WPA3认证OWE

1024041120刘旭

2025 年 6 月 9 日

目录

摘要

传统的开放式网络往往面临缺乏加密或采用公用PSK的隐患。为解决这一问题，机遇性无线加密（OWE）作为一种新兴技术，利用Diffie-Hellman密钥交换在802.11协议的关联阶段实现了无认证动态加密，提供了一种无需身份认证的加密方案，增强了无线网络的安全性。

1 研究背景

1.1 WPA3和OWE简介

为了便于用户随时随地接入到Wi-Fi网络中，大多数公共场所都采用开放认证方式，用户无需输入密码即可接入Wi-Fi网络。然而，开放式Wi-Fi网络是存在风险的，所有用户都无需输入密码即可接入Wi-Fi网络，增加了非法攻击者接入网络的风险。同时，用户与Wi-Fi网络之间的数据传输也是透明的、未经过加密的，这就使得数据传输过程可能被非法攻击者进行侦听，窃取用户数据。

WPA3（Wi-Fi Protected Access 3）是Wi-Fi联盟组织于2018年发布的新一代Wi-Fi加密协议它对WPA2进行了改进，增加了许多新的功能，为用户和Wi-Fi网络之间的数据传输提供更加强大的加密保护。

根据Wi-Fi网络的用途和安全需求不同，WPA3分为WPA3个人版、WPA3企业版以及针对开放性Wi-Fi网络的OWE认证。

个人模式（WPA3-Personal）取代 WPA2-PSK（预共享密钥），采用 SAE（Simultaneous Authentication of Equals，对等同时认证），也称为 Dragonfly 密钥交换。抗离线字典攻击：防止攻击者通过捕获握手数据离线破解密码。前向安全性（Forward Secrecy）：即使长期密码泄露，过去的通信仍无法解密。不依赖弱加密：WPA2 使用 4 次握手的 PSK 方式，WPA3 使用更安全的 SAE 握手。企业模式（WPA3-Enterprise）要求 192 位最小安全强度（WPA2 支持 128 位），适用于政府、金融等高安全需求场景。强制执行 AES-256-GCM 加密（比 AES-CCMP 更强）。支持 CNSA（Commercial National Security Algorithm）标准，符合美国国家安全局（NSA）的严格要求。

公开网络保护（Opportunistic Wireless Encryption, OWE）取代开放网络（无密码 Wi-Fi）： WPA2：开放 Wi-Fi 数据明文传输，易受嗅探攻击。 WPA3：引入 OWE（Opportunistic Wireless Encryption），为未认证的网络提供临时加密（类似 HTTPS），防止流量窃听。 WPA3 修复了 WPA2 的密钥重装攻击（Key Reinstallation Attack，KRACK）漏洞，确保握手过程安全。

关系	说明
WPA3 → 三大模式	SAE（个人模式）、OWE（开放网络模式）、Enterprise（企业模式）
SAE → 用于 WPA3-Personal	替代 WPA2-PSK 的密码认证，防暴力破解
OWE → 用于开放网络	无密码 Wi-Fi 加密方案（取代 WPA2 的开放无加密）

图 1: WPA3介绍

1.2 Diffie-Hellman密钥交换介

Diffie-Hellman（DH）密钥交换是一种允许双方在不安全的信道上安全协商共享密钥的加密协议，由Whitfield Diffie和Martin Hellman在1976年提出。它是现代密码学的基石之一，广泛应用于SSL/TLS、SSH、OWE等协议中。

Algorithm 1: Diffie-Hellman密钥交换协议（基于有限域）

公共参数大素数p（$|p| \geq 2048$位）和生成元g（模p的原根）

Alice端操作:

1. 选择随机私钥a　$(1 < a < p-1)$

2. 计算公钥$A \equiv g^a \pmod{p}$

Bob端操作:

1. 选择随机私钥b　$(1 < b < p-1)$

2. 计算公钥$B \equiv g^b \pmod{p}$

密钥交换阶段:

