基于国密技术的 Wi-Fi 安全通信模型设计*

黄爱玲 黄赢 李建**

南宁学院信息工程学院， 南宁 530200

摘 要 针对当前网络境下的网络安全问题，提出 Wi-Fi 安全通信需求，构建一种基于国密技术的 Wi-Fi 安全通信模型，并利用 SM2、SM3、SM4 国家商用密码算法、数字签名、数字证书等技术，设计了 Wi-Fi 安全通信协议。在双向认证的过程中，使用 SM3 国密算法对发送的身份信息、时间戳和证书进行哈希运算，实现了防篡改、防假冒、防重放等功能；在数据传输过程中，使用 SM4 国密算法加密数据，实现了防非法监听、保证数据的机密性等功能，从而提高了网络安全性能。实验结果验证了所提方案的有效性和可行性。

关键字 Wi-Fi 安全通信协议, CA, 数字签名,数字证书,国家商用密码算法

Design of Financial IC Card Issuing System Model Based on National Commercial Password Technology

Huang Ailing Huang Ying Li Jian

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

Abstract—Abstract—Aiming at the current network security issues in the network environment, this paper proposes the requirements for Wi-Fi secure communication, constructs a Wi-Fi secure communication model based on national security technology, and designs a Wi-Fi secure communication protocol using technologies such as SM2, SM3, and SM4 national commercial cryptographic algorithms, digital signatures, and digital certificates. In the process of bidirectional authentication, the SM3 national encryption algorithm is used to hash the identity information, timestamp, and certificate sent, achieving functions such as tamper resistance, anti-counterfeiting, and replay prevention. During the data transmission process, the SM4 national encryption algorithm is used to encrypt data, achieving functions such as preventing illegal listening and ensuring data confidentiality, thereby improving network security performance. Experiments results verify the effectiveness and feasibility of the proposed solution.

Keywords—Wi-Fi secure communication protocol, CA, Digital signature, Digital certificate, National commercial cryptography algorithm

1 引 言

随着信息技术的不断发展， Wi-Fi （Wireless Fidelity）[1]无线网络已经成为网络扩展的一种重要方式，它传播速度快是其最大的优点，而其凭借安装便捷、 开放性、可移动性等特点，被当代人广泛接受，同时 Wi-Fi 网络的安全性问题也越来越引发人们的关注,研究如何实现 Wi-Fi 安全通信是当务之急[2]。

Wi-Fi 通信面临的安全问题主要可以分成两类:一类是基于网络访问控制协议和漏洞进行的攻击。另一类是围绕无线网络环境本身的属性来进行的攻击。比如钓鱼 AP 导致的接入终端设备的信息面临泄露的风险，SSLStrip 中间人攻击导致的通信窃听和 DNS 欺骗导致的窃密行为。

Wi-Fi 网络所采用的安全机制大体可分为两种，即以早期 IEEE 802.11 协议为基础的安全机制与以 IEEE 802.11i 协议为基础的安全机制。IEEE 802.11 协议的安全子协议，即 WEP 链路加密协议，采用静态密钥管理机制，使用 24 位IV(初始向量)，且使用脆弱的 RC4 加密算法加密数据流，使得攻击者极易在分析后得到加密密钥。如 Fluhrer 等人就利用 WEP 数据帧的数据负载中第一个字节的可预测性与IV重放性等已知信息,成功的计算出了 WEP 帧所使用的加密密钥[3]。直到 WPA/WPA2 安全协议的出现才有效的制止了这一现象。WPA 是一种过渡协议，其采用 TKIP+MIC 的方法进行加密与校验。WPA2 使用更安全的 CCMP 取代了 TKIP+MIC 的安全机制，其使用基于 AES 的 CTR 进行数据加密以及 CBC-MAC 进行数据完整性校验。采用 WPA2 安全机制的 Wi-Fi 网络，即使攻击者使用彩

*基金资助：本文得到南宁学院一流专业培育项目(2020YLZYPY01) 和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。

**通讯作者：李建，教授，943667593@qq.com

虹表，专用字典并结合“内存-时间平衡”方法也很难进行破解。

文献[4]的研究表明，WPA2 安全加密协议已经被破解，其原因在于 WPA2 是一种保护所有现代 Wi-Fi 网络的安全加密协议，攻击者可以使用新颖的攻击技术来读取之前被认为是安全加密的信息。为此，新发布的安全标准 WPA3[5] 为支持 Wi-Fi 的设备进行重点改动，大大增强了配置、身份验证和加密功能。包括针对暴力破解攻击的防护功能、正向加密功能、个性化数据加密、增强关键网络防护性。

本文在研究分析 Wi-Fi 通信面临的安全风险的基础上，提出 Wi-Fi 安全通信需求，构建并实现一个安全的 Wi-Fi 通信模型。最后，通过实现模型的安全通信功能，进一步分析 Wi-Fi 通信协议的安全性。

2 Wi-Fi 安全通信系统模型需求分析

2．1 系统需求分析

目前无线网络已应用于人们生活的方方面面，比如公众的 internet 接入服务、移动警务、远程无线医疗等等。可以说，无线网络的安全问题涉及到我们每个人，因此，无线网络的安全问题也显得尤为重要，这些安全问题大致有以下几种[6]:

