Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Bacharelado em Sistemas de Informação

# Estudo e Avaliação do Método de Criptografia Sem Fio Oportunista OWE

**Giovane Machado Aguiar**

JUIZ DE FORA
JULHO, 2026

# Estudo e Avaliação do Método de Criptografia Sem Fio Oportunista OWE

Giovane Machado Aguiar

Universidade Federal de Juiz de Fora

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Bacharelado em Sistemas de Informação

Orientador: Edelberto Franco Silva

JUIZ DE FORA

JULHO, 2026

# Estudo e Avaliação do Método de Criptografia Sem Fio Oportunista OWE

Giovane Machado Aguiar

MONOGRAFIA SUBMETIDA AO CORPO DOCENTE DO INSTITUTO DE CIÊNCIAS EXATAS DA UNIVERSIDADE FEDERAL DE JUIZ DE FORA, COMO PARTE INTEGRANTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE BACHAREL EM SISTEMAS DE INFORMAÇÃO.

Aprovada por:

Edelberto Franco Silva
Doutorado em Computação

Alex Borges Vieira
Doutor em Ciência da Computação

Luciano Jerez Chaves
Doutor em Ciência da Computação

JUIZ DE FORA
DE JULHO, 2026

# Agradecimentos

À minha família, à minha namorada e aos meus amigos, que estiveram ao meu lado durante toda a graduação, agradeço pelo apoio incondicional, pela compreensão e pelo incentivo constante, sobretudo nos momentos mais desafiadores.

Ao meu orientador, expresso minha gratidão pela dedicação, pela orientação atenta e pelas contribuições indispensáveis ao longo de toda a pesquisa.

Por fim, estendo meus agradecimentos a todos que, direta ou indiretamente, contribuíram para o desenvolvimento deste trabalho.

# Resumo

Com a contínua evolução das redes sem fio e a consolidação do padrão Wi-Fi 6, a segurança da informação em ambientes de acesso público tornou-se um desafio crítico. O método *Opportunistic Wireless Encryption* (OWE), padronizado pela RFC 8110, apresenta-se como uma solução capaz de fornecer criptografia individualizada nessas redes, eliminando a dependência de senhas pré-compartilhadas. Este trabalho propõe um estudo aprofundado e a avaliação prática do desempenho e da segurança do OWE dentro dessa nova arquitetura de conectividade. A pesquisa traça a evolução dos protocolos desde o WPA2 até o advento do WPA3, detalhando o mecanismo matemático de troca de chaves Diffie-Hellman e seu impacto na latência inicial da camada de enlace. Além da fundamentação teórica, foram conduzidos testes práticos focados na camada de aplicação para comprovar a eficácia da ocultação dos dados de navegação do usuário. A metodologia baseia-se na construção de um ambiente de testes rigorosamente controlado, simulando um roteador de acesso via Linux com adaptadores Wi-Fi 6, aliado a ferramentas de auditoria forense. Os resultados obtidos confirmam a viabilidade do OWE como sucessor definitivo das redes abertas tradicionais, atestando a blindagem robusta do tráfego web com um custo computacional tolerável frente ao expressivo ganho em privacidade.

**Palavras-chave:** Wi-Fi 6, OWE, Criptografia Sem Fio, Segurança de Redes, WPA3, Wireshark.

# Abstract

With the continuous evolution of wireless networks and the consolidation of Wi-Fi 6 standards, information security in public access environments has become a critical challenge. The Opportunistic Wireless Encryption (OWE) method, standardized by RFC 8110, presents itself as an innovative solution capable of providing individualized encryption in these networks, eliminating the reliance on pre-shared passwords. This work proposes an in-depth study and practical evaluation of the performance and security of OWE within this new connectivity architecture. The research traces the evolution of protocols from WPA2 to the advent of WPA3, unraveling the mathematical Diffie-Hellman key exchange mechanism and its direct impact on the initial link-layer latency. In addition to the theoretical foundations, practical tests focused on the application layer were conducted to prove the effectiveness of concealing user browsing data. The methodology is based on the construction of a rigorously controlled test environment, simulating a Linux-based access router with Wi-Fi 6 adapters, combined with forensic auditing tools. The obtained results confirm the high viability of OWE as the definitive successor to traditional open networks, attesting to the robust shielding of web traffic through a computational cost that proved negligible compared to the exponential improvement in privacy.


**Keywords:** Wi-Fi 6, OWE, Wireless Encryption, Network Security, WPA3, Wireshark.

# Conteúdo

**Lista de Figuras** **6**

**Lista de Tabelas** **7**

**1 Introdução** **9**
1.1 Apresentação do Tema . . . 9
1.2 Motivação . . . 9
1.3 Delimitação do Problema . . . 10
1.4 Objetivos . . . 11
1.4.1 Objetivo Geral . . . 11
1.4.2 Objetivos Específicos . . . 11
1.5 Organização do Trabalho . . . 11

**2 Fundamentação Teórica** **12**
2.1 A Evolução do Protocolo Wi-Fi . . . 12
2.2 A Evolução dos Protocolos WPA . . . 13
2.2.1 Wi-Fi Protected Access . . . 14
2.2.2 WPA3 . . . 15
2.2.3 Vulnerabilidades Dragonblood e o Algoritmo Dragonfly . . . 16
2.2.4 Modo de Transição . . . 16
2.3 O Protocolo OWE e a Criptografia Oportunística . . . 17
2.3.1 A Padronização pela RFC 8110 . . . 20
2.3.2 4-Way *Handshake* . . . 20
2.3.3 Diffie-Hellman . . . 21
2.3.4 Representação Visual do Diffie-Hellman . . . 22

**3 Materiais e Métodos** **24**
3.1 Classificação da Pesquisa . . . 24
3.2 Arquitetura do Ambiente de Testes . . . 24
3.2.1 Recursos de Hardware e Software . . . 25
3.2.2 Aferição Computacional (*Overhead*) . . . 26
3.3 Preparação do Roteador . . . 26
3.3.1 Cenário A: Rede Wi-Fi Aberta . . . 26
3.3.2 Cenário B: Rede com Protocolo OWE . . . 27
3.4 Inicialização da Interface de Monitoramento . . . 29

**4 Resultados e Discussões** **30**
4.1 *Beacon Frame* . . . 30
4.2 Troca de Chaves Diffie-Hellman . . . 31
4.3 Validação do *4-Way Handshake* . . . 32
4.4 Análise Forense da Rede Wi-Fi Aberta . . . 33
4.5 Interceptação Passiva de Tráfego . . . 35
4.6 Análise Forense na Camada de Aplicação . . . 35
4.7 *Overhead* . . . 37
4.7.1 Extrapolação para Múltiplos Dispositivos . . . 39

**5 Considerações Finais** **42**

**Bibliografia** **45**

# Lista de Figuras


2.1 Canais disponíveis na banda de 2,4 GHz, destacando as zonas de sobreposição. Fonte: Adaptado de (TANENBAUM; WETHERALL, 2011). . . . . 13
2.2 Processo de conexão de uma estação a uma rede OWE, da descoberta ao tráfego cifrado. Fonte: Elaborado pelo autor. . . . . 17
2.3 Diagrama de sequência da troca de mensagens no estabelecimento de uma conexão OWE, da descoberta ao tráfego cifrado. Fonte: Elaborado pelo autor. 19
2.4 Fluxograma matemático e visual do acordo de chaves Diffie-Hellman. Fonte: Adaptado de (PIRES, 2010). . . . . 22

3.1 Arquitetura e topologia do laboratório. Fonte: Elaborado pelo autor. . . . . 24
3.3 Dispositivo móvel associado à rede do Cenário A (Rede Wi-Fi Aberta). Fonte: Elaborado pelo autor. . . . . 27
3.4 Dispositivo móvel associado à rede do Cenário B (Rede com Protocolo OWE). Fonte: Elaborado pelo autor. . . . . 28

4.1 *Beacon Frame* evidenciando a utilização do AKM Suite 18. Fonte: Elaborado pelo autor. . . . . 30
4.2 *Association Request* exibindo a chave pública do cliente (OWE Diffie-Hellman Parameter). Fonte: Elaborado pelo autor. . . . . 31
4.3 *Association Response* evidenciando a devolução do componente Diffie-Hellman pelo AP. Fonte: Elaborado pelo autor. . . . . 32
4.4 Capturas sequenciais do 4-Way *Handshake* (EAPOL) e estabelecimento das chaves criptográficas. Fonte: Elaborado pelo autor. . . . . 34
4.5 *Association Request* em rede aberta, atestando a flag de privacidade como falsa. Fonte: Elaborado pelo autor. . . . . 34
4.6 Pacote DHCP Discover exposto e decodificado na rede legada. Fonte: Elaborado pelo autor. . . . . 35
4.7 Comparativo do tráfego da camada de aplicação capturado nas redes aberta e OWE. Fonte: Elaborado pelo autor. . . . . 36
4.8 Comparativo da latência (*delta* temporal) de associação. Fonte: Elaborado pelo autor. . . . . 37
4.9 Distribuição dos custos temporais (*overhead*) integrados ao OWE. Fonte: Elaborado pelo autor. . . . . 38
4.10 Evolução temporal do estabelecimento de conexão (Rede Aberta vs OWE). Fonte: Elaborado pelo autor. . . . . 38

# Lista de Tabelas

2.1 Evolução das gerações Wi-Fi quanto à banda de frequência e à velocidade máxima . . . . . 12

4.1 Tempo total de conexão OWE (*Association Request* até a Mensagem 4 do *4-Way Handshake*) em cinco execuções independentes . . . . . 39
4.2 Extrapolação analítica do tempo agregado de processamento no ponto de acesso, em função do número de dispositivos conectantes . . . . . 40

# Lista de Abreviações

| | |
|---|---|
| AES | Advanced Encryption Standard |
| AP | Access Point |
| CCMP | Counter Mode Cipher Block Chaining Message Authentication Code Protocol |
| DH | Diffie-Hellman |
| ECDH | Elliptic Curve Diffie-Hellman |
| GTK | Group Temporal Key |
| IEEE | Institute of Electrical and Electronics Engineers |
| MIMO | Multiple Input Multiple Output |
| MU-MIMO | Multi-User, Multiple-Input, Multiple-Output |
| OFDM | Orthogonal Frequency-Division Multiplexing |
| OFDMA | Orthogonal Frequency-Division Multiple Access |
| OWE | Opportunistic Wireless Encryption |
| PMF | Protected Management Frames |
| PMK | Pairwise Master Key |
| PSK | Pre-Shared Key |
| PTK | Pairwise Transient Key |
| RFC | Request for Comments |
| SAE | Simultaneous Authentication of Equals |
| STA | Station |
| TWT | Target Wake Time |
| WPA | Wi-Fi Protected Access |

# 1 Introdução

## 1.1 Apresentação do Tema

A profunda dependência global de conectividade sem fio, especialmente em localidades públicas de grande circulação, impulsionou de maneira irreversível a necessidade de protocolos que equilibrem a praticidade de acesso com a proteção integral dos dados do usuário. Historicamente, redes Wi-Fi abertas, comuns em praças, aeroportos, hotéis e cafeterias, operam sob um formato permissivo que não oferece qualquer camada de criptografia durante o estabelecimento inicial da conexão. Consequentemente, os pacotes de dados fluem pelo espectro em texto claro.

Para compreender a vulnerabilidade desta arquitetura convencional, basta imaginar o tráfego de dados pessoais como um cofre residencial deixado aberto no meio de uma via pública. Sem os protocolos de segurança adequados, não existem barreiras lógicas, permitindo que qualquer indivíduo munido de ferramentas simples intercepte o tráfego alheio. Esta falha estrutural viabiliza ataques de monitoramento passivo, conhecidos tecnicamente como *sniffing* ou *eavesdropping*, nos quais agentes maliciosos conseguem extrair credenciais e dados sensíveis de usuários que compartilham o mesmo meio de transmissão (SANTOS, 2024).

Foi exatamente para erradicar essa lacuna crítica que surgiu o protocolo Opportunistic Wireless Encryption (OWE). Em linhas gerais, ele estabelece uma conexão firmemente criptografada e individualizada, de forma transparente para o usuário final, promovendo segurança sem a necessidade de digitar senhas ou realizar pré-cadastros.

## 1.2 Motivação

Motivado pela rápida adoção do padrão Wi-Fi 6, que opera utilizando tecnologias avançadas de transmissão, faz-se necessário compreender como o OWE interage com esses novos recursos espectrais, e a importância e impacto da adoção desse tipo de protocolo. O

protocolo antecessor, o WPA2, introduzido em 2004, serviu como alicerce da segurança por quase duas décadas. Entretanto, sua arquitetura apresenta uma limitação relevante sob a ótica da cibersegurança ao ignorar as redes públicas e não oferecer suporte nativo para cifrar dados quando não há senha definida. A motivação principal deste trabalho reside na urgência em validar se a promessa de segurança do OWE se sustenta na prática, e, principalmente, se essa camada extra de segurança degrada (ou não) a experiência de conexão do usuário devido a um possível incremento da latência. O OWE integra a certificação WPA3, sucessora do WPA2, na qual atua — sob a denominação comercial *Enhanced Open* — como o mecanismo específico destinado às redes sem senha. Uma vez que o WPA3 se tornou obrigatório para todos os dispositivos certificados com Wi-Fi 6 a partir de 2020 (NETO, 2021), o OWE já acompanha de fábrica o parque de equipamentos recentes, posicionando-se como sucessor natural das redes abertas. Portanto, um estudo forense detalhado do seu funcionamento e de suas exigências de processamento mostra-se vital no contexto atual de redes de computadores e cibersegurança.

