基于国密技术的 WiFi 安全接入认证协议研究*

李建 陈积常 杨颖

南宁学院信息工程学院，南宁，530200

摘 要 分析 WiFi 环境下的网络安全风险，针对其存在的单向认证的弱点，基于国密技术的双向认证安全需求，设计了一套基于自主可控技术的 WiFi 安全接入系统的认证协议。该协议利用 SM2-SM4-SM3 国家商用密码算法、802.1x、数字签名、数字证书、CA 认证等技术，可以为 WiFi 安全接入系统提供安全接入认证。安全性分析和对比的结果表明，所提出的协议是有效的、安全的。

关键字 国密技术，WiFi，安全接入，系统模型，认证协议

Research on Authentication Protocol of WiFi Secure Access System Based on State Secret Technology

Li Jian Chen Jichang Yang Ying

School of Information Engineering
Nanning University
Nanning 530200, China
943667593@qq.com

Abstract—This paper analyzes the network security risks in WiFi environment. Aiming at the weakness of one-way authentication, based on the security requirements of two-way authentication of state secret technology, an authentication protocol of WiFi secure access system based on autonomous controllable technology is designed. This protocol uses SM2-SM4-SM3 national commercial cryptographic algorithm, 802.1x, digital signature, digital certificate, CA authentication and other technologies to provide secure access authentication for WiFi secure access systems. The results of security analysis and comparison show that the proposed protocol is effective and secure.

Key words— State secret technology, WiFi, Secure access , System model, Authentication protocol

1 引 言

随着网络技术的快速发展,无线 WiFi 广泛应用于家庭、商场、各类企事业单位，从而改善了传统的上网方式，人们实现了通过手机连接 WiFi 访问丰富的网络资源，大大降低了流量成本。但是在公共 WiFi 网络环境下，黑客通过截取、字典攻击等方式，截取和套取用户名、口令等敏感信息，给用户造成重大损失。因此，如何改进 WiFi 安全机制是迫在眉睫的重要研究课题。

无线 WiFi 接入安全应用的加密技术有 WEP 加密、WPA 加密等技术，对无线网络进行加密，WPA 协议保护无线网络(WiFi)安全，使用 TKIP 临时密钥协议，保证网络通信安全。WPA2 升级版，是 WiFi 联盟验证的 IEEE 802.11i 标准认证形式，提供对局域网的保护能力。除此之外，还采用了安全管理协议：四次握手和组密钥握手，它提供了 IEEE802.11 所不具备的密钥管理功能，还提供了更安全的双向认证[1]。

常见的针对 WiFi 的无线网络的入侵方式主要分为主动式攻击和被动式攻击。其中主动式攻击主要包括身份假冒、重放攻击、中间人攻击和拒绝服务攻击等，被动式攻击主要包括网络窃听和网络通信量分析等[2-4]。如果用户连接了攻击者搭建的网络，那么用户的一些敏感信息就会泄露出去，对用户的账户密码、财产、照片等信息造成了严重的威胁。例如，通过连接不良 WiFi 导致信息泄露和银行卡资金被盗的事件屡见不鲜。

对于 WiFi 环境中日益凸显的网络安全问题，国外主要从 WiFi 接入时的授权和数据的加密等两个方面展开研究，其中接入控制保证 WiFi 热点只能被认证后的用户接入，数据加密保证传输的数据只能被授权用

* **基金资助**：本文得到南宁学院一流专业培育项目（通信工程）(2020YLZYPY01)、南宁学院教学质量与教学改革工程项目（《网络安全》核心课程）(2022BKHXK09)资助.

户所接收和读取。为了进一步加强网络安全，早在2005年，我国密码学教授王小云带领团队对多种密码算法进行了研究，发现了当时被认为是上百万年找不出碰撞攻击的MD5和SHA-1等算法存在漏洞，引起了国际社会的巨大轰动。国外研究员ErikTews认为，WiFi网络使用的WiFi保护访问技术已经不再安全，他于2008年在15分钟内破解WPA加密技术[4]。事隔不久，WPA2于2010年上半年被黑客破解并在网上公布。