（1） 重传攻击。重传攻击是网络黑客截取网络中大量的数据，然后将这些数据重复回传给接收方，从而让数据大量充斥网络，造成网络拥堵，使得网络数据的传输速度变得缓慢，延长用户接受新信息的时间。这样反复多次地将大量数据传入网络就会造成网络出现问题，极易导致用户的信息丢失。网络黑客就趁网络出现问题时窃取用户信息或是篡改用户信息等，这种行为对用户的隐私安全构成威胁，严重时整个服务器会因攻击而瘫痪。

（2） 非法窃听。无线网络不同于传统的有线信息传输方式，在信息传递的过程中没有实体的通信渠道，因此网络黑客很容易通过先进的接收设备窃取网络中传输的信息，从而造成非法窃听现象的发生。这就导致了用户信息的遗失以及用户信息的泄露，也让用户的生活和工作遭遇极大的不便，同时也对信息安全构成威胁。

（3） 钓鱼攻击。无线网络遭遇钓鱼攻击[18]是指正常使用无线网络的情况下无意中访问了“钓鱼”网络链接，从而造成无线网络被袭击的安全问题。通常无线网络遭遇钓鱼攻击分为以下步骤 ：首先黑客创建一个虚假无线网络接入点并吸引终端用户接入该接入点，一旦用户进入此虚假接入点，则所使用的计算机电脑系统就可能被入侵或攻击等，导致的直接结果就是用户电脑上的机密文件、网银账号和网络账号等信息被盗以及电脑系统被病毒感染等一系列的网络安全威胁。

（4）假冒攻击是指两个方面[7]，一方面是指网络黑客利用无线网络的技术漏洞进行网络定位，利用虚拟网络假冒实体，从而对无线网络造成安全威胁；二是指网络黑客盗窃我国网络环境中存储的用户信息，篡改帐号和密码、冒用用户信息，给用户的信息安全带来威胁，导致整个无线网络的通信出现问题甚至完全瘫痪。

（5）无线 AP 被控制。无线 AP[8]通常指的就是无线网络的接入点，比如家庭、商店和企业都比较常见的无线路由器便是无线 AP 中的一种。无线 AP 被控制通常是指未经授权的非法分子窃取无线路由器管理权限。日常多见的无线 AP 被控制多是因为用户设置较为简单的无线 AP 密码。当用户的无线 AP 被他人入侵后，入侵者就能通过无线网络直接访问无线 AP 的终端管理界面，此时如果用户的无线 AP 密码设置的非常简单，那么入侵者就能随意更改和设置用户的无线 AP 的终端管理界面。

2．2 模型功能需求分析

（1）通信双方的身份鉴别需求。手机客户端、无线路由器、服务器和摄像头之间传输信息和数据时，首先要进行双方身份认证，以确保通信双方身份的真实，能够防止黑客侵入Wi-Fi安全通信系统进行假冒、篡改、传播虚假信息。

（2） 不可否认性需求。为了防止发送方或接收方否认发送或接收过某条信息，需要采用数字签名技术对数据进行处理,以保证双方的一致性。

（3） 数据传输机密性和完整性需求。作为一种安全的通信系统，最基本的要求便是确定数据的完整性和对数据保密，在通信双方进行数据交换时，使用密码技术将数据加密，确保数据在传输过程中得到保护。

3 基于国密技术的 Wi-Fi 安全通信模型

3．1 安全通信系统架构

Wi-Fi 安全通信系统由手机客户端、无线路由器、服务器和摄像头组成。通信流程：手机客户端通过连接无线路由器向摄像头获取数据。Wi-Fi 安全通信系统架构如图 1 所示。

（1）加密设备：主要包括由服务器部署的密码设备和无线路由器上部署的安全芯片。这些设备使用由国家商用密码算法，如 SM2、SM3 和 SM4 等进行密钥生成、加密等操作，以确保数据的机密性和完整性。

（2） 无线路由器：是 Wi-Fi 安全通信系统的核心设备之一，负责处理所有的安全、控制和管理任务，并提供全面的无线接入服务，包括移动管理、身份验证、VLAN 划分、数据包转发等。为了确保身份鉴别、数据传输确认、数据加解密的顺利进行，我们还需要利用调用密码设备来提供支持。

（3） 服务器：是整个系统的中枢。该设备负责数据存储、管理、分析、控制等功能，以及故障、配置、性能计费分析等工作。此外，服务器还可以承担大量数据信息存储、查询、分析和提供数据内容快速审计跟踪的作用。。

