基于国密技术的 WiFi 安全接入系统的实现*

杨颖 李建** 陈积常

南宁学院信息工程学院，南宁，530200

摘 要 基于国密技术，在 Linux 操作系统平台上实现了一个 WiFi 安全接入系统的样机系统。该系统使用 Xshell 终端模拟软件、PKI 技术、GmSSL 密码工具箱搭建了数字证书机构 CA，为用户终端、接入设备、WiFi 认证中心颁发了数字证书，为用户身份认证提供了网络信任环境。性能测试结果表明，系统了实现防篡改、防假冒、防抵赖、防重放、防泄密等功能，提高了网络安全性能。

关键字 国密技术，WiFi，安全接入系统，Linux，数字证书

Implementation of the WiFi Secure Access System Model based on State Secret Technology

Yang Ying Li Jian Chen Ji Chang

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

Abstract—Based on the state secret technology, a WiFi secure access system was implemented on the Linux operating system platform. The system used Xshell terminal simulation software, PKI technology and GmSSL password toolbox to build a digital certificate authority(CA), which issues digital certificates to user terminals, access devices and WiFi certification centers, and provides a network trust environment for user identity authentication. The performance test results show that the system realizes the functions of anti tampering, anti counterfeiting, anti repudiation, anti replay and anti disclosure, and improves the network security performance.

Key words— State secret technology, WiFi, Secure access system,Linux, Certificate authority

1 引 言

近几年，无线网络的发展使得网络信息传输量急剧增加，以无线网络为主要架构的网络环境日益凸显出来。无线网络的应用大大方便了人们的日常工作、生活的需求，但是也给黑客提供了便利。黑客可以通过嗅探窃取无线网络上他人的账户信息，也可以通过架设一个 WiFi 钓鱼热点来获取他人的敏感信息[1]。因此，为了保护无线网络环境中用户的安全，如何在无线网络构建一个 WiFi 安全接入系统是一项非常重要而且有意义的工作。

目前，国内在无线网络安全接入系统方面的研究成果不是很多。文献[2]对长距离无线网络安全接入技术进行分析研究。文献[3] 从用户身份认证、加密传输协议、无线入侵检测、安全管理制度等四个方面入手，对无线办公网络的安全性进行研究，从方便管理的角度，提出一个能保证无线办公网络的整体方案。在电力系统方面，为了保证电力网络的安全，人们分析了电力监控系统无线接入安全风险[4]，设计了基于无线网络的能源电厂安全接入平台[5]，提出了实现网络安全接入的技术方案[6][7]。

在 WiFi 无线网络方面，文献[8]设计实现了一种 WiFi 网络环境下的安全监控系统，通过 VPN 集群来保障用户接入安全。该系统在用户和 WiFi 之间加入一个安全网关并对用户上网产生的流量进行实时检测来保障用户上网安全。文献[9]对轨道交通 Wi-Fi 服务网络构架进行研究，提出了一个考虑移动用户安全接入的对总体技术方案。但是，目前鲜见利用国家商用密码算法实现 WiFi 安全接入系统的研究与开发成果。

本文利用国家商用密码算法 SM2-SM3-SM4[5-9]，运用 Linux 操作系统、SHELL 脚本编程技术、PKI 技

* **基金资助**：本文得到南宁学院一流专业培育项目（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.
**通讯作者：李建，教授，943667593@qq.com

术、MySQL 数据库管理技术、数字签名技术，搭建 WiFi 安全接入运行环境，实现通信双方的身份鉴别和数据传输的机密性和完整性保护。

2 WiFi 安全接入系统架构设计

2.1 WiFi安全接入系统架构

WiFi 接入安全系统是对移动终端用户设备信息进行认证、管理及宽带访问、安全控制、实时监控、告警和数据分析的信息认证授权系统，系统由 WiFi 认证中心、无线 AP/AC 接入设备、和用户终端组成。具备易扩展性、安全性好、便于集中管理的特点，对实时性通信成功率要求高。为防范系统执行数据转发操作时，出现非法用户伪造截获、重用、篡改关键数据等风险，密码应用架构设计的重点在于 WiFi 认证中心和无线 AP/AC 接入设备之间的身份鉴别，以及系统关键数据在传输过程中的保密性和完整性保护。

WiFi 用户接入安全模型分为用户终端、无线 AC/AP 接入层、WiFi 认证三层，WiFi 安全接入系统整体架构与密码应用部署如图 1 所示。

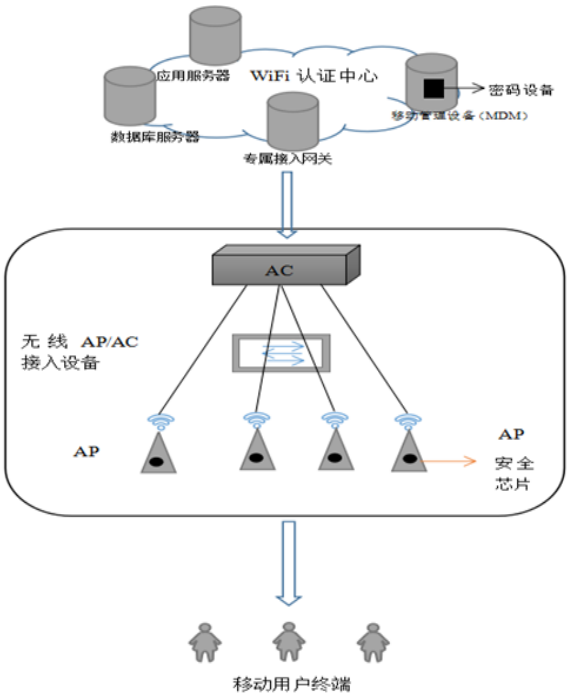

图 1 WiFi 安全接入系统整体架构与密码应用部署

（1） WiFi 认证中心主要由接入网关、应用服务器、数据服务器、移动管理设备、密码设备组成，主要实现数据存储、管理、分析、控制功能。接入网关提供网络通信通畅；应用服务器负责实现故障、配置、性能计费和处理分析数据的功能；数据服务器用于大量数据信息存储、查询、分析的数据运算中心；移动管理设备用于从一个或多个源系统识别并整合重复记录，对宽泛的单元格级别关联和历史记录，为数据内容提供了详细的审计跟踪，提供完整的移动设备生命周期；密码设备负责利用国家商用密码算法进行密钥生成、存储、导入、导出和加密操作。

（2） 用户终端和接入设备负责集中处理所有的安全、控制和管理、完成无线接入的功能，例如移动管理、身份验证、VLAN 划分、数据包转发等，并通过调用密码设备来提供身份鉴别、数据传输确认、数据加解密和完整性验证服务。

2.2 重要设备和关键数据

（1） WiFi 用户接入系统密码设备

密码设备：部署在 WiFi 认证中心的移动管理设备上，使用 SM2、SM3 和 SM4 等国家商用密码算法进行密钥生成、存储、导入、导出和加密操作。

安全芯片：部署在 AC/AP 接入设备中，以保护数据的机密性和完整性，并识别设备身份，使用国家商用密码算法，如 SM2、SM3 和 SM4。

（2） 系统服务器

数据库服务器：用于大量数据信息存储、查询、分析的数据运算中心。

接入网关服务器：用于维护公共网络通信信道的链路畅通；

移动管理设备（MDM): 用于从一个或多个源系统识别并整合重复记录，对宽泛的单元格级别关联和历史记录，为数据内容提供了详细的审计跟踪，提供完整的移动设备生命周期。

应用服务器：负责实现故障、配置、性能计费和处理分析数据的功能。

（3） 系统应用

AP/AC 应用：用于集中处理所有的安全、控制和管理、完成无线接入的功能，例如移动管理、身份验证、VLAN 划分、数据包转发等，并通过调用密码设备来提供身份鉴别、数据传输确认、数据加解密和完整性验证服务。

（4） 系统关键数据

用户业务数据：由多个无线网络用户接入 AP/AC 的数据信息，包括实时、统计及异常事件记录、用户信息数据等业务信息，提供完整性需求。

参数业务数据：AP/AC 接入设备的配置信息，可以控制数据传输格式和同步方式，提供机密性和完整性需求。

控制业务数据：控制 AP/AC 接入设备执行动作的程序指令数据，安全需求为同时满足保密性和完整性。

3 样机系统的实现

3．1 实现的环境与工具

WiFi 安全接入协议实现是基于 Linux 操作系统，使用 Xshell 终端模拟软件和 GmSSL 密码工具箱。Xshell 是一款终端模拟器，功能强大且安全，它支持 SSH1、SSH2 协议及 RSA 公开密钥的用户认证方法，并支持加密所有流量的加密算法，可通过互联网到远程主机的安全连接以及它创新性的设计和特色来帮助用户在极其复杂的网络环境当中进行工作与模拟。