东南大学钱怡对比了IEEE 802.11和IEEE 802.11i两种协议标准的性能和安全性后，提出了一种改进的IEEE 802.11标准的WiFi安全接入的方案[5]。通过接入时的认证和授权来保障用户的接入安全。文献针对无线WiFi部署认证均各自为营、网络部署不标准、安全接入认证不统一及平台级的安全防护问题，分别对外网和内网的WiFi接入进行UID认证用户身份实现用户登录。然而我们正常情况下，一般是通过数字签名+数字证书来进行验证的。研究表明，国外密码算法存在诸多安全隐患，对于WiFi安全存在巨大的威胁。

本文通过分析WiFi用户接入认证和授权流程，发现WiFi接入面临的安全威胁，提出WiFi接入安全需求，构建基于国家商用密码技术的WiFi接入系统安全模型，设计WiFi安全接入认证协议，并用程序实现模型的用户身份认证功能，最后分析WiFi安全接入认证协议的安全性。

2 WiFi安全接入系统安全需求分析

2.1 802.1X协议概述

802.1X协议是一种基于端口的网络接入控制协议。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的用户设备进行认证和控制。

端口可以是一个物理端口，也可以是一个逻辑端口(如VLAN)。对于无线局域网来说，一个端口就是一个信道。802.1x认证的最终目的就是确定一个端口是否可用。连接在端口上的用户设备如果能通过认证，这个“端口”就打开了，意味着就可以访问局域网中的资源；如果不能通过认证，这个端口将保持“关闭”，则意味着无法访问局域网中的资源。

它的体系结构中包括3个部分，即请求者系统、认证系统和认证服务器系统，对应到无线局域网，即用户终端、无线接入点和认证服务器3部分[6]。

802.1X的认证系统工作方式又分为EAP中继方式和EAP终结方式与远端RADIUS服务器交互完成认证。当认证系统为EAP中继方式时，EAP（可扩展认证协议）承载在其它高层协议中，如EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP中继方式需要RADIUS服务器支持EAP属性：EAP-Message和Message-Authenticator，分别用来封装EAP报文及对携带EAP-Message的RADIUS报文进行保护。当认证系统工作于终结方式时，认证系统终结EAPoL消息，并转换为其它认证协议（如RADIUS、LDAP），传递用户认证信息给认证服务器系统[7]。

设备端为客户端提供接入局域网的端口，这个端口被划分为两个逻辑端口：受控端口和非受控端口。任何到达该端口的帧，在受控端口与非受控端口上均可见。非受控端口始终处于双向连通状态，主要用来传递EAPOL协议帧，保证客户端始终能够发出或接收认证报文。受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。

2.2 WiFi安全接入系统安全需求分析

（1）系统需求概述

随着网络的快速发展，无线WiFi在网络媒体、日常休闲、交通、安防等领域有着的广泛应用，对此在WiFi安全方面的需求也不断在增加。如今，大家都在数据透明的时代，如果没有固定的安全保护环境，就很容易遭受黑客的攻击，其中攻击的形式分为主动攻击和被动攻击。

主动攻击是攻击者通过网络线路将虚假信息或计算机病毒传入信息系统内部,破坏信息的真实性、完整性及系统服务的可用性,即通过中断、伪造、篡改、重放和重排信息内容造成信息破坏,使系统无法正常运行。包括拒绝服务攻击（DoS）、分布式拒绝服务（DDos）、信息篡改、资源使用、欺骗、伪装等攻击方法，对WiFi用户存在较大的网络安全，除此之外，主动攻击会利用大量的攻击包将带宽占满，使其合法网络包无法到达主机完成正常的访问。

被动攻击主要是攻击方通过在传输中偷听或者监视的手段，从传输中截取双方消息内容并对业务流进行分析，从而窃取到相关的密文信息再通过算法恢复出明文信息和有价值的信息，造成用户信息的泄露，对此威胁了数据的机密性。对此，我们需要对这些网络设备进行保护性措施，如隐私保护、数据安全保护、通信安全保护等,从而达到一定程度的安全预防作用。

（2）功能性需求

①通信双方的身份鉴别需求。WiFi认证中心负责接入网关、用户终端和ap/ac接入设备之间交换信息和数据时，首先需要对通信双方的身份真实性进行认证，以保证通信双方身份的真实性，有效防止非法第三方

