FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Emerson de Paula dos Reis
Gabriel Antonio Freire de Souza
Marcos Vinicius Ferreira dos Reis Galice

EVIL TWIN EM REDES PÚBLICAS

Americana, SP
2026

FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Emerson de Paula dos Reis

Gabriel Antonio Freire de Souza

Marcos Vinicius Ferreira dos Reis Galice

EVIL TWIN EM REDES PÚBLICAS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação do (a) Prof. Dr. Daives Araken Bergamasco.

Americana, SP

2026

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

REIS, Emerson de Paula dos

Evil twin em redes públicas. / Emerson de Paula dos Reis, Gabriel Antonio Freire de Souza, Marcos Vinicius Ferreira dos Reis Galice – Americana, 2026.

48f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro
Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Dr. Daives Araken Bergamasco

1. Redes de computadores 2. Redes sem fio 3. Segurança em sistemas de informação. I. REIS, Emerson de Paula dos, II. SOUZA, Gabriel Antonio Freire de, III. GALICE, Marcos Vinicius Ferreira dos Reis IV. BERGAMASCO, Daives Araken V. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681519
681519
681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Emerson de Paula dos Reis

Gabriel Antonio Freire de Souza

Marcos Vinicius Ferreira dos Reis Galice

EVIL TWIN EM REDES PÚBLICAS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – Faculdade de Tecnologia de Americana – Ministro Ralph Biasi.
Área de concentração: Tecnologia da informação.

Americana, 12 de Junho de 2026

Banca Examinadora:

Daives Araken Bergamasco
(Presidente) Doutor
FATEC Americana

Eduardo Guilin Penhachek (Membro)
Especialista
FATEC Americana

Benedito Aparecido Cruz (Membro)
Mestre
FATEC Americana

RESUMO

As redes públicas sem fio abertas estão presentes em cada vez mais espaços, de aeroportos a comércios, frequentemente priorizando a comodidade em vez da segurança. Um ataque que amplia muito a superfície de risco nesse cenário é o *Evil Twin*, no qual um ponto de acesso malicioso assume o tráfego de forma transparente para o usuário. Neste trabalho, exploramos os mecanismos de associação de rede, focando no *Evil Twin* sozinho e combinado com o ataque de desautenticação. Por meio de pesquisa teórica e testes práticos em laboratório, avaliamos o comportamento de dispositivos clientes conectados a roteadores legados (Wi-Fi 4) e modernos (Wi-Fi 6). Nossos experimentos mostraram que a troca automática de rede baseada apenas na intensidade de sinal exige uma grande queda do sinal verdadeiro. No entanto, o envio de pacotes de desautenticação forçou a desconexão e a troca imediata para o *Evil Twin* em redes vulneráveis. Verificamos também que a proteção de pacotes de gerenciamento (PMF), presente em padrões mais novos, impede esse ataque ativo. Isso nos levou à conclusão de que uma defesa efetiva depende da adoção de equipamentos atualizados (IEEE 802.11ax) e de mudanças nos sistemas operacionais clientes, que não devem usar apenas o nome da rede (SSID) para se conectar automaticamente.

Palavras-chave: Redes públicas, *Evil Twin*, desautenticação.

ABSTRACT

Open public wireless networks exist in an increasing number of spaces, from airports to stores, often prioritizing convenience over security. An attack that significantly expands the risk surface in this scenario is the Evil Twin, where a malicious access point transparently intercepts user traffic. In this study, we explored network association mechanisms, focusing on the standalone Evil Twin and its combination with a deauthentication attack. Through theoretical research and practical laboratory tests, we evaluated the behavior of client devices connected to legacy (Wi-Fi 4) and modern (Wi-Fi 6) routers. Our experiments showed that automatic network switching based on signal strength requires a significant drop in the legitimate signal. However, sending deauthentication packets forced immediate disconnection and switching to the Evil Twin on vulnerable networks. We also verified that management frame protection (PMF), present in newer standards, prevents this active attack. This led us to conclude that effective defense relies on adopting updated equipment (IEEE 802.11ax) and changes to client operating systems, which should not rely solely on the network name (SSID) for automatic connection.

Keywords: *Public networks, Evil Twin, deauthentication.*

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

O alto número de dispositivos utilizados em nosso dia a dia que são conectados à rede tornou dominante o uso de redes sem fio, especialmente o Wi-Fi, em ambientes residenciais, corporativos e comerciais. Essa predominância se intensifica com a evolução das tecnologias móveis, deixando de atender apenas aos requisitos mais básicos e passando a atender as demandas mais amplas que geram um consumo de banda mais alta, como por exemplo o streaming em alta resolução, automações industriais e até a realidade virtual.

Impulsionados pela conveniência, baixo custo de implantação e pela expectativa dos usuários, diversos ambientes como escolas, shoppings, aeroportos e estabelecimentos comerciais disponibilizam o acesso Wi-Fi gratuito. Contudo, para garantir tal facilidade, essas redes frequentemente deixam de implementar mecanismos de segurança essenciais, sendo disponibilizadas como redes abertas, sem autenticação e, em muitos casos, sem que haja criptografia de dados.

A falta de proteção transforma as redes em ambientes propícios para a realização de ataques cibernéticos, que podem ser dos mais variados tipos, expondo assim o usuário a um risco que por muitas vezes acaba sendo desconhecido por ele.

1.2 Problema de pesquisa

Diante desse cenário, destaca-se uma vulnerabilidade crítica associada a funcionalidade de conexão automática dos dispositivos a redes que contém o mesmo dado. Esta funcionalidade que tem como objetivo proporcionar conveniência ao usuário permite que dispositivos se conectem de forma automática a redes já conhecidas com base apenas no nome da rede (SSID).

No entanto, essa característica pode ser explorada por atacantes, levantando o seguinte questionamento: Quão expostos estão os usuários de redes públicas quando essa funcionalidade é explorada por meio de ataques como o *Evil Twin*?

A hipótese deste trabalho é que usuários de redes sem fio públicas estão altamente suscetíveis a ataques de fácil execução e difícil detecção, especialmente em ambientes com grande fluxo de conexões.

1.3 Justificativa

A relevância deste estudo está diretamente relacionada à ampla presença de redes Wi-Fi públicas em locais de grande circulação e ao comportamento comum dos usuários de se conectarem automaticamente a redes disponíveis sem se preocupar com a segurança.

Esse comportamento amplia significativamente a superfície de ataque, tornando dispositivos e dados vulneráveis a interceptação e fraudes. Assim, ao evidenciar a facilidade de exploração dessa vulnerabilidade, este trabalho tem como objetivo contribuir tanto para a conscientização dos usuários quanto para o desenvolvimento de estratégias de mitigação mais eficazes contra esse tipo de ataque.

1.4 Objetivo geral

Demonstrar a facilidade de execução do modelo de ataque *Evil Twin* em redes Wi-Fi públicas, tendo como foco evidenciar os riscos associados a sua utilização juntamente com o ataque de desautenticação.

1.5 Objetivos específicos

Analisar o funcionamento do modelo de ataque *Evil Twin* em cenários de redes abertas, evidenciando por meio de experimentação prática os mecanismos que levam dispositivos clientes à associação com pontos de acesso maliciosos. Investigar, a partir dos dados experimentais, o impacto da combinação técnica entre o *Evil Twin* e o ataque de desautenticação. Avaliar a exposição e os riscos inerentes à interceptação de tráfego em redes públicas e, por fim, apresentar estratégias de

mitigação voltadas à conscientização do usuário e defesa contra tais vulnerabilidades.

2 FUNDAMENTAÇÃO TEÓRICA

Para contextualizarmos o ataque principal que é foco do trabalho, contextualizamos algumas técnicas de exploração e como são potencializadas por ele. Iniciamos pelo *Evil Twin*, o ataque central da hipótese deste trabalho. Seguimos para duas das principais possíveis explorações realizadas com um ponto de acesso malicioso, a exploração com um *Fake Captive Portal* para roubo de credenciais e / ou dados sensíveis e o ataque *Man-in-the-Middle* para interceptar o tráfego de dados e coletar dados sensíveis não criptografados. Por fim, é abordado o Ataque de Desautenticação, uma técnica fundamental quando trata-se de um ponto de acesso malicioso e não autorizado, frequentemente empregada para viabilizar o sucesso dos ataques anteriores e outros mais não explorados no trabalho.

2.1 Evil Twin

Evil Twin é um ataque que acontece, em redes WiFi, quando há um ponto de acesso malicioso com o objetivo de que ele assuma conexões de usuários como uma rede legítima através da replicação do nome da rede que a identifica, chamado de *Service Set Identifier* (SSID). Normalmente o ponto de acesso malicioso é posicionado fisicamente no ambiente para oferecer um sinal mais forte que o do ponto de acesso legítimo, fazendo com que os próximos dispositivos se conectem a ele, para que o tráfego deles aconteça em uma rede controlada pelo atacante.

O impacto é ainda maior em redes públicas abertas, que são as redes que não necessitam de autenticação para o cliente se conectar, mas a ausência de autenticação facilita o configurar de um ponto de acesso *Evil Twin*, pois não há necessidade de replicar o processo de autenticação.

A mitigação da vulnerabilidade em redes abertas é complexa, pois ela acontece com a implementação de protocolos de autenticação, assim como aponta Pereira (2011), uma solução eficaz poderia ser a autenticação na rede via servidor RADIUS (protocolo de segurança WPA2/3-*Enterprise*), mas a autenticação é raramente implementada em ambientes públicos devido a queda de comodidade.

Uma vez que o dispositivo da vítima se conecta ao ponto de acesso malicioso, o atacante tem controle e visibilidade sobre todo o seu tráfego na rede. Uma posição privilegiada que facilita diversas explorações na rede e direcionadas ao dispositivo, assim como descreve Moraes (2010), um atacante pode capturar um volume significativo de informações sensíveis, incluindo senhas, em um curto período. Uma das diversas táticas que podem ser aplicadas para o roubo de dados, especialmente para um contexto de redes abertas e públicas é a implementação de um *Fake Captive Portal*.

O *Fake Captive Portal*, apresenta uma página de autenticação, igual às frequentemente encontradas em redes Wi-Fi públicas, utilizadas para um cadastro, login ou aceite de termos de uso ou proteção de dados para liberar o acesso à internet, de forma a enganar o usuário para que ele forneça credenciais de login de serviços como redes sociais ou dados sensíveis. Com ataques cada vez mais transparentes e sofisticados, a tarefa de prevenção muitas vezes dependerá do usuário, pois a depender da implementação, por exemplo, um portal com esse fim usualmente não seria apontado como ameaça por softwares de proteção do dispositivo. Bücheler (2025) descreve que uma medida preventiva contra um ponto de acesso malicioso começa com a desativação do recurso de conexão automática do sistema operacional nos dispositivos cliente, impedindo que eles se conectam a redes conhecidas sem interação direta do usuário, reduzindo o risco de uma conexão a um *Evil Twin* que leva a um risco maior de ser vítima de outros ataques como o *Fake Captive Portal*.

2.2 *Fake Captive Portal*

Em redes Wi-Fi públicas sem autenticação, ou seja, redes abertas, o *Captive Portal* é uma ferramenta de portal de autenticação que oferece controle e registro sobre o uso da rede. É uma ferramenta essencial para que se faça cumprir as obrigações legais, presentes, por exemplo, no Marco Civil da Internet no Brasil (Brasil, 2014). De acordo com BluePex (2025), ao exigir que o usuário se identifique antes de liberar o acesso à internet, a organização gera os registros de conexão ligados para um indivíduo específico. Essa rastreabilidade é fundamental para

auxiliar em caso de investigações criminais e manter a conformidade legal, que inclui manter os registros de acesso por um período legal e de forma segura.

A legitimidade e a frequência em que os *Captive Portal* estão sendo utilizados criam uma oportunidade para atacantes. Esta vulnerabilidade é explorada através do Fake Captive Portal, uma técnica que explora a confiança do usuário. Ghimiray (2023) afirma que é crucial para um atacante desenvolver uma página de login visualmente idêntica a uma página legítima para assim enganar a vítima. O objetivo é induzir a vítima a inserir seus dados pessoais, que são então capturados e armazenados em um servidor controlado pelo atacante.

Para evitar o risco de se expor a esse tipo de ataque é necessário que o usuário tenha consciência da página em que está inserindo os dados e qual a sensibilidade deles. Ventas de Seguridad (2023) propõe práticas para evitar a captura de dados sensíveis, sendo a primeira a chamada desconfiança ativa, que pode ser realizada ao inserir informações falsas no formulário de cadastro. Outra proposta é evitar o principal vetor de ataque, que é a rede pública, utilizando redes seguras como a rede de dados móveis em vez de se conectar a redes Wi-Fi não confiáveis.

2.3 Man-in-the-middle

A partir do controle da rede gerado por um *Evil Twin*, há forte tendência para que o ataque *Man-in-the-Middle* seja combinado, pois é uma espionagem das vítimas, tal como afirma Baker (2025), ele explora redes mal configuradas ou desprotegidas, onde um atacante se posiciona como um intermediário invisível entre a vítima e o serviço legítimo que ela deseja acessar, agindo como se fosse o gateway da rede para interceptar todo o tráfego, analisando e só depois enviar ao destino final real. Para a vítima e o servidor é algo transparente, pois a comunicação continua fluindo, apesar de estar sendo monitorada e capturada pelo atacante.

O ataque é ainda mais alarmante quando consideramos informações confidenciais sendo transmitidas, pois caso a vítima realize operações em sistemas e sites que envolvam dados pessoais ou financeiros, o atacante pode capturá-los no caso de uma comunicação não criptografada, pois todos os dados são trocados em

texto claro. No caso de criptografia há uma proteção maior, mas ainda assim o atacante pode aplicar outros ataques para burlar ela e obter a informação, pois permitiria o mesmo acesso de uma conexão desprotegida.

Um estudo conduzido por Paula Filho et al. (2022) mostrou que 87% dos participantes já realizaram operações que envolvem dados sensíveis, como logins e