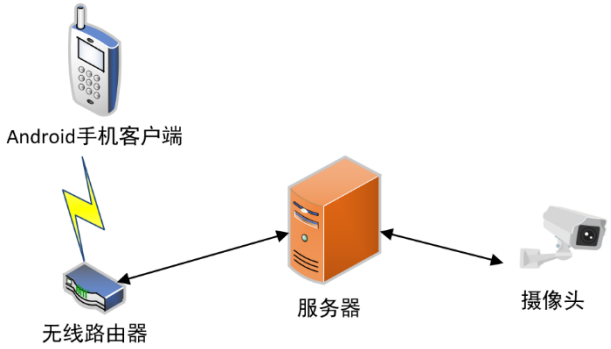

图 1 Wi-Fi 安全通信系统架构图

3．2 关键的数据

主要来自于摄像头获取的文件、图片、视频等数据。这些数据具有重要的价值，必须配备高水平计算机安全系统和数据传输技术，以保证数据的保密性和完整性。同时，还需要采取安全措施，防止网络攻击和其他事件对数据造成损害。

4 身份认证及数据传输密码应用工作流程

4．1 Wi-Fi 安全通信协议设计

本协议使用 SM2、SM3、数字签名技术以及数字证书实现手机客户端 T、无线路由器 R、服务器 S 和摄像头 C 之间的双向身份认证[9-10],认证通过后再使用 SM4 算法实现摄像头 C、服务器 S、无线路由器 R 和手机客户端 T 之间的数据传输[11-12]。协议通信符号说明如表 1 所示，Wi-Fi 安全通信协议流程如图 2 所示。

4．2 Wi-Fi 安全通信协议流程说明

(1) $ID_T||T_1||E_{SKT}[H(ID_T||T_1)]||E_{SKCA}(T_2||ID_T||PK_T)$

客户端T向路由器R发送身份ID_T、时间戳T_1、客户端T对$ID_T||T_1$进行签名$E_{SKT}[H(ID_T||T_1)]$，以及CA签发的客户端T的证书$E_{SKCA}(T_2||ID_T||PK_T)$ 。

(2) 路由器R对客户端T进行身份鉴别：

① 路由器R用CA的公钥验证客户端T证书真实性

$CertT=D_{PKT}[E_{SKCA}(T_2||ID_T||PK_T)]=T_2||ID_T||PK_T$

表 1 协议通信符号说明

符号	说 明
ID_T	手机客户端T身份
ID_R	无线路由器R身份
ID_S	服务器S身份
ID_C	摄像头C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
D_{PKT}	手机客户端T用SM2算法的公钥
D_{SKT}	手机客户端T用SM2算法的私钥
D_{PKR}	无线路由器R用SM2算法的公钥
D_{SKR}	无线路由器R用SM2算法的私钥
D_{PKS}	服务器S用SM2算法的公钥
D_{SKS}	服务器S用SM2算法的私钥
D_{PKC}	摄像头C用SM2算法的公钥
D_{SKC}	摄像头C用SM2算法的公钥
Data	数据
Datakey	SM4密钥

② 用客户端T的公钥验证T的签名

$H_1= D_{PKT}[E_{SKT}(H(ID_T||T_1))]=H(ID_T||T_1)$

③ 路由器R计算哈希值H_2

$H_2=H(ID_T||T_1)$

④ 判断H_1、H_2是否相等，如果相等则路由器R确认对方就是客户端T，否则无法确认对方的真实身份。

(3) $ID_R||ID_T||T_3||E_{SKR}[H(ID_R||ID_T||T_3)]||E_{SKCA}(T_4||ID_R||PK_R)$

路由器R向客户端T发送身份、时间戳T_3、R对$(ID_R||ID_T||T_3)$的签名$E_{SKR}[H(ID_R||ID_T||T_3)]$，以及CA签发的R的证书$E_{SKCA}(T_4||ID_R||PK_R)$。

(4) 客户端T对路由器R进行身份鉴别：

① 客户端T用CA的公钥验证路由器R证书真实性

$CertR= D_{PKR}[E_{SKCA}(T_4||ID_R||PK_R)]=T_4||ID_R||PK_R$

② 用路由器R的公钥验证R的签名

$H_3=D_{PKR}[E_{SKR}(H(ID_R||ID_T||T_3))]=H(ID_R||ID_T||T_3)$

③ 客户端T计算哈希值H_4

$H_4=H(ID_R||ID_T||T_3)$

④ 判断H_3、H_4是否相等，如果相等则客户端T确认对方就是路由器R，否则无法确认对方的身份。

(5) $ID_T||T_5||E_{SKT}[H(ID_T||T_5)]||E_{SKCA}(T_2||ID_T||PK_T)$

客户端T向服务器S发送身份ID_T、时间戳T_5、T对$ID_T||T_5$的签名E_{SKT} $[H(ID_T||T_5)]$，以及CA签发的T的证书$E_{SKCA}(T_2||ID_T||PK_T)$ 。