GmSSL 是一个开源的密码工具箱，支持 SM2/SM3/SM4/SM9/ZUC 等国家商用密码算法、SM2 国密数字证书及基于 SM2 证书的 SSL/TLS 安全通信协议，支持国密硬件密码设备，提供符合国密规范的编程接口与命令行工具，可以用于构建 PKI/CA、安全通信、数据加密等符合国密标准的安全应用。GmSSL 项目是 OpenSSL 项目的分支，并与 OpenSSL 保持接口兼容。因此 GmSSL 可以替代应用中的 OpenSSL 组件，并使应用自动具备基于国密的安全能力。

3.2 三方双向身份鉴别

首先 CA 颁发机构为用户终端和接入设备的公钥做认证，获取数字证书。因为数字证书是经过权威机构认证的，所以公钥具有安全性、唯一性。数字证书是双方通信时，在签名后再加上数字证书就可以对对方的身份进行鉴别来确保消息的真实可靠性。

三方双向身份鉴别的实现过程如下：

Step1：CA 自签根证书。首先 CA 机构 touch /etc/pki/CA/index.txt 生成证书索引数据库文件（index.txt）并 echo 01 > /etc/pki/CA/serial 指定第一个颁发证书的序列号，然后 CA 生成 SM2 私钥并加密私钥（cakey.pem），生成证书申请请求自签发生成根证书（cacert.pem）。

Step2：CA 签发用户终端 C 证书。利用 sm2 算法加密用户终端 C 的私钥（c.pem）,随后生成包含用户终端 C 的相关信息和公钥的证书申请文件（c.csr），然后把证书申请文件发送给 CA 进行签发。CA 用根证书和私钥为用户终端 C 签署证书（c.crt）。待 CA 签署完毕之后将证书传送给用户终端 C。

Step3：CA 签发 AP/AC 接入设备 D 证书。利用 sm2 算法加密 AP/AC 接入设备 D 的私钥（d.pem），随后生成包含 AP/AC 接入设备 D 的相关信息和公钥的证书申请文件（d.csr），然后把证书申请文件发送给 CA 进行签发。CA 用根证书和私钥为 AP/AC 接入设备 D 签署证书（d.crt）。待 CA 签署完毕之后将证书传送给 AP/AC 接入设备 D。

Step4：CA 签发 WiFi 认证中心 S 证书。利用 sm2 算法加密 WiFi 认证中心 S 的私钥（s.pem）,随后生成包含 WiFi 认证中心 S 的相关信息和公钥的证书申请文件（s.csr），然后把证书申请文件发送给 CA 进行签发。CA 用根证书和私钥为 WiFi 认证中心 S 签署证书（s.crt）。待 CA 签署完毕之后将证书传送给 WiFi 认证中心 S。

Step5：用户终端 C 使用 SM3 算法对身份信息、时戳、证书进行哈希运算生成摘要，再使用私钥加密哈希值形成签名，然后分别发送到 AP/AC 接入设备 D、WiFi 认证中心 S。

Step6：AP/AC 接入设备 D 使用 SM3 算法对身份信息、时戳、证书进行哈希运算生成摘要，再使用私钥加密哈希值形成签名，然后分别发送到用户终端 C、WiFi 认证中心 S。

Step7：WiFi 认证中心 S 使用 SM3 算法对身份信息、时戳、证书进行哈希运算生成摘要，再使用私钥加密哈希值形成签名，然后分别发送到 AP/AC 接入设备 D、用户终端 C。

Step8：用户终端 C 从 D 证书、S 证书提取 CA 公钥，然后用 CA 的公钥验证 D 证书、S 证书的真实性，显示 Verified OK 则 D 证书、S 证书验证成功；用户终端 C 用 D 的公钥和 S 的公钥分别校验 D、S 的签名，显示 Verified OK 则 D、S 签名验证成功。

Step9：AP/AC 接入设备 D 从 C 证书、S 证书提取 CA 公钥，然后用 CA 的公钥验证 C 证书、S 证书的真实性，显示 Verified OK 则 C 证书、S 证书验证成功；AP/AC 接入设备 D 用 C 的公钥和 S 的公钥分别校验 C、S 的签名，显示 Verified OK 则 C、S 签名验证成功。