混入WiFi接入系统进行篡改、恶意伪造、传播欺骗信息，从而满足WiFi用户接入接入系统和防范主动攻击的需要。

②关键数据存储的完整性和保密性需求。WiFi用户接入认证授权系统AP、AC、MDM、接入网关架构和移动应用设备构建密码应用架构。移动终端设备中存储的一些关键数据需要采用密码技术，以确保其机密性和完整性，防止数据丢失或非法篡改，并满足WiFi用户接入系统对被动攻击的要求。

③数据传输的完整性和保密性需求。由于通信双方之间的数据交换需要通过公网通道，因此需要采用密码技术，确保传输过程中的机密性和完整性保护，以满足WiFi用户接入系统对主动攻击和被动攻击的要求。

（2）非功能性需求

① 可扩展性：随着网络技术的广泛应用和各行业设备的快速发展，新的用户需求将不断涌现，这就要求系统安全模型具有良好的可扩展性，并可根据实际需要进行增减和配置。

② 性能需求：网络延迟和可预测的响应时间，并发用户支持当多个用户同时进入WiFi安全接入系统进行数据交换时，不会严重影响系统的传输性能。

3 WiFi 安全接入认证协议

3.1 WiFi安全接入认证协议设计

本文的协议WiFi安全接入认证协议的设计思路是：利用数字签名技术、SM2、SM3算法实现用户终端C和接入设备D、WiFi认证中心S三方之间的双向身份认证,认证通过后再利用自己的私钥对方公钥加密解密相关的数据。协议中用到的符号做如表1所示。协议流程图设计如图1所示。

表 1 协议通信符号说明

符号	说明
IDc	用户终端C身份
ID_D	接入设备D身份
IDs	WiFi认证中心S身份
T	时间戳
H	杂凑值
‖	拼接操作
Ex[Y]	用x对Y进行加密
Dx[Y]	用x对Y进行解密
Dpkc	用户终端C用SM2算法的公钥
Dskc	用户终端C用SM2算法的私钥
Dpk_D	接入设备D用SM2算法的公钥
Dsk_D	接入设备D用SM2算法的私钥
Dpks	WiFi认证中心S用SM2算法的公钥
Dsks	WiFi认证中心S用SM2算法的私钥
PASSWORD	口令

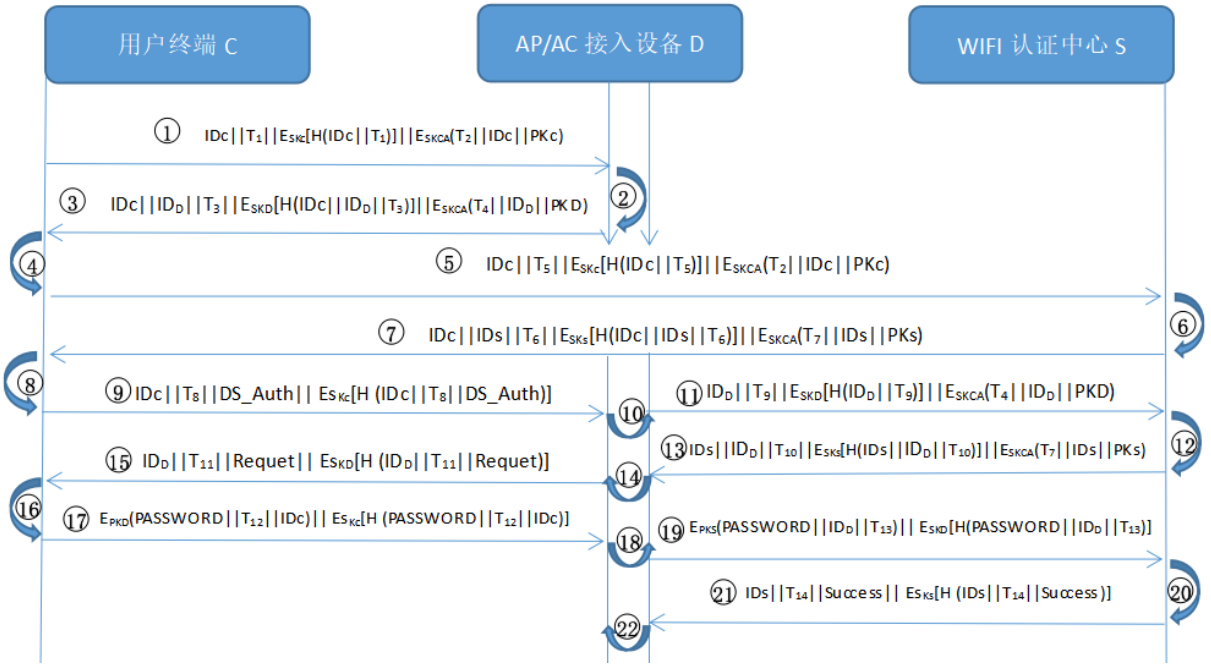

图 1 WiFi安全接入认证协议流程图

3.2 WiFi安全接入认证协议流程图说明

本文的 WiFi 安全接入认证协议流程图说明如下：

① $IDc||T_1||E_{SKC}[H(IDc||T_1)]||E_{SKCA}(T_2||IDc||PKc)$

其含义是：用户终端C向AP/AC接入设备D发送身份IDc、时间戳T_1、用户终端C对$IDc||T_1$进行签名，以及CA签发的用户终端C的证书$E_{SKCA}(T_2||IDc||PKc)$ 。

②AP/AC接入设备S对用户终端C进行身份鉴别的过程如下：

a. AP/AC接入设备通过CA的公钥验证用户终端C证书的真实性，形式表述如下：

$$CertC=D_{PKCA}[E_{SKCA}(T_2||IDc||PKc)]=T_2||IDc||PKc$$

b. 用AP/AC接入设备D的公钥验证C的签名，形式表述如下：

$$H_1=D_{PKC}[E_{SKC}(H(ID_C||T_1))]=H(ID_C||T_1)$$

c. AP/AC接入设备D计算哈希值H_2，形式表述如下：

$$H_2=H(ID_C||T_1)$$

d. 判断H_1、H_2是否相等，如果相等则AP/AC接入设备D确认对方就是用户终端C，否则无法确认对方的真实身份。

③ $IDc||ID_D||T_3||E_{SKD}[H(IDc||ID_D||T_3)]||E_{SKCA}(T_4||ID_D||PK_D)$

其含义是：AP/AC接入设备D向用户终端C发送身份、时间戳、D对$(IDc||ID_D||T_3)$的签名，以及CA签发的D的证书。

④用户终端C对AP/AC接入设备D进行身份鉴别：

a. 用CA的公钥验证AP/AC接入设备D证书的真实性，形式表述如下：

$$CertD=D_{PKCA}[E_{SKCA}(T_4||ID_D||PK_D)]=T_4||ID_D||PK_D$$

b.用AP/AC接入设备D的公钥验证D的签名，形式表述如下：

$$H_3=D_{PKD}[E_{SKD}(H(ID_C||ID_D||T_3))]=H(ID_C||ID_D||T_3)$$

c. AP/AC接入设备D计算哈希值H_4，形式表述如下：

$$H_4=H(ID_C||ID_D||T_3)$$

接着，判断H_3、H_4是否相等，如果相等则用户终端C确认对方就是AP/AC接入设备D，否则无法确认对方的身份。

⑤$ID_C||T_5||E_{SKC}[H(ID_C||T_5)]||E_{SKCA}(T_2||ID_C||PK_C)$

其含义是：用户终端C向WiFi认证中心S发送身份ID_C、时间戳T_5、C对$ID_C||T_5$的签名，以及CA签发的C的证书$E_{SKCA}(T_2||ID_C||PK_C)$ 。

⑥ WiFi认证中心S对用户终端C进行身份鉴别：

a. 用证书中心CA的公钥验证用户终端C证书的真实性；

b. 用用户终端C的公钥验证C的签名得到哈希值；

c. WiFi认证中心S计算哈希值；

d. 判断哈希值是否相等，如果相等采WiFi认证中心S则确认对方就是用户终端C，否则无法确认对方的身份。

⑦ $ID_C||ID_S||T_6||E_{SKS}[H(ID_C||ID_S||T_6)]||E_{SKCA}(T_7||ID_S||PK_S)$

其含义是：WiFi认证中心S向用户终端C发送身份、时间戳T6、S对$(ID_C||ID_S||T_6$的签名，以及CA签发的证书$E_{SKCA}(T_7||ID_S||PK_S)$ 。