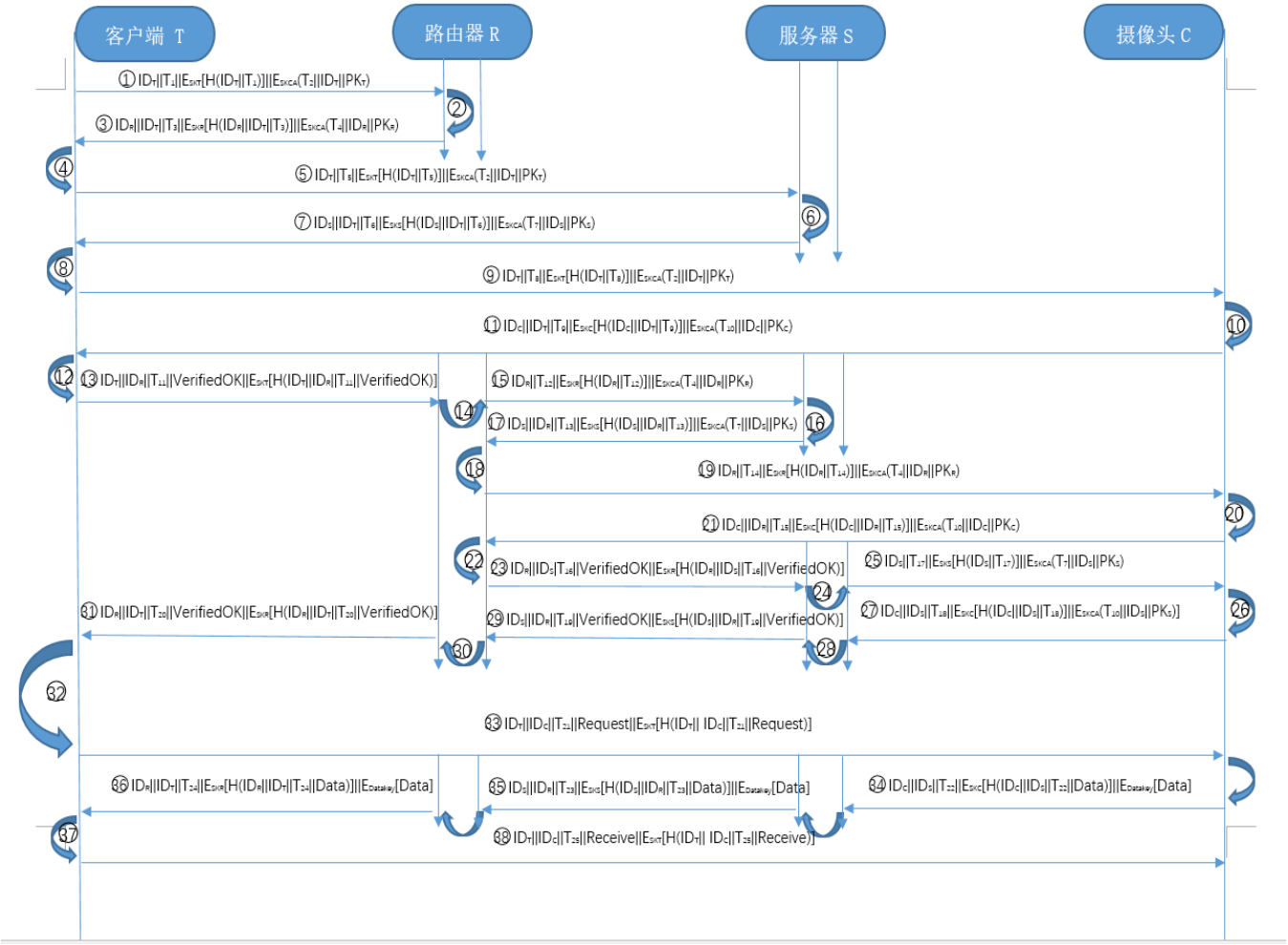

图 2 Wi-Fi安全通信协议流程

(6) 服务器S对客户端T进行身份鉴别：

① 服务器S用CA的公钥验证客户端T证书真实性

$CertT= D_{PKT}\ [E_{SKCA}(T_5||ID_T||PK_T)]=T_5||ID_T||PK_T$

② 用客户端T的公钥验证T的签名

$H_5=D_{PKT}[E_{SKT}(H(ID_T||T_1))]=H(ID_T||T_1)$

③ 服务器S计算哈希值

$H_6=H(ID_T||ID_S||T_3)$

④ 判断哈希值H_5、H_6是否相等，如果相等则服务器S确认对方就是客户端T，否则无法确认对方的身份

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

服务器S向客户端T发送身份、时间戳T6、S对$ID_T||ID_S||T_6$的签名$E_{SKS}[H(ID_S||ID_T||T_6)]$，以及CA签发的证书$E_{SKCA}(T_7||ID_S||PK_S)$ 。

(8) 同(2)、(4)、（6）步骤：客户端T对服务器S进行身份鉴别；鉴别通过客户端T确认对方就是服务器S。

(9) $ID_T||T_8||\ E_{SKT}\ [H(ID_T||T_8)]||E_{SKCA}(T_2||ID_T||PK_T)$

客户端T向摄像头C发送身份ID_T、时间戳T_8、T对$ID_T||T_8$的签名E_{SKT} $[H(ID_T||T_8)]$，以及CA签发的T的证书$E_{SKCA}(T_2||ID_T||PK_T)$。