## 1.3 Delimitação do Problema

O problema investigado reside na inércia da transição tecnológica, onde a maioria das redes públicas ainda opera sob o modelo de rede aberta não criptografada herdado do passado (SOUZA, 2022). Além disso, o antigo WPA2 provou ser vulnerável a ataques estruturais críticos e permite que invasores realizem pesadas tentativas de adivinhação de senhas por meio de dicionários *offline* (VANHOEF; PIESSENS, 2017).

Embora o OWE surja como a solução para o problema de redes sem senha, a sua adoção esbarra na escassez de dados sobre o custo prático de sua implementação. A complexidade imposta pelos cálculos algébricos na troca de chaves Diffie-Hellman gera um *overhead* (*i.e.*, uma sobrecarga de processamento computacional em roteadores e clientes) que ainda carece de métricas experimentais consolidadas (MACEDO, 2023). Avaliar se esse processamento matemático introduz uma latência não tolerável no instante em que o usuário tenta se conectar à rede define o problema central desta pesquisa.

## 1.4 Objetivos

### 1.4.1 Objetivo Geral

Avaliar sistematicamente o desempenho prático, a eficácia na ocultação de dados de navegação e o impacto na latência causado pelo protocolo OWE em ambientes simulados conforme os padrões da tecnologia Wi-Fi 6.

### 1.4.2 Objetivos Específicos

- Desenvolver uma análise sobre a evolução técnica e a correção de falhas do padrão WPA2 para a arquitetura moderna do WPA3.
- Aprofundar o entendimento matemático do algoritmo Diffie-Hellman empregado pelo OWE e mensurar o seu custo computacional via análise forense.
- Implementar um ambiente de testes laboratorial (real) utilizando o sistema operacional Linux (como um *Soft AP*) e interfaces de rádio Wi-Fi 6.
- Contrastar, por meio de captura de pacotes em modo monitor, a exposição visual do tráfego do usuário e a velocidade de associação em uma rede aberta comparada a uma rede protegida pelo OWE.

## 1.5 Organização do Trabalho

Além deste capítulo introdutório, o trabalho está organizado em mais quatro capítulos. O Capítulo 2, Fundamentação Teórica, apresenta a evolução dos padrões Wi-Fi e dos protocolos WPA2 e WPA3, o funcionamento do OWE e os fundamentos do algoritmo Diffie-Hellman em curvas elípticas. O Capítulo 3, Materiais e Métodos, descreve o ambiente de testes e a configuração dos cenários de rede aberta e protegida por OWE. O Capítulo 4, Resultados e Discussões, apresenta as evidências forenses coletadas, incluindo a análise do *handshake*, o contraste da exposição do tráfego e a mensuração do *overhead*. Por fim, o Capítulo 5, Considerações Finais, sintetiza as conclusões e aponta os trabalhos futuros.

# 2 Fundamentação Teórica

## 2.1 A Evolução do Protocolo Wi-Fi

A demanda exponencial por conectividade ininterrupta impôs uma marcha evolutiva agressiva aos padrões Wi-Fi, exigindo inovações contínuas no mapeamento de frequências, na largura de banda dos canais e na técnica de modulação dos sinais — isto é, na forma como informações digitais são embutidas em uma onda eletromagnética para a transmissão de dados (TANENBAUM; WETHERALL, 2011; IEEE, 2021a). A Tabela 2.1 sintetiza essa evolução, comparando a banda de frequência e a velocidade máxima teórica de cada geração.

Tabela 2.1: Evolução das gerações Wi-Fi quanto à banda de frequência e à velocidade máxima

| **Geração** | **Padrão IEEE** | **Ano** | **Banda** | **Velocidade Máxima** |
|---|---|---|---|---|
| Wi-Fi 1 | 802.11b | 1997 | 2,4 GHz | 1–2 Mbps |
| Wi-Fi 2 | 802.11a | 1999 | 5 GHz | 54 Mbps |
| Wi-Fi 3 | 802.11g | 2003 | 2,4 GHz | 54 Mbps |
| Wi-Fi 4 | 802.11n | 2009 | 2,4/5 GHz | 600 Mbps |
| Wi-Fi 5 | 802.11ac | 2013 | 5 GHz | 433 Mbps (por fluxo) |
| Wi-Fi 6 | 802.11ax | 2019 | 2,4/5/6 GHz | até 9,6 Gbps (agregado) |

Na banda de 2,4 GHz, utilizada desde o Wi-Fi 1, a maior propagação do sinal tem como contrapartida uma suscetibilidade elevada a interferências, uma vez que apenas três canais independentes (1, 6 e 11) não se sobrepõem, conforme ilustra a Figura 2.1. Essa limitação motivou a migração parcial para a faixa de 5 GHz a partir do Wi-Fi 2 (802.11a), que ofereceu canais mais largos e menor congestionamento, ainda que às custas de maior atenuação diante de obstáculos físicos. O Wi-Fi 3 (802.11g) manteve a operação em 2,4 GHz, mas herdou o mesmo método de modulação Orthogonal Frequency-Division Multiplexing (OFDM) do 802.11a, atingindo a mesma velocidade máxima de 54 Mbps.

A evolução mais significativa em termos de vazão ocorreu no Wi-Fi 4 (802.11n), com a consolidação da tecnologia Multiple Input Multiple Output (MIMO): o uso de múltiplos fluxos espaciais simultâneos, por meio de matrizes de antenas transmissoras e receptoras, multiplicou a taxa de vazão (*throughput*) da rede.

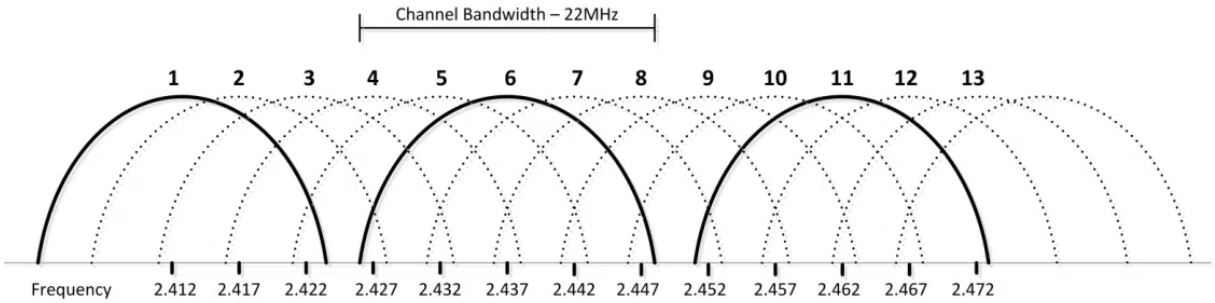



Figura 2.1: Canais disponíveis na banda de 2,4 GHz, destacando as zonas de sobreposição. Fonte: Adaptado de (TANENBAUM; WETHERALL, 2011).

Com o crescimento do consumo de mídia, o Wi-Fi 5 (802.11ac) concentrou-se em extrair a máxima capacidade da faixa de 5 GHz, com canais de até 80 MHz e modulação QAM de alta densidade. Já o Wi-Fi 6 (802.11ax) deslocou a filosofia de projeto da taxa de transmissão bruta para a eficiência espectral em cenários de alta densidade de estações, sendo por isso designado *High Efficiency WLAN* (BELLALTA, 2016; KHOROV et al., 2019). Seu principal mecanismo, o OFDMA, subdivide o canal em unidades de recurso menores, permitindo que múltiplas estações sejam atendidas dentro de uma mesma oportunidade de transmissão e reduzindo o *overhead* de acesso ao meio (KHOROV et al., 2019; IEEE, 2021b). Esse histórico evolutivo, contudo, serve neste trabalho apenas como base para compreender as premissas tecnológicas do Wi-Fi 6, o cenário de testes adotado nesta pesquisa. O foco central da fundamentação teórica — e o que de fato se relaciona ao problema investigado — reside na evolução paralela dos mecanismos de segurança que acompanharam essas gerações: do frágil WEP, ao transitório WPA, passando pelo consolidado WPA2, até chegar ao WPA3, apresentados a seguir.

## 2.2 A Evolução dos Protocolos WPA

Sob a ótica da segurança, enfoque deste trabalho, serão apresentados os protocolos e as iniciativas relacionados à segurança no Wi-Fi, nos quais os protocolos WPA atuam como

a proteção lógica da rede, regulando como as informações são cifradas e autenticadas. A base dessa proteção fundamenta-se na tríade clássica da área de cibersegurança: Confidencialidade, Integridade e Disponibilidade (CID) (SANTOS, 2024). A confidencialidade exige chaves criptográficas que tornam os dados ilegíveis para interceptadores, enquanto a integridade garante que o pacote não seja modificado no trajeto (SANTOS, 2024).

### 2.2.1 Wi-Fi Protected Access

Antes de tratar do Wi-Fi Protected Access (WPA), convém explicitar uma distinção que costuma ser obscurecida pela terminologia comercial: o termo "Wi-Fi" não designa um padrão técnico, mas uma marca de certificação administrada pela Wi-Fi Alliance. A especificação técnica que fundamenta a tecnologia é o conjunto de normas IEEE 802.11 e suas sucessivas emendas, elaboradas por grupos de trabalho (*task groups*) identificados por sufixos, como 802.11a, 802.11n, 802.11i, 802.11ax, entre outros (IEEE, 2021a). Em termos práticos, todo mecanismo observado em uma rede sem fio doméstica ou corporativa deriva dessas normas. Assim, a Wi-Fi Alliance atua sobre elas definindo perfis de interoperabilidade e rótulos comerciais (como WPA, WPA2 e Wi-Fi 6). Disso decorre uma ressalva relevante: a existência de um recurso no padrão IEEE não garante sua presença em um equipamento específico, uma vez que a implementação efetiva depende da adesão de cada fabricante, o que gera lacunas de compatibilidade e comportamento entre produtos que nominalmente atendem à mesma certificação. No campo específico da segurança, o marco normativo é a emenda IEEE 802.11i, ratificada em 2004, que introduziu o conceito de *Robust Security Network* (RSN) e substituiu o mecanismo original de proteção, o WEP, que é parte da norma de 1997 e reconhecidamente frágil (IEEE, 2004). O 802.11i definiu o Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), baseado no algoritmo Advanced Encryption Standard (AES), como método de confidencialidade e integridade, além de reestruturar o processo de estabelecimento de chaves por meio do *4-way handshake* (IEEE, 2004). Foi sobre esse arcabouço técnico que a Wi-Fi Alliance construiu suas certificações: o WPA, lançado em 2003, correspondeu a uma solução transitória baseada em uma versão preliminar do 802.11i, empregando o TKIP para viabilizar retrocompatibilidade com hardware existente, enquanto o WPA2,

de 2004, passou a exigir a implementação completa do RSN, com uso obrigatório do AES-CCMP. Apesar da ampla adoção e da robustez do AES, o WPA2 revelou algumas limitações ao longo do tempo. A mais notória é a vulnerabilidade KRACK (*Key Reinstallation Attack*), uma falha no *4-way handshake* que permite ao atacante forçar a reinstalação de uma chave já em uso, comprometendo as garantias criptográficas e possibilitando, em determinadas condições, a leitura do tráfego (VANHOEF; PIESSENS, 2017). Sua superfície de ataque também abrange a captura da transação inicial de autenticação, que habilita ataques de dicionário e de força bruta realizados *offline* contra a chave pré-compartilhada. Sob a ótica da proteção de infraestrutura, o padrão original não cifra nativamente os quadros de gerenciamento (*Protected Management Frames* — PMF) (SANTOS, 2024), o que expõe a rede a ataques de desautenticação e dissociação. Por fim, o WPA2 não oferece *Forward Secrecy*: comprometida a senha da rede, todo o tráfego previamente capturado pode ser descriptografado, já que as chaves de sessão derivam diretamente da chave pré-compartilhada. Tais limitações constituem justamente a motivação para as revisões posteriores consolidadas no WPA3, que incorpora o SAE e o PMF obrigatório como respostas diretas a esses vetores (VANHOEF; RONEN, 2020).

### 2.2.2 WPA3

Lançado em 2018 e obrigatório para dispositivos Wi-Fi 6 a partir de 2020, o WPA3 reestruturou a forma como a autenticação e a criptografia são tratadas, sanando as vulnerabilidades do seu antecessor (NETO, 2021). A terceira geração foi desenhada para impedir interceptações passivas e ataques diretos, introduzindo o mecanismo de Autenticação Simultânea de Iguais (SAE). Este mecanismo substitui o método clássico de senha ao exigir uma interação ativa com o roteador a cada tentativa de autenticação (NETO, 2021), o que inviabiliza ataques de dicionário *offline*. Outra vantagem arquitetônica fundamental é o Sigilo Perfeito de Encaminhamento (*Forward Secrecy*), que garante que, mesmo que a senha principal seja descoberta futuramente, a comunicação passada dos usuários permanece criptografada matematicamente (NETO, 2021). Finalmente, para atender às redes sem senha, o padrão incorpora o OWE — comercialmente denominado *Enhanced Open* —, que provê criptografia individual e oportunística, eliminando o risco de interceptação

passiva (NETO, 2021).

### 2.2.3 Vulnerabilidades Dragonblood e o Algoritmo Dragonfly

O algoritmo Dragonfly é a base matemática do WPA3. Contudo, pesquisas revelaram falhas conhecidas como Dragonblood (NETO, 2021). Estas vulnerabilidades baseiam-se em ataques de canais laterais (*side-channel*), onde invasores analisam o tempo de processamento das multiplicações matemáticas no hardware para deduzir padrões da chave de acesso, o que forçou revisões posteriores no protocolo (NETO, 2021).