⑧ 同②④⑥步骤，即用户终端C对对方进行身份鉴别；鉴别通过确认对方就是WiFi认证中心S。

⑨ $IDc||T_8||DS\_Auth||\ Es_{Kc}[H\ (IDc||T_8||DS\_Auth)]$）

其含义是：用户终端C向AP/AC接入设备D发送身份IDc、时间戳、DS_Auth认证信号

⑩AP/AC接入设备D对用户终端C发送过来的信号进行鉴别：

a. 用用户终端C的公钥验证C的签名，形式表述如下：

$$H_5=D_{PKC}[E_{SKc}[H\ (IDc||T_8||DS\_Auth))]$$
$$=H(IDc||T_1||DS\_Auth)$$

b. AP/AC接入设备D计算哈希值H_6，形式表述如下：

$$H_6=H(IDc||T_1||DS\_Auth)$$

c. 判断H_5、H_6是否相等，如果相等则确认该信号由用户终端C发送而来，否则无法确认该信息的来源。

⑪ $ID_D||T_9||E_{SKD}[H(ID_D||T_9)]||E_{SKCA}(T_4||ID_D||PK_D)$

其含义是：AP/AC接入设备D向WiFi认证中心S发送身份ID_D、时间戳T_8、D对$ID_D||T_9$的签名，以及CA签发的D的证书$E_{SKCA}(T_4||ID_D||PK_D)$。

⑫ 同②④⑥步骤，即WiFi认证中心S对对方进行身份鉴别；鉴别通过确认对方就是AP/AC接入设备D。

⑬ $IDs||ID_D||T_{10}||E_{SKs}[H(IDs||ID_D||T_{10})]||E_{SKCA}(T_7||IDs||PKs)$

其含义是：WiFi认证中心S向AP/AC接入设备D发

送身份、时间戳T_{10}、S对$IDs||ID_D||T_{10}$的签名，以及CA签发的S的证书$E_{SKCA}(T_7||IDs||PKs)$ 。

⑭ AP/AC接入设备D对对方进行身份鉴别；鉴别通过确认对方就是WiFi认证中心S。

⑮ $ID_D||T_{11}||Request||E_{SKD}[H(ID_D||T_{11}||Request)]$)

其含义是：AP/AC接入设备D向用户终端C发送身份、时间戳、D对$(ID_D||T_{11}||Request$的签名， ⑯同⑩步骤，用户终端C对对方发送的信息进行鉴别；鉴别发送的信息是AP/AC接入设备D发送过来的。

⑰ $E_{PKD}(PASSWORD||T_{12}||IDc)||Es_{Kc}[H$

$(PASSWORD||T_{12}||IDc)]$

其含义是：用户终端C使用SM3算法加密数据PASSWORD、T_{12}、IDc，对数据进行机密性和完整性保护；以及利用C的私钥使用SM2算法对M2、IDc、T_{12}的哈希值进行数字签名，作用是用户终端C发送到AP/AC接入设备D的信息不可抵赖。

⑱ AP/AC接入设备D执行以下操作：

a. 使用AP/AC接入设备D的私钥解密签名信息获取哈希值H13，计算哈希值

$H_7=H(PASSWORD||T_{12}||IDc)$

b. 用用户终端C的公钥解密签名信息获取哈希值H14，计算哈希值

$H_8=H(PASSWORD||T_{12}||IDc)$

c. 判断H13和H14是否相等，如果相等AP/AC接入设备D可确认该消息是由用户终端C发送的且没有被篡改，用户终端C对发送过来的数据无法抵赖；否则无法判断该消息是由用户终端C发送过来的。

⑲$E_{PKS}(PASSWORD||ID_D||T_{13})||E_{SKD}[H(PASSWORD||ID_D||T_{13})]$

其含义是：AP/AC接入设备D使用SM3算法加密数据PASSWORD、T_{13}、ID_D，对数据进行机密性和完整性保护；以及利用AP/AC接入设备D的私钥使用SM2算法对PASSWORD、ID_D、T_{13}的哈希值进行数字签名，作用是AP/AC接入设备D发送到WiFi认证中心S的信息不可抵赖。