(10) 同(2)、(4)、（6）步骤：摄像头C对客户端T进行身份鉴别；鉴别通过，摄像头C确认对方就是客户端T。

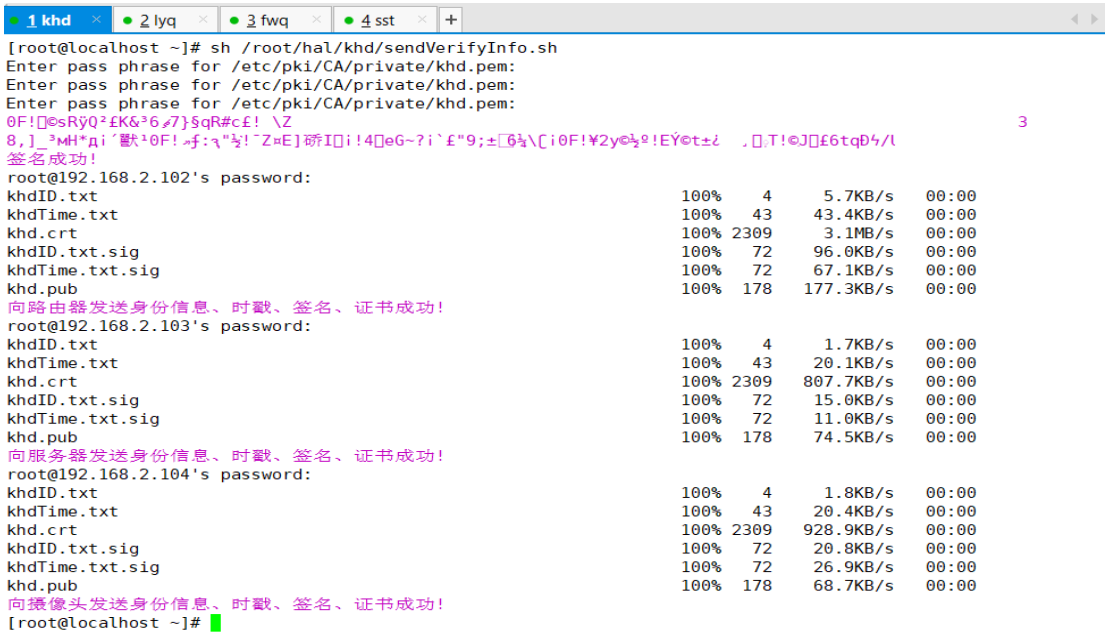

图 3 客户端 T 双向认证运行结果截图

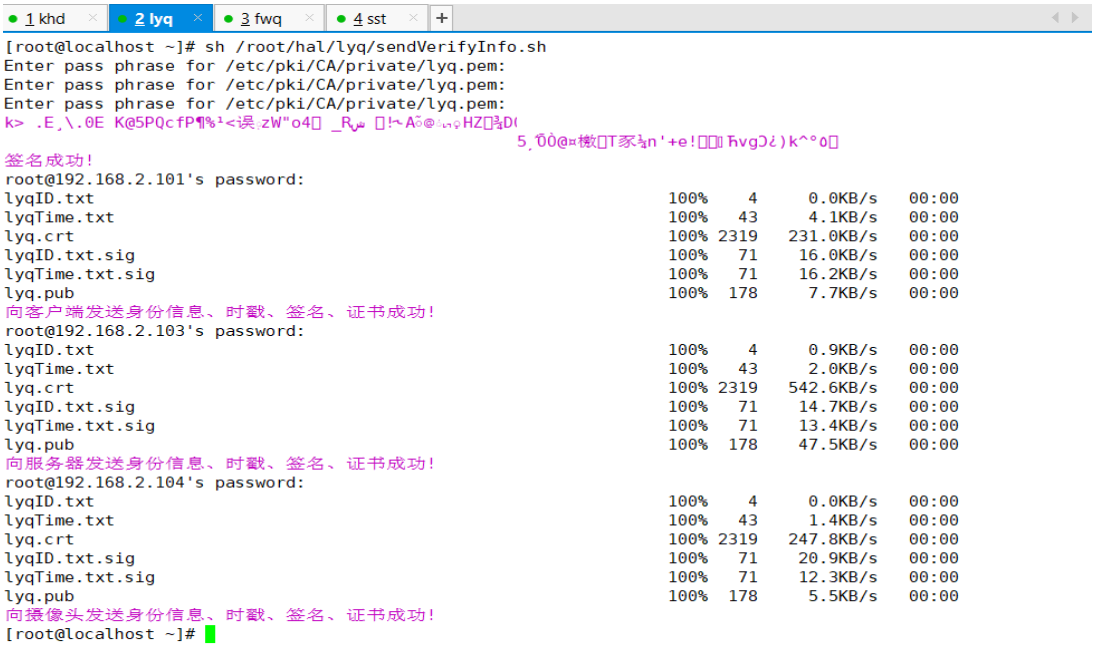

图 4 路由器 R 双向认证运行结果截图

图 5 客户端 T 数据请求下发运行结果截图

(11) $ID_C||ID_T||T_9||E_{SKC}[H(ID_C||ID_T||T_9)]||E_{SKCA}(T_{10}||ID_C||PK_C)$

摄像头C向客户端T发送身份、时间戳T9、C对$ID_C||ID_T||T_9$的签名$E_{SKC}[H(ID_T||ID_C||T_9)]$，以及CA签发的证书$E_{SKCA}(T_{10}||ID_C||PK_C)$。

(12) 同(2)、(4)、(6)步骤：客户端T对摄像头C进行身份鉴别；鉴别通过，客户端T确认对方就是摄像头C。

(13) $ID_T||ID_R||T_{11}||$Verified OK$||E_{SKT}[H(ID_T||ID_R||T_{11}||$Verified OK$)]$

客户端T向路由器R发送身份ID_T、时间戳T_{11}、确认信息、数字签名。

(14) 路由器R对客户端T发送过来的确认信息进行鉴别：

① 用客户端T的公钥验证A的签名

$H_7= D_{PKT}[E_{SKT}(H(ID_T||T_{11}||$Verified OK$))]$

$= H(ID_T||T_1||$Verified OK$)$

② 路由器R计算哈希值H_8

$H_8=H(ID_T||T_1||$Verified OK$)$

③ 判断H_7、H_8是否相等，如果相等则路由器R确认发送者就是客户端T，否则无法确认发送者的身份。

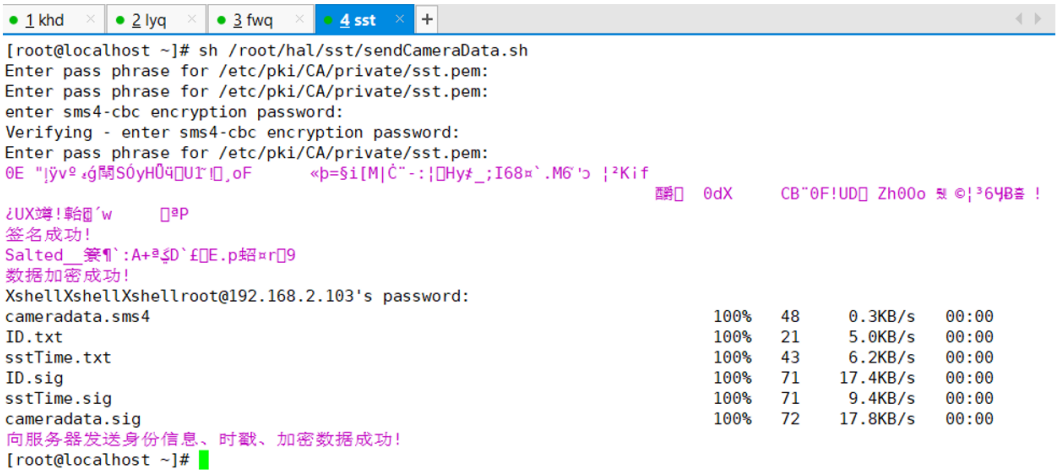

图 6 摄像头 C 加密数据传输运行结果截图

图 7 路由器 R 加密数据传输运行结果截图

(15) $ID_R||T_{12}||E_{SKR}[H(ID_R||T_{12})]||E_{SKCA}$

$(T_4||ID_R||PK_R)$

路由器R向服务器S发送身份ID_R、时间戳T_{12}、B对$ID_R||T_{12}$的签名$E_{SKR}[H(ID_R||T_{12})]$，以及CA签发的R的证书$E_{SKCA}(T_4||ID_R||PK_R)$。

(16) 同(2)、(4)、(6)步骤：服务器S对路由器R进行身份鉴别；鉴别通过,服务器S确认对方就是路由器R。

(17) $ID_S||ID_R||T_{13}||E_{SKS}[H(ID_S||ID_R||T_{13})]||E_{SKCA}$

$(T_7||ID_S||PK_S)$

服务器S向路由器R发送身份、时间戳T_{13}、C对$ID_S||ID_R||T_{13}$的签名$E_{SKS}[H(ID_S||ID_R||T_{13})]$，以及CA签发的S的证书$E_{SKCA}(T_7||ID_S||PK_S)$。

(18) 同(2)、(4)、(6)步骤：路由器R对服务器S进

行身份鉴别；鉴别通过,路由器R确认对方就是服务器S。

(19) $ID_R||T_{14}||E_{SKR}[H(ID_R||T_{14})]||E_{SKCA}(T_4||ID_R||PK_R)$

路由器R向摄像头C发送身份ID_R、时间戳T_{12}、R对$ID_R||T_{14}$的签名$E_{SKR}[H(ID_R||T_{14})]$，以及CA签发的R的证书$E_{SCA}(T_4||ID_R||PK_R)$。

(20) 同(2)、(4)、(6)步骤：摄像头C对路由器R进行身份鉴别；鉴别通过,摄像头C确认对方就是路由器R。

(21) $ID_C||ID_R||T_{15}||E_{SKC}[H(ID_C||ID_R||T_{15})]||E_{SKCA}(T_{10}||ID_C||PK_C)$

摄像头C向路由器R发送身份、时间戳T_{15}、C对$ID_C||ID_R||T_{15}$的签名$E_{SKC}[H(ID_C||ID_R||T_{15})]$，以及CA签发的C的证书$E_{SKCA}(T_{10}||ID_C||PK_C)$。