1. Alice发送A给Bob　← 通过不安全信道

2. Bob发送B给Alice　← 通过不安全信道

共享密钥计算:

- Alice计算：$s \equiv B^a \equiv (g^b)^a \equiv g^{ab} \pmod{p}$
- Bob计算：$s \equiv A^b \equiv (g^a)^b \equiv g^{ab} \pmod{p}$

输出:

双方获得相同的共享机密s（用作对称密钥）

椭圆曲线DH（ECDH）将椭圆曲线加密与DH密钥交换相结合，利用椭圆曲线上的点运算来执行密钥交换，从而提供了一种比传统DH更高效的方法来协商共享密钥。ECDH协议的安全性基于椭圆曲线离散对数问题（ECDLP），与传统的基于有限域的DH协议相比，它在相同安全强度下可使用更短的密钥长度，显著提升了计算效率，适用于资源受限的环境（如移动设备）。

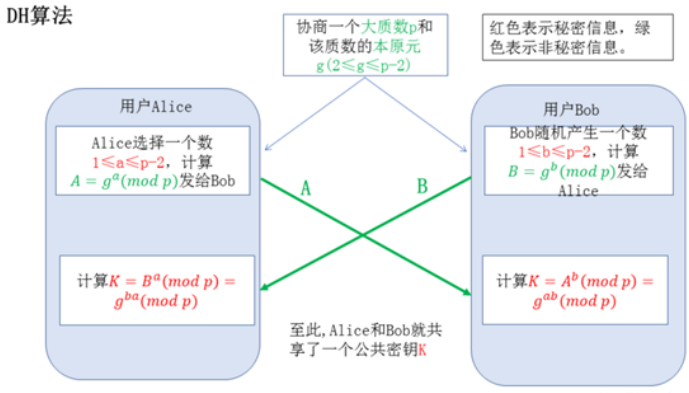

图 2: Diffie-Hellman算法示意图

在具体应用中，例如RFC 8110定义的OWE协议，支持两种群组选择方式：ECC（椭圆曲线加密）和FFC（基于有限域的加密）。这两种群组的选择直接影响密钥生成的哈希算法：对于ECC群组，哈希算法根据椭圆曲线素数域的位数动态选择（如SHA-256用于≤256位曲线，SHA-384用于257–384位曲线）；对于FFC群组，则根据有限域素数p的位数决定（如SHA-256适用于≤2048位素数）。

这一设计确保了密钥派生过程的安全性与群组特性紧密匹配，既兼容不同密码学场景的需求，又通过算法分级优化了性能与安全性间的平衡。

2 OWE组成

OWE由以下几个核心部分构成，共同实现开放Wi-Fi网络的安全加密：

1. **密钥交换机制**

OWE基于ECDH（椭圆曲线Diffie-Hellman）或FFDH（有限域Diffie-Hellman）密钥交换协议，确保双方在不安全信道中协商出共享密钥。

支持的群组（RFC 8110定义）：

- ECC（椭圆曲线）：例如19（Curve25519）、20（Curve448）。
- FFC（有限域）：例如15（2048-bit MODP Group）、16（3072-bit MODP Group）。

密钥派生：使用HKDF（基于哈希的密钥派生函数）从共享密钥中生成主密钥（PMK），其计算过程满足：

$$\text{PMK} = \text{HKDF-Expand}(\text{HKDF-Extract}(\text{共享密钥}, \text{salt}), \text{info}, L)$$

2. **网络发现与关联**

信标帧（Beacon）：AP广播包含OWE能力指示的信标，表明支持OWE加密。

关联请求/响应（Association Request/Response）：

- 客户端与AP交换DH公钥（通过RSNE信息元素中的OWE Diffie-Hellman参数）。
- 若使用过渡模式（混合开放/OWE网络），AP可能同时广播开放SSID和OWE SSID，其信标帧结构满足：

$$\text{Beacon} = [\text{SSID}_{open}] \parallel [\text{SSID}_{OWE}] \parallel \text{OWE Parameter Element}$$

3. **四步握手（4-Way Handshake）**

与传统WPA2/WPA3类似，OWE通过四步握手生成临时密钥（PTK），用于加密单播流量：

- ANonce → SNonce交换：验证双方活跃性，防止重放攻击。
- PTK派生：基于PMK、ANonce、SNonce、MAC地址等参数生成：

$$\text{PTK} = \text{PRF-512}(\text{PMK}, \text{"OWE Key Expansion"}, \text{Min}(A, B) \parallel \text{Max}(A, B))$$

- 密钥确认：最后两条消息携带MIC（消息完整性校验码），确保密钥一致性。 4. **组密钥分发（可选）**

如果需要组播加密（如ARP、广播流量），AP通过组密钥握手指令分发GTK（Group Temporal Key），其封装格式

为：

$$\text{GTK} = \text{Enc}(\text{KEK}, \text{Key Data} \parallel \text{Key RSC} \parallel \text{IGTK})$$

5. **安全策略与防降级攻击**

• 强制加密：OWE无开放模式，所有连接必须满足Enc(Data, PTK/GTK)加密要求。

• 防降级保护：客户端拒绝回退到开放网络（满足安全策略$\text{SP}_{\text{no-fallback}}$）。

• 密钥隔离：每个会话生成独立PTK，满足前向保密性$\text{FS} = \{\text{PTK}_i \not\rightarrow \text{PTK}_j\}_{i \neq j}$。

3 安全体系

3.1 OWE 的安全域划分

1. **密钥交换安全域**

核心功能：通过ECDH/FFDH生成共享密钥（PMK）。

依赖的安全假设：

• 椭圆曲线离散对数问题（ECDLP）的困难性：

$$\forall G \in \mathbb{G}, \text{给定 } P = kG, \text{ 计算 } k \text{ 在多项式时间内不可行}$$

• 有限域离散对数问题（DLP）的困难性：

$$\forall g \in \mathbb{Z}_p^*, \text{给定 } g^k \mod p, \text{ 计算 } k \text{ 为NP难问题}$$

• 密钥派生函数（HKDF）满足抗碰撞性：

$$\Pr[\text{HKDF}(K_1) = \text{HKDF}(K_2) | K_1 \neq K_2] \leq \epsilon(\lambda)$$

2. **会话密钥安全域**

四步握手生成PTK（单播加密）和GTK（组播加密）。

依赖的安全机制：

• 临时随机数（Nonce）的不可预测性：

$$\text{Entropy}(\text{ANonce}) \geq 256 \text{ bits}, \ \text{Entropy}(\text{SNonce}) \geq 256 \text{ bits}$$

• 消息完整性校验（MIC）防范重放攻击：

$$\text{MIC} = \text{CMAC}_{K_{MIC}}(\text{Msg} \parallel \text{SeqNum})$$

• 密钥派生满足前向保密（FS）要求：

$$\text{PTK}_t = f(\text{PMK}, \text{Nonces}, \text{MAC}_A, \text{MAC}_B), \ \text{PTK}_t \not\Rightarrow \text{PTK}_{t+1}$$

3. **网络发现与关联安全域**

信标帧和关联请求/响应的公钥交换需满足：

• 抗篡改保护（Tamper-proof）：通过数字签名验证：

$$\sigma = \text{Sign}_{SK_{AP}}(\text{DH}_{pub} \parallel \text{Timestamp})$$

• 防降级攻击（Downgrade Resistance）：

$$\text{ClientPolicy} = \{\text{if OWE\_present} \Rightarrow \text{Reject\_Open}\}$$

4. **前向保密域**

每次会话生成独立的临时密钥，确保：

• 会话密钥隔离性：

$$\{\text{PTK}_i\}_{i=1}^n \text{ 满足 } \text{PTK}_i \not\equiv \text{PTK}_j \ (\forall i \neq j)$$

• 历史会话不可解密性（Past Secrecy）：

$$\text{Compromise}(\text{PTK}_t) \not\Rightarrow \text{Decrypt}(\text{Data}_{t-1})$$

• 密钥生命周期约束：

$$\text{KeyLifetime}(\text{PTK}) \leq \min(2^{48}\ \text{frames},\ 24h)$$

3.2 OWE所受的典型安全攻击及防御方案

中间人攻击（MITM, Man-in-the-Middle） 在密钥交换阶段，攻击者$\mathcal{A}$可通过篡改ECDH公钥实施劫持，具体表现为$\text{ECDH}_{pub}^{\mathcal{A}} \leftarrow f(\text{ECDH}_{pub}^{AP}, \text{ECDH}_{pub}^{STA})$。降级攻击则尝试强制回退到开放模式，其威胁模型为$\text{Tr}(\text{Beacon}) \rightarrow \text{Open Auth}$。 OWE采用三重防御机制：通过协议约束确保$\Pr[\text{OWE} \rightarrow \text{Open}] = 0$实现强制加密；在Association帧中部署$\text{MIC}_K(\text{DH}_{pub} \parallel \text{Nonce})$校验保障公钥完整性；虽然未采用SAE机制，但通过HKDF-SHA384(DH_{shared})强化密钥派生安全性。

密钥重装攻击（Key Reinstallation Attack, KRACK） 攻击者通过重放握手消息诱导Reinstall(PTK_t)，导致IV reuse漏洞。该攻击的数学表征为$\exists t_1 \neq t_2, \text{Nonce}_{t_1} = \text{Nonce}_{t_2}$。防御体系构建于WPA3改进方案：消息3/4采用$\text{MIC}_{\text{strict}} = \text{HMAC-SHA384}(\text{Msg} \parallel \text{Nonce}_{\text{unique}})$实现强化校验；临时随机数满足$\text{Nonce} \in \{0,1\}^{256}$空间约束，使得重装概率$\Pr[\text{KRACK}] \leq 2^{-256}$。

拒绝服务攻击（DoS） 资源耗尽攻击可建模为$\lim_{n\to\infty} \text{AssocReq}(n) \Rightarrow \text{AP}_{\text{load}} = 100\%$，消息泛洪攻击表现为$\bigcup_{i=1}^{N} \text{HandshakeMsg}_i$的笛卡尔积式爆发。防护策略采用分层控制：在物理层实施$\frac{d(\text{AssocReq})}{dt} \leq 5$ fps的速率限制；对未认证客户端启用$\text{QoS}_{\text{low}} \leq 1$ Mbps的带宽管制；握手消息处理引入$\tau > 100$ms的队列延迟缓冲。

密钥泄露后攻击（Retrospective Decryption） 当长期密钥泄露$\mathcal{A} \leftarrow \text{PMK}$时，前向保密性要求满足$\frac{\partial \text{PTK}_t}{\partial \text{PMK}} = 0$。OWE通过临时ECDH密钥实现FS-Advantage $\leq \text{negl}(384)$的安全强度。具体措施包括：每24小时强制更新DH_{temp}密钥对；PTK派生函数满足$\text{PTK}_t = \text{HKDF}(\text{DH}_t, \cdot)$的密钥隔离特性；会话密钥生命周期严格限定为$\min(2^{48}\ \text{frames}, 24\text{h})$。

3.3 OWE的安全局限性

无身份认证：OWE 加密但不验证 AP/客户端身份，仍可能遭受恶意热点欺骗。改进方向：结合 WPA3-Enterprise（802.1X）或 DANE/TLS（基于证书）。依赖 DH 安全群组：若 ECDH曲线或 FFC 群组存在漏洞（如弱素数），可能导致密钥破解。实施漏洞：部分设备可能错误实现 OWE，如未正确防御 KRACK。

4 关键技术

OWE认证流程在开放认证流程的基础上，增加了采用Diffie-Hellman（DH）算法的密钥交换机制，在不改变用户接入习惯的前提下，提升了开放式Wi-Fi网络的安全性。在OWE模式下，用户仍然无需输入密码即可接入网络，保持了开放式Wi-Fi网络的便利性；同时，它通过DH密钥交换算法（如ECDH或FFDH）在用户和AP之间动态协商加密密钥，实现了数据的端到端加密，并利用密钥派生函数（如HKDF）生成会话密钥，避免了传统开放网络的明文传输漏洞。通过这种方式，OWE既保留了开放网络的易用性，又为用户与Wi-Fi网络之间的数据传输提供了加密保护，有效防范了窃听和中间人攻击等安全威胁。

4.1 开放认证流程

AP采用开放认证，所有终端的认证请求都会通过。具体认证流程如下图所示：

1.Authentication Request：终端向AP请求认证。

2.Authentication Response：AP采用开放认证，终端请求认证通过，返回认证结果。

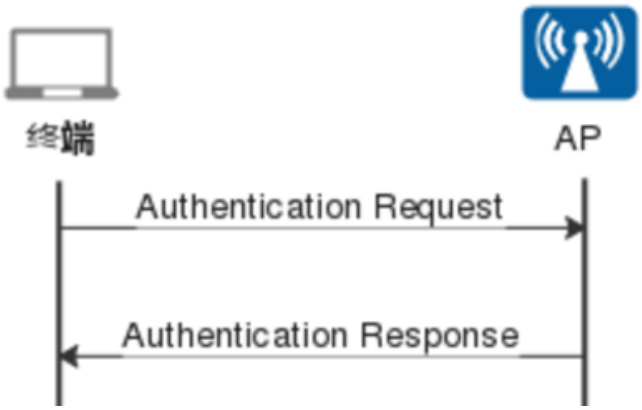

图 3: 开放认证流程

4.2 OWE认证流程

AP采用OWE认证，包括OWE Discovery和OWE Association两个阶段。具体认证流程如下图所示：

OWE Discovery阶段：

1.Authentication Request：终端向AP请求认证。

2.Authentication Response：AP采用OWE认证，终端请求认证通过，返回认证结果。认证结果中包含AKM（Authentication and Key Management）字段，向终端宣称自己支持OWE认证。支持OWE认证的终端收到认证结果后，进入OWE Association阶段，不支持OWE认证的终端将以开放认证的方式接入。

OWE Association阶段：

1.Association Request：终端向AP发起关联请求，并在Diffie-Hellman Parameter字段中添加终端侧公钥（Public Key）。

2.Association Response：AP向终端返回关联结果，并在Diffie-Hellman Parameter字段中并添加AP侧公钥（Public Key）。终端和AP完成公钥交换后生成PMK（Pairwise Master Key，成对主密钥）。3.4-Way Handshake：终端和AP进行四次握手，确定双方通信所要采用的密钥。

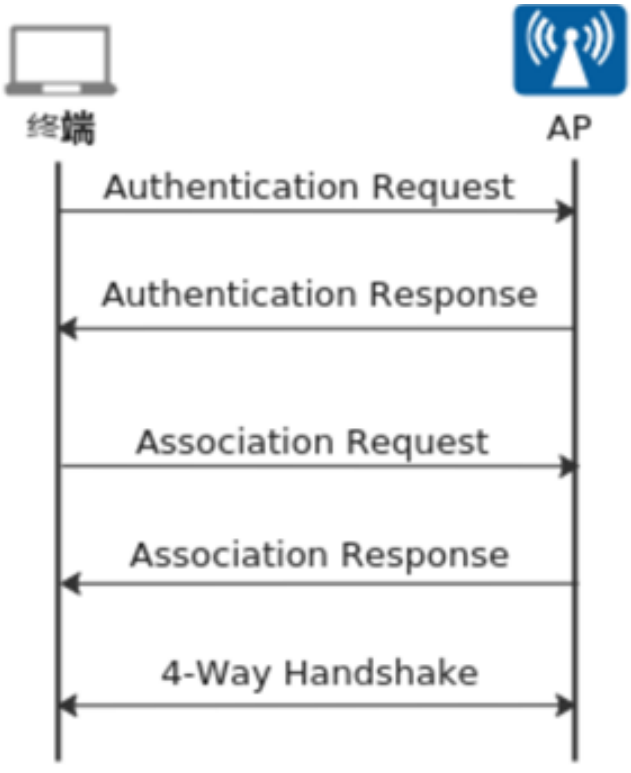

图 4: OWE认证流程

4.3 密钥派生

(1) Diffie-Hellman（DH）密钥交换

客户端（STA）和 AP 各自生成临时 ECDH 密钥对。在 Association Request/Response 阶段交换公钥（ECPubAP 和 ECPubSTA），计算共享密钥（ECDH 密钥协商得出 PMK 的基础）。

(2) PMK 生成（Pairwise Master Key）

使用 HKDF-SHA256 从 Shared Secret 派生 PMK。 (3) 4-Way Handshake 派生 PTK（Pairwise Transient Key）

OWE 使用和 WPA3 类似的 4-Way Handshake 机制： AP → STA（Msg1） PTK 计算（128/256 位 AES 密钥）

(4) GTK 生成（Group Temporal Key）

AP 生成随机 GTK，并使用 PTK 加密后发送给客户端（Msg3）。 GTK 用于组播/广播数据加密（如 ARP、IPv6 组播等

4.4 四次握手

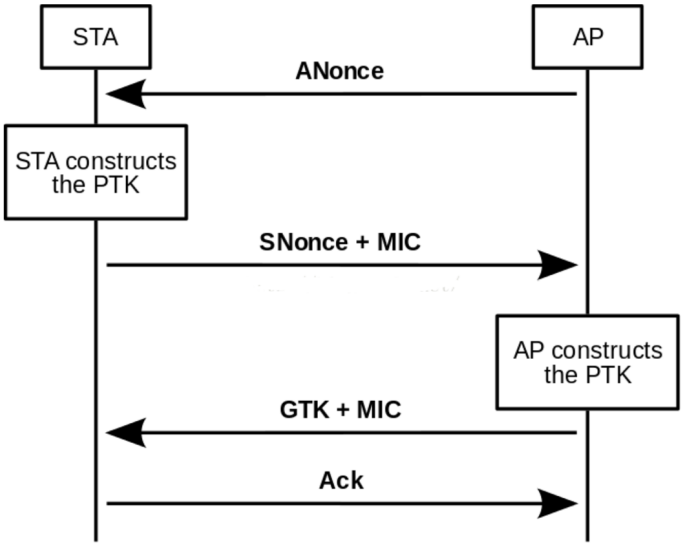

图 5: 四次握手示意图

（1）消息 1：AP → Client（发送 ANonce） AP 生成一个随机数 ANonce（Authenticator Nonce）。发送给 Client，用于计算 PTK。

（2）消息 2：Client → AP（发送 SNonce + MIC） Client 生成随机数 SNonce（Supplicant Nonce）。结合 ANonce 和 DH 共享密钥（PMK，Pairwise Master Key），使用 PBKDF2-HMAC-SHA256 计算 PTK。发送 SNonce 和 MIC（Message Integrity Code，消息完整性校验码）给 AP，证明自己拥有正确的 PMK。

（3）消息 3：AP → Client（安装 PTK + 发送 GTK） AP 收到 SNonce 后，用同样的方式计算 PTK。验证 MIC 是否正确（防止伪造）。发送 GTK（Group Temporal Key，组播密钥）给 Client，并通知 Client 安装 PTK。