⑳WiFi认证中心S执行以下操作：

a. 使用D的私钥解密签名信息获取哈希值H_9，计算哈希值

$H_9=H(PASSWORD||ID_D||T_{13})$

b. 用A的公钥解密签名信息获取哈希值H21，计算哈希值

$H_{10}=H(PASSWORD||ID_D||T_{13}$）

c. 判断H_9和H_{10}是否相等，如果相等WiFi认证中心S可确认该消息是由AP/AC接入设备D发送的且没有被篡改，D对发送过来的数据无法抵赖；否则无法判断该消息是由AP/AC接入设备D发送过来的。WiFi认证中心收到AP/AC接入设备发送的已加密的用户身份消息和经过加密运算后的口令信息与数据库进行比对。

㉑ $IDs||T_{14}||Success||Es_{Ks}[H(IDs||T_{14}||Success)$

对比成功后，WiFi认证中心S向AP/AC接入设备D发送身份信息、时间戳，及WiFi认证中心S用私钥对$IDs||T_{14}||Success$进行签名。

㉒同步骤⑩，AP/AC接入设备D鉴别该信息进行鉴别，如确认该信息来自WiFi认证中心S，则AP/AC接入设备D开放端口，用户终端C接入网络。

4 安全分析和方案比选

4.1 抗身份假冒攻击

本次方案由用户终端C和接入设备D、WiFi认证中心S三方之间都进行了双向身份认证,接入设备D的私钥由安全芯片内的随机数发生器生成，它存储在安全芯片的存储单元中,无法导出。受信任的第三方CA通过PKI技术发布用户的签名证书。证书包括用户的公钥,只有合法用户才能拥有与签名公钥对应的正确签名私钥[7]。用户终端C发送$ID_C||T_1||E_{SKC}[H(ID_C||T_1)]||E_{SKCA}(T_2||ID_C||PK_C)$ 给接入设备D。接入设备D通过验证$D_{PKC}[E_{SKC}(H(ID_C||T_1))]$是否等于$H(ID_C||T_1)$认证用户A的身份,其中用户D的运算涉及用户C的公钥。如果相等,则表明消息的确由持有私钥的合法用户C发送的。同样地,用户C通过计算$D_{PKD}[E_{SKC}(H(ID_D||ID_C||T_3))]$是否等于$H(ID_D||ID_C||T_3$） 认证用户D。因此，用户终端C和接入设备D之间实现了双向身份认证，同样原理，接入设备D与WiFi认证中心进行双方身份认证。如果黑客要伪造签名，他就要试图从对方的公钥获取对应的私钥，其难度就相当于求椭圆曲线上的离散对数，到目前为止，这个问题是无解的。也就是说只要签名方保护好自己的私钥，其他人就不能伪造他的签名，即不能伪造其身份。因此攻击者无法利用假冒攻击所提出协议的认证阶段[8]。

4.2 抗重放攻击

用户终端C发送给和接入设备D的认证请求中包含时间戳,时间戳是使用数字签名技术产生的数据，签名的对象包括了原始文件信息、签名参数、签名时间等信息。其消息为$ID_C||T_1||E_{SKC}[H(ID_C||T_1)]||E_{SKCA}(T_2||ID_C||PK_C)$，即由密文传输。因此,如果攻击者重放一条之前来自于用户终端C的消息给接入设备D,接入设备

D能够通过计算$D_{PKC}[E_{SKC}(H(ID_C||T_1))]$与$H(ID_C||T_1)$验证时间戳的新鲜性。因此,即使攻击者发送相同的消息给接入设备D,通过接入设备D验证时间戳的新鲜性确定其为非法用户。因此提出的协议可以防止重放和防篡改的攻击。

4.3 抗篡改攻击

该协议在通过双方身份认证时,身份信息经过了签名运算，如在用户终端端C与接入设备D的相互认证中$(ID_C||T_1||E_{SKC}[H(ID_C||T_1)]||E_{SKCA}(T_2||ID_C||PK_C))$，如果黑客改变了身份信息$ID_C$，在计算哈希值时，$H_1=H(ID_C||T_1)$就会改变，即不等于验证签名时等到的哈希值$H_2=H(ID_C||T_1)$，不能通过身份验证，接入设备D可以判断对方不是合法的用户终端C，或者用户终端C的身份信息在网络传输过程中被黑客篡改，或因为偶然原因引起改变，接入设备可以根据不同的情形来处理，或者按黑客攻击行为处理，直接断开网络连接，或者要求客户端重新发送身份认证信息。

如果黑客企图篡改身份信息的同时，篡改客户端的签名信息，那么他就要从客户端的公钥得到私钥，正如前述理由，这是不可行的。因此，公钥数字签名技术有效地抗击了黑客发起的篡改攻击，有效地保护了信息的完整性。

4.4 认证方案比较

参照GB/T39786-2021《信息安全技术 信息系统应用基本要求》，现将论文方案与参考文献[9]、[10]分身份验证、密码算法、安全协议、抵抗篡改攻击、抵抗假冒攻击、抵抗重放攻击、提供双向认证、抗密钥攻击、密码应用正确、密码应用合规、密码应用有效等方面进行比较，如表2所示。

表 2 各身份认证方案安全性能比较

安全性能	文献[9]方案	文献[10]方案	论文方案
身份验证	UID 证书	多因素认证	数字签名、数字证书
密码算法	MD5	SM2、SM3	SM2、SM3、SM4
安全协议	有	无	有
抵抗篡改攻击	是	是	是
抵抗假冒攻击	是	是	是
抵抗重放攻击	否	是	是
提供双向认证	否	否	是
抵抗密钥攻击	否	否	是
密码应用正确	否	是	是
密码应用合规	否	是	是
密码应用有效	否	否	是

对比表 2 的结果可以看出，文献[9]使用的是 UID 证书进行身份认证，且没有提供双向身份认证，存在着安全缺陷。文献[10]没有提供用户与电子身份认证系统交互消息安全防护。本文的方案提供了双向认证，采用国密算法 SM2/SM3/SM4，能防篡改、防假冒、防重放攻击，具有较高的安全性。

5 结束语

本文首先根据 WiFi 用户接入认证和授权流程，对 WiFi 用户接入认证和授权系统密码应用需求进行分析，结合 WiFi 接入安全需求，设计了 WiFi 安全接入认证协议，实现了通信双方的身份鉴别。本文分析了 WiFi 安全接入认证协议的安全性，并将本文提出的身份认证方案与文献[9]和[10]的身份认证方案进行了比较，对比结果表明，本文提出的身份认证方案在身份验证、密码算法、安全协议、抵抗篡改攻击、抵抗假冒攻击、抵抗重放攻击、提供双向认证、抗密钥攻击、密码应用正确、密码应用合规、密码应用有效等方面优于参考文献的方案。

参 考 文 献

[1] 李斌. WiFi 接入安全监控系统的研究[D]. 天津:天津理工大学,2015. DOI:10.7666/d.D632025

[2] Sanders C. Practical Packet Analysis[M]. 2ND EDITION. No Starch Press, Inc., 2011.

[3] Nichols RK, Lekkas PC. Wireless security[M]. New York: McGraw-Hill, 2002.

[4] Gu W,Yang Z,Que C, et al. On security vulnerabilities of null data frames in ieee 802.11 basedwlans[C]//The 28th International Conference on Distributed Computing Systems. IEEE press ,2008: 28-35.

[5] 钱怡.无线局域网安全接入控制方法的研究[5].南京：东南大学，2005

[6] 戴聪. 基于国密算法和模糊提取的多因素身份认证方案[J]. 计算机应用,2021,41(z2):139-145

[7] 秦亮. 基于 802.1x 协议网络认证系统的设计与实现[D]. 湖北:华中科技大学,2006.

[8] 吕良,李瑞. 基于数字签名和 SM2 算法的终端接入认证协商协议[J]. 计算机与数字工程,2021,49(3):530-535

[9] 蒋笑冰，胡福强，李 赟.铁路无线 WiFi 接入安全防护技术方案的研究[J].铁道通信信号，2017(3):49-53

[10] 陈亮,张鹏,陈旭翔,等. 基于统一账号认证的无线接入综合管理平台[J]. 电信工程技术与标准化,2010,23(6):48-51