(22) 同(2)、(4)、(6)步骤：路由器R对摄像头C进行身份鉴别；鉴别通过,路由器R确认对方就是摄像头C。

(23) $ID_R||ID_S||T_{16}||$Verified OK$||E_{SKR}[H(ID_R||ID_S||T_{16}||$ Verified OK)]

路由器R向服务器S发送身份ID_R、时间戳T_{16}、确认信息、数字签名。

(24) 同(14)步骤：服务器S对路由器R发送过来的确认信息进行鉴别；鉴别通过，则服务器S确认发送者就是路由器R，否则无法确认发送者的身份。

(25) $ID_S||T_{17}||E_{SKS}[H(ID_S||T_{17})]||E_{SKCA}(T_7||ID_S||PK_S)$

服务器S向摄像头C发送身份ID_S、时间戳T_{17}、S对$ID_S||T_{17}$的签名$E_{SKS}[H(ID_S||T_{17})]$，以及CA签发的S的证书$E_{SKCA}(T_7||ID_S||PK_S)$。

(26) 同(2)、(4)、(6)步骤：摄像头C对服务器S进行身份鉴别；鉴别通过,摄像头C确认对方就是服务器S。

(27) $ID_C||ID_S||T_{18}||E_{SKC}[H(ID_C||ID_S||T_{18})]||E_{SKCA}(T_{10}||ID_C||PK_C)]$

摄像头C向服务器S发送身份ID_C、时间戳T_{18}、D对$ID_C||ID_S||T_{18}$的签名$E_{SKC}[H(ID_C||ID_S||T_{18})]$，以及CA签发的C的证书$E_{SKCA}(T_{10}||ID_S||PK_S)$。

(28) 同(2)、(4)、(6)步骤：服务器S对摄像头C进行身份鉴别；鉴别通过,服务器S确认对方就是摄像头C。

(29) $ID_S||ID_R||T_{19}||$Verified OK$||E_{SKS}[H(ID_S||ID_R||T_{19}||$Verified OK)]

服务器S向路由器R发送身份ID_S、时间戳T_{19}、确认信息、数字签名。

(30) 同(14)步骤：路由器R对路服务器S发送过来的确认信息进行鉴别；鉴别通过，则路由器R确认发送者就是服务器S，否则无法确认发送者的身份。

(31) $ID_R||ID_T||T_{20}||$Verified OK$||E_{SKR}[H(ID_R||ID_T||T_{20}||$ Verified OK)]

路由器R向客户端T发送身份ID_R、时间戳T_{20}、确认信息、数字签名。

(32) 同(14)步骤：客户端T对路由器R发送过来的确认信息进行鉴别；鉴别通过，则客户端T确认发送者就是路由器R，否则无法确认发送者的身份。

(33) $ID_T||ID_C||T_{21}||$Request$||$ $E_{SKT}[H(ID_T||$ $ID_C||T_{21}||$ Request)]

客户端T向摄像头C发送身份ID_T、时间戳T_{21}、数据请求、数字签名E_{SKT} $[H(ID_T||$ $ID_C||T_{21}||$Request)]。

(34) $ID_C||ID_S||T_{22}||E_{SKC}[H(ID_C||ID_S||T_{22}||$Data)] $||E_{Datakey}$[Data]

摄像头C生成Data向服务器S发送身份ID_C、时间戳T_{22}、数字签名$E_{SKC}[H(ID_C||ID_S||T_{22}||$Data)]、以及SM4密钥Datakey加密的数据Data。

(35) $ID_S||ID_R||T_{23}||E_{SKS}[H(ID_S||ID_R||T_{23}||$Data)]$||E_{Datakey}$[Data]

服务器S向路由器R发送身份ID_S、时间戳T_{23}、数字签名$E_{SKS}[H(ID_S||ID_R||$ $T_{23}||$Data))]、以及SM4密钥Datakey加密的数据Data。

(36) $ID_R||ID_T||T_{24}||E_{SKR}[H(ID_R||ID_T||T_{24}||$Data)]$||E_{Datakey}$[Data]

路由器R向客户端T发送身份ID_R、时间戳T_{24}、数字签名$E_{SKR}[H(ID_R||ID_T||T_{24}||$Data)]、以及SM4密钥Datakey加密的数据Data。

(37) $D_{Datakey}[E_{Datakey}[Data]]$=Data

客户端T用SM4密钥Datakey解密得到数据Data。

(38) $ID_T||ID_C||T_{25}||$Receive$||$ $E_{SKT}[H(ID_T||$ $ID_C||T_{25}||$ Receive)]

客户端T向摄像头C发送身份ID_T、时间戳T_{25}、数据接收、数字签名E_{SKT} $[H(ID_T||$ $ID_C||T_{25}||$Receive)]。