（4）消息 4：Client → AP（确认安装完毕） Client 确认 PTK 和 GTK 安装成功。发送最后一条确认消息，完成握手。 OWE协议在建立连接时，会通过4次握手派生出多个密钥，包括： KCK（Key Confirmation Key）：用于消息完整性校验。 KEK（Key Encryption Key）：用于加密组密钥。 TK（Temporal Key）：用于加密数据流的密钥。这些密钥在握手过程中通过HMAC-SHA-256等算法加密生成，确保数据传输的保密性和完整性。

4.5 OWE的过渡模式

开放式网络到增强型开放式网络的迁移是循序渐进的，用户设备的更新换代也是逐步进行，为了兼容部分不支持OWE认证的终端，OWE还支持过渡模式（OWE Transition Mode），即不支持OWE认证的终端将以开放认证方式接入Wi-Fi网络，支持OWE认证的终端以OWE认证方式接入Wi-Fi网络。 OWE过渡模式的工作原理如下：

1.AP需要创建两个SSID，SSID 1启用开放认证，SSID 2启用OWE认证。

2.SSID 2将被设置为隐藏，只有SSID 1对外广播它的SSID名称，因此对于终端而言，只能看到SSID 1。

3.SSID 1中包含了过渡模式字段和对应SSID 2的信息，终端连接到SSID1时，如果终端支持OWE认证，则会通过过渡模式直接连接到SSID 2。

5 改进

安全优势OWE的最大优势在于其前向保密性：每次会话使用独立的临时密钥，历史流量无法用旧密钥解密，从而大大提升了安全性。此外，OWE通过基于Diffie-Hellman的加密交换方式，有效防止了中间人攻击（MITM）和被动嗅探。

风险与限制尽管OWE在防止嗅探攻击方面表现出色，但它仍然面临中间人攻击的威胁。攻击者可伪造AP并诱骗客户端连接，并在客户端和真实AP之间进行桥接通信。为应对这种威胁，结合HTTPS或VPN等加密协议可进一步提高安全性。此外，OWE并不提供身份验证，AP和客户端无法彼此验证对方的身份，这意味着其适用于相对可信的环境，如公共Wi-Fi网络，但在企业级应用中可能需要更多的安全措施。

1. 增强身份认证机制

(1) 集成基于证书的认证（类似WPA3-Enterprise）在DH密钥交换后，增加 AP证书验证（如TLS证书），确保客户端连接的AP是合法的。可结合 DNSSEC + DANE（DNS-Based Authentication of Named Entities），通过DNS记录验证AP证书。

(2) 设备绑定认证（MAC/硬件令牌）在首次连接时，客户端和AP交换并存储可信的设备标识（如MAC哈希或硬件密钥）。后续连接时验证标识，阻止未授权设备冒充AP。

2. 引入前向保密（PFS）与密钥更新

(1) 强制使用高强度DH算法

禁用弱曲线（如P-192），强制使用 NIST P-256/384 或 X25519（Curve25519）。定期（如每小时）重新协商DH密钥，避免长期密钥泄露风险。提升前向保密性（PFS），即使长期密钥泄露，历史会话仍安全。

(2) 动态密钥轮换

改进方案：在现有4次握手基础上，增加周期性PTK/GTK更新（如每GB数据传输后更换密钥）。限制单个密钥的暴露时间，降低被破解概率。

3. 防御中间人攻击（MITM）

(1) 引入轻量级AP身份验证 Wi-Fi Enhanced Open（IEEE 802.11-2020扩展）：在OWE握手阶段添加 AP签名，由客户端预置可信CA验证。或使用 Opportunistic TLS（类似HTTPS），客户端首次连接时缓存AP公钥。无需完整PKI，适合开放网络。

(2) 客户端主动探测伪造AP 客户端通过 RSSI（信号强度）、BSSID历史记录、地理位置等数据，检测异常AP。结合威胁情报服务（如已知恶意热点数据库）报警。

6 参考文献

[1]RFC 8110: Opportunistic Wireless Encryption

[2]IEEE 802.11-2016: Wireless LAN MAC and PHY Specifications

[3]RFC 5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF)