442 A, 2013. 03. 27,

(73) 专利权人 东北大学

CN 1564626 A, 2005. 01. 12,

地址 110819 辽宁省沈阳市和平区文化路 3 号巷 11 号

高天寒等. 节点证书与身份相结合的 HMIPv6 网络接入认证机制. 《软件学报》. 2012, 第 23 卷 (第 9 期), 全文.

(72) 发明人 高天寒

审查员 霍远征

(74) 专利代理机构 沈阳东大知识产权代理有限公司 21109

代理人 梁焱

(51) Int. Cl.

H04W 12/06(2009. 01)

H04W 12/08(2009. 01)

(56) 对比文件

CN 1697370 A, 2005. 11. 16,

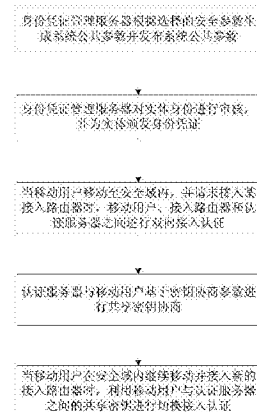
权利要求书4页 说明书14页 附图7页

(54) 发明名称

一种基于身份凭证的无线局域网双向接入认证系统及方法

(57) 摘要

一种基于身份凭证的无线局域网双向接入认证系统及方法属于无线网络安全领域,该系统包括接入路由器,设置在安全域内,还包括身份凭证管理服务器和认证服务器;身份凭证管理服务器用于对安全域内实体的身份凭证进行管理,包括颁发身份凭证和维护身份凭证;认证服务器用于验证移动用户的接入认证申请并完成与移动用户间的共享密钥协商;接入路由器用于根据认证服务器返回的验证结果控制移动用户是否接入无线局域网,同时接入路由器接收和转发移动用户与认证服务器间的认证消息。本发明在一个自治安全域内,既能实现移动用户与访问网络间的双向接入认证和密钥协商,又支持移动用户于不同接入路由器间切换时的高效接入认证,提高了接入认证效率。



1. 一种基于身份凭证的无线局域网双向接入认证方法,采用基于身份凭证的无线局域网双向接入认证系统,包括设置在安全域内的接入路由器、身份凭证管理服务器和认证服务器;

所述身份凭证管理服务器用于对安全域内实体的身份凭证进行管理,包括颁发身份凭证和维护身份凭证;所述身份凭证包括颁发者身份、颁发者公钥、用户身份、用户公钥、用户身份证书和身份凭证有效期;所述安全域内实体包括:移动用户和接入路由器;

所述认证服务器用于验证移动用户的接入认证申请并完成与移动用户间的共享密钥协商;

所述接入路由器用于根据认证服务器返回的验证结果控制移动用户是否接入无线局域网,同时接入路由器接收和转发移动用户与认证服务器间的认证消息;

其特征在于:该方法包括以下步骤:

步骤1:身份凭证管理服务器根据选择的安全参数生成系统公共参数并发布系统公共参数;

所述系统公共参数包括循环群 G_1 和循环群 G_2 、双线性对 e 、循环群 G_1 上的基点 P 和 G ,字符集至循环群 G_1 的单向哈希函数 H_1 ,循环群 G_2 至 Z_q^* 的单向哈希函数 H_2 ; Z_q^* 为1到 $q-1$ 范围的正整数, q 为身份凭证管理服务器选择的安全参数,身份凭证管理服务器的公钥;

步骤2:身份凭证管理服务器对实体身份进行审核,并为实体颁发身份凭证;

步骤2.1:在实体申请身份凭证前,基于系统公共参数生成实体的公钥私钥对,其中,实体的私钥 $SK_{EN} \in Z_q^*$,由实体随机选择,实体的公钥 $PK_{EN} = SK_{EN} \cdot P$,即循环群 G_1 上的基点 P 与实体的私钥 SK_{EN} 的乘积;

步骤2.2:实体向身份凭证管理服务器发送身份信息和实体的公钥,向身份凭证管理服务器申请身份凭证;

所述身份信息为网络地址标识符;

步骤2.3:身份凭证管理服务器在接收到实体的身份凭证申请后,验证该实体身份信息的合法性,如果身份信息合法,则生成身份凭证颁发给该实体,否则不向该实体颁发身份凭证;

所述身份凭证包括颁发者身份、颁发者公钥、用户身份、用户公钥、用户身份证书和身份凭证有效期,其中,用户身份证书由基于证书签名算法CBS生成;

步骤2.4:实体接收到身份凭证后,使用实体的私钥和身份凭证内的实体身份证书生成实体的签名密钥;

步骤3:当移动用户移动至安全域内,并请求接入某接入路由器时,移动用户、接入路由器和认证服务器之间进行双向接入认证;

步骤3.1:移动用户向接入路由器发送身份凭证出示消息,接入路由器将该消息转发至认证服务器;

步骤3.1.1:移动用户发送路由器请求消息以寻找当前所在安全域内的接入路由器;

步骤3.1.2:接入路由器收到移动用户发送的路由器请求消息后进行接入认证;

步骤3.1.3:接入路由器向移动用户发送路由器应答消息,请求移动用户的身份凭证;

步骤3.1.4:移动用户发送身份凭证出示消息给接入路由器,该消息包含移动用户的身

份凭证、当前时间戳、移动用户密钥协商参数及基于移动用户的签名密钥使用CBS算法对身份凭证出示消息的CBS签名结果；

所述移动用户密钥协商参数即移动用户的公钥与随机数的乘积；

步骤3.1.5:接入路由器接收到移动用户的身份凭证出示消息后,将该消息转发至认证服务器；

步骤3.2:认证服务器接收到移动用户的身份凭证出示消息后,对移动用户的身份凭证进行验证:若验证成功,则执行步骤3.3;若验证失败,则拒绝移动用户接入,并将验证失败消息发送给接入路由器；

步骤3.2.1:验证移动用户的身份凭证出示消息中的时间戳的新鲜性以防止重放攻击:如果时间戳新鲜,则认证服务器验证身份凭证的有效期,执行步骤3.2.2,否则验证失败,拒绝移动用户接入,将验证失败消息发送给接入路由器；

步骤3.2.2:如果身份凭证处于有效期内,则认证服务器对身份凭证出示消息的CBS签名结果进行验证,执行步骤3.2.3,如果身份凭证过期,将验证失败消息发送给接入路由器；

步骤3.2.3:认证服务器根据身份凭证中的颁发者公钥和用户公钥对身份凭证出示消息的CBS签名结果进行验证:如果验证通过,则认证服务器确认移动用户为合法接入用户;如果验证失败,则拒绝移动用户接入,将验证失败消息发送给接入路由器；

步骤3.3:认证服务器将对移动用户身份凭证验证成功消息发送给移动用户；

步骤3.3.1:认证服务器发送验证成功消息给接入路由器,此消息包含认证服务器密钥协商参数；

所述认证服务器密钥协商参数即认证服务器的公钥与随机数的乘积；

步骤3.3.2:接入路由器接收到认证服务器发送的验证成功消息后,在消息中插入接入路由器的身份凭证和当前时间戳；

步骤3.3.3:接入路由器基于接入路由器的签名密钥使用CBS算法对验证成功消息进行CBS签名,接入路由器将验证成功消息和对验证成功消息的CBS签名结果发送给移动用户；

步骤3.4:移动用户接收到接入路由器的验证成功消息后,对接入路由器的身份凭证进行验证:若验证成功,接入当前接入路由器,完成双向接入认证;若验证失败,则拒绝接入当前接入路由器；

步骤4:认证服务器与移动用户基于密钥协商参数进行共享密钥协商；

步骤4.1:认证服务器基于移动用户密钥协商参数计算认证服务器与移动用户间的共享密钥；

步骤4.2:移动用户基于认证服务器密钥协商参数计算移动用户与认证服务器间的共享密钥；

步骤5:当移动用户在安全域内继续移动并接入新的接入路由器时,利用移动用户与认证服务器之间的共享密钥进行切换接入认证；

步骤5.1:当移动用户在安全域内继续移动并接入新的接入路由器时,移动用户向接入路由器发送身份凭证出示消息,接入路由器将该消息转发至认证服务器；

步骤5.1.1:移动用户发送路由器请求消息以寻找当前所在安全域内的接入路由器；

步骤5.1.2:接入路由器收到移动用户发送的路由器请求消息后进行接入认证；

步骤5.1.3:接入路由器向移动用户发送路由器应答消息,请求移动用户的身份凭证；

步骤5.1.4:移动用户发送身份凭证出示消息给接入路由器,该消息包含移动用户的身份凭证、当前时间戳和基于该移动用户与认证服务器所协商的共享密钥使用HMAC算法对身份凭证出示消息的HMAC认证结果;

步骤5.1.5:接入路由器接收到移动用户的身份凭证出示消息后,将该消息转发至认证服务器;

步骤5.2:认证服务器接收到移动用户的身份凭证出示消息后,对移动用户的身份凭证进行验证:若验证成功,则执行步骤5.3;若验证失败,则拒绝移动用户接入,并将验证失败消息发送给接入路由器;

步骤5.3:认证服务器将对移动用户的身份凭证验证成功消息发送给移动用户;

步骤5.3.1:认证服务器发送验证成功消息给接入路由器,此消息包含认证服务器通过接入路由器公钥对共享密钥的加密结果;

步骤5.3.2:接入路由器接收到认证服务器发送的验证成功消息后,利用接入路由器私钥对共享密钥进行解密,提取出共享密钥;

步骤5.3.3:接入路由器在验证成功消息中插入接入路由器的身份凭证和当前时间戳,接入路由器利用共享密钥使用HMAC算法对验证成功消息进行HMAC认证,接入路由器将验证成功消息和对验证成功消息的HMAC认证结果发送给移动用户;

步骤5.4:移动用户利用其与认证服务器协商的共享密钥验证接入路由器的合法性,若接入路由器合法,则移动用户切换接入该合法接入路由器,完成切换接入认证;若接入路由器不合法,则移动用户拒绝接入该接入路由器。

2.根据权利要求1所述的基于身份凭证的无线局域网双向接入认证方法,其特征在于:所述步骤3.4移动用户接收到接入路由器的验证成功消息后,对接入路由器的身份凭证进行验证,具体步骤如下:

步骤3.4.1:移动用户验证接收到的验证成功消息中的时间戳新鲜性,以防止重放攻击:如果时间戳新鲜,则验证接入路由器身份凭证的有效期,执行步骤3.4.2;否则验证失败,拒绝接入当前接入路由器;

步骤3.4.2:如果身份凭证处于有效期内,则移动用户对验证成功消息的CBS签名结果进行验证,执行步骤3.4.3;如果身份凭证过期,则拒绝接入当前接入路由器;

步骤3.4.3:移动用户根据身份凭证中的颁发者公钥和用户公钥对验证成功消息的CBS签名结果进行验证:如果验证通过,则移动用户确认接入该合法接入路由器,完成双向接入认证;若验证失败,则移动用户拒绝接入当前接入路由器。

3.根据权利要求1所述的基于身份凭证的无线局域网双向接入认证方法,其特征在于:所述步骤4.1认证服务器基于移动用户密钥协商参数计算认证服务器与移动用户间的共享密钥,具体步骤如下:

步骤4.1.1:认证服务器以移动用户密钥协商参数和循环群G1上的基点G与认证服务器私钥的乘积为输入,利用双线性对e计算认证服务器共享密钥值;

步骤4.1.2:认证服务器以认证服务器共享密钥值为输入,利用单向哈希函数H2计算其与移动用户的共享密钥。

4.根据权利要求1所述的基于身份凭证的无线局域网双向接入认证方法,其特征在于:所述步骤4.2移动用户基于认证服务器密钥协商参数计算移动用户与认证服务器间的共享

密钥,具体步骤如下:

步骤4.2.1:移动用户以认证服务器密钥协商参数和循环群G1上基点G与移动用户私钥的乘积为输入,利用双线性对e计算移动用户共享密钥值;

步骤4.2.2:移动用户以移动用户共享密钥值为输入,利用单向哈希函数H2计算其与认证服务器的共享密钥。

5.根据权利要求1所述的基于身份凭证的无线局域网双向接入认证方法,其特征在于:所述步骤5.2认证服务器接收到移动用户的身份凭证出示消息后,对移动用户的身份凭证进行验证,具体步骤如下:

步骤5.2.1:验证移动用户的身份凭证出示消息中时间戳的新鲜性以防止重放攻击:如果时间戳新鲜,则认证服务器验证身份凭证的有效期,执行步骤5.2.2,否则验证失败,拒绝移动用户接入,将验证失败消息发送给接入路由器;

步骤5.2.2:如果身份凭证处于有效期内,则认证服务器对身份凭证出示消息的HMAC认证结果进行验证,执行步骤5.2.3,如果身份凭证过期,将验证失败消息发送给接入路由器;

步骤5.2.3:认证服务器根据其与移动用户协商的共享密钥对身份凭证出示消息的HMAC认证结果进行验证:如果验证通过,则认证服务器确认移动用户为合法接入用户;如果验证失败,则拒绝移动用户接入,将验证失败消息发送给接入路由器。

6.根据权利要求1所述的基于身份凭证的无线局域网双向接入认证方法,其特征在于:所述步骤5.4移动用户利用其与认证服务器协商的共享密钥验证接入路由器的合法性,具体步骤如下:

步骤5.4.1:移动用户验证接收到的验证成功消息中的时间戳新鲜性,以防止重放攻击:如果时间戳新鲜,则验证接入路由器身份凭证的有效期,执行步骤5.4.2;否则验证失败,拒绝接入当前接入路由器;

步骤5.4.2:如果身份凭证处于有效期内,则移动用户对验证成功消息的HMAC认证结果进行验证,执行步骤5.4.3;如果身份凭证过期,拒绝接入当前接入路由器;

步骤5.4.3:移动用户根据其与认证服务器协商的共享密钥对验证成功消息的HMAC认证结果进行验证:如果验证通过,则移动用户确认接入该合法接入路由器,完成切换接入认证;若验证失败,则移动用户拒绝接入当前接入路由器。

一种基于身份凭证的无线局域网双向接入认证系统及方法

技术领域

[0001] 本发明属于无线网络安全领域,特别涉及一种基于身份凭证的无线局域网双向接入认证系统及方法。

背景技术

[0002] 随着计算机网络和移动通信技术的飞速发展,大量移动设备涌现,人们对无处不在的泛在网络接入需求越发迫切。作为Internet的扩展和延伸,IEEE802.11无线局域网(Wireless Local Area Network,WLAN)以其部署灵活、异构兼容、低成本、带宽丰富等优势成为“最后一公里”接入领域的最佳解决方案。

[0003] 然而随着WLAN的广泛部署,其安全性问题开始凸现。下一代无线通信系统要求WLAN能够在开放性环境中为用户提供高效安全的接入服务,接入安全是确保WLAN安全的关键。当移动用户接入WLAN时,访问网络需要认证移动用户的身份以防止其对网络资源的非法使用,另一方面移动用户需认证访问网络从而获得可靠的接入服务。访问网络和移动用户间的双向认证是实现WLAN安全接入的基础。

[0004] 现有的针对WLAN安全接入的解决方案主要包括:基于802.11i框架的集中式接入认证方法、基于PKI体系的分布式接入认证方法和基于身份密码体制的接入认证方法。(1)在基于802.11i的集中式认证方法中,当移动用户接入访问网络时,首先向接入路由器提出认证请求,接入路由器中转认证请求至中心认证服务器,由中心认证服务器认证移动用户身份并完成移动用户与接入路由器间的密钥协商。集中式认证模式需要认证实体同远程中心认证服务器进行大量消息交互,降低了接入认证效率。(2)在基于PKI的分布式接入认证方法中,数字证书权威(Certificate Authority,CA)分别为移动用户和接入路由器颁发X.509数字证书,当移动用户接入WLAN时,移动用户与接入路由器交换并验证对方数字证书从而实现本地双向接入认证。然而移动用户和接入路由器对数字证书的管理和维护代价限制了相关方案的实用性。(3)基于身份密码体制(IBC)近年兴起并开始被应用到WLAN接入认证领域,以身份作为实体公钥能够减轻PKI体系下的数字证书管理和维护代价。移动用户和接入路由器可以通过验证对方的基于身份的签名实现双向接入认证。但实体的私钥由私钥生成中心(Private Key Generator,PKG)分配,导致密钥托管和密钥传输等一系列安全问题产生,使得此类方案仅局限于小范围可信网络内应用。

[0005] 可见上述WLAN安全机制在认证消息交互延迟、数字证书维护代价和适用性等方面存在缺陷,更为重要的是当移动用户在访问网络的不同接入路由器间切换时,完整的接入认证过程需重新执行,进一步降低了接入认证效率。

发明内容

[0006] 针对现有技术存在的不足,本发明提供一种基于身份凭证的无线局域网双向接入认证系统及方法。

[0007] 本发明的技术方案是:

[0008] 一种基于身份凭证的无线局域网双向接入认证系统,包括接入路由器,设置在安全域内,还包括身份凭证管理服务器和认证服务器;

[0009] 所述身份凭证管理服务器用于对安全域内实体的身份凭证进行管理,包括颁发身份凭证和维护身份凭证;所述身份凭证包括颁发者身份、颁发者公钥、用户身份、用户公钥、用户身份证书和身份凭证有效期;所述安全域内实体包括:移动用户和接入路由器;

[0010] 所述认证服务器用于验证移动用户的接入认证申请并完成与移动用户间的共享密钥协商;

[0011] 所述接入路由器用于根据认证服务器返回的验证结果控制移动用户是否接入无线局域网,同时接入路由器接收和转发移动用户与认证服务器间的认证消息。

[0012] 采用所述的基于身份凭证的无线局域网双向接入认证系统进行无线局域网双向接入认证的方法,包括以下步骤:

[0013] 步骤1:身份凭证管理服务器根据选择的安全参数生成系统公共参数并发布系统公共参数;

[0014] 所述系统公共参数包括循环群 G_1 和循环群 G_2 、双线性对 e 、循环群 G_1 上的基点 P 和 G ,字符集至循环群 G_1 的单向哈希函数 H_1 ,循环群 G_2 至 Z_q^* 的单向哈希函数 H_2 ; Z_q^* 为1到 $q-1$ 范围的正整数, q 为身份凭证管理服务器选择的安全参数,身份凭证管理服务器的公钥;

[0015] 步骤2:身份凭证管理服务器对实体身份进行审核,并为实体颁发身份凭证;

[0016] 步骤2.1:在实体申请身份凭证前,基于系统公共参数生成实体的公钥私钥对,其中,实体的私钥 $SK_{EN} \in Z_q^*$,由实体随机选择,实体的公钥 $PK_{EN} = SK_{EN} \cdot P$,即循环群 G_1 上的基点 P 与实体的私钥 SK_{EN} 的乘积;

[0017] 步骤2.2:实体向身份凭证管理服务器发送身份信息和实体的公钥,向身份凭证管理服务器申请身份凭证;

[0018] 所述身份信息为网络地址标识符;

[0019] 步骤2.3:身份凭证管理服务器在接收到实体的身份凭证申请后,验证该实体身份信息的合法性,如果身份信息合法,则生成身份凭证颁发给该实体,否则不向该实体颁发身份凭证;

[0020] 所述身份凭证包括颁发者身份、颁发者公钥、用户身份、用户公钥、用户身份证书和身份凭证有效期,其中,用户身份证书由基于证书签名算法CBS生成;

[0021] 步骤2.4:实体接收到身份凭证后,使用实体的私钥和身份凭证内的实体身份证书生成实体的签名密钥;

[0022] 步骤3:当移动用户移动至安全域内,并请求接入某接入路由器时,移动用户、接入路由器和认证服务器之间进行双向接入认证;

[0023] 步骤3.1:移动用户向接入路由器发送身份凭证出示消息,接入路由器将该消息转发至认证服务器;

[0024] 步骤3.1.1:移动用户发送路由器请求消息以寻找当前所在安全域内的接入路由器;

[0025] 步骤3.1.2:接入路由器收到移动用户发送的路由器请求消息后进行接入认证;

[0026] 步骤3.1.3:接入路由器向移动用户发送路由器应答消息,请求移动用户的身份凭

证；

[0027] 步骤3.1.4:移动用户发送身份凭证出示消息给接入路由器,该消息包含移动用户的身份凭证、当前时间戳、移动用户密钥协商参数及基于移动用户的签名密钥使用CBS算法对身份凭证出示消息的CBS签名结果；

[0028] 所述移动用户密钥协商参数即移动用户的公钥与随机数的乘积；

[0029] 步骤3.1.5:接入路由器接收到移动用户的身份凭证出示消息后,将该消息转发至认证服务器;步骤3.2:认证服务器接收到移动用户的身份凭证出示消息后,对移动用户的身份凭证进行验证;若验证成功,则执行步骤3.3;若验证失败,则拒绝移动用户接入,并将验证失败消息发送给接入路由器；

[0030] 步骤3.2.1:验证移动用户的身份凭证出示消息中的时间戳的新鲜性以防止重放攻击:如果时间戳新鲜,则认证服务器验证身份凭证的有效期,执行步骤3.2.2,否则验证失败,拒绝移动用户接入,将验证失败消息发送给接入路由器；

[0031] 步骤3.2.2:如果身份凭证处于有效期内,则认证服务器对身份凭证出示消息的CBS签名结果进行验证,执行步骤3.2.3,如果身份凭证过期,将验证失败消息发送给接入路由器；

[0032] 步骤3.2.3:认证服务器根据身份凭证中的颁发者公钥和用户公钥对身份凭证出示消息的CBS签名结果进行验证:如果验证通过,则认证服务器确认移动用户为合法接入用户;如果验证失败,则拒绝移动用户接入,将验证失败消息发送给接入路由器；

[0033] 步骤3.3:认证服务器将对移动用户身份凭证验证成功消息发送给移动用户；

[0034] 步骤3.3.1:认证服务器发送验证成功消息给接入路由器,此消息包含认证服务器密钥协商参数；

[0035] 所述认证服务器密钥协商参数即认证服务器的公钥与随机数的乘积；

[0036] 步骤3.3.2:接入路由器接收到认证服务器发送的验证成功消息后,在消息中插入接入路由器的身份凭证和当前时间戳；

[0037] 步骤3.3.3:接入路由器基于接入路由器的签名密钥使用CBS算法对验证成功消息进行CBS签名,接入路由器将验证成功消息和对验证成功消息的CBS签名结果发送给移动用户；

[0038] 步骤3.4:移动用户接收到接入路由器的验证成功消息后,对接入路由器的身份凭证进行验证:若验证成功,接入当前接入路由器,完成双向接入认证;若验证失败,则拒绝接入当前接入路由器；

[0039] 步骤4:认证服务器与移动用户基于密钥协商参数进行共享密钥协商；

[0040] 步骤4.1:认证服务器基于移动用户密钥协商参数计算认证服务器与移动用户间的共享密钥；

[0041] 步骤4.2:移动用户基于认证服务器密钥协商参数计算移动用户与认证服务器间的共享密钥；

[0042] 步骤5:当移动用户在安全域内继续移动并接入新的接入路由器时,利用移动用户与认证服务器之间的共享密钥进行切换接入认证；

[0043] 步骤5.1:当移动用户在安全域内继续移动并接入新的接入路由器时,移动用户向接入路由器发送身份凭证出示消息,接入路由器将该消息转发至认证服务器；

- [0044] 步骤5.1.1:移动用户发送路由器请求消息以寻找当前所在安全域内的接入路由器;
- [0045] 步骤5.1.2:接入路由器收到移动用户发送的路由器请求消息后进行接入认证;
- [0046] 步骤5.1.3:接入路由器向移动用户发送路由器应答消息,请求移动用户的身份凭证;
- [0047] 步骤5.1.4:移动用户发送身份凭证出示消息给接入路由器,该消息包含移动用户的身份凭证、当前时间戳和基于移动用户与认证服务器所协商的共享密钥使用HMAC算法对身份凭证出示消息的HMAC认证结果;
- [0048] 步骤5.1.5:接入路由器接收到移动用户的身份凭证出示消息后,将该消息转发至认证服务器;
- [0049] 步骤5.2:认证服务器接收到移动用户的身份凭证出示消息后,对移动用户的身份凭证进行验证:若验证成功,则执行步骤5.3;若验证失败,则拒绝移动用户接入,并将验证失败消息发送给接入路由器;
- [0050] 步骤5.3:认证服务器将对移动用户的身份凭证验证成功消息发送给移动用户;
- [0051] 步骤5.3.1:认证服务器发送验证成功消息给接入路由器,此消息包含认证服务器通过接入路由器公钥对共享密钥的加密结果;
- [0052] 步骤5.3.2:接入路由器接收到认证服务器发送的验证成功消息后,利用接入路由器私钥对共享密钥进行解密,提取出共享密钥;
- [0053] 步骤5.3.3:接入路由器在验证成功消息中插入接入路由器的身份凭证和当前时间戳,接入路由器利用共享密钥使用HMAC算法对验证成功消息进行HMAC认证,接入路由器将验证成功消息和对验证成功消息的HMAC认证结果发送给移动用户;
- [0054] 步骤5.4:移动用户利用其与认证服务器协商的共享密钥验证接入路由器的合法性,若接入路由器合法,则移动用户切换接入该合法接入路由器,完成切换接入认证;若接入路由器不合法,则移动用户拒绝接入该接入路由器。
- [0055] 所述步骤3.4移动用户接收到接入路由器的验证成功消息后,对接入路由器的身份凭证进行验证,具体步骤如下:
- [0056] 步骤3.4.1:移动用户验证接收到的验证成功消息中的时间戳新鲜性,以防止重放攻击:如果时间戳新鲜,则验证接入路由器身份凭证的有效期,执行步骤3.4.2;否则验证失败,拒绝接入当前接入路由器;
- [0057] 步骤3.4.2:如果身份凭证处于有效期内,则移动用户对验证成功消息的CBS签名结果进行验证,执行步骤3.4.3;如果身份凭证过期,则拒绝接入当前接入路由器;
- [0058] 步骤3.4.3:移动用户根据身份凭证中的颁发者公钥和用户公钥对验证成功消息的CBS签名结果进行验证:如果验证通过,则移动用户确认接入该合法接入路由器,完成双向接入认证;若验证失败,则移动用户拒绝接入当前接入路由器。
- [0059] 所述步骤4.1认证服务器基于移动用户密钥协商参数计算认证服务器与移动用户间的共享密钥,具体步骤如下:
- [0060] 步骤4.1.1:认证服务器以移动用户密钥协商参数和循环群G1上的基点G与认证服务器私钥的乘积为输入,利用双线性对 e 计算认证服务器共享密钥值;
- [0061] 步骤4.1.2:认证服务器以认证服务器共享密钥值为输入,利用单向哈希函数H2计

算其与移动用户的共享密钥。

[0062] 所述步骤4.2移动用户基于认证服务器密钥协商参数计算移动用户与认证服务器间的共享密钥,具体步骤如下:

[0063] 步骤4.2.1:移动用户以认证服务器密钥协商参数和循环群G1上基点G与移动用户私钥的乘积为输入,利用双线性对e计算移动用户共享密钥值;

[0064] 步骤4.2.2:移动用户以移动用户共享密钥值为输入,利用单向哈希函数H2计算其与认证服务器的共享密钥。

[0065] 所述步骤5.2认证服务器接收到移动用户的身份凭证出示消息后,对移动用户的身份凭证进行验证,具体步骤如下:

[0066] 步骤5.2.1:验证移动用户的身份凭证出示消息中时间戳的新鲜性以防止重放攻击:如果时间戳新鲜,则认证服务器验证身份凭证的有效期,执行步骤5.2.2,否则验证失败,拒绝移动用户接入,将验证失败消息发送给接入路由器;

[0067] 步骤5.2.2:如果身份凭证处于有效期内,则认证服务器对身份凭证出示消息的HMAC认证结果进行验证,执行步骤5.2.3,如果身份凭证过期,将验证失败消息发送给接入路由器;

[0068] 步骤5.2.3:认证服务器根据其于移动用户协商的共享密钥对身份凭证出示消息的HMAC认证结果进行验证:如果验证通过,则认证服务器确认移动用户为合法接入用户;如果验证失败,则拒绝移动用户接入,将验证失败消息发送给接入路由器。

[0069] 所述步骤5.4移动用户利用其与认证服务器协商的共享密钥验证接入路由器的合法性,具体步骤如下:

[0070] 步骤5.4.1:移动用户验证接收到的验证成功消息中的时间戳新鲜性,以防止重放攻击:如果时间戳新鲜,则验证接入路由器身份凭证的有效期,执行步骤5.4.2;否则验证失败,拒绝接入当前接入路由器;

[0071] 步骤5.4.2:如果身份凭证处于有效期内,则移动用户对验证成功消息的HMAC认证结果进行验证,执行步骤5.4.3;如果身份凭证过期,拒绝接入当前接入路由器;

[0072] 步骤5.4.3:移动用户根据其于认证服务器协商的共享密钥对验证成功消息的HMAC认证结果进行验证:如果验证通过,则移动用户确认接入该合法接入路由器,完成切换接入认证;若验证失败,则移动用户拒绝接入当前接入路由器。

[0073] 有益效果:

[0074] 本发明的系统及方法在一个自治安全域内,既能实现移动用户与访问网络间的双向接入认证和密钥协商,又支持移动用户于不同接入路由器间切换时的高效接入认证,提高了接入认证效率。

附图说明

[0075] 图1为本发明具体实施方式的基于身份凭证的无线局域网双向接入认证系统示意图;

[0076] 图2为本发明具体实施方式的对实体身份进行审核并为实体颁发身份凭证流程图;

[0077] 图3为本发明具体实施方式的移动用户向认证服务器发送身份凭证出示消息过程

示意图；

[0078] 图4为本发明具体实施方式的认证服务器对移动用户认证流程图；

[0079] 图5为本发明具体实施方式的认证服务器向移动用户发送验证成功消息过程示意图；

[0080] 图6为本发明具体实施方式的移动用户对接入路由器认证流程图；

[0081] 图7为本发明具体实施方式的切换认证过程示意图；

[0082] 图8为本发明具体实施方式的系统模块通信流程图；

[0083] 图9为本发明具体实施方式的无线局域网双向接入认证的方法流程图。

具体实施方式

[0084] 下面结合附图对本发明的具体实施方式做详细说明。

[0085] 本实施方式是将基于身份凭证的无线局域网双向接入认证系统及方法应用于某无线局域网接入认证环节。实施过程中采用成熟的802.11i认证框架,对于认证消息的承载,移动用户与接入路由器间采用EAP协议,接入路由器与认证服务器间采用RADIUS协议。

[0086] 如图1所示,基于身份凭证的无线局域网双向接入认证系统,包括若干接入路由器(包括AR1和AR2),设置在一个自治安全域内,还包括一个身份凭证管理服务器(ICM)和一个认证服务器(AS)；

[0087] 身份凭证管理服务器用于对安全域内实体(接入路由器AR和移动用户MN)的身份凭证(Identity Credential, IC)进行管理,包括颁发身份凭证和维护身份凭证；

[0088] 身份凭证是双向接入认证过程中的重要依据,此凭证与PKI体系下的X.509数字证书有着本质区别。X.509数字证书主要实现了用户身份信息与所持公钥的绑定,而本实施方式的身份凭证包括颁发者身份、颁发者公钥、用户身份、用户公钥、用户身份证书和身份凭证有效期；

[0089] 认证服务器用于验证移动用户的接入认证申请并完成与移动用户间的共享密钥协商；

[0090] 接入路由器用于根据认证服务器返回的验证结果控制是否允许移动用户接入无线局域网,同时接入路由器接收和转发移动用户与认证服务器间的认证消息。

[0091] 为便于后续描述,给出如表1所示的标识及说明。

[0092] 表1 标识及说明

标识	说明
Entity	安全域内实体, 包括 MN 和 AR
ID _{EN}	实体的身份信息
Cred _{EN}	实体的身份凭证
Cert _{EN}	实体的身份证书
PK _{EN} /SK _{EN}	实体的公钥私钥对
Ta	MN 密钥协商参数
Tb	AS 密钥协商参数
[0093] Sig _{EN}	实体的 CBS 签名操作
HMAC _{EN}	实体的 HMAC 认证操作
Enc _{EN}	实体的公钥加密操作
Ts	当前时间戳
SignKey _{EN}	实体的签名密钥
ShareKey_Value _{A-B}	实体 A、B 间的共享密钥值
ShareKey _{A-B}	实体 A、B 间的共享密钥
SessionKey _{A-B}	CBS 签名结果
[0094] σ	HMAC 认证结果

[0095] 采用所述的基于身份凭证的无线局域网双向接入认证系统进行无线局域网双向接入认证的方法,如图9所示,包括以下步骤:

[0096] 步骤1:身份凭证管理服务器ICM根据选择的安全参数生成系统公共参数并发布系统公共参数;

[0097] ICM为安全域内的可信第三方,生成系统公共参数并发布系统公共参数;

[0098] 系统公共参数 $\{G1, G2, e, P, G, H1, H2, PK_{ICM}\}$,包括循环群 $G1$ 和循环群 $G2$ 、双线性对 e 、循环群 $G1$ 上的基点 P 和 G ,字符集至循环群 $G1$ 的单向哈希函数 $H1$,循环群 $G2$ 至 Z_q^* 的单向哈希函数 $H2(H1: \{0, 1\}^* \rightarrow G1, H2: G2 \rightarrow Z_q^*, Z_q^*$ 为1到 $q-1$ 范围的正整数, q 为身份凭证管理服务器选择的安全参数),身份凭证管理服务器的公钥 $PK_{ICM}=SK_{ICM} \cdot P$,身份凭证管理服务器私钥 $SK_{ICM} \in Z_q^*$,由身份凭证管理服务器随机选择;

[0099] 步骤2:身份凭证管理服务器对实体身份进行审核,并为实体颁发身份凭证,如图2所示;

[0100] 步骤2.1:在实体申请身份凭证前,基于系统公共参数生成实体的公钥私钥对,其中,实体的私钥 $SK_{EN} \in Z_q^*$,由实体随机选择,实体的公钥 $PK_{EN}=SK_{EN} \cdot P$,即循环群 $G1$ 上的基点 P 与实体的私钥 SK_{EN} 的乘积;

[0101] 步骤2.2:实体向身份凭证管理服务器发送身份信息和实体的公钥,向身份凭证管理服务器申请身份凭证;

[0102] 所述身份信息为网络地址标识符,如Entity@Domain;

[0103] 步骤2.3:身份凭证管理服务器在接收到实体的身份凭证申请后,验证该实体身份信息的合法性,如果身份信息合法,则生成身份凭证颁发给该实体,否则不向该实体颁发身份凭证;

[0104] 身份凭证包括颁发者身份、颁发者公钥、用户身份、用户公钥、用户身份证书和身份凭证有效期,其中,用户身份证书由基于证书签名算法CBS生成;

[0105] 身份凭证中的实体身份证书为:

[0106] $Cert_{EN} = SK_{ICM} \cdot P_{EN}, P_{EN} = H_1(PK_{ICM} || PK_{EN} || ID_{EN}) \in G_1.$

[0107] 步骤2.4:实体接收到身份凭证后,使用实体的私钥和身份凭证内的实体身份证书生成实体的签名密钥;

[0108] 实体的签名密钥为:

[0109] $SignKey_{EN} = Cert_{EN} + SK_{EN} \cdot P_{EN}.$

[0110] 步骤3:当移动用户移动至安全域内,并请求接入某接入路由器AR时,移动用户MN、接入路由器AR和认证服务器AS之间进行双向接入认证;

[0111] 步骤3.1:移动用户向接入路由器发送身份凭证出示消息,接入路由器AR将该消息转发至认证服务器,如图3所示;

[0112] 步骤3.1.1:移动用户发送路由器请求消息以寻找当前所在安全域内的接入路由器;

[0113] MN以EAP协议发送数据包(EAP-Start)寻找安全域内某AR,发送的EAP组播帧中只有EAP包含帧的必需字段;

[0114] 步骤3.1.2:接入路由器收到移动用户发送的路由器请求消息后进行接入认证;

[0115] 步骤3.1.3:接入路由器向移动用户发送路由器应答消息,请求移动用户的身份凭证;

[0116] AR在接收到MN的EAP-Start后,向MN发送EAP数据包(EAP-Request-Credential),请求MN的身份凭证信息;

[0117] 步骤3.1.4:移动用户发送身份凭证后示消息给接入路由器,该消息包含移动用户的身份凭证、当前时间戳(Ts1)、移动用户密钥协商参数及基于移动用户的签名密钥使用CBS算法对身份凭证后示消息的CBS签名结果 σ ;

[0118] 移动用户通过EAP数据包(EAP-Response)发送身份凭证后示消息给接入路由器;

[0119] 移动用户密钥协商参数即移动用户的公钥与随机数的乘积, $Ta = a \cdot PK_{MN} (a \in Z_q^*);$

[0120] 基于移动用户的签名密钥使用CBS算法对身份凭证后示消息的CBS签名结果 $\sigma = (U, V), U = r \cdot P_{MN}, h = H_2(m, U), V = (r+h) \cdot SignKey_{MN}, r \in Z_q^*, m$ 为身份凭证后示消息;

[0121] 步骤3.1.5:接入路由器接收到移动用户的身份凭证后示消息后,将该消息转发至认证服务器;

[0122] AR接收到MN的身份凭证出示消息后,从EAP协议中的数据部分获取相应数据,然后重新封装到RADIUS协议之中,通过RADIUS数据包(RADIUS-Access-Request)转发身份凭证

出示消息至AS;

[0123] 步骤3.2:认证服务器接收到移动用户的身份凭证出示消息后,如图4所示,对移动用户的身份凭证进行验证:若验证成功,则执行步骤3.3;若验证失败,则拒绝移动用户接入,并将验证失败消息发送给接入路由器;

[0124] 步骤3.2.1:验证移动用户的身份凭证出示消息中的时间戳Ts1的新鲜性以防止重放攻击:如果时间戳Ts1新鲜,则认证服务器验证身份凭证的有效期,执行步骤3.2.2,否则验证失败,拒绝移动用户接入,将验证失败消息发送给接入路由器;

[0125] 步骤3.2.2:如果身份凭证处于有效期内,则认证服务器对身份凭证出示消息的CBS签名结果进行验证,执行步骤3.2.3,如果身份凭证过期,将验证失败消息发送给接入路由器;

[0126] 步骤3.2.3:认证服务器根据身份凭证中的颁发者公钥和用户公钥对身份凭证出示消息的CBS签名结果进行验证:如果验证通过,则认证服务器确认移动用户为合法接入用户;如果验证失败,则拒绝移动用户接入,将验证失败消息发送给接入路由器;

[0127] 认证服务器对身份凭证出示消息的CBS签名结果 σ 进行如下验证:

[0128] $e(PK_{ICM}+PK_{MN}, U+hP_{MN})=?e(P, V)$.

[0129] 步骤3.3:认证服务器将对移动用户身份凭证验证成功消息发送给移动用户,如图5所示;

[0130] 步骤3.3.1:认证服务器发送验证成功消息给接入路由器,此消息包含认证服务器密钥协商参数;

[0131] 认证服务器通过RADIUS数据包(RADIUS-Access-Success)发送验证成功消息给接入路由器;

[0132] 所述认证服务器密钥协商参数即认证服务器的公钥与随机数的乘积, $Tb=b \cdot PK_{AS} (b \in Z_q^*)$;

[0133] 步骤3.3.2:接入路由器接收到认证服务器发送的验证成功消息后,在消息中插入接入路由器的身份凭证和当前时间戳(Ts2);

[0134] 接入路由器接收到认证服务器的验证成功消息后,从RADIUS协议中的数据部分获取相应数据,插入接入路由器的身份凭证和当前时间戳(Ts2),然后重新封装到EAP协议之中;

[0135] 步骤3.3.3:接入路由器基于接入路由器的签名密钥使用CBS算法对验证成功消息进行CBS签名,接入路由器将验证成功消息和对验证成功消息的CBS签名结果发送给移动用户;

[0136] 基于接入路由器的签名密钥使用CBS算法对验证成功消息的CBS签名结果 $\sigma'=(U', V')$, $U'=r' \cdot P_{AR}$, $h'=H2(m', U')$, $V'=(r'+h') \cdot \text{SignKey}_{AR}$, 其中, $r' \in Z_q^*$, m' 为验证成功消息;

[0137] 接入路由器通过EAP数据包(EAP-Success)转发验证成功消息和CBS签名结果至移动用户;

[0138] 步骤3.4:如图6所示,移动用户接收到接入路由器的验证成功消息后,对接入路由器的身份凭证进行验证:若验证成功,接入当前接入路由器,完成双向接入认证;若验证失

败,则拒绝接入当前接入路由器;

[0139] 所述移动用户接收到接入路由器的验证成功消息后,对接入路由器的身份凭证进行验证,具体步骤如下:

[0140] 步骤3.4.1:移动用户验证接收到的验证成功消息中的时间戳(Ts2)新鲜性,以防止重放攻击:如果时间戳(Ts2)新鲜,则验证接入路由器身份凭证的有效期,执行步骤3.4.2;否则验证失败,拒绝接入当前接入路由器;

[0141] 步骤3.4.2:如果身份凭证处于有效期内,则移动用户对验证成功消息的CBS签名结果进行验证,执行步骤3.4.3;如果身份凭证过期,则拒绝接入当前接入路由器;

[0142] 步骤3.4.3:移动用户根据身份凭证中的颁发者公钥和用户公钥对验证成功消息的CBS签名结果进行验证:如果验证通过,则移动用户确认接入该合法接入路由器,完成双向接入认证;若验证失败,则移动用户拒绝接入当前接入路由器。

[0143] 移动用户对验证成功消息的CBS签名结果 σ' 进行如下验证:

[0144] $e(PK_{ICM}+PK_{AR}, U' + h' P_{AR}) = ? e(P, V')$.

[0145] 步骤4:认证服务器与移动用户基于密钥协商参数进行共享密钥协商;

[0146] 步骤4.1:认证服务器基于移动用户密钥协商参数计算认证服务器与移动用户间的共享密钥;

[0147] 步骤4.1.1:认证服务器以移动用户密钥协商参数和循环群G1上的基点G与认证服务器私钥的乘积为输入,利用双线性对e计算认证服务器共享密钥值;

[0148] $ShareKey_Value_{AS-MN} = e(b \cdot T_a, SK_{AS} \cdot G), b \in Z_q^*$

[0149] 其中,ShareKey_Value_{AS-MN}为AS与MN间的共享密钥值,b为AS随机选择参数;

[0150] 步骤4.1.2:认证服务器以认证服务器共享密钥值为输入,利用单向哈希函数H2计算认证服务器与移动用户的共享密钥。

[0151] $ShareKey_{AS-MN} = H2(ShareKey_Value_{AS-MN})$.

[0152] 其中,ShareKey_{AS-MN}为AS与MN间的共享密钥;

[0153] 步骤4.2:移动用户基于认证服务器密钥协商参数计算移动用户与认证服务器间的共享密钥;

[0154] 步骤4.2.1:移动用户以认证服务器密钥协商参数和循环群G1上基点G与移动用户私钥的乘积为输入,利用双线性对e计算移动用户共享密钥值;

[0155] $ShareKey_Value_{MN-AS} = e(a \cdot T_b, SK_{MN} \cdot G), a \in Z_q^*$

[0156] 其中,ShareKey_Value_{MN-AS}为MN与AS间的共享密钥值,a为MN随机选择参数;

[0157] 步骤4.2.2:移动用户以移动用户共享密钥值为输入,利用单向哈希函数H2计算其与认证服务器的共享密钥。

[0158] $ShareKey_{MN-AS} = H2(ShareKey_Value_{MN-AS})$

[0159] 其中,ShareKey_{MN-AS}为MN与AS间的共享密钥;

[0160] 步骤5:如图7所示,当移动用户在安全域内继续移动并接入新的接入路由器时,利用移动用户与认证服务器之间的共享密钥进行切换接入认证;

[0161] 步骤5.1:当移动用户在安全域内继续移动并接入新的接入路由器AR'时,移动用户向接入路由器发送身份凭证出示消息,接入路由器将该消息转发至认证服务器;

[0162] 步骤5.1.1:移动用户发送路由器请求消息以寻找当前所在安全域内的接入路由器;

[0163] 步骤5.1.2:接入路由器收到移动用户发送的路由器请求消息后进行接入认证;

[0164] 步骤5.1.3:接入路由器向移动用户发送路由器应答消息,请求移动用户的身份凭证;

[0165] 步骤5.1.4:移动用户发送身份凭证出示消息给接入路由器,该消息包含移动用户的身份凭证、当前时间戳Ts3和基于移动用户与认证服务器所协商的共享密钥使用HMAC算法对身份凭证出示消息的HMAC认证结果 \varnothing ;

[0166] \varnothing 的生成过程如下:

[0167] $\varnothing = \text{HMAC}_{\text{MN}}(\text{Cred}_{\text{MN}} \parallel \text{Ts3} \parallel \text{ShareKey}_{\text{MN-AS}})$

[0168] 步骤5.1.5:接入路由器接收到移动用户的身份凭证出示消息后,将该消息转发至认证服务器;

[0169] AR接收到MN的身份凭证出示消息后,从EAP协议中的数据部分获取相应数据,然后重新封装到RADIUS协议之中,通过RADIUS数据包(RADIUS-Access-Request)转发身份凭证出示消息至AS;

[0170] 步骤5.2:认证服务器接收到移动用户的身份凭证出示消息后,对移动用户的身份凭证进行验证:若验证成功,则执行步骤5.3;若验证失败,则拒绝移动用户接入,并将验证失败消息发送给接入路由器;

[0171] 所述认证服务器接收到移动用户的身份凭证出示消息后,对移动用户的身份凭证进行验证,具体步骤如下:

[0172] 步骤5.2.1:验证移动用户的身份凭证出示消息中时间戳Ts3的新鲜性以防止重放攻击:如果时间戳Ts3新鲜,则认证服务器验证身份凭证的有效期,执行步骤5.2.2,否则验证失败,拒绝移动用户接入,将验证失败消息发送给接入路由器;

[0173] 步骤5.2.2:如果身份凭证处于有效期内,则认证服务器对身份凭证出示消息的HMAC认证结果进行验证,执行步骤5.2.3,如果身份凭证过期,将验证失败消息发送给接入路由器;

[0174] 步骤5.2.3:认证服务器根据其与移动用户协商的共享密钥对身份凭证出示消息的HMAC认证结果进行验证:如果验证通过,则认证服务器确认移动用户为合法接入用户;如果验证失败,则拒绝移动用户接入,将验证失败消息发送给接入路由器。

[0175] 认证服务器对身份凭证出示消息的HMAC认证结果 \varnothing 进行如下验证:

[0176] $\text{HMAC}_{\text{AS}}(\text{Cred}_{\text{MN}} \parallel \text{Ts3} \parallel \text{ShareKey}_{\text{AS-MN}}) = ? \varnothing$

[0177] 步骤5.3:认证服务器将对移动用户的身份凭证验证成功消息发送给移动用户;

[0178] 步骤5.3.1:认证服务器发送验证成功消息给接入路由器,此消息包含认证服务器通过接入路由器公钥对共享密钥的加密结果;

[0179] 步骤5.3.2:接入路由器接收到认证服务器发送的验证成功消息后,利用接入路由器私钥对共享密钥进行解密,提取出共享密钥;

[0180] 步骤5.3.3:接入路由器在验证成功消息中插入接入路由器的身份凭证和当前时间戳,接入路由器利用共享密钥使用HMAC算法对验证成功消息进行HMAC认证,接入路由器