4．3 安全性分析

（1） 抗身份假冒攻击

该协议通过客户端 T、路由器 R、服务器 S 和摄像头 C 之间的双向身份认证来抗拒身份假冒攻击。在认证过程中，客户端 T 向路由器 R 发送

IDT||T1||ESKT[H(IDT||T1)]||ESKCA(T2||IDT|| PKT)。路由器 R 通过验证 DPKT [ESKT (H(IDT||T1))] 和 H(IDT||T1)是否相等来认证客户端 T 的身份, 其中路由器 R 利用了客户端 T 的公钥进行运算。同样地,客户端 T 也能通过计算 DPKR [ESKT (H(IDR||IDT|| T3))]是否等于 H(IDR||IDT||T3）来认证路由器 R 的身份。服务器 S 和摄像头 C 之间也是同理。黑客如果想伪造签名，则需要从对方的公钥获取对应的私钥，其难度很高，几乎无法完成这一级别的破解攻击。

（2） 抗重放攻击

为了避免重放攻击，客户端 T 在向路由器 R 发送认证请求时会包含时间戳。该时间戳是使用数字签名技术产生的数据，并能够验证消息是否实时。客户端 T 发出的消息内容为 IDT||T1|| ESKT H(IDT||T1)]||ESKCA(T2||IDT||PKT)，消息以密文传输的。因此，如果黑客试图重放以前来自客户端 T 的消息给路由器 R，则路由器 R 可以通过计算 DPKT [ESKT (H(IDT||T1))]与 H(IDT||T1)验证时间戳的新鲜性。因此，即使攻击者发送相同的消息给路由器 R，路由器 R 验证时间戳的新鲜性，以确定其是否为非法用户。

（3） 抗篡改攻击

该协议抗击黑客发起的篡改攻击。当完成双方身份认证时，协议会对身份信息进行数字签名运算。例如，在客户端 T 和路由器 R 之间的双向认证过程中，消息内容为(IDT||T1|| ESKT [H(IDT||T1)]||ESKCA(T2|| IDT||PKT))，如果黑客改变了身份信息 IDT，则 H1=H(IDT||T1)将会改变，从而导致无法通过身份验证。在这种情况下，路由器 R 可以判断对方不是合法客户端 T 或者客户端 T 的身份信息被黑客篡改了。如果黑客试图同时篡改身份信息和客户端的签名信息，则需要从客户端的公钥获取私钥。然而，这是由于离散对数问题的存在该难度很高，因此使用公钥数字签名技术有效地抵抗了黑客发起的篡改攻击，并保护了信息的完整性。

（4） 防非法窃听

该协议有效防止非法窃听。在数据传输时，使用 SM4 加密密钥加密数据，如摄像头 C 与服务器 S 的传输，SM4 算法属于对称密钥算法，其加密密钥与解密密钥相同且数据加解密速度快，适用于数据量大的场景。如果黑客使用非法手段窃取到了传输的数据，就必须要使用相同 SM4 密钥对数据进行解密，否则得到的只是一串无法解析的乱码密文。

4．4 代码运行测试

为了验证本文设计的的可行 ing，我们基于 Linux 操作系统，使用 Xshell 终端模拟软件和 GmSSL 密码工具箱，编码实现了 Wi-Fi 安全通信系统的功能模块和安全通信协议。四方双向身份鉴别和数据传输实现的代码运行的部分结果如图 3~图 7 所示。从代码运行的结果来看，本文设计的 Wi-Fi 安全通信模型是可行和有效的。

5 结束语

本文通过对 Wi-Fi 安全通信流程的分析，提出了国密技术在 Wi-Fi 安全通信领域的应用需求，并构建了基于国密技术的 Wi-Fi 安全通信模型。安全性分析结果表明，该模型能够实现通信双方的身份认证、关键数据传输的保密性和完整性。本文使用 Xshell 终端模拟软件和 GmSSL 密码工具箱，成功实现了模型的身份认证及数据传输功能，代码运行结果说明了 Wi-Fi 安全通信协议的安全性和有效性。

参 考 文 献

[1] 刘岳.Wi-Fi 网络安全现状与攻防策略研究[J]．电脑知识与技术，2017,(6)：47-50.

[2] 谭悦平.Wi-Fi 无线网络的安全与防范措施探讨[J]．信息与电脑，2018,(9)：192-193，196.

[3] 黎云芽.基于 Wi-Fi 的无线网络安全分析[J].电子世界，2018,(18)：75，77.

[4] 俞灵琦.你所连接上的 WI-FI 是否安全[J].华东科技,2017,(12)：72-73.

[5] 姜唐.Wi-Fi 联盟发布新一代 WPA3 安全标准[J]．计算机与网络，2018,(7)：51.

[6] 刘东.基于 Wi-Fi 技术的无线网络安全问题及对策[J].智能建筑与智慧市,2018，(9):27-28.

[7] 黄院平，吴越，孟凡超.公共 Wi-Fi 安全检测技术研究与实现[J]．微型电脑应用，2017，(4):1-3，8.

[8] 刘怡然，刘倩，刘元昕.基于校园 WI-FI 无线网络的安全方案研究[J].自动化与仪器仪表，2017,(9):30-31,34.

[9] 蒋笑冰，胡福强，李赟.铁路无线 Wi-Fi 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] 宋晓锐.一种基于 Wi-Fi 的数据安全传输系统的设计与实现[D]. 大连：大连海事大学,2018.