Step10：用户终端 C 用自己的私钥加密认证信号、时戳然后发送到 AP/AC 接入设备 D，通知 AP/AC 接入设备 D 与 WiFi 认证中心进行双向认证。

Step11：接入设备 D 收到用户终端 C 的认证信号后使用 C 的公钥查看认证信号是否发生篡改，验证显示 Verified OK ，认证信号无篡改，D 即将开始双向认证操作。

Step12：WiFi 认证中心 S 从 C 证书、D 证书提取 CA 公钥，然后用 CA 的公钥验证 C 证书、D 证书的真实性，显示 Verified OK 则 C 证书、D 证书验证成功；WiFi 认证中心 S 用 C 的公钥和 D 的公钥分别校

验 C、D 的签名，显示 Verified OK 则 C、D 签名验证成功。

3. 3 身份信息和口令传输

Step1：AP/AC 接入设备 D 用自己的私钥加密身份信息和口令请求消息，然后发送到用户终端 C，通知用户终端发送身份信息与口令。

Step2：用户终端 C 接收到接入设备 D 的身份信息和口令请求消息后使用接入设备 D 的公钥查看身份信息和口令请求消息是否发生篡改，显示 Verified OK，消息无篡改，即将发送身份信息及口令至接入设备 D。

Step3：用户终端 C 分别用自己的私钥和 D 的公钥加密身份信息和口令，然后发送到 AP/AC 接入设备 D。

Step4：AP/AC 接入设备 D 分别用 C 的公钥和自己的私钥解密由用户终端 C 发送过来的身份信息和口令，接着再分别用自己是私钥和 S 的公钥加密身份信息和口令发送到 WiFi 认证中心 S。

Step5：WiFi 认证中心用自己的私钥和接入设备 D 的公钥解密由接入设备 D 发送过来的身份信息和口令，解密前的信息为 78963，解密后为 78963，信息无篡改，接着 WiFi 认证中心 S 核查数据库身份信息。

Step6：WiFi 认证中心 S 用自己的私钥和接入设备 D 的公钥加密 Succese 信号，然后发送到 AP/AC 接入设备 D。

Step7：接入设备收到 WiFi 认证中心 S 的 Succese 信号消息后分别用自己的私钥和 WiFi 认证中心 S 的公钥进行解密，消息无篡改，接入设备 D 开放用户终端 C 的网络端口，用户终端 C 接入网络。

4 系统性能测试

为了说明本文设计的基于国密技术的 WiFi 安全接入系统的有效性，我们对样机系统的性能进行了测试。性能测试分为以下 4 个方面。

（1） 证书申请和签发结果

证书申请与签发过程通过两个命令来测试。第一个是 S 生成证书申请文件的过程，其中包含 S 自身的签名信息，以及证书的有效期，结果是加密的。第二个命令为 CA 签发 S 证书的过程,CA 通过私钥签名生成 S 证书，其中需要输入 S 的各项信息，包括国家、城市、机构、地址与邮箱等，明细中包含颁发者、使用者、使用版本以及证书。测试结论见表 1。

（2） 身份鉴别结果

性能测试结果显示：Verified OK，说明身份鉴别成功，可以确认对方身份的真实性。具体测试结果见表 1。

（3） 身份信息加密结果

身份信息加密的测试结果如图 2 所示。加密了的文件显示为乱码，证明身份信息已经加密。

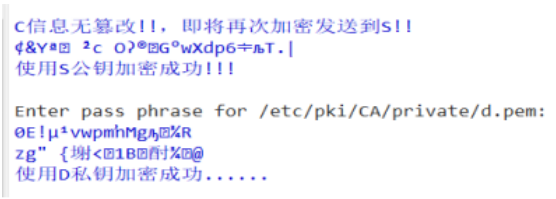

图 2 身份信息加密结果图

（4） 身份信息完整性结果

身份信息完整性的测试结果如图 3 所示，从图中可以看到，加密前的内容为 78963，加密后的内容也为 78963，对此加密前和加密后的内容无篡改，保持了身份信息的完整性。