将验证成功消息和对验证成功消息的HMAC认证结果发送给移动用户；

[0181] 对验证成功消息的HMAC认证结果 δ' 如下：

[0182] $\delta' = \text{HMAC}_{AS}(\text{Cred}_{AS} || \text{Ts4} || \text{ShareKey}_{AS-MN})$

[0183] 步骤5.4：移动用户利用其与认证服务器协商的共享密钥验证接入路由器的合法性，若接入路由器合法，则移动用户切换接入该合法接入路由器，完成切换接入认证；若接入路由器不合法，则移动用户拒绝接入该接入路由器。

[0184] 所述移动用户利用其与认证服务器协商的共享密钥验证接入路由器的合法性，具体步骤如下：

[0185] 步骤5.4.1：移动用户验证接收到的验证成功消息中的时间戳Ts4新鲜性，以防止重放攻击：如果时间戳Ts4新鲜，则验证接入路由器身份凭证的有效期，执行步骤5.4.2；否则验证失败，拒绝接入当前接入路由器；

[0186] 步骤5.4.2：如果身份凭证处于有效期内，则移动用户对验证成功消息的HMAC认证结果进行验证，执行步骤5.4.3；如果身份凭证过期，拒绝接入当前接入路由器；

[0187] 步骤5.4.3：移动用户根据其与认证服务器协商的共享密钥对验证成功消息的HMAC认证结果进行验证：如果验证通过，则移动用户确认接入该合法接入路由器，完成切换接入认证；若验证失败，则移动用户拒绝接入当前接入路由器。

[0188] 移动用户对验证成功消息的HMAC认证结果 δ' 进行如下验证：

[0189] $\text{HMAC}_{MN}(\text{Cred}_{AR} || \text{Ts4} || \text{ShareKey}_{MN-AS}) = ? \delta'$

[0190] 基于上述描述过程，对基于身份凭证的无线局域网双向接入认证系统进行设计与实现。系统在Windows平台上开发实现，编程语言是C++，开发工具为Visual Studio，使用到的库函数有Winpcap，网络层通信协议为UDP。

[0191] MN模块主要功能是：发现AR、出示凭证和验证凭证。在MN模块中设计初始化类、示证类、验证类和加解密类。初始化类主要对系统进行初始化，然后监听网络适配器数据；根据接收到的数据调用示证类发送身份凭证出示消息；最后调用验证类和加解密类对接收到的验证成功消息进行双向验证。MN模块类设计如表2所示。

[0192] 表2 MN模块的类设计

[0193]

类名	成员方法	功能
Init_MN (初始化类)	Init(const USERDATA *pUserData) GetAdaptersInfo()	初始化相应变量 获取客户端适配器信息，设置要接入网络的适配器

[0194]

	OpenAdapter() ReceiveDataFromAdapters() GetDataFromPath(char* credPath,char* paramsPath,char key)	打开要操作的网络适配器 从设置好的适配器中接收 AR 返回的数据 从指定路径获取凭证和私钥等信息
SendEAPToAR (示证类)	SendStart() SendCredential(const char id) InitEAPHeader(u_char *buf) BuildECC() GenerateTimestamp() GenerateSessionKeyParam(ECPoint PKa) SpliceMessage(u_char *credential, u_char * timestamp, ECPoint ta) GenerateSign(u_char *msg) PackEAPData()	发送请求验证数据帧 向 AR 发送身份凭证等消息 初始化 EAP 数据帧 通过 ICM 公共参数构建椭圆域 生成时间戳 通过用户公钥及生成元计算密钥协商参数 对要签名信息进行拼接 对拼接消息进行签名 EAP 消息封装
Verify_MN (验证类)	AnalysisData(u_char *buf) VerifyTimestamp(u_char * timestamp) CalcShareKey(ECPoint tb) VerifySign(u_char *buf)	对接收到的数据进行分析 检验时间戳 计算共享密钥 验证签名
Enc (加解密类)	Cipher(u_char * input) InvCipher(u_char * input) MDString(u_char *string,int len, u_char * result)	加密函数 解密函数 HMAC 函数

[0195] AR模块的主要功能是：从MN接收身份凭证出示消息并转发至AS、从AS接收验证成功消息、解密共享密钥、HMAC认证、转发相应消息至MN。在AR模块中设计初始化类、数据分析处理类和加解密类。初始化类主要负责系统初始化及从MN和AS接收数据；在接收到数据后调用数据分析处理类和加解密类对接收到的数据进行分析和处理，并对相应的数据进行协议封装；最后在认证完成后控制MN的接入。AR模块类设计如表3所示。

[0196] 表3 AR模块的类设计

[0197]

类名	成员方法	功能
Init_AR (初始化类)	Init(const APDATA *pAPData) GetAdaptersInfo() OpenAdapter() InitSocket() ReceiveDataFromAdapters() ReceiveDataFromSocket()	初始化相应变量 获取适配器信息, 设置要接入网络的适配器 打开要操作的网络适配器 初始化 Socket 从设置好的适配器中接收 MN 发送的认证消息 从 Socket接收 AS 返回认证消息
Analysis_AR (数据分析处理类)	AnalysisEAPData(u_char *buf) AnalysisRADIUSData(u_char *buf) SendEAPRequestCredential() SendRadiusCredential(u_char *credential ,int length,u_char id) AnalysisCheck(u_char *buf)	对接收到的链路层数据进行分析和处理 对接收到的传输层数据进行分析和处理 请求 MN 的身份凭证等信息 向 RADIUS 服务器发送认证消息 分析从 RADIUS 服务器接收到

[0198]

	SendEAPRequestSuccess(int id, BYTE *data)	的数据完整性 协议封装
	SendEAPRequestFailure(int id)	向 MN 发送失败报文
	RandomAuthenticator(BYTE * data)	计算 RADIUS 协议的认证码
Enc (加解密类)	Cipher(u_char * input)	加密函数
	InvCipher(u_char * input)	解密函数
	MDString(u_char *string, int len, u_char * result)	HMAC 函数

[0199] AS模块的主要功能是：对MN进行接入认证、与MN协商共享密钥。在AS模块中设计初始化类、数据分析处理类、验证类、示证类和加解密类。初始化类主要负责系统初始化及接收数据；数据分析处理类则负责对接收到的数据进行分析处理；然后调用验证类对MN进行验证；验证通过后调用示证类返回验证成功消息给AR。AS模块类设计如表4所示。

[0200] 表4 AS模块的类设计

[0201]

类名	成员方法	功能
Init_AS (初始化类)	Init(const ASDATA *pASData)	初始化相应变量
	GetDataFromPath(char* credPath, char* paramsPath, char key)	从指定路径获取凭证和私钥等信息
	InitSocket()	初始化 Socket
	ReceiveDataFromSocket()	从 Socket 接收数据
Analysis_AS (数据分析处理类)	AnalysisData(u_char *buf)	对接收到的数据进行分析
	AnalysisCheck(u_char *buf)	分析接收数据的完整性
	PackRADIUSData()	RADIUS 协议封装
	SendData(u_char buf)	发送 RADIUS 消息
Verify_AS (验证类)	VerifyTimestamp(u_char * timestamp)	检验时间戳
	VerifySign(u_char *buf)	验证签名或 HMAC 结果
	GenerateSessionKeyParam(ECPoint PKa)	通过用户公钥或生成元生成计算共享密钥的参数
	CalcShareKey(ECPoint tb) GenerateTimestamp()	共享密钥计算 生成时间戳
Prover (示证类)	SpliceMessage(u_char *Credential, u_char * Timestamp, ECPoint tb)	签名信息拼接
	GenerateSign(u_char *msg)	拼接消息签名
Enc (加解密类)	Cipher(u_char * input)	加密函数
	InvCipher(u_char * input)	解密函数
	MDString(u_char *string, int len, u_char * result)	HMAC 函数

[0202] 结合上述模块和类设计，可以按图8所示流程对接入认证所涉及的MN模块、AR模块和AS模块进行编程实现。

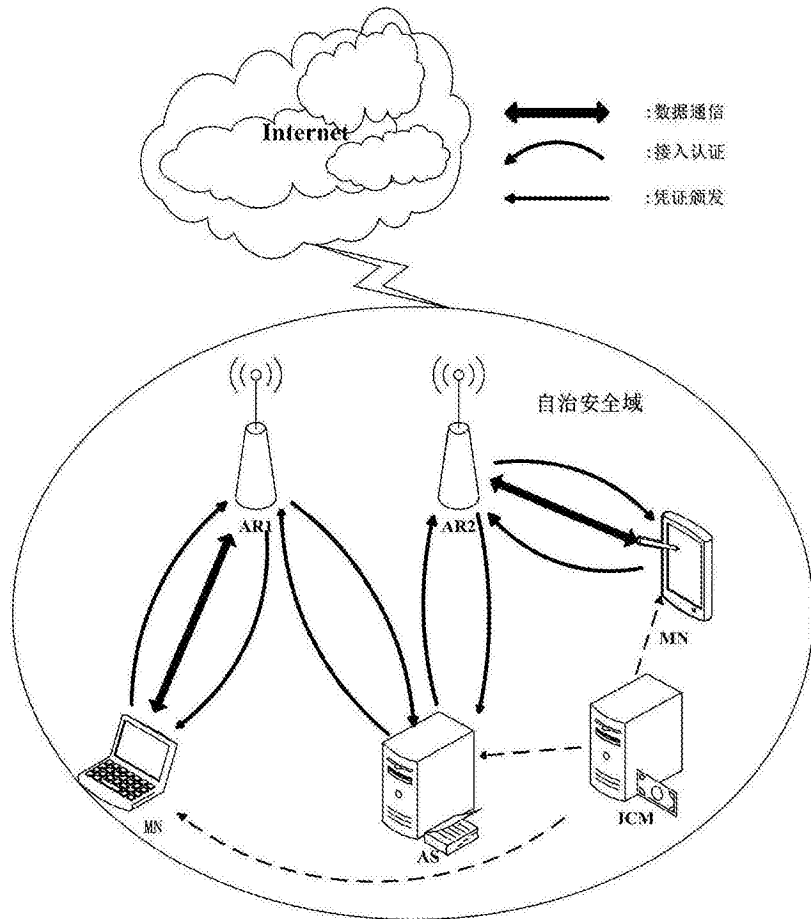


图1

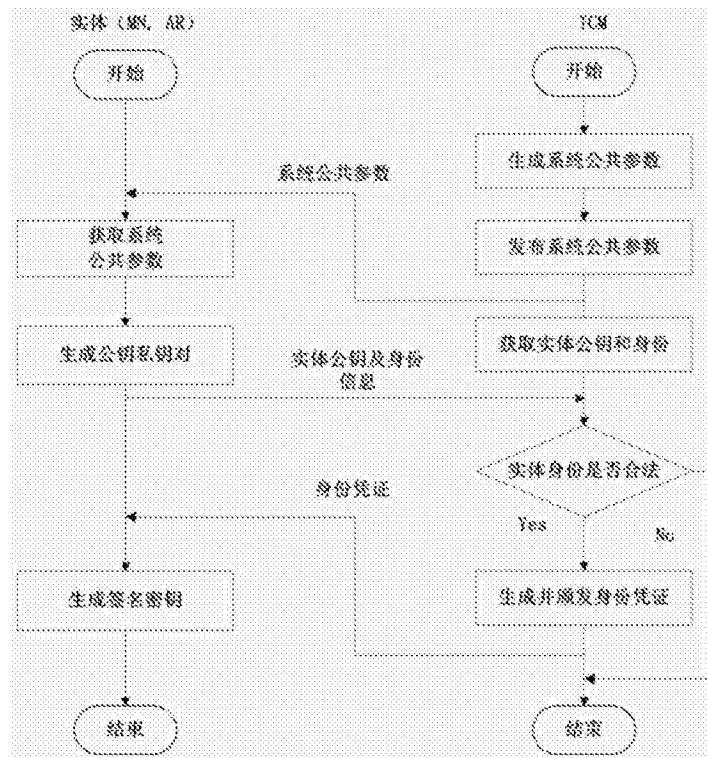


图2

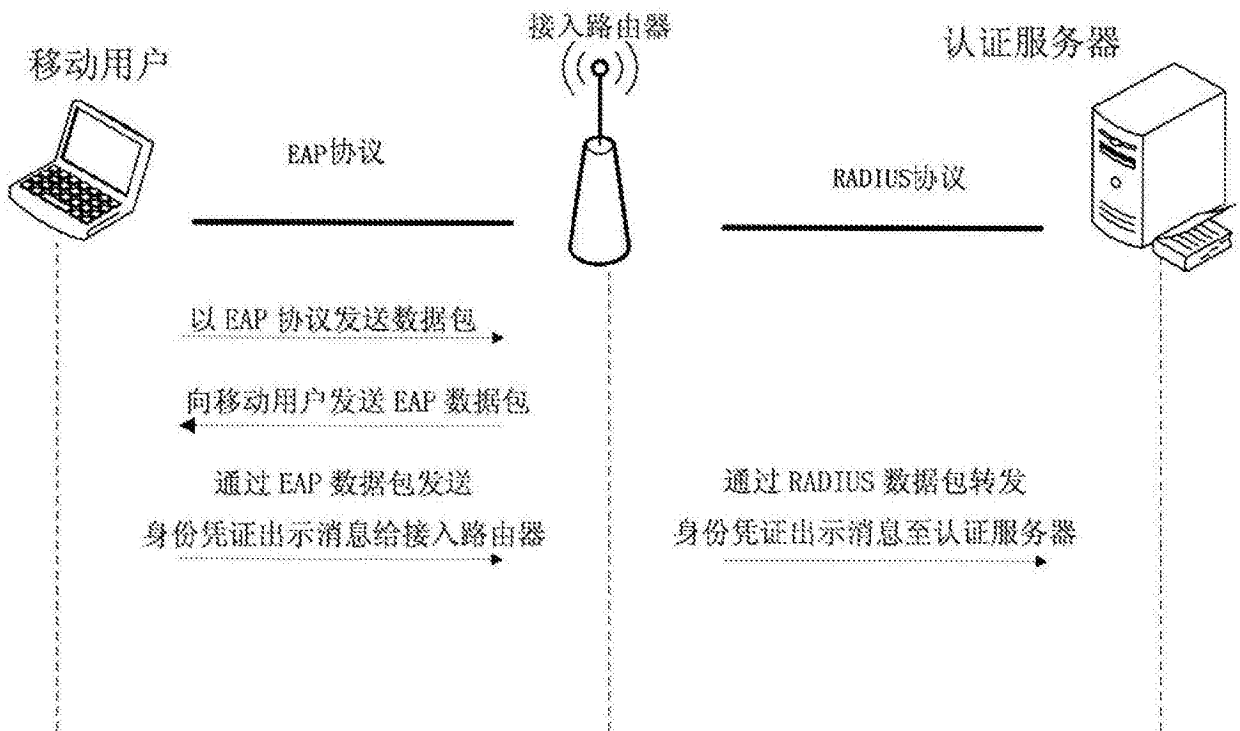


图3

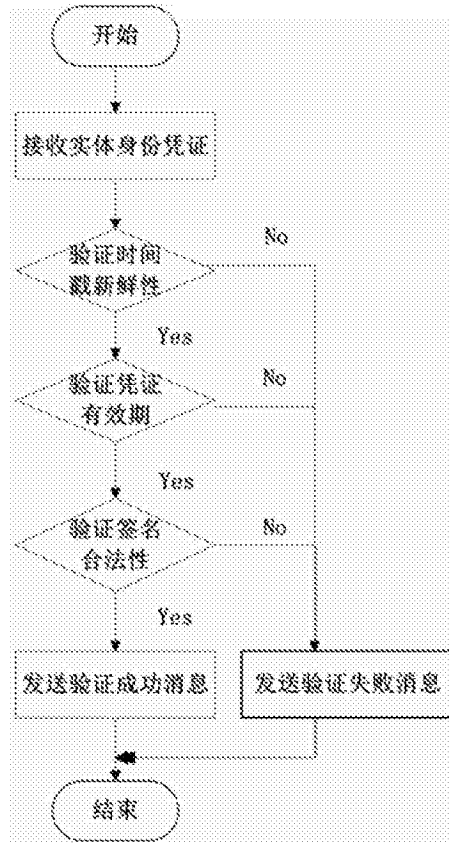


图4

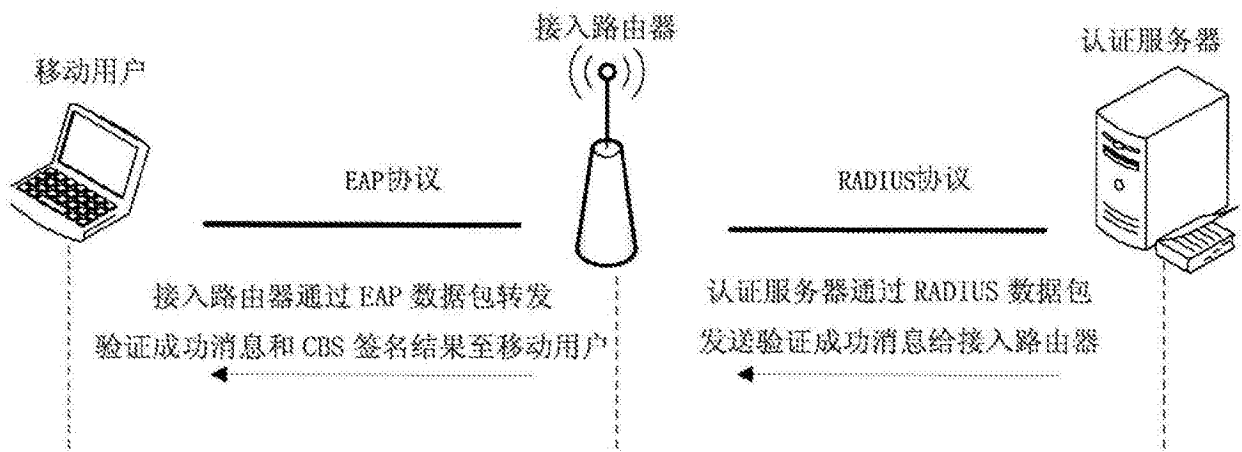


图5

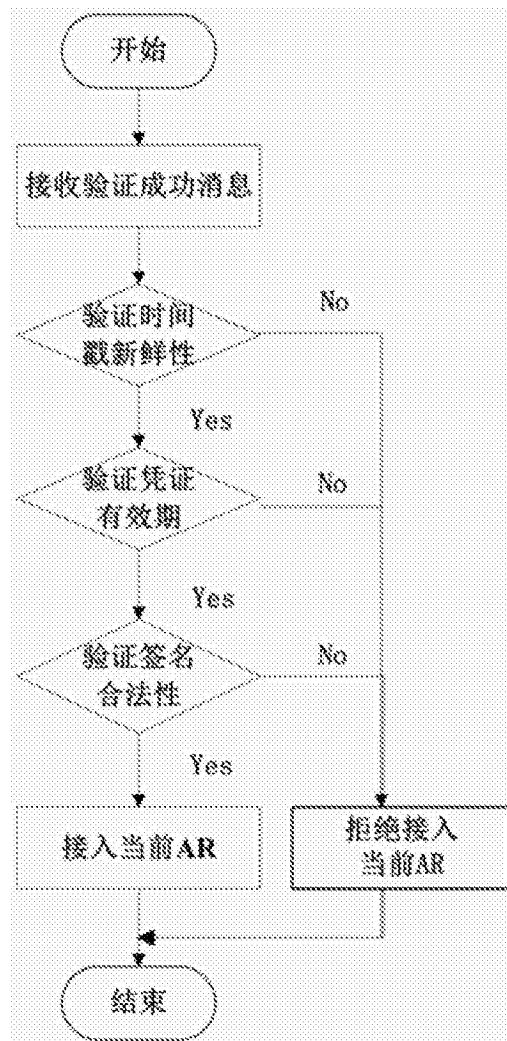


图6

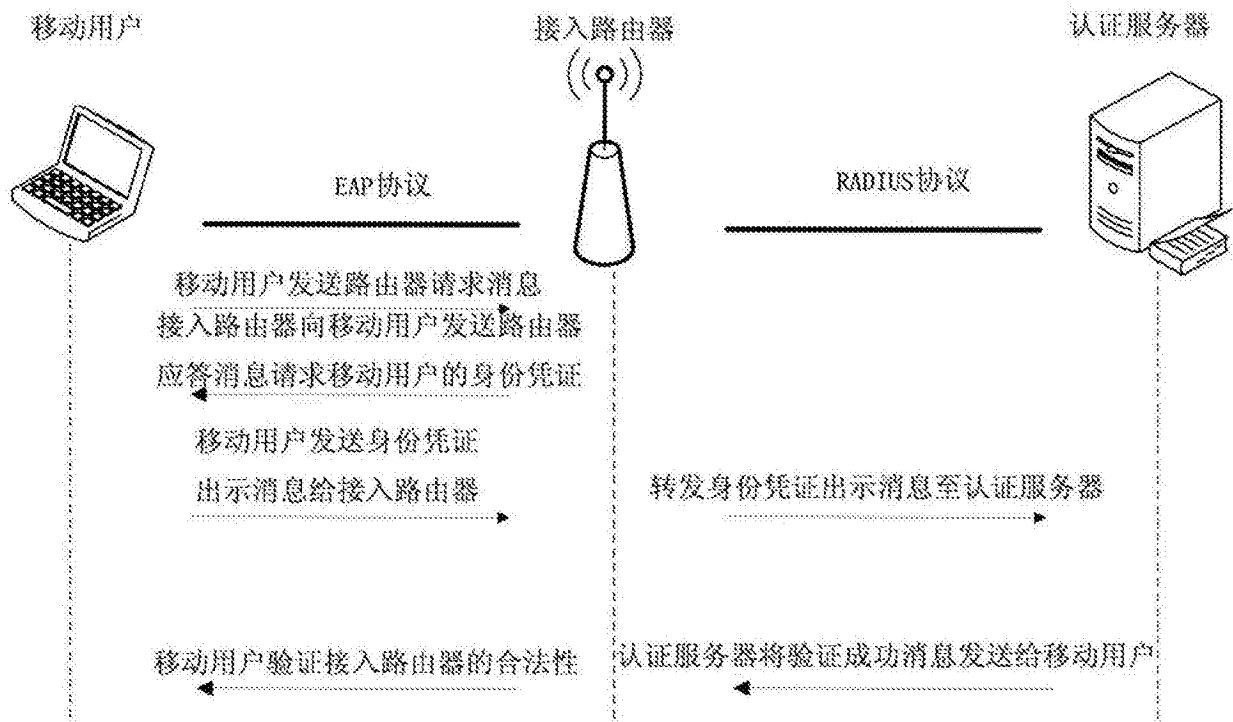


图7

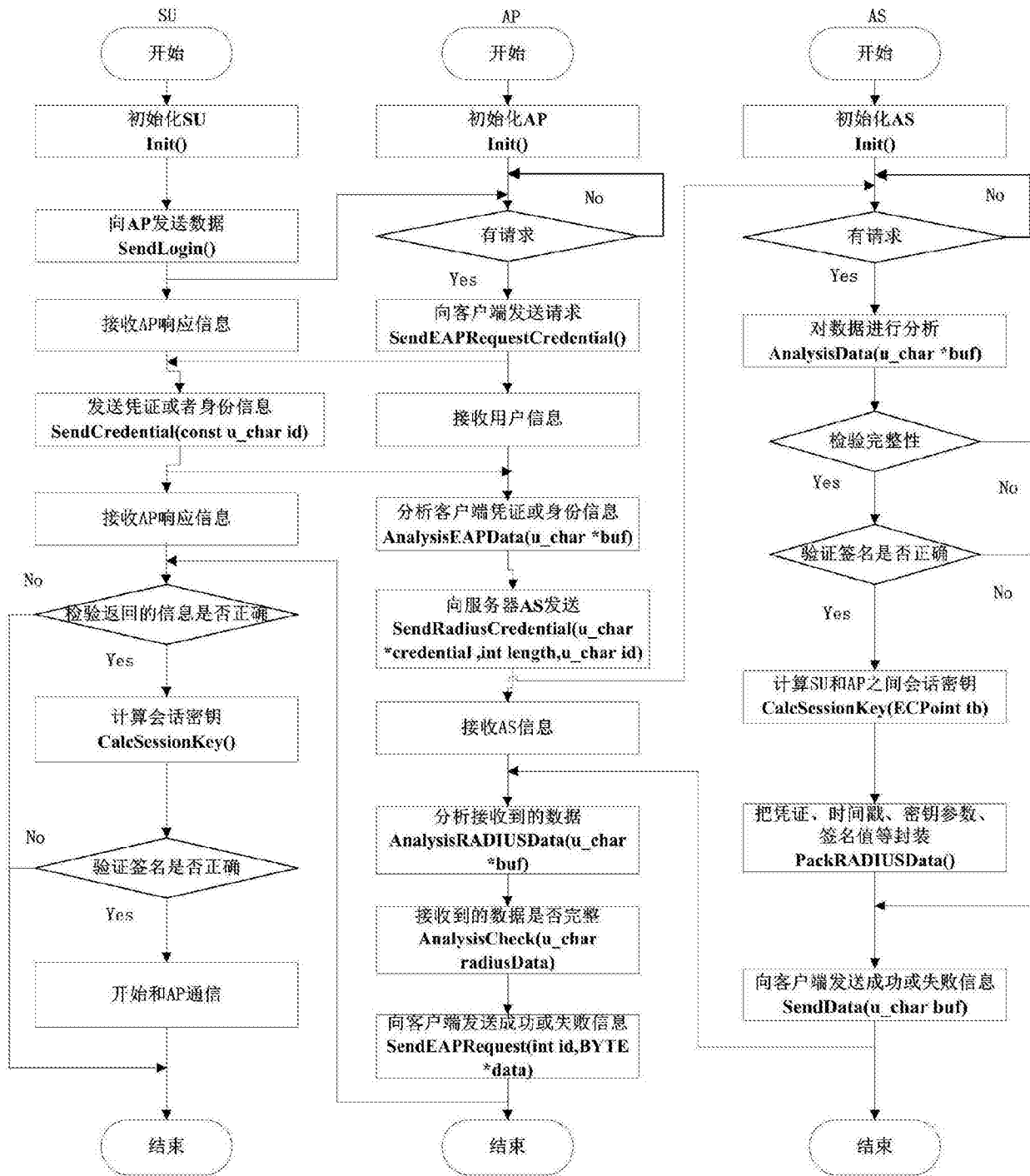


图8

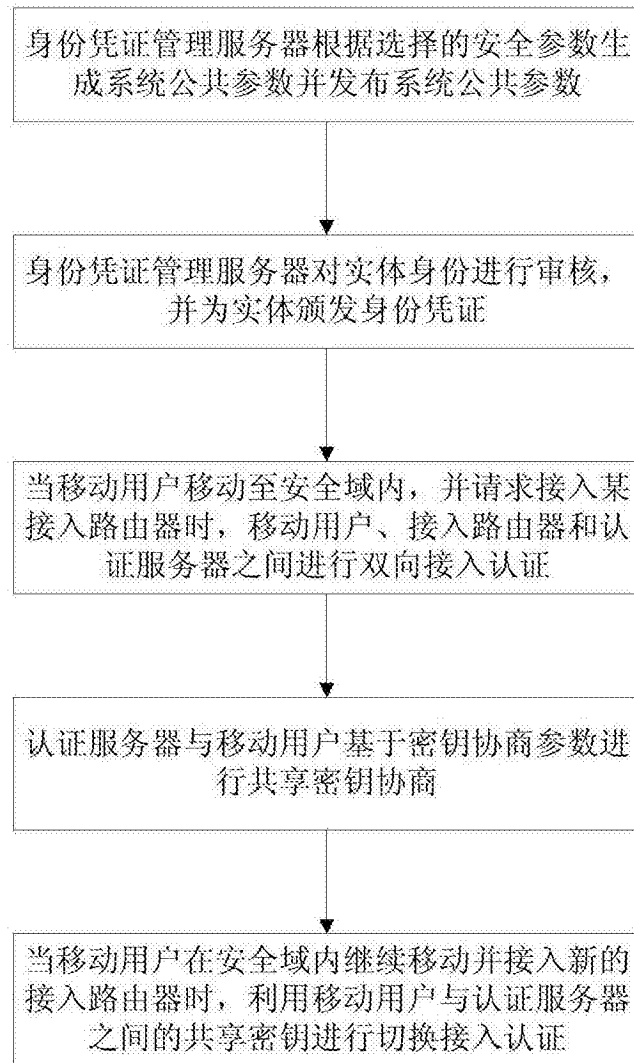


图9