WPA–PSK 加密的 Wi–Fi 网络的安全性研究

孔维东 谭军 *
百色学院，中国·广西 百色 533000

摘 要：论文深入探讨了 WPA-PSK 加密的 Wi-Fi 网络安全性问题。首先详细解析了 WPA-PSK 的加密原理，包括 WEP 的加密原理、RC4 算法及其弱点，以及 TKIP 和 MIC 等。后评估了 WPA-PSK 加密的安全性，探讨了 Wi-Fi 网络面临的安全威胁。为了提高 Wi-Fi 网络的安全性，提出了一种增强方案，包括优化加密算法和改进身份验证机制，并设计了相应的安全性测试与评估方法。在实施增强方案并进行测试后，对实验结果进行了详细分析，验证了优化算法和身份验证机制的有效性。

关键词：WPA-PSK 加密；Wi-Fi 网络安全；加密算法优化；身份验证机制改进

Research on the Security of Wi-Fi Networks with WPA-PSK Encryption

Weidong Kong Jun Tan*
Baise University, Baise, Guangxi, 533000, China

Abstract: This paper delves into the security issues of Wi-Fi networks encrypted with WPA-PSK. Firstly, the encryption principle of WPA-PSK was analyzed in detail, including the encryption principle of WEP, RC4 algorithm and its weaknesses, as well as TKIP and MIC. After evaluating the security of WPA-PSK encryption, the security threats faced by Wi-Fi networks were discussed. In order to improve the security of Wi-Fi networks, an enhancement scheme has been proposed, including optimizing encryption algorithms and improving authentication mechanisms, and corresponding security testing and evaluation methods have been designed. After implementing the enhancement plan and conducting testing, a detailed analysis of the experimental results was conducted to verify the effectiveness of the optimization algorithm and identity verification mechanism.

Keywords: WPA-PSK encryption; Wi-Fi network security; optimization of encryption algorithms; improvement of identity verification mechanism

0 前言

随着信息技术的飞速发展，无线局域网（Wireless Local Area Network，WLAN）技术在全球范围内得到了广泛的应用。作为 WLAN 中最常用的安全协议之一，Wi-Fi Protected Access with Pre-Shared Key（WPA-PSK）旨在为用户提供安全的网络连接。然而，随着黑客攻击手段的不断升级，WPA-PSK 加密的 Wi-Fi 网络面临着越来越多的安全挑战。研究 WPA-PSK 加密的 Wi-Fi 网络安全性至关重要，它不仅增强网络安全性，保护用户信息和隐私，还促进加密、身份验证和密钥管理技术的发展，推动无线网络技术进步。研究有助于了解网络攻击手段，制定有效防御策略，降低被攻击风险，为网络管理员提供优化建议，如选择更安全的加密算法和设置复杂密码。在国家层面，研究对提升国家网络安全具有重要意义，为国家网络安全策略制定提供科学依据，加强网络安全防护能力 [1]。

1 WPA–PSK 加密的 Wi–Fi 网络安全分析

WPA-PSK（Wi-Fi Protected Access with Pre-Shared Key）是一种广泛使用的 Wi-Fi 网络安全协议，用于保护无线网络不被未授权访问。

1.1 WPA–PSK 加密的 Wi–Fi 网络安全威胁

①字典攻击：攻击者可以使用预先计算的 PSK 哈希值字典来尝试破解 PSK。如果用户选择的密码较弱，这种攻击可能会成功。②暴力攻击：攻击者可以尝试所有可能的 PSK 组合，直到找到正确的密码。这种方法的成功取决于密码的复杂性和长度。③侧信道攻击：攻击者可以通过分析无线信号的特性，如信号强度和传输时间，来获取有关加密密钥的信息。④重放攻击：攻击者可以捕获合法的数据包并在稍后的时间重新发送它们，试图欺骗系统。⑤密钥重用：如果 PTK（Pairwise Transient Key）被重用，攻击者可能会利用这个漏洞来破解加密。

1.2 WPA–PSK 加密的安全性评估

①密码强度：PSK 的强度是 WPA-PSK 安全性的关键。强密码应该足够长，并且包含大小写字母、数字和特殊字符的组合。②密钥交换过程：四次握手过程中的密钥交换应该能够抵御重放攻击和其他类型的攻击。③加密算法：WPA-PSK 支持 TKIP 和 AES-CCMP 两种加密算法。TKIP 由于存在已知漏洞，其安全性不如 AES-CCMP。④协议实现：WPA-PSK 的实现应该没有错误或漏洞，以防止诸如 KRACK 攻击之类的安全漏洞。⑤网络配置：网络的配置，

包括 SSID 隐藏、频道选择和接入点的固件更新，都会影响 WPA-PSK 的安全性。⑥周边安全：除了技术层面的安全性评估，物理安全也很重要。防止未授权人员物理访问接入点可以减少安全风险。

2 WPA–PSK 加密的 Wi–Fi 网络增强方案设计

2.1 WPA–PSK 加密算法优化

①采用 AES：使用 AES（Advanced Encryption Standard），它提供了更好的安全性和性能 [2]。

②增加密钥长度：使用更长的密钥长度通过增加 SSID 和 PSK 的长度，以提高加密强度。

2.2 身份验证机制改进

2.2.1 启用 802.1X 认证

在无线接入点（AP）上启用 802.1X 认证，意味着需要对 AP 进行相关设置，使其能够要求所有连接的设备进行身份验证。

2.2.2 部署认证服务器

为了使 802.1X 认证正常工作，需要部署 RADIUS（远程认证拨号用户服务）或 Diameter 服务器作为后端认证服务器。RADIUS 服务器负责接收来自无线接入点的认证请求，对用户身份进行验证，并根据验证结果向接入点发送认证结果。在部署 RADIUS 服务器时，需要对其进行配置，以支持所选的 EAP（可扩展认证协议）方法。EAP 是一种可扩展的认证协议，支持多种认证方法，如密码、证书等。根据实际情况，可以选择合适的认证方法。

2.3 安全性测试与评估方法

在评估 WPA-PSK 加密的 Wi-Fi 网络的安全性时，可以考虑以下几个关键指标。

2.3.1 认证成功率

①通过模拟器和实际抓包，评估设备在尝试连接到 Wi-Fi 网络时的认证成功率。

②确保所有的设备都能成功通过 802.1X 认证。

2.3.2 密钥交换和数据传输安全性

①使用抓包工具（如 Wireshark）监控数据包，确保在四次握手过程中没有未授权的设备尝试接入网络。

②检查数据包中是否使用了正确的加密算法（如 TKIP 或 AES-CCMP）和 MIC（Message Integrity Check）。

2.3.3 密钥泄漏风险

①评估密钥轮换和密钥分层的有效性，确保密钥管理策略能够减少密钥泄露的风险。

②检查是否有任何异常的密钥交换尝试，这可能表明密钥已经泄露或被破解。

2.3.4 重放攻击防范

①检查四次握手过程中是否有任何重放攻击的迹象，确保网络能够有效抵御重放攻击。

②使用模拟器模拟重放攻击，并评估网络的安全性。

2.3.5 密码破解尝试

①监控网络中是否有暴力破解或字典攻击的尝试，评估密码的强度和安全性。

②检查是否使用了足够的 PBKDF2 迭代次数来增强密码的安全性 [3]。

2.3.6 监控和日志记录

①检查 RADIUS 服务器和无线接入点的日志记录，评估监控系统的有效性。

②确保所有的认证尝试和网络安全事件都被记录下来，以便进行分析和响应。

2.3.7 安全配置一致性

①检查所有设备上的安全配置是否一致，确保没有配置错误或不一致的地方。

②确保所有的设备都遵循最佳实践，如定期更新固件和软件 [4]。

通过这些关键指标的评估，可以全面了解 WPA-PSK 加密的 Wi-Fi 网络的安全性，并采取必要的措施来提高网络的安全性。

3 增强方案的实施与测试

3.1 实施环境搭建

实验环境的构建旨在达成实施 WPA-PSK 加密算法优化与身份验证机制改进目的。

3.1.1 明确目标

目标一：实施 WPA-PSK 加密算法优化。

更好的密钥管理：优化密钥生成和分发过程，确保密钥的安全性和随机性。例如，可以使用更复杂的 PSK，或者定期更换 PSK[5]。

改进的加密算法：随着计算能力的提升，可以考虑使用更强大的加密算法，如 AES-GCM（高级加密标准 -Galois/Counter 模式），以提高加密强度 [6]。

目标二：身份验证机制改进。

增强的认证机制：虽然 WPA-PSK 使用 PSK 进行认证，但可以进一步研究使用其他认证方法，如证书 -based 认证，以提供更高的安全性。

更好的安全协议：虽然 WPA-PSK 相对安全，但可以考虑转向更新的安全协议，如 WPA3，它提供更好的安全特性，如改进的加密算法和增强的防护措施。

3.1.2 设备与环境搭建

第一，设备配置。

①在 ENSP 模拟软件中设计一个基本的 Wi-Fi 网络拓扑，一个无线接入点和一个无线客户端，一台交换机同时作 DHCP 服务器，连通 Cloud 用于 VM 中 kali 的连接。

②使用 VM 虚拟软件搭建 RADIUS 服务器，连接 Wi-Fi 以加强认证。

③使用路由器设置一个 WPA-PSK 无线网络，在 kali 中

用扩展的无线网卡连接 Wi-Fi。

第二，实验场景设计。

①设计不同的实验场景，例如，测试不同长度的 PSK、不同加密算法（如 AES、TKIP）的安全性。

②模拟使用 RADIUS 服务器进行认证，以测试加强验证的安全性。

③模拟不同的攻击场景，如字典攻击、暴力破解等，以测试网络的安全性。

第三，环境搭建。

①在 ENSP 中，搭建如下的拓扑。AC 负责对 AP 进行统一管理，并且进行 WLAN 的配置，使无线客户端 STA（Station，站点）能够连接到 AP 并访问网络，ENSP 拓扑如图 1 所示。

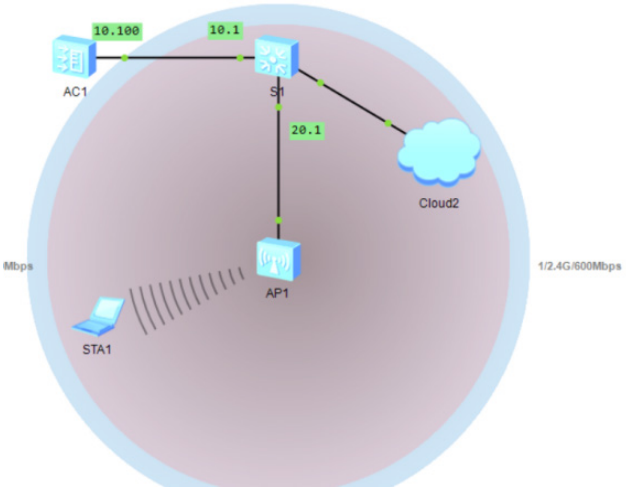

图 1 ENSP 拓扑图

②模块设置。

模块设置如表 1 所示。

表 1 模板配置总览

配置项	配置参数
AP 组	名称：group 应用模板：域管理模板 domain、VAP 模板 vap
域管理模板	名称：domain 国家码：cn
SSID 模板	名称：ssid SSID 名称：swlan
安全模板	名称：sec 安全策略：WPA-WPA2+PSK+AES 密码：KwdKwd@123
VAP 模板	名称：vap 转发模式：直接转发 业务 VLAN：VLAN20 应用模板：SSID 模板 ssid、安全模板 sec

3.1.3 实施前情况

如图 2、3 所示，为了对比方案实施前后，先使用工具展示方案实施前的真实 Wi-Fi 网络环境。使用 kali 的 aircrack-ng 获取握手包并使用字典攻击，如果是弱密码且密钥加强不高则很快被破解。

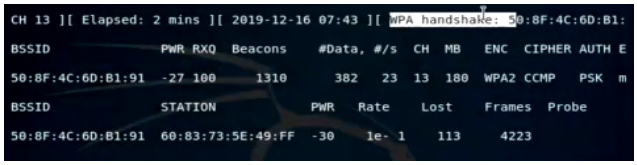

图 2 抓取握手包的监听

图 3 利用 Aircrack–ng 进行字典攻击

3.2 WPA–PSK 加密算法优化实施

通过修改安全模板中的配置命令来升级加密算法，采用 AES，并使用强密码。修改安全模板的配置命令是 security wpa2 psk pass-phrase Rh+9zEG）Doc3 aes。从 WPA 升级到 WPA2，提供了更强的安全性和更多的安全功能。将加密算法从 TKIP 更改为 AES，这是更现代和更安全的加密标准，提供了更好的数据保护和抗攻击能力。使用了新的、更复杂的密码短语，这增加了猜测或暴力破解密码的难度。

3.3 身份验证机制改进实施

为了实施身份验证机制的改进，需要替换 VM 中的 kali 改为 Win7 做 Radius，使用 winradius 软件来充当 radius 服务器。

① RADIUS 服务器配置。

radius-server template radius1 // 创建名为 radius1 的 RADIUS 服务器模板

radius-server authentication 10.23.200.1 1812

radius-server accounting 10.23.200.1 1813

radius-server shared-key cipher 123456 // 配置 RADIUS 服务器预共享密钥

undo radius-server user-name domain-included

radius-server authorization 10.23.200.1 shared-key cipher 123456 // 配置 RADIUS 授权服务器的地址，共享密钥为 123456，必须与认证密钥和计费密钥一致。

② AAA 配置。

authentication-scheme radius1 // 创建名为 radius1 的认证方案

authentication-mode radius

accounting-scheme radius1　// 创建名为 radius1 的计费方案

accounting-mode radius　// 配置计费方案为 RADIUS 方式

domain radius1　// 创建名为 radius1 的域

authentication-scheme radius1　// 绑定认证方案 radius1

accounting-scheme radius1　// 绑定计费方案 radius1

radius-server radius1　// 绑定 RADIUS 服务器模板 radius

③ vap 模板配置。

在 VAP 模板 vap 中，配置了认证配置文件为 radius1，这意味着无线客户端的认证将通过 RADIUS 服务器进行。

vap-profile name vap

authentication-profile radius1

④在 AC 上测试连通性。

＜ AC1 ＞ test-aaa myuser 123456 radius-template radiusl

3.4 安全性测试与评估

3.4.1 对 WPA-PSK 加密算法优化实施后的安全性测试与评估

①加密算法测试。使用 Wireshark 捕获无线网络的流量数据。分析捕获的数据包，确认无线网络正在使用 AES 加密（WPA2-PSK/AES）。

②密码强度评估。使用 Aircrack-ng 等密码破解工具尝试破解使用新密码的 WPA-PSK 握手包。记录破解所需的时间，并与优化前的情况进行比较，以评估密码强度的提升。

③字典攻击测试。使用字典攻击工具（如 John the Ripper、Hashcat）进行密码破解尝试。评估所需字典的覆盖度，以确定密码的复杂性和不可预测性。

④安全配置审查。使用 Nmap 等网络扫描工具检查无线接入点的配置。确认所有安全设置都已正确应用，没有遗留的不安全配置或默认设置。

3.4.2 对身份验证机制改进实施后的安全性评测与评估

① RADIUS 服务器测试。使用 NTRadPing 等工具测试 RADIUS 服务器的运行状态和响应。确认 RADIUS 服务器（如 WinRadius）已正确配置并运行。

②认证过程测试。使用不同的用户账户尝试连接 Wi-Fi 网络，测试认证机制正常工作。在不同设备和操作系统上进行认证测试，确保兼容性和稳定性。

4 实验结果与分析

4.1 WPA–PSK 加密算法优化效果分析

为了方便起见，接下来将在实际设备上，使用相同的配置建立 SSID 为“MERCURY_1E0E”的 Wi-Fi 来测试分析。

在进行 WPA-PSK 加密算法优化后，通过实施以下步骤来分析其效果。

4.1.1 加密算法测试结果

首先，在 Kali Linux 操作系统中，需要将无线网卡切换到监听模式。这一步骤通过执行命令 `airmon-ng start wlan0mon` 实现，其中 `wlan0mon` 代表无线网卡设备。切换到监听模式后，网卡将能够捕获周围的无线网络流量，而不会发送任何信号，如图 4 所示。

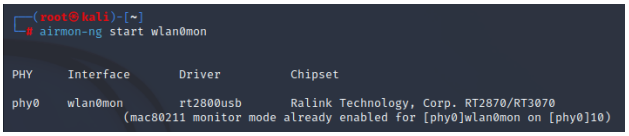

图 4 命令 `airmon–ng start wlan0mon` 实现

其次，使用 Wi-Fite 这一自动化工具来执行抓取握手包的过程。Wi-Fite 是一个专为渗透测试设计的工具，它简化了捕获 WPA 握手过程。通过执行命令 `Wi-Fite --skip-crack` 来启动工具，并跳过密码破解阶段，因为目前的目标仅是捕获握手包。这个参数可以节省时间，因为不需要等待不必要的破解过程。

在 Wi-Fite 运行后，将选择一个目标 Wi-Fi 网络。工具将开始抓取该网络上的数据包，等待握手过程的发起。为了诱导目标网络发起握手，可以尝试连接到该 Wi-Fi 网络。一旦看到了保存的握手信息，这表明工具已经成功地捕获了 WPA 四次握手过程的数据包。效果如图 5 所示。

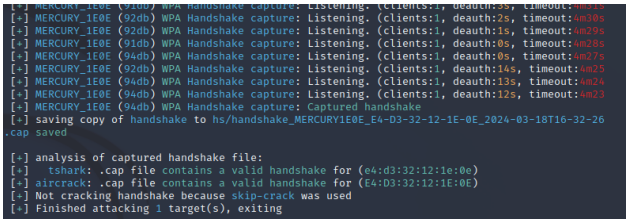

图 5 捕捉到握手包

最后，使用 Wireshark 这一网络协议分析工具来进一步分析捕获的数据包。通过打开捕获的文件并过滤出 EAPOL（可扩展认证协议 _OVER_ 局域网）包，可以深入查看 WPA 协议的详细内容。EAPOL 包在 WPA 四次握手过程中用于传输认证信息。如果能够清晰地看到 WPA 握手过程中的 EAPOL 帧，这表明实验成功地捕获并分析了 WPA 协议的握手过程。如图 6 所示。

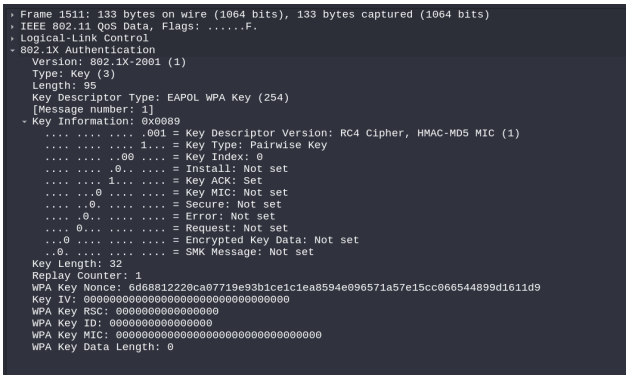

图 6 EAPOL 包内容

4.1.2 密码强度评估结果

首先，需要将无线网卡切换到监听模式。接下来，使用 `airodump-ng wlan0mon` 命令来确定目标 Wi-Fi 网络的信道、加密方式、MAC 地址等信息。如图 7 所示。

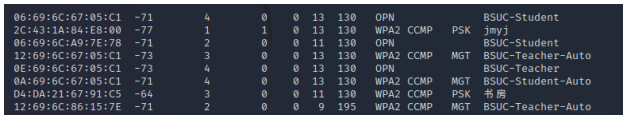

图 7 扫描网络

确定了目标网络的信道后，使用 `airodump-ng wlan0mon -c 1 --ivs -w /root/Wi-Fi/1E0E --bssid E4:D3:32:12:1E:0E` 命令对目标网络所在的信道进行抓包。这里的 `-c 1` 指定了目标网络的信道，`--ivs` 表示仅捕获包含加密信息的 IVs（初始向量），`-w` 参数后跟的是保存捕获数据包的文件名前缀，而 `--bssid` 后面则是目标网络的 BSSID（基本服务集标识符），即网络的 MAC 地址。如图 8 所示。

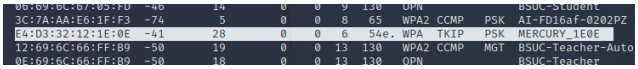

图 8 获取目标网络的 BSSID

为了诱导目标网络发起握手，手动连接到该 Wi-Fi 网络，然后断开连接并重新连接。这一操作有助于触发四次握手过程，从而使得监听设备能够捕获到握手包。一旦成功地捕获了握手包，就可以使用 Aircrack-ng 尝试破解密码。如图 9 所示。

图 9 获取握手包

尝试使用一个英文单词列表字典 `wordlist.TXT` 进行破解，命令为 `aircrack-ng -w /root/Dictionaries/ 破解字典 /WPA 英文字典 /wordlist.TXT /root/Wi-Fi/1E0E-01.ivs`。发现并不能破解，由此看到密码强度提高了。如图 10 所示。

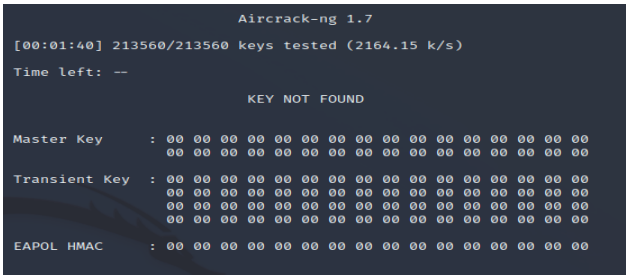

图 10 密码破解

4.1.3 字典攻击测试结果

继续使用一个规模更大的字典 \（401W-500W\）.TXT，命令为 aircrack-ng -w /root/Dictionaries/ 破解字典 /\（401W-500W\）.TXT /root/Wi-Fi/1E0E-01.ivs。因为密码的强度和长度都有所增加，且字典不具有针对性，所以依旧无法破解。如图 11 所示。

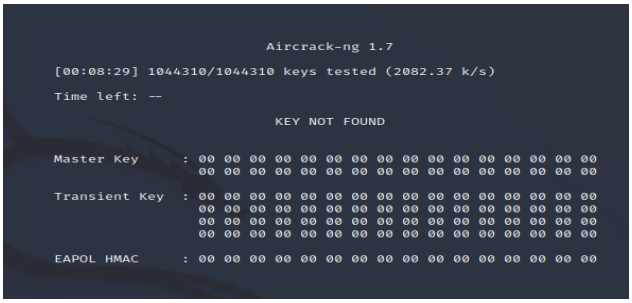

图 11 使用规模较大的字典破解

4.2 身份验证机制改进效果分析

在改进身份验证机制后，通过实施以下步骤来分析其效果。

4.2.1 RADIUS 服务器测试结果

NTRadPing 测试显示 RADIUS 服务器响应迅速，没有延迟或失败的情况。所有认证请求都得到了正确处理。如图 12 所示。

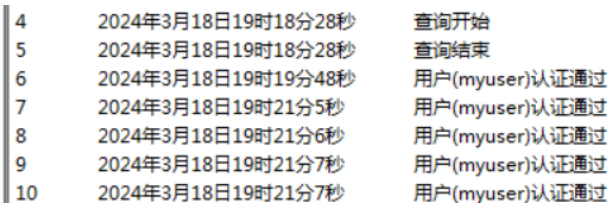

图 12 NTRadPing 多次测试结果反馈

4.2.2 认证过程测试结果

多个用户账户的认证测试均成功，用户能够顺利连接到 Wi-Fi 网络。认证过程在不同设备和操作系统上表现一致，没有兼容性问题。

4.3 安全性测试与评估结果分析

综合以上实验结果，可以得出以下结论：

① WPA-PSK 加密算法的优化显著提高了网络的安全性，通过使用 AES 加密和强密码，网络的加密强度得到了增强，使得密码破解变得更加困难。

②身份验证机制的改进，特别是引入 RADIUS 服务器进行认证，为网络访问提供了更加严格的控制，确保只有经过认证的用户能够连接到网络。

③安全性测试与评估表明，新的安全措施有效地抵御了潜在的攻击，同时保持了良好的用户体验。

监控和日志记录为网络管理员提供了审计和监控网络活动的工具，有助于及时发现和响应安全威胁。

5 结语

通过深入研究了 WPA-PSK 加密的 Wi-Fi 网络安全性，分析了加密原理，探讨了安全威胁，并提出了增强方案。实验证明，这些方案能有效提升 Wi-Fi 网络安全。然而，研究存在不足：未涉及最新加密技术如 WPA3，未详细探讨其他安全措施如入侵检测系统和防火墙，实验结果仅在模拟环境中评估，未在实际应用中验证。未来研究可考虑将这些新技术和安全措施纳入分析，结合实际网络环境验证方案效果，并将研究成果应用于物联网安全。总之，尽管存在不足，论文为 Wi-Fi 网络安全提供了理论支持和实践指导，未来研究应继续优化安全措施，提高网络安全性能。

参考文献：

[1] 刘峙晨,梁丽琴,陈荣贵,等.基于WPA/WPA2协议的无线攻击漏洞分析研究[J].网络安全技术与应用,2020(3):71-72.

[2] 李晔桃.WPA2身份认证协议安全研究与改进[D].西安:西安电子科技大学,2021.

[3] 陆浩.WPA/WPA2_PSK密码高速暴力破解方的研究与实现[D].武汉:武汉邮电科学研究院,2020.

[4] 郭一缜.无线网络安全与防范技术[J].无线通信技术,2022,31(2):27-31.

[5] 徐志伟,郑宝森.无线Wi-Fi攻击技术及防范对策研究[J].网络安全技术与应用,2022(3):78-80.

[6] 刘仁山.无线局域网安全策略分析与应用研究[J].呼伦贝尔学院学报.2021,29(4):72-77.

作者简介：孔维东（2001-），中国甘肃古浪人。

通讯作者：谭军（1979-），中国广西合浦人，副教授。