### 2.2.4 Modo de Transição

Nem todos os dispositivos em uso hoje suportam o WPA3, e forçar essa migração de uma vez deixaria muita gente sem conseguir se conectar. Para contornar isso, o padrão prevê o Modo de Transição, em que a mesma rede aceita tanto o protocolo novo quanto o antigo. Quem tem um aparelho atual se conecta com a segurança máxima do WPA3; quem tem um aparelho mais velho ainda consegue entrar pelo método anterior.

Em redes com senha, isso é feito pelo WPA3-Personal *Transition Mode*: o mesmo ponto de acesso divulga tanto o SAE (WPA3) quanto o PSK (WPA2), os dois usando a mesma senha. Um celular compatível fecha a conexão via SAE, que resiste a ataques de dicionário *offline*, enquanto um aparelho antigo cai no PSK de sempre.

Nas redes abertas, o mecanismo é outro, chamado OWE *Transition Mode* e descrito no apêndice da Request for Comments (RFC) 8110 (HARKINS; KUMARI, 2017). Aqui o roteador não mistura os dois métodos numa rede só: ele sobe duas redes ao mesmo tempo, uma aberta com o nome visível e outra OWE com o nome oculto. As duas ficam ligadas entre si, e cada uma carrega, nos seus quadros de gerenciamento, uma informação que aponta para a outra (o *OWE Transition Mode element*), indicando o *BSSID* e o nome da rede parceira.

O que acontece na prática depende do aparelho. Um dispositivo que entende OWE enxerga a rede aberta, percebe pelo elemento que existe uma rede OWE oculta associada e se conecta direto nela, já com o tráfego criptografado, sem o usuário perceber nada. Um aparelho antigo simplesmente ignora essa informação, que não sabe interpretar,

e se conecta à rede aberta comum: continua funcionando, só que sem criptografia. É assim que o Modo de Transição permite adotar o OWE aos poucos, sem deixar ninguém para trás nem obrigar a troca imediata de todos os equipamentos.

## 2.3 O Protocolo OWE e a Criptografia Oportunística

O protocolo OWE resgata a privacidade do usuário em redes públicas, mitigando os riscos de interceptação passiva. Sua operação baseia-se na Criptografia Oportunística, pela qual a infraestrutura estabelece canais cifrados de forma autônoma. O processo ocorre em segundo plano: o usuário seleciona a rede aberta e é conectado sem digitar senhas, porém com proteção do tráfego (Paiva Neto, 2022). O processo de conexão de uma estação (*station* — STA, isto é, o dispositivo do usuário, e.g., um notebook ou celular) a uma rede protegida por OWE é ilustrado na Figura 2.2 e pode ser descrito como uma sequência de etapas encadeadas. Tudo se inicia com a descoberta da rede: o ponto de acesso (*Access Point* — AP, o roteador que provê o sinal) difunde periodicamente quadros de *beacon*, pequenos avisos transmitidos em intervalos regulares para sinalizar a existência da rede (e.g., o nome que aparece na lista de redes disponíveis do celular, o SSID). Esses avisos anunciam, entre outros parâmetros de segurança, o método de autenticação OWE. É por esse anúncio que a estação identifica que a rede, embora não exija senha, oferece cifragem oportunista, ou seja, criptografia automática sem necessidade de credencial compartilhada.

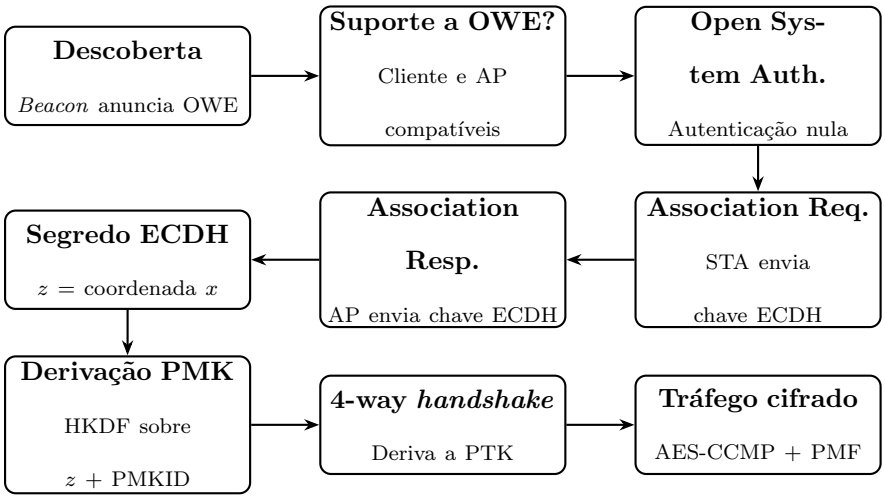



Figura 2.2: Processo de conexão de uma estação a uma rede OWE, da descoberta ao tráfego cifrado. Fonte: Elaborado pelo autor.

A partir daí, verifica-se o suporte ao protocolo. Caso a estação ou o ponto de acesso não implementem OWE, a associação recai, quando o AP opera em Modo de Transição, sobre a versão aberta e sem criptografia da mesma rede, garantindo compatibilidade com aparelhos mais antigos. Havendo suporte em ambos os lados, o fluxo prossegue pela via segura. A primeira etapa dessa via é a *Open System Authentication*, uma autenticação apenas formal, herdada do modo aberto e mantida por compatibilidade com o funcionamento interno do padrão 802.11. Nesse ponto não há qualquer verificação de identidade, apenas o cumprimento do procedimento previsto na norma. Segue-se então o núcleo criptográfico do protocolo, embutido no próprio processo de associação. No ***Association Request***, a estação gera um par de chaves efêmeras, isto é, chaves temporárias criadas apenas para aquela sessão e descartadas em seguida (e.g., como uma senha de uso único que perde a validade após o uso), e transmite ao ponto de acesso a metade pública desse par de chaves. A chave pública pode ser divulgada livremente, enquanto a chave privada correspondente permanece secreta em cada dispositivo. No ***Association Response***, o ponto de acesso responde com a sua própria chave pública efêmera. De posse da chave pública do outro lado e da sua própria chave privada, cada dispositivo calcula, de forma independente, um mesmo segredo compartilhado. Esse cálculo baseia-se na troca Diffie-Hellman em curva elíptica (ECDH), um método matemático que permite a duas partes chegarem a um valor secreto comum sem jamais transmiti-lo pelo ar. Por essa razão, um observador que apenas escute a comunicação não consegue reconstruir o segredo. O segredo obtido não é usado diretamente como chave. Na etapa de derivação da PMK, ele passa por uma função de derivação de chaves (HKDF), um procedimento que transforma um valor bruto em uma chave criptográfica de boa qualidade, produzindo a chave-mestra da sessão (*Pairwise Master Key* — PMK) e um identificador associado (PMKID), usado para agilizar reconexões futuras. A partir da PMK, executa-se o 4-way *handshake*, o mesmo mecanismo de troca de mensagens empregado pelo WPA2 e pelo WPA3, responsável por gerar a chave efetivamente utilizada no tráfego (*Pairwise Transient Key* — PTK) e instalá-la nos dois lados da conexão. Concluída essa etapa, a conexão atinge o estado final de tráfego cifrado, no qual os dados são protegidos pelo algoritmo AES (padrão de criptografia amplamente adotado, e.g., também usado em bancos e apli-

cativos de mensagens) no modo CCMP, e os quadros de gerenciamento são resguardados pelo PMF (*Protected Management Frames*), obrigatório neste protocolo.

Cabe destacar que, por não haver verificação da identidade do ponto de acesso em nenhuma dessas etapas, o OWE assegura sigilo contra a escuta passiva, isto é, contra quem apenas intercepta o tráfego, mas não impede que um atacante ativo se passe pelo ponto de acesso legítimo e se posicione no meio da comunicação, limitação retomada na análise de segurança apresentada adiante. A fim de tornar mais explícita a ordem cronológica e a direção de cada mensagem trocada entre os dois dispositivos, a Figura 2.3 apresenta o mesmo processo sob a forma de um diagrama de sequência, no qual o tempo decorre de cima para baixo e cada seta representa um quadro efetivamente transmitido pelo meio sem fio.

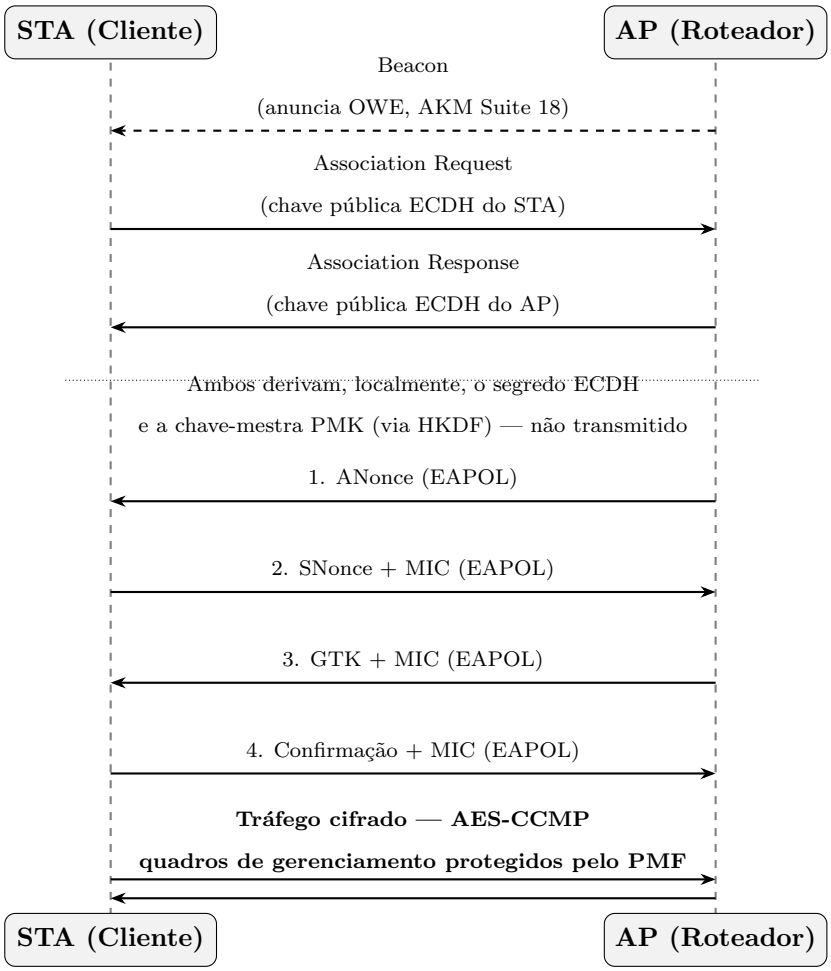



Figura 2.3: Diagrama de sequência da troca de mensagens no estabelecimento de uma conexão OWE, da descoberta ao tráfego cifrado. Fonte: Elaborado pelo autor.

### 2.3.1 A Padronização pela RFC 8110

A formalização técnica do OWE foi estabelecida pela publicação da RFC 8110 (*Request for Comments* número 8110), elaborada pela *Internet Engineering Task Force* (IETF) em março de 2017 (HARKINS; KUMARI, 2017). O documento define uma extensão ao padrão IEEE 802.11 voltada para fornecer confidencialidade e proteção de dados em conexões não autenticadas.

Conforme detalhado no texto da RFC, a principal motivação para a criação do protocolo foi a realidade do cenário comercial, no qual operadoras e estabelecimentos preferiam manter redes Wi-Fi abertas para maximizar a facilidade de acesso. Contudo, essa conveniência expunha todo o tráfego a ataques de escuta passiva (*passive eavesdropping*). O documento especifica que o OWE deve utilizar algoritmos de troca de chaves Diffie-Hellman embutidos diretamente nos quadros de associação da rede, gerando uma Chave Mestre (PMK) única para cada dispositivo de forma transparente.

Um aspecto relevante ressaltado pela própria RFC 8110 é a delimitação do seu escopo de segurança: o protocolo foi projetado estritamente para mitigar ataques passivos e injeções simples de tráfego. Como a arquitetura oportunística não exige credenciais prévias ou certificados, ela não oferece autenticação criptográfica que ateste a identidade do roteador (HARKINS; KUMARI, 2017). Portanto, embora o OWE estabeleça um canal seguro contra escuta passiva, ele, operando isoladamente, não previne ataques ativos do tipo *Man-in-the-Middle* (como roteadores falsos do tipo *Evil Twin*), pois o dispositivo do usuário não tem como verificar previamente se o ponto de acesso ao qual está se conectando é legítimo.

### 2.3.2 4-Way *Handshake*

Após a associação inicial, a segurança consolida-se em quatro etapas. O Ponto de Acesso envia um desafio aleatório (ANonce) ao cliente. O cliente processa a informação e devolve a segunda mensagem (SNonce) com um código de integridade. O roteador valida os dados e envia a terceira mensagem contendo a chave de grupo (GTK) (NETO, 2021). Por fim, o cliente confirma a operação na quarta mensagem, ativando o canal criptografado.

### 2.3.3 Diffie-Hellman

O pilar do OWE é a troca de parâmetros utilizando o algoritmo Diffie-Hellman (DH), adaptado para operar com Curvas Elípticas (ECDH). Ele baseia-se no Problema do Logaritmo Discreto, permitindo que dois dispositivos derivem uma mesma chave secreta a partir de informações transmitidas publicamente, sem a necessidade de transmitir a chave no canal (PIRES, 2010). O processo criptográfico ocorre em etapas bem definidas. Primeiramente, o Ponto de Acesso e o cliente acordam abertamente sobre o número primo (frequentemente denotado como $q$) e a raiz primitiva base ($\alpha$). Na sequência, cada dispositivo gera e armazena localmente um número aleatório e secreto ($X_a$ e $X_b$), que não serão transmitidos sob nenhuma hipótese. A etapa seguinte consiste no cálculo das chaves públicas: cada nó aplica a exponenciação modular utilizando o seu segredo interno para derivar a chave pública de transmissão ($Y_a$ e $Y_b$), onde $Y_a = \alpha^{X_a} \pmod q$ e $Y_b = \alpha^{X_b} \pmod q$. Por fim, ao receber a chave pública da outra parte, cada dispositivo a combina com o seu próprio segredo interno para derivar a Chave Mestre ($K$). Devido às propriedades comutativas da exponenciação modular, o cálculo efetuado independentemente por ambas as partes converge para a mesma chave, sem expor os componentes confidenciais. Adotando-se a notação clássica da literatura, em que a base $\alpha$ é escrita como $g$, o primo $q$ como $p$ e os segredos $X_a$ e $X_b$ como $a$ e $b$, o cruzamento obedece à seguinte propriedade matemática (PIRES, 2010):

$$S = (g^b)^a \pmod p = g^{ab} \pmod p = (g^a)^b \pmod p \tag{2.1}$$

A segurança desta troca fundamenta-se no Problema do Logaritmo Discreto (PLD). Conforme Oliveira (2021) aponta em seus estudos sobre o algoritmo, embora os computadores resolvam rapidamente exponenciais usando o módulo de um número primo, a operação inversa é computacionalmente inviável. Portanto, um invasor não conseguirá extrair as chaves originais mesmo que intercepte os valores públicos transmitidos no ar.

**A Aplicação Prática no Wi-Fi 6 (Curvas Elípticas - ECDH)**

Para reduzir o custo computacional em roteadores e dispositivos móveis, o modelo Diffie-Hellman moderno apoia-se na geometria das Curvas Elípticas (ECDH). O cálculo por logaritmos extensos é substituído pela multiplicação de pontos a partir de um ponto público ($G$) na curva. Os segredos ($d_A$ e $d_B$) permanecem locais, mas as chaves públicas tornam-se coordenadas na curva ($Q_A = d_A \times G$ e $Q_B = d_B \times G$). O Segredo Compartilhado ($S$) é derivado assim que as partes combinam as coordenadas recebidas com seus segredos locais:

$$S = d_A \times Q_B = d_A \times (d_B \times G) = d_B \times (d_A \times G) = d_B \times Q_A \tag{2.2}$$

Um interceptador capturará apenas os valores públicos ($Q_A$ ou $Q_B$). Reverter a geometria da curva elíptica para descobrir os segredos privados é computacionalmente inviável com os recursos atuais (PIRES, 2010).

### 2.3.4 Representação Visual do Diffie-Hellman

A representação visual do processo pode ser compreendida por meio do fluxograma da Figura 2.4.

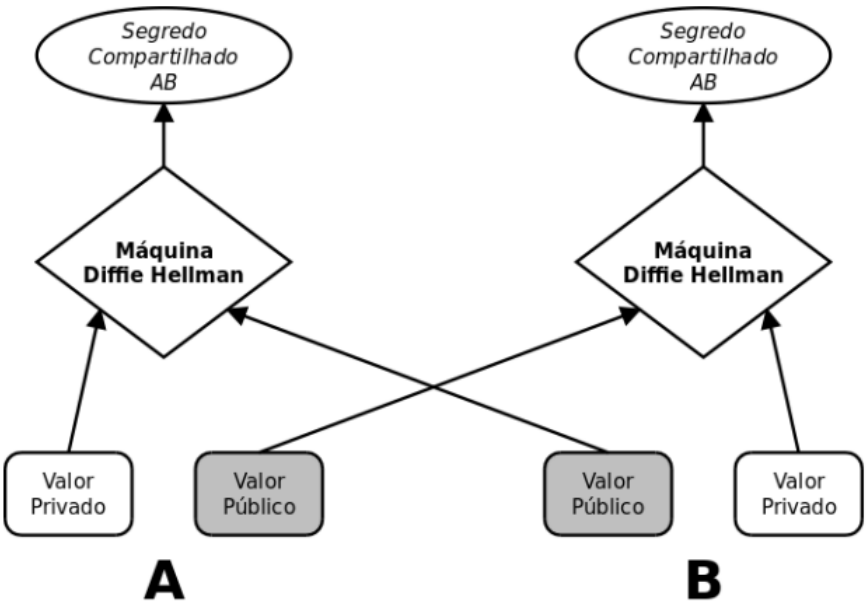



Figura 2.4: Fluxograma matemático e visual do acordo de chaves Diffie-Hellman. Fonte: Adaptado de (PIRES, 2010).

Nesta representação, duas entidades independentes, A e B, utilizam um canal público não seguro para iniciar a troca. Cada uma delas insere o seu valor privado — correspondente aos expoentes secretos $X_a$ e $X_b$ da formulação apresentada anteriormente — na respectiva "máquina" de cálculo, obtendo um valor público que pode trafegar abertamente pelo canal, equivalente às chaves híbridas $Y_a$ e $Y_b$. Ao combinar o valor público recebido do outro lado com o próprio valor privado, cada máquina converge para o mesmo segredo compartilhado. O diagrama evidencia, de forma esquemática, a propriedade central do método: como o valor privado nunca é transmitido pelo canal — apenas os valores públicos o são —, um invasor que intercepte a comunicação não consegue reconstituir o segredo comum a partir do que foi capturado.

# 3 Materiais e Métodos

## 3.1 Classificação da Pesquisa

Esta pesquisa categoriza-se como aplicada e de natureza experimental. O trabalho baseia-se na implementação de um ambiente de testes controlado para submeter a estrutura de protocolos de rede a auditorias passivas, avaliando as camadas de enlace e aplicação nas negociações criptográficas e no sequenciamento cronológico das capturas.

## 3.2 Arquitetura do Ambiente de Testes

Os roteadores comerciais limitam o acesso para auditorias analíticas profundas devido às restrições de *firmware*. Para contornar essa limitação, foi implementado o formato ***Soft AP*** (*Software Access Point*), gerenciado via sistema operacional Linux. O modelo virtualiza a controladora primária de uma interface Wi-Fi USB, submetendo o gerenciamento de pacotes ao controle direto do sistema (MALINEN, 2024).

A topologia deste ambiente de testes está detalhada na Figura 3.1.

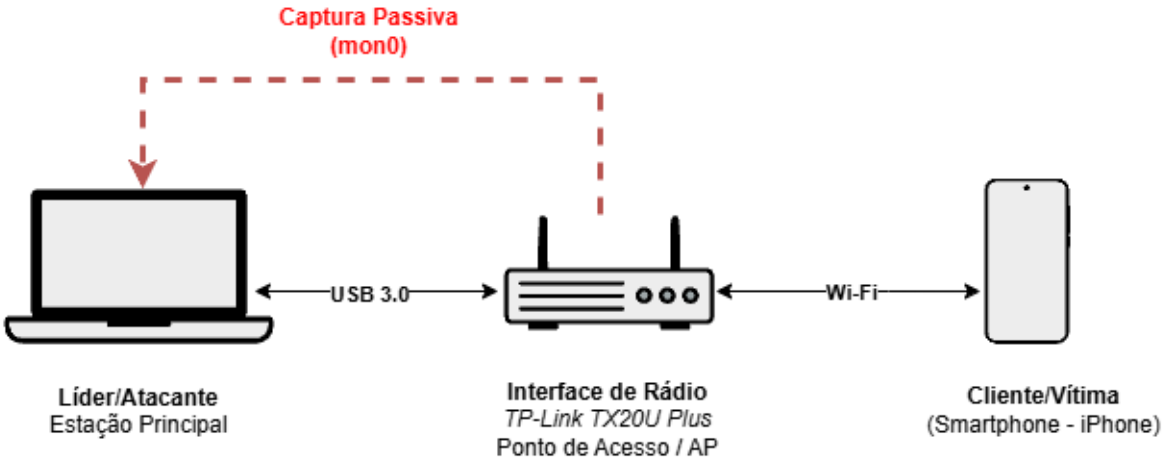



Figura 3.1: Arquitetura e topologia do laboratório. Fonte: Elaborado pelo autor.

O fluxo do sistema apoia-se no barramento USB 3.0, que intermedeia a comunicação entre o *host* Linux e o adaptador de rádio. Os canais de rádio transmitem os

pacotes através da interface `wlan0`. Para a coleta de dados, inicializou-se uma interface paralela em **Modo Monitor** (`mon0`). Esta interface opera sem endereço IP, atuando de forma unidirecional para escuta contínua. Diferentemente do *modo promíscuo* de redes cabeadas, o modo monitor permite que a placa Wi-Fi intercepte quadros de rádio sem a necessidade de associação com o roteador (SANTOS, 2024).

### 3.2.1 Recursos de Hardware e Software

A infraestrutura contou com o adaptador de rede **TP-Link Archer TX20U Plus**, compatível com o padrão AX1800 e as diretivas WPA3 e PMF (TP-LINK PORTUGAL, 2026).


testes. Fonte: Elaborado pelo autor.
testes. Fonte: Elaborado pelo autor.

Figura 3.2: Adaptador de rede TP-Link Archer TX20U Plus utilizado no ambiente de testes. Fonte: Elaborado pelo autor.

Como dispositivo cliente, utilizou-se um **Apple iPhone 16E**, compatível nativamente com o protocolo OWE. O suporte lógico foi provido pelo serviço `hostapd` (MALINEN, 2024), que atuou como roteador virtual. A captura e a decodificação forense dos pacotes foram executadas com o software Wireshark.

### 3.2.2 Aferição Computacional (*Overhead*)

Para mensurar a sobrecarga de processamento gerada pelas operações criptográficas, avaliaram-se os *timestamps* registrados pelo Wireshark em cada requisição. O resultado foi cruzado com o volume total de bytes gerados durante o estabelecimento de conexão. A fim de mitigar a influência de variações momentâneas do canal de rádio e do escalonamento do sistema operacional sobre uma medição isolada, o procedimento de estabelecimento de conexão OWE foi repetido em $N = 5$ execuções independentes, permitindo reportar o tempo total de conexão como uma média acompanhada do respectivo desvio padrão.

## 3.3 Preparação do Roteador

Para assegurar o isolamento de processos concorrentes no Linux, os serviços de rede nativos foram encerrados com a ferramenta `airmon-ng` (SMITH, 2008). Posteriormente, os cenários de testes foram parametrizados e executados em dois perfis distintos.

### 3.3.1 Cenário A: Rede Wi-Fi Aberta

A configuração `aberta.conf` instanciou uma rede pública sem chaves de segurança no canal 1 da frequência de 2,4 GHz. Este cenário forneceu a linha de base necessária para o comparativo temporal das conexões. As diretivas aplicadas no *hostapd* estão detalhadas no bloco abaixo:

Listing 3.1: Configurações do *hostapd* para a rede aberta (*baseline*). Fonte: Elaborado pelo autor.

```
interface=wlan0
driver=nl80211
ssid=REDE_ABERTA_PERIGOSA
```

```
hw_mode=g

channel=1
```

Diferentemente do Cenário B, aqui não há qualquer diretiva de criptografia ou gerenciamento de chaves (`wpa`, `wpa_key_mgmt`, `ieee80211w`). É justamente essa ausência que caracteriza a rede aberta: sem negociação de chaves e sem proteção dos quadros de gerenciamento, todo o tráfego circula em texto claro.


Figura 3.3: Dispositivo móvel associado à rede do Cenário A (Rede Wi-Fi Aberta). Fonte: Elaborado pelo autor.

### 3.3.2 Cenário B: Rede com Protocolo OWE

O cenário B ativou os requisitos normativos do OWE documentados na RFC 8110 (HARKINS; KUMARI, 2017), por meio do arquivo `owe.conf`. As configurações aplicadas no *hostapd* estão detalhadas no bloco abaixo:

Listing 3.2: Configurações do *hostapd* para habilitar a rede OWE. Fonte: Elaborado pelo autor.

```
interface=wlan0

driver=nl80211

ssid=TESTE_OWE_FINAL
```

```
hw_mode=g
channel=1
wpa=2
wpa_key_mgmt=OWE
rsn_pairwise=CCMP
ieee80211w=2
group_mgmt_cipher=AES-128-CMAC
```

O parâmetro `ieee80211w=2` aplica a obrigatoriedade da proteção de quadros de gerenciamento (PMF). A ausência dessa configuração inviabiliza a consolidação da criptografia oportunística na rede.


Figura 3.4: Dispositivo móvel associado à rede do Cenário B (Rede com Protocolo OWE). Fonte: Elaborado pelo autor.

Cabe uma ressalva quanto à interface do dispositivo cliente exibida na Figura 3.4: mesmo tratando-se da rede protegida pelo OWE, o iOS classifica-a como "Rede Não Protegida". Essa rotulagem decorre do fato de o sistema operacional basear sua indicação de segurança na exigência de uma credencial compartilhada (senha), e não na presença de criptografia no enlace. Como o próprio OWE dispensa esse tipo de autenticação — e, conforme discutido na RFC 8110, não oferece verificação criptográfica da identidade do ponto de acesso (HARKINS; KUMARI, 2017) —, o dispositivo o enquadra visualmente

na mesma categoria das redes abertas tradicionais, ainda que o tráfego permaneça cifrado por trás dessa interface, como demonstrado adiante na análise forense dos resultados.

## 3.4 Inicialização da Interface de Monitoramento

A interface virtual de monitoramento foi iniciada e atrelada ao rótulo `mon0` através da linha de comando:

```
sudo iw dev wlan0 interface add mon0 type monitor && sudo ip link
    set mon0 up
```

O Wireshark foi parametrizado para registrar todos os *frames* de comunicação que circundavam os SSIDs utilizados no experimento.

# 4 Resultados e Discussões

## 4.1 *Beacon Frame*

A etapa inicial do estudo consistiu no monitoramento forense do quadro de anúncio da rede (*Beacon Frame*). Quando o roteador operou sob as diretivas do OWE, o *frame* de transmissão refletiu imediatamente as alterações estruturais na configuração de segurança.

Ao analisar o pacote capturado no Wireshark (Figura 4.1), nota-se a inserção do elemento normativo obrigatório `RSN Information`.

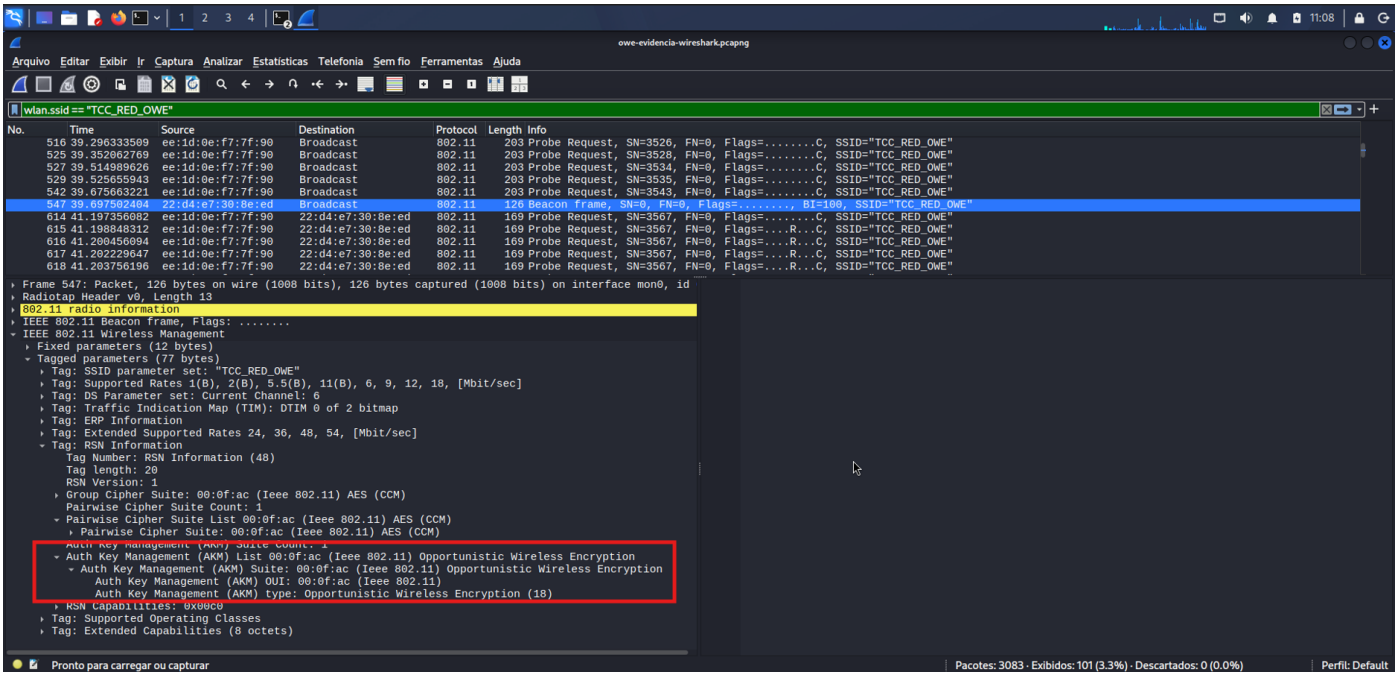



Figura 4.1: *Beacon Frame* evidenciando a utilização do AKM Suite 18. Fonte: Elaborado pelo autor.

A presença do campo *AKM Suite* assinalado com o valor **18** informa às estações receptoras que a rede em operação requer suporte ao padrão Opportunistic Wireless Encryption.

## 4.2 Troca de Chaves Diffie-Hellman

A captura de rede revelou que a requisição de associação (*Association Request*) enviada pelo dispositivo cliente integra a troca inicial de parâmetros matemáticos necessários para a formulação da chave em curvas elípticas. A expansão do pacote gerencial evidencia o uso obrigatório da extensão `OWE Diffie-Hellman Parameter`, conforme documentado na Figura 4.2.

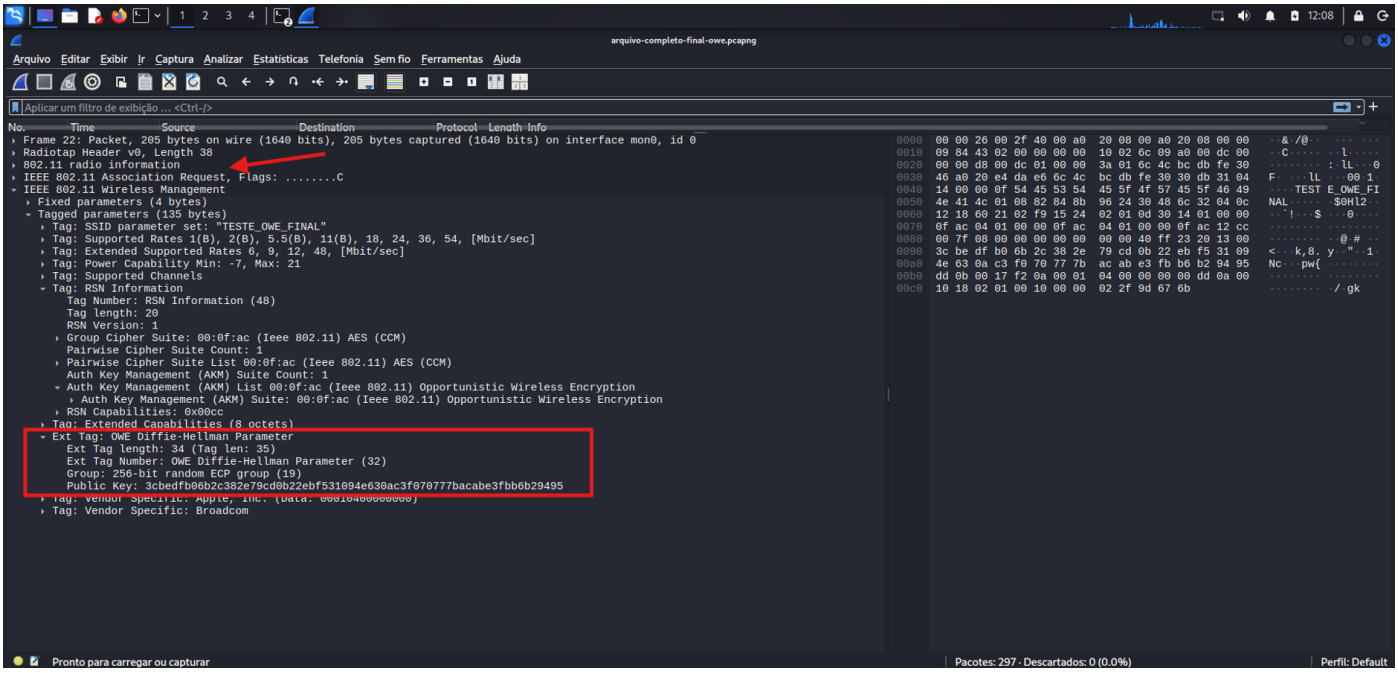



Figura 4.2: *Association Request* exibindo a chave pública do cliente (OWE Diffie-Hellman Parameter). Fonte: Elaborado pelo autor.

A análise confirma que a estação cliente submete suas variáveis criptográficas atreladas ao grupo operacional padrão da curva elíptica. O roteador, processando a proposta com sucesso, finaliza a primeira fase matemática ao enviar o seu respectivo componente na resposta de associação, materializado na Figura 4.3.

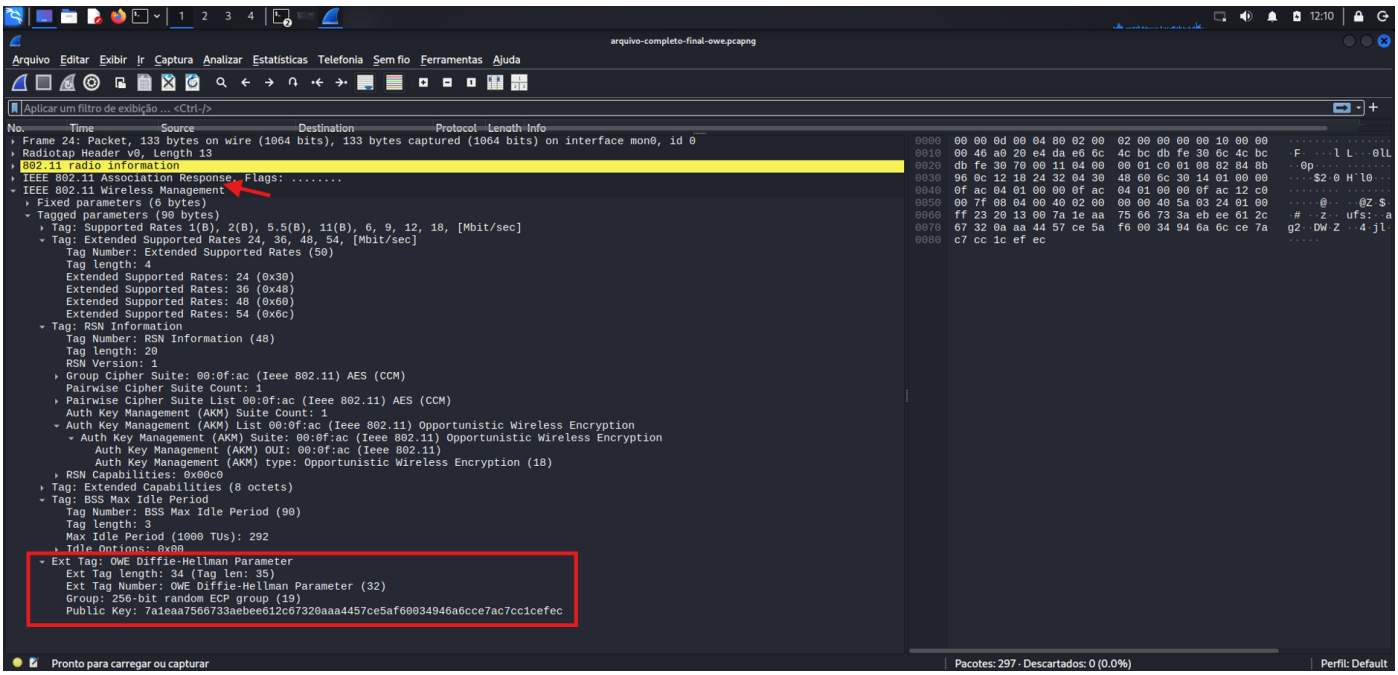



Figura 4.3: *Association Response* evidenciando a devolução do componente Diffie-Hellman pelo AP. Fonte: Elaborado pelo autor.

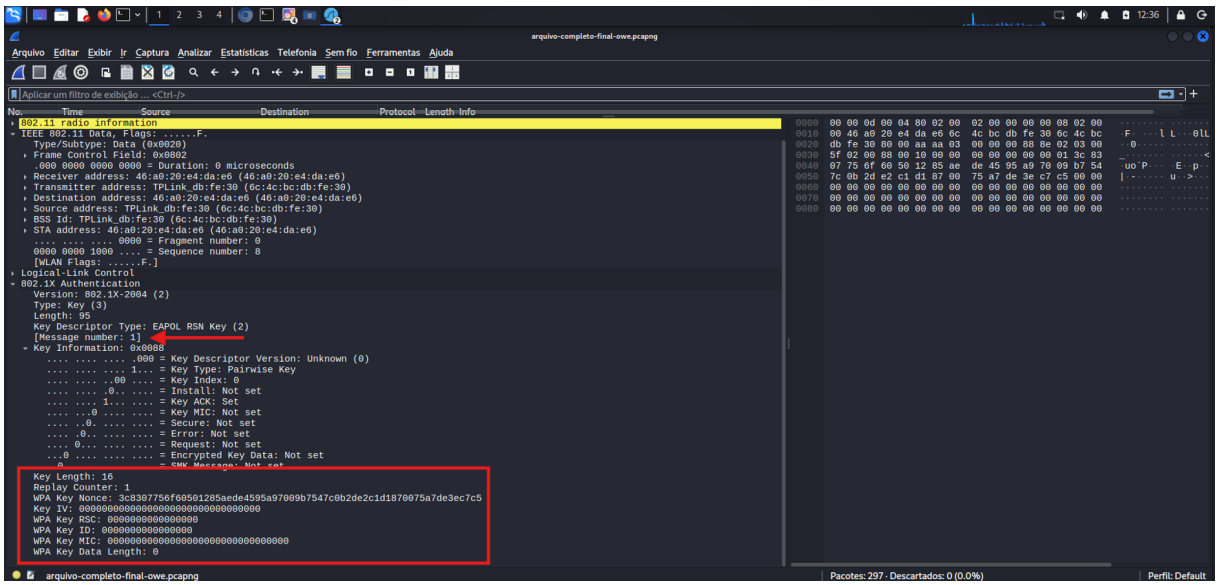
Com a troca de parâmetros devidamente documentada no tráfego, confirma-se a viabilidade do cálculo criptográfico independente realizado pelos dispositivos para a derivação do Segredo Compartilhado (PMK).

## 4.3 Validação do *4-Way Handshake*

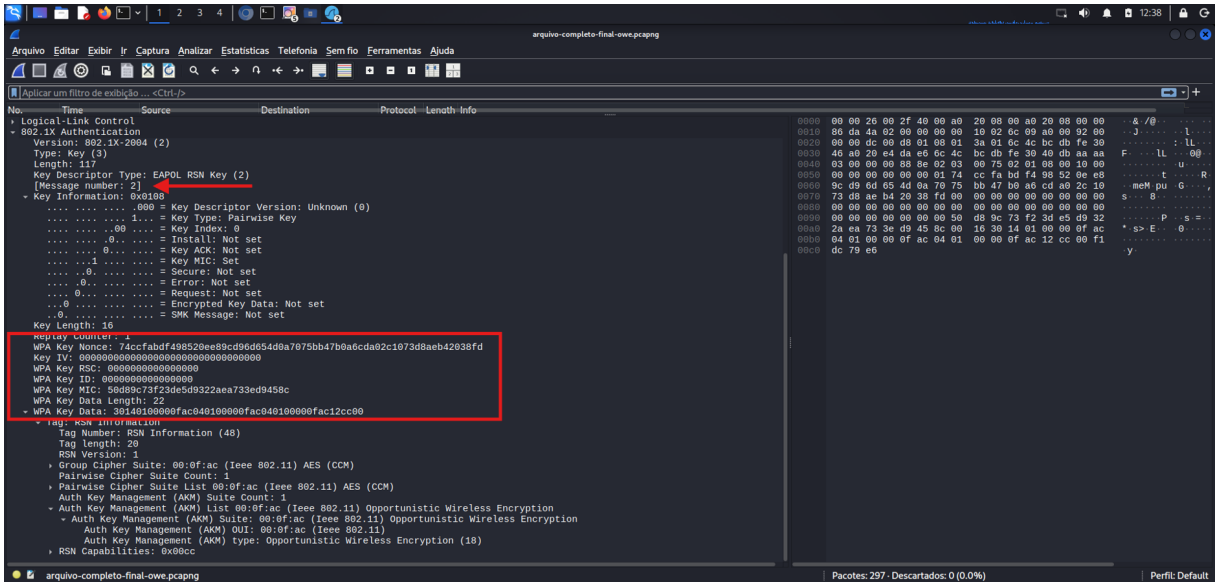
Após a derivação do segredo compartilhado, o sistema inicia automaticamente a autenticação sequencial do protocolo EAPOL (*4-Way Handshake*). Essa etapa é responsável por verificar a autenticidade das partes e ativar a criptografia em todo o tráfego subsequente.

As capturas sequenciais, documentadas na Figura 4.4, descrevem o fluxo dos pacotes de autenticação e distribuição de chaves de grupo.

O sucesso nesta fase confirma que os cálculos baseados no Diffie-Hellman em curvas elípticas foram corretamente executados. Os pacotes do usuário passam a ser protegidos pela suíte AES-CCMP de 128 bits.



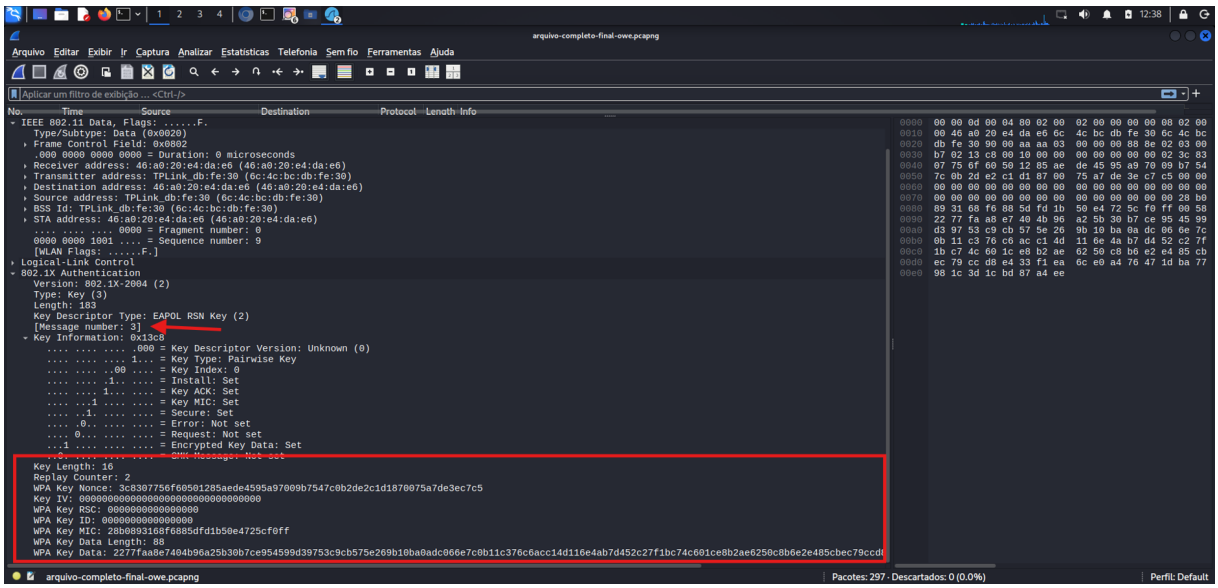

(a) Mensagem 1 do 4-Way *Handshake*: Envio do ANonce pelo AP.



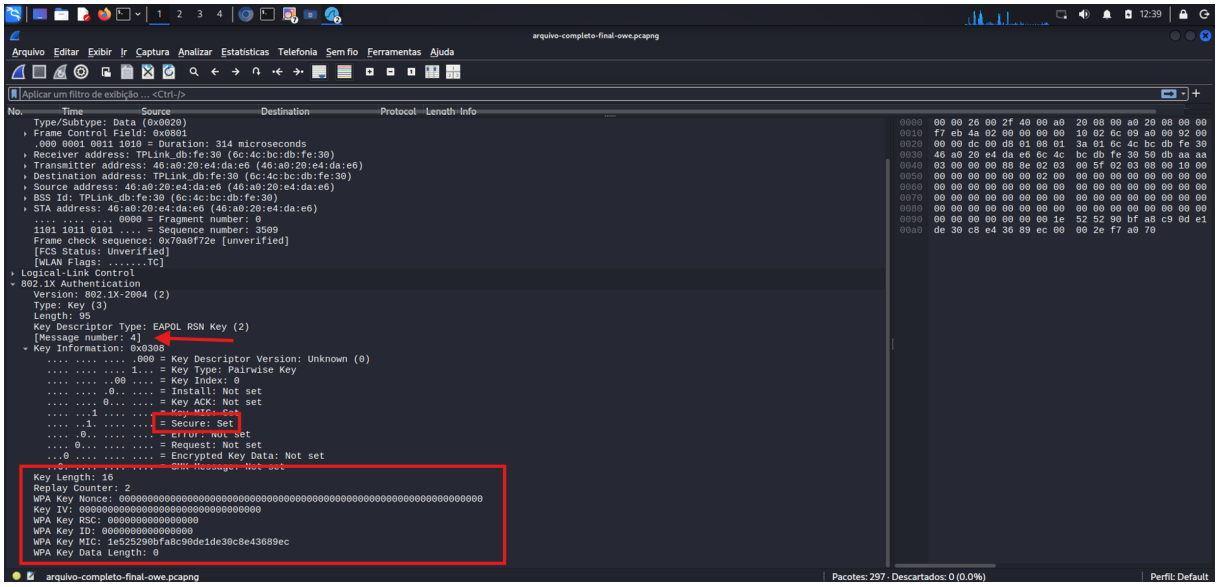

(b) Mensagem 2 do 4-Way *Handshake*: Retorno do SNonce e MIC pela estação.

## 4.4 Análise Forense da Rede Wi-Fi Aberta

Para avaliar o contraste de segurança proporcionado pelo OWE, a simulação testou o comportamento da arquitetura legada (rede aberta). A captura do *Association Request* expôs a ausência de diretivas de segurança no tráfego. A análise revela que, no modelo aberto, o campo de privacidade das comunicações é transmitido como negativo, conforme evidenciado na Figura 4.5.

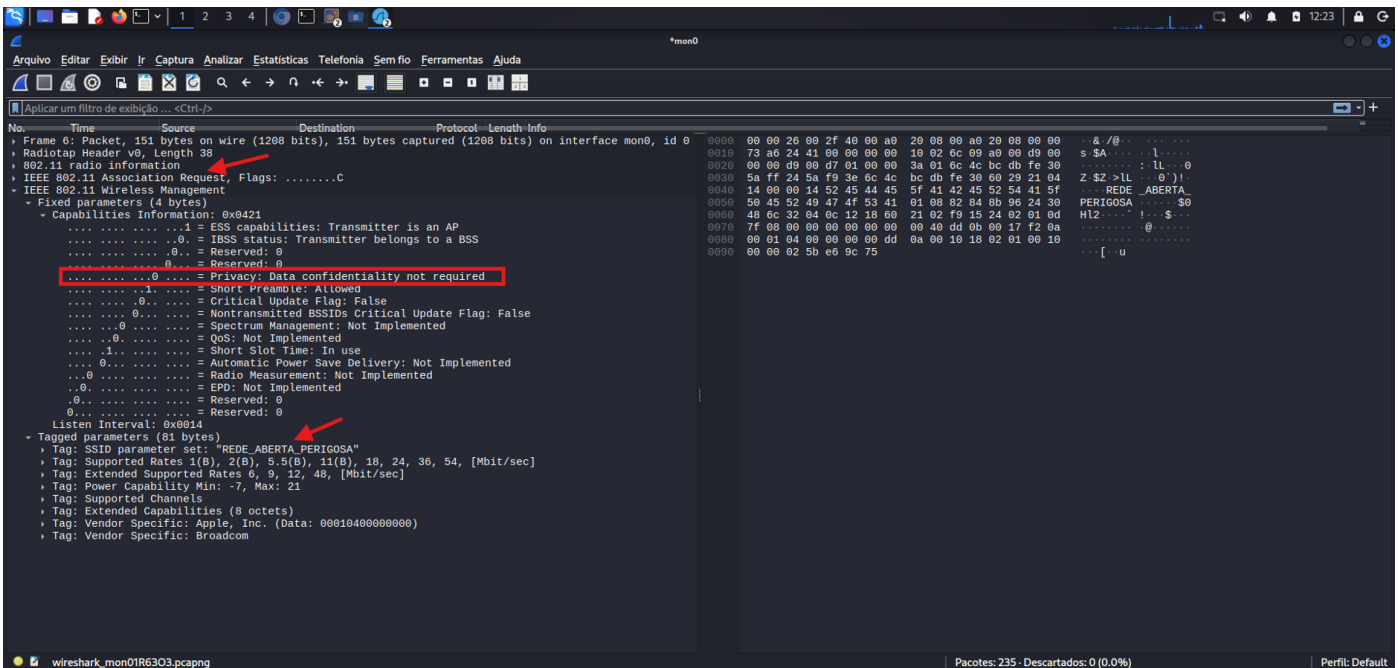



(c) Mensagem 3 do 4-Way *Handshake*: Estabelecimento da GTK.




(d) Mensagem 4 do 4-Way *Handshake*: Confirmação e estabelecimento do canal seguro.

Figura 4.4: Capturas sequenciais do 4-Way *Handshake* (EAPOL) e estabelecimento das chaves criptográficas. Fonte: Elaborado pelo autor.



Esta flag confirma que a rede e o roteador não realizam qualquer negociação criptográfica ou troca de chaves. Os dados trafegam sem encapsulamento, expondo o usuário a uma vulnerabilidade intrínseca de projeto.

## 4.5 Interceptação Passiva de Tráfego

O impacto prático do modelo aberto tornou-se evidente quando o cliente realizou a solicitação de endereço na rede local. Conforme registrado na Figura 4.6, o pacote DHCP foi inteiramente decodificado pela escuta passiva.

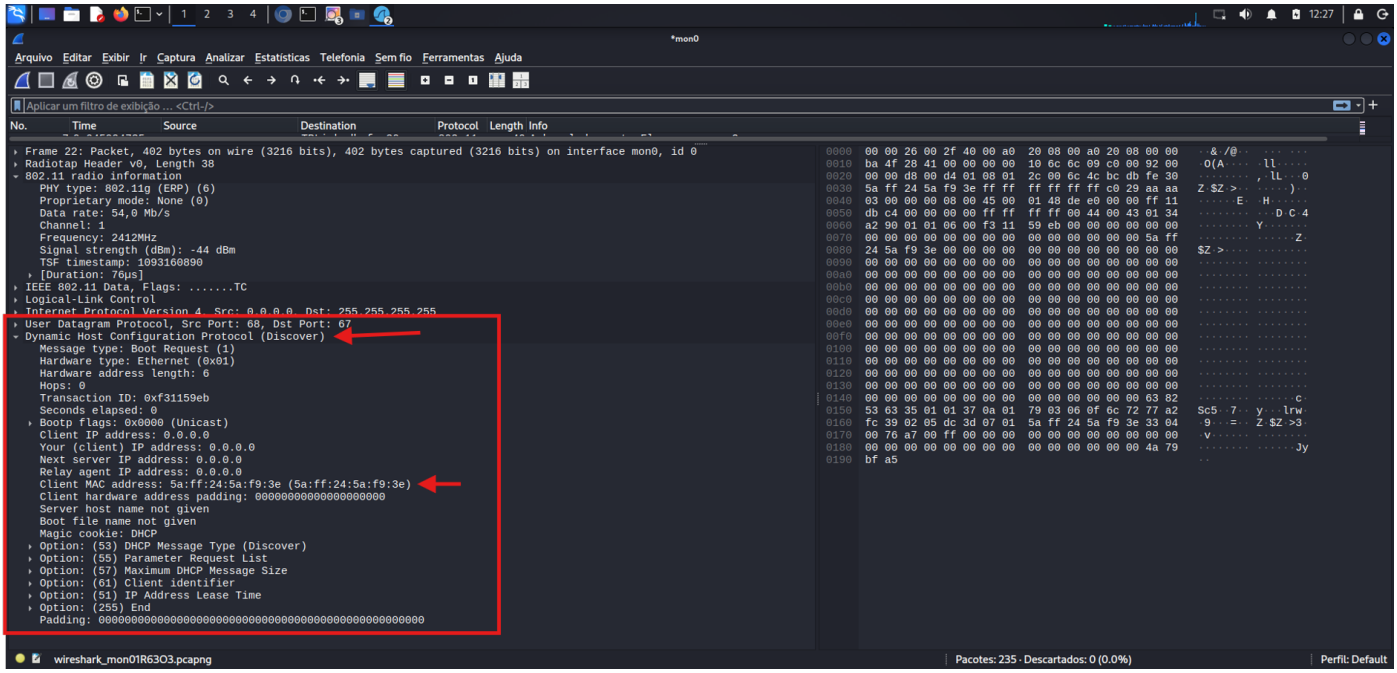


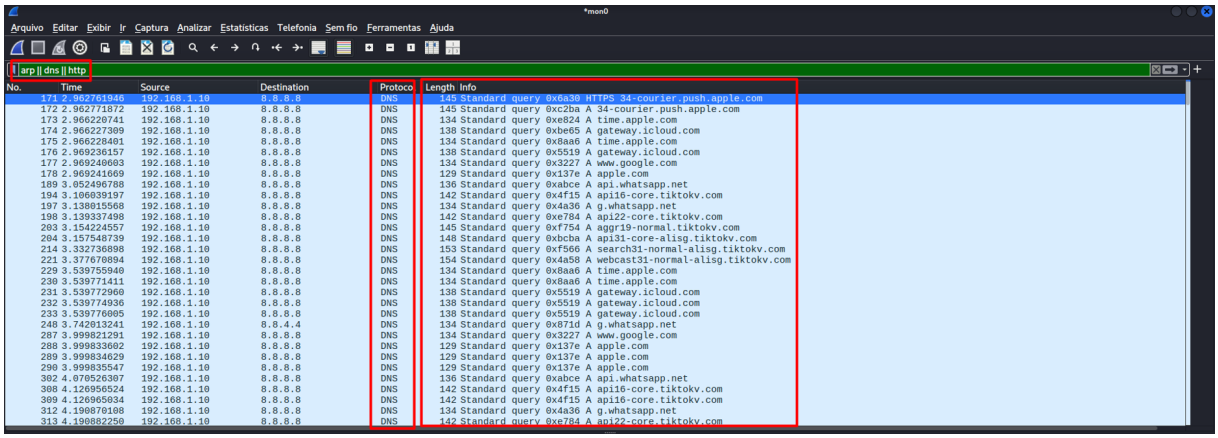

Figura 4.6: Pacote DHCP Discover exposto e decodificado na rede legada. Fonte: Elaborado pelo autor.

A interface de monitoramento extraiu o endereço MAC real e os parâmetros completos de roteamento do dispositivo, comprovando que, sem o OWE, não há confidencialidade nesse modelo de rede. Esse resultado ilustra os riscos práticos dos ataques do tipo *eavesdropping* (SANTOS, 2024).

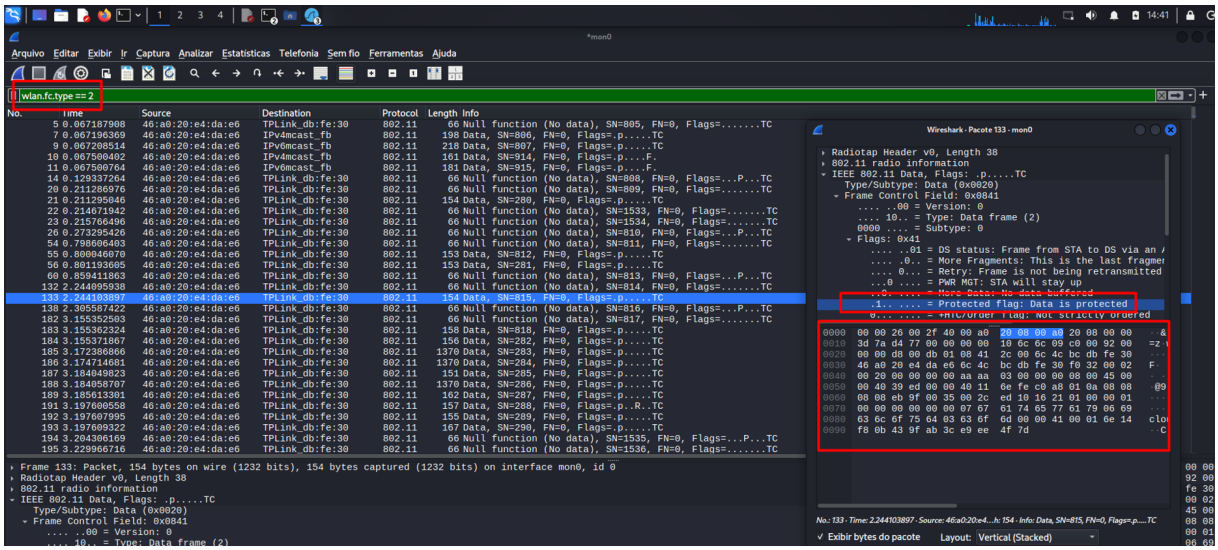
## 4.6 Análise Forense na Camada de Aplicação

A bateria de testes avaliou o vazamento de informações na Camada 7 do modelo OSI, cobrindo os protocolos HTTP e DNS. Um acesso direto foi realizado via navegador web

para o domínio de teste `neverssl.com`. Na **Rede Aberta** (Figura 4.7a), a interface de monitoramento capturou as URLs de destino em texto claro, demonstrando a facilidade em catalogar as preferências de acesso de qualquer usuário. Na **Rede OWE**, a mesma rotina de monitoramento não obteve informações legíveis. A criptografia da camada de enlace bloqueou qualquer interpretação superior, classificando os dados unicamente como tráfego `QoS Data`. A marcação da `Protected flag: 1` (Figura 4.7b) confirma o encapsulamento dos cabeçalhos.



(a) Tráfego HTTP/DNS legível em rede pública não criptografada.

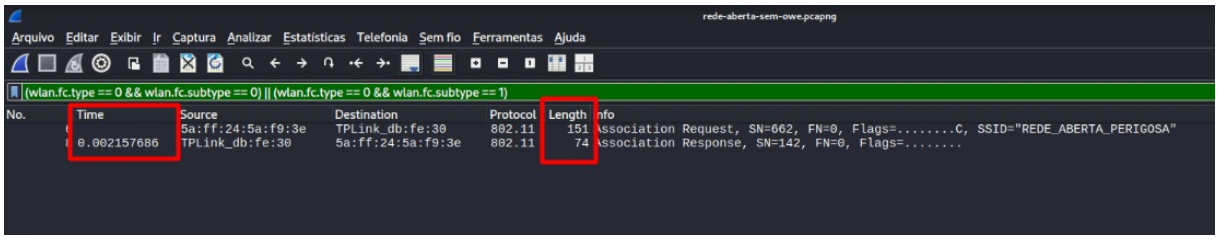


(b) Tráfego encapsulado (QoS Data) sob a proteção do OWE.

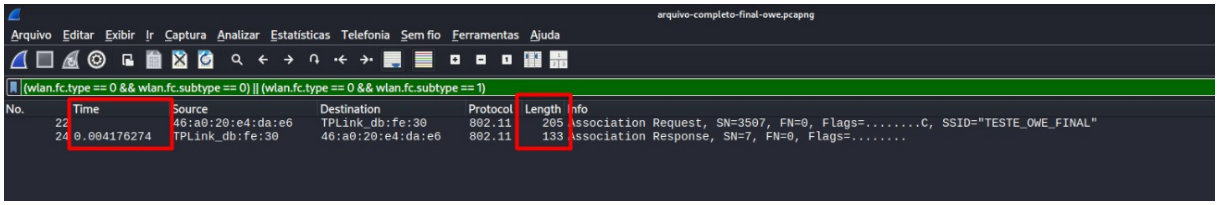
Figura 4.7: Comparativo do tráfego da camada de aplicação capturado nas redes aberta e OWE. Fonte: Elaborado pelo autor.

## 4.7 *Overhead*

A introdução de operações criptográficas adiciona penalizações de velocidade (*latência*) e tamanho do pacote (*payload*). Os *timestamps* registrados pelo Wireshark foram coletados para avaliar esse impacto no cenário prático. A título ilustrativo, uma captura representativa individual evidencia a composição do tempo de conexão: a Figura 4.8a mostra que a associação em rede aberta necessita de uma transação de **151 bytes**, concluída em **2,15 milissegundos**. Com o OWE habilitado, a adição do envelope criptográfico ECDH ampliou o tamanho do pacote para **205 bytes**, com tempo de processamento de **4,17 milissegundos** (Figura 4.8b). Essa diferença representa um aumento de aproxi-




(a) Latência e dimensões do pacote na associação em rede aberta.




(b) Aumento das dimensões e latência na associação OWE devido ao ECDH.

Figura 4.8: Comparativo da latência (*delta* temporal) de associação. Fonte: Elaborado pelo autor.

madamente 100% no tempo de associação e de 35% no tamanho do pacote. Contudo, variações na faixa de poucos milissegundos são imperceptíveis ao usuário durante a navegação. O comparativo detalhado na Figura 4.9 apresenta a composição do tempo total de estabelecimento de conexão.

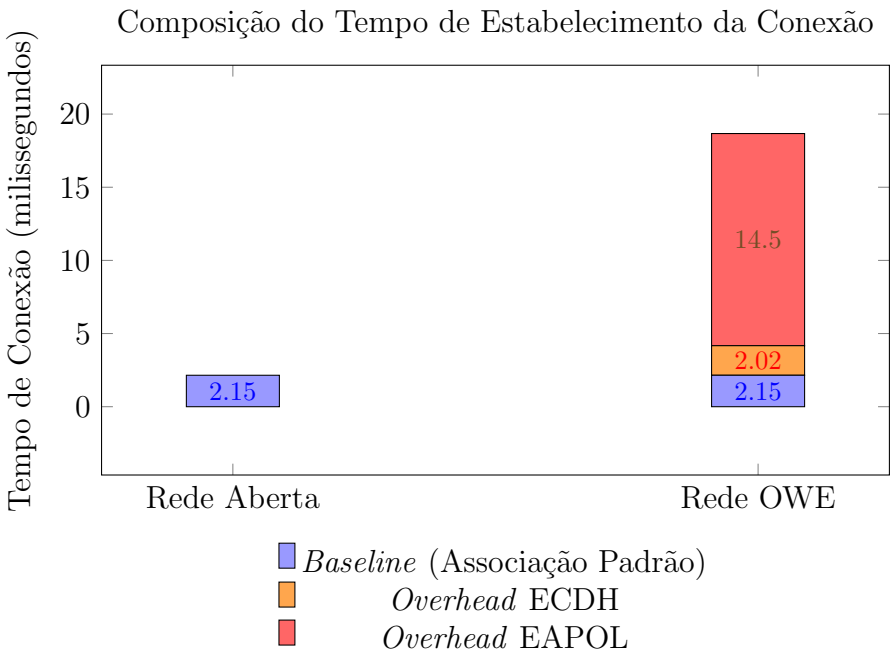



Figura 4.9: Distribuição dos custos temporais (*overhead*) integrados ao OWE. Fonte: Elaborado pelo autor.

A Figura 4.10 apresenta, para essa mesma captura ilustrativa, a evolução temporal acumulada do processo de conexão, atingindo 18,67 milissegundos no total para a rede OWE naquela execução específica.

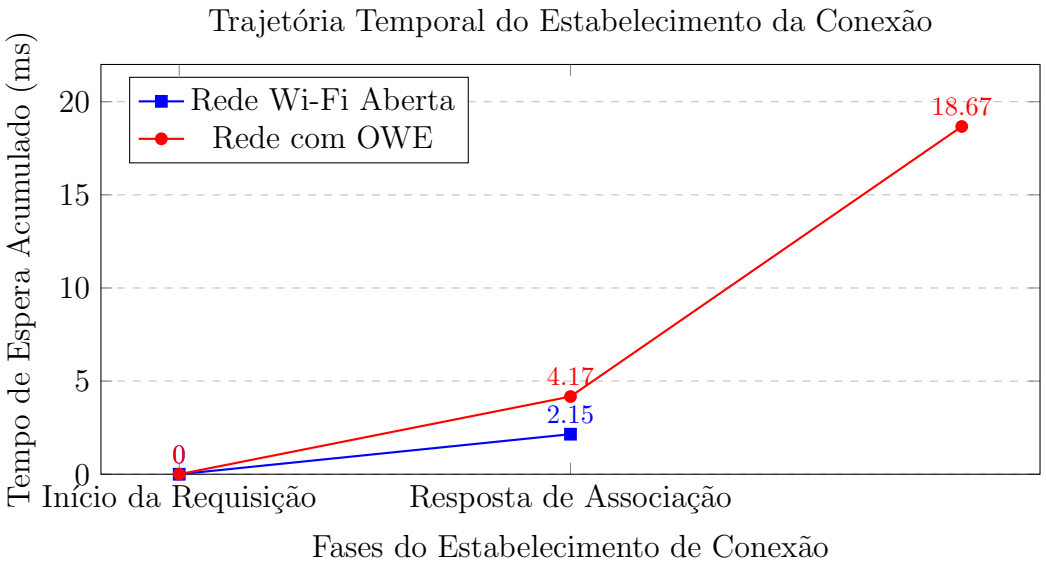



Figura 4.10: Evolução temporal do estabelecimento de conexão (Rede Aberta vs OWE). Fonte: Elaborado pelo autor.

Embora ilustrativa da composição do custo temporal, uma única captura não é suficiente para caracterizar o comportamento do protocolo diante de variações momentâneas do canal de rádio e do escalonamento do sistema operacional. Por esse motivo, o procedi-

mento completo de conexão OWE — da requisição de associação até a quarta mensagem do *4-Way Handshake* — foi repetido em $N = 5$ execuções independentes, detalhadas na Tabela 4.1. O tempo total de conexão observado nessas repetições apresentou média de **40,29 milissegundos**, com desvio padrão de **4,58 milissegundos** (coeficiente de variação de aproximadamente 11%), indicando uma sobrecarga consistente e reprodutível, ainda que superior à observada na captura ilustrativa isolada. Atribui-se essa diferença, ao menos em parte, à natureza do ambiente de testes: por se tratar de um *Soft AP* executado em um sistema operacional de propósito geral, sem aceleração criptográfica em *hardware* dedicado, o processamento está sujeito a trocas de contexto e a um escalonamento não determinístico que um roteador comercial com *firmware* dedicado tende a não apresentar. Ainda assim, mesmo no cenário mais conservador, um acréscimo da ordem de 40 milissegundos por conexão permanece imperceptível ao usuário final.

Tabela 4.1: Tempo total de conexão OWE (*Association Request* até a Mensagem 4 do *4-Way Handshake*) em cinco execuções independentes

| **Execução** | **Tempo de conexão (ms)** |
|---|---|
| 1 | 37,97 |
| 2 | 47,79 |
| 3 | 35,69 |
| 4 | 40,73 |
| 5 | 39,28 |
| **Média** | **40,29** |
| **Desvio padrão** | **4,58** |

### 4.7.1 Extrapolação para Múltiplos Dispositivos

A avaliação anterior caracteriza o custo de uma única conexão OWE. Contudo, cenários de alta densidade de estações — como estádios, aeroportos e centros de eventos, mencionados na fundamentação teórica do Wi-Fi 6 — podem submeter o ponto de acesso a dezenas ou centenas de tentativas de associação em um curto intervalo de tempo. Como o ambiente de testes não permitiu a conexão física simultânea de múltiplos dispositivos, propõe-se aqui uma extrapolação analítica preliminar, a partir do custo médio por conexão

mensurado experimentalmente, para estimar a ordem de grandeza do impacto agregado sobre o processamento do ponto de acesso. Assumindo, como cenário conservador de pior caso, que o ponto de acesso processe as solicitações de associação de forma estritamente serial — isto é, sem paralelismo de *hardware* ou particionamento de carga entre múltiplos núcleos de processamento —, o tempo agregado de processamento cresce linearmente com o número $N$ de dispositivos conectantes:

$$T_{AP}(N) = N \times \overline{T}_{OWE} \tag{4.1}$$

em que $\overline{T}_{OWE} = 40{,}29$ ms corresponde ao tempo médio de conexão OWE mensurado experimentalmente. A Tabela 4.2 apresenta essa projeção para diferentes valores de $N$, comparando-a ao custo equivalente em uma rede aberta (sem criptografia) e ao acréscimo específico atribuível ao OWE.

Tabela 4.2: Extrapolação analítica do tempo agregado de processamento no ponto de acesso, em função do número de dispositivos conectantes

| **N dispositivos** | **Rede aberta (ms)** | **Rede OWE (ms)** | **Acréscimo do OWE (ms)** |
|---|---|---|---|
| 1 | 2,15 | 40,29 | 38,14 |
| 10 | 21,50 | 402,90 | 381,40 |
| 25 | 53,75 | 1.007,25 | 953,50 |
| 50 | 107,50 | 2.014,50 | 1.907,00 |
| 100 | 215,00 | 4.029,00 | 3.814,00 |
| 200 | 430,00 | 8.058,00 | 7.628,00 |

A projeção evidencia que, embora o custo por conexão individual permaneça imperceptível, o custo agregado cresce de forma proporcional a $N$ e passa a ser perceptível em cenários de alta densidade: com 100 dispositivos conectando-se em uma janela de tempo reduzida, o processamento criptográfico serializado poderia acumular da ordem de 4 segundos no ponto de acesso, sob a hipótese conservadora de ausência de paralelismo. Convém ressaltar que essa é uma extrapolação analítica baseada em hipóteses simplificadoras, e não uma medição direta: pontos de acesso comerciais tipicamente dispõem de algum grau de paralelismo de processamento, de modo que o impacto real tende a ser

inferior ao estimado por este modelo conservador. A validação experimental desse comportamento sob carga real de múltiplas conexões simultâneas permanece como uma das frentes de investigação futura indicadas ao final deste trabalho.

# 5 Considerações Finais

A disponibilização de redes Wi-Fi públicas frequentemente implicava um dilema entre usabilidade e segurança. O formato defasado do WPA2 permitia que o tráfego desprotegido circulasse sem restrições, expondo os usuários à interceptação passiva de dados. A partir da consolidação do protocolo WPA3 em conjunto com o padrão Wi-Fi 6, a Criptografia Oportunística (OWE) foi introduzida como resposta a essa lacuna.

O presente trabalho demonstrou, por meio de metodologia analítica e experimental, as vantagens do OWE. O ambiente de laboratório configurado como *Soft AP* permitiu mapear e extrair dados forenses detalhados que a arquitetura legada deixava expostos. Durante a simulação de tráfego desprotegido, constatou-se a incapacidade do Wi-Fi aberto em mitigar interceptações passivas, com os dados do cliente visíveis para qualquer interface em modo monitor. A implementação detalhou as bases do algoritmo Diffie-Hellman em Curvas Elípticas (ECDH). Observou-se a correta formulação e o intercâmbio de chaves públicas entre o roteador e o cliente, que culminou no protocolo EAPOL e garantiu a criptografia simétrica em AES de 128 bits. Destaca-se a eficácia obtida na auditoria da Camada de Aplicação, em que requisições HTTP e fluxos de DNS tornaram-se inacessíveis ao monitoramento passivo sob a proteção do OWE. Em relação ao *overhead* avaliado, o processo completo de conexão OWE acumulou, em média, 40,29 milissegundos (desvio padrão de 4,58 ms, sobre cinco execuções independentes) em relação aos 2,15 milissegundos da rede aberta. Para o usuário individual, esse acréscimo permanece imperceptível, o que confirma a viabilidade do protocolo para o uso cotidiano. Contudo, a extrapolação analítica realizada indica que, sob cenários de alta densidade de conexões simultâneas, o custo agregado no ponto de acesso pode se tornar não trivial, o que reforça a necessidade de validação experimental sob carga real como direção prioritária de trabalhos futuros. Ainda assim, o custo computacional imposto pelo OWE por conexão individual representa uma sobrecarga mínima diante do ganho significativo em privacidade para o usuário em redes abertas.

Como perspectivas de continuidade para os estudos sobre redes sem fio segu-

ras, identificam-se três frentes de pesquisa relevantes. A primeira consiste em realizar testes de desempenho em larga escala sob condições de alta concorrência, submetendo o controlador a múltiplas associações OWE simultâneas, de modo a quantificar o custo de processamento das operações de troca de chaves ECDH e identificar os limites de escalabilidade e os pontos de saturação da infraestrutura. A segunda frente propõe conduzir experimentos controlados de avaliação de resiliência das diretivas PMF (*Protected Management Frames*), aplicando vetores de ataque como o *Evil Twin* e tentativas de desautenticação, a fim de verificar a eficácia da proteção de integridade baseada em AES-CMAC diante de ataques ativos. Por fim, sugere-se investigar a viabilidade de adoção do protocolo em cenários com restrição de energia (Internet das Coisas – IoT), mensurando o custo computacional e energético das operações sobre curvas elípticas em implantações que não utilizam o Modo de Transição (*Transition Mode*).

Em conformidade com as diretrizes do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e com o Código de Conduta da Sociedade Brasileira de Computação (SBC), declaro que ferramentas de Inteligência Artificial Generativa foram empregadas de maneira assistiva durante o desenvolvimento desta monografia. O uso limitou-se à revisão gramatical, à formatação estrutural do código-fonte em LaTeX e à elaboração do código para os gráficos analíticos (via pacote *pgfplots*). A metodologia, a coleta no ambiente de testes, a análise de pacotes e a interpretação científica dos resultados são frutos de elaboração exclusivamente humana e intelectual do autor.

# Bibliografia

BELLALTA, B. IEEE 802.11ax: High-efficiency WLANs. *IEEE Wireless Communications*, v. 23, n. 1, p. 38–46, 2016.

HARKINS, D.; KUMARI, W. *Opportunistic Wireless Encryption*. [S.l.], 2017. Disponível em: ⟨https://www.rfc-editor.org/info/rfc8110⟩. Acesso em: 09 jun 2026.

IEEE. *IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 6: Medium Access Control (MAC) Security Enhancements*. [S.l.]: IEEE, 2004. IEEE Std 802.11i-2004.

IEEE. *IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. [S.l.]: IEEE, 2021. IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016).

IEEE. *IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 1: Enhancements for High-Efficiency WLAN*. 2021. IEEE Std 802.11ax-2021.

KHOROV, E. et al. A tutorial on IEEE 802.11ax high efficiency WLANs. *IEEE Communications Surveys & Tutorials*, v. 21, n. 1, p. 197–216, 2019.

MACEDO, K. de L. *Um estudo sobre a segurança de redes sem fio com o protocolo WPA3*. Dissertação (Mestrado) — Universidade Federal de Alagoas, Maceió, 2023.

MALINEN, J. *hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator*. 2024. Disponível em: ⟨https://w1.fi/hostapd/⟩. Acesso em: 09 jun 2026.

NETO, J. A. da S. *Segurança em Redes Wireless IEEE 802.11 e suas Vulnerabilidades*. Monografia (Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação)) — Pontifícia Universidade Católica de Goiás, 2021.

OLIVEIRA, C. J. G. de. *Protocolo Diffie-Hellman: contexto histórico, matemático e aplicações em sala de aula*. Monografia (Monografia (Especialização em Matemática)) — Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Cajazeiras, 2021.

Paiva Neto, E. de. *dh-aes-p4: Criptografia Oportunística Entre Dispositivos de Rede Programáveis*. Dissertação (Mestrado) — Universidade Federal do Rio Grande do Norte, Natal, 2022. Disponível em: ⟨https://repositorio.ufrn.br/⟩.

PIRES, R. de M. *Aplicação do Algoritmo Diffie-Hellman no Compartilhamento de Volumes Criptografados do TrueCrypt*. Monografia (Projeto Final de Curso (Bacharelado em Ciência da Computação)) — Universidade Federal de Goiás, Catalão, 2010.

SANTOS, L. M. dos. *Análise dos principais tipos de ataques em redes sem fio IEEE 802.11N*. Monografia (Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação)) — Universidade Federal de Alagoas, Maceió, 2024.

SMITH, J. *airmon-ng: Habilitar o Modo Monitor em interfaces sem fio*. [S.l.], 2008. Disponível em: ⟨https://www.aircrack-ng.org/doku.php?id=pt-br:airmon-ng⟩. Acesso em: 09 jun 2026.

SOUZA, C. E. de. *Uma análise comparativa dos protocolos de segurança WPA2 e WPA3 em redes sem fio*. Dissertação (Mestrado) — Pontifícia Universidade Católica de Goiás, Goiânia, 2022.

TANENBAUM, A. S.; WETHERALL, D. *Redes de Computadores*. 5. ed. São Paulo: Pearson, 2011.

TP-LINK PORTUGAL. *Placa de Rede USB Wireless AX1800 Dual Antenas de Alto Ganho — Archer TX20U Plus*. [S.l.], 2026. Disponível em: ⟨https://www.tp-link.com/pt/home-networking/adapter/archer-tx20u-plus/⟩. Acesso em: 09 jun 2026.

VANHOEF, M.; PIESSENS, F. Key reinstallation attacks: Forcing nonce reuse in WPA2. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. [S.l.]: ACM, 2017. p. 1313–1328.

VANHOEF, M.; RONEN, E. Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd. In: *Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP)*. [S.l.]: IEEE, 2020. p. 517–533.