表 1 性能测试结果汇总

测试名称	测试用例	期望结果	结论
证书申请签发测试	1.S生成证书请求文件 2.CA为其签发证书	生成私钥加密的s.csr证书申请文件；CA签发证书生成s.crt文件	通过
身份鉴别测试	1.查看到对方发来的身份、时戳信息乱码 2.首先用CA公钥验证对方证书真实性 3.用对方公钥验证其签名	1.查看显示乱码 2.提示“Verified OK”,使用CA公钥验证证书成功! 3.提示“Verified OK”，签名校验成功!	通过
身份信息加密测试	1.利用自己的私钥使用SM3算法加密身份信息文件 3.利用对方的公钥使用SM3算法加密身份信息文件	身份信息文件password.txt私钥加密后的文件pwd.sig，公钥加密后的文件pwd.enc，显示加密文件为乱码、ASCII格式	通过
身份信息完整性测试	使用SM3算法计算数据，并进行比较	加密前的信息为C 78963 解密后的信息为C 78963	通过

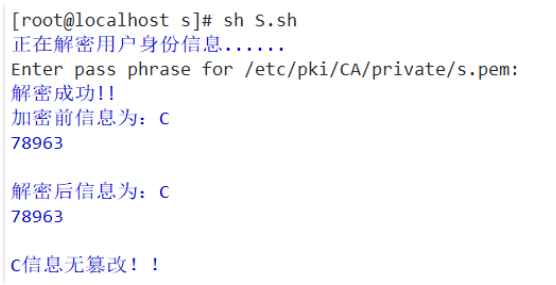

图 3 身份信息完整性结果图

从表 1 给出的系统性能测试结果来看，系统在证书申请签发身份鉴别、身份信息加密、身份信息完整性等方面实现了系统设计预定的功能，说明系统的方案设计是可行和有效的。

5 结束语

论文根据 WiFi 用户接入认证和授权流程,在构建基于国密技术的 WiFi 接入系统安全模型和设计 WiFi 安全接入认证协议的基础上，基于 Linux 操作系统，使用 Xshell 终端模拟软件和 GmSSL 密码工具箱实现实现了一个 WiFi 安全接入系统的样机系统，初步实现了通信双方的身份鉴别，关键数据传输的保密性和完整性及关键数据存储的保密性和完整性需求。通过 WiFi 安全增强实践表明：国外的网络服务平台与国内的网络安全技术完全能够有机融合，相互兼容，密码技术是构筑网络空间安全防线的最可靠、最有效、最经济的技术手段。

但是，我们实现的只是一个 WiFi 安全接入模型功能，并没有实现一个真实完整的 WiFi 安全接入系统。还需要深入研究，进一步开发。

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

[2] 林凡，黄建青，杨峰等. 长距离无线网络安全接入技术研究[J]. 移动通信. 2014,38(24):31-35

[3] 王辉.无线办公网络接入的安全性[J]. 环球市场信息导报. 2017,(33):123-124

[4] 官丽, 焦阳, 张彩霞等.电力监控系统无线接入安全风险的模糊评估方法研究[J].能源与环保,2021,43(6):163 -167

[5] 赖欢欢, 黄佳佳, 叶茜茜等.基于无线网络的新能源电厂安全接入平台研究[J].电气技术, 2019,20(03):111- 114,121

[6] 廖翼, 王涛, 施武作等.配网智能终端无线网络接入电力系统安全技术研究[J].机电信息,2019,2019,(21): 26-28

[7] 程琦, 黄太贵.基于无线公网 VPN 的电力监控系统安全接入区研究[J].电气自动化, 2018,40(5):98-100

[8] 金久强.轨道交通 Wi-Fi 服务网络构架的研究与实现[D]. 北京：中国铁道科学研究院，2016

[9] 高一凡,林德辉,夏志成等.城市轨道系统安全信息集成接入与融合应用平台研究[J].交通工程,2021,21(02):38-44

[10] 密码行业标准化技术委员会.GM/T 0002-2012 《SM4 分组密码算法》[S].国家密码管理局，2012

[11] 密码行业标准化技术委员会.GM/T 0003.2-2012 SM2 《椭圆曲线公钥密码算法第 2 部分：数字签名算法》[S]. 国家密码管理局，2012

[12] 密码行业标准化技术委员会.GM/T 0003.4-2012 《SM2 椭圆曲线公钥密码算法第 4 部分：公钥加密算法》[S]. 国家密码管理局，2012

[13] 密码行业标准化技术委员会.GM/T 0015-2012《基于 SM2 密码算法的数字证书格式规范》 [S].国家密码管理局，2012

[14] 密码行业标准化技术委员会.GM/T 0004-2012《SM3 杂凑算法》 [S]. 国家密码管理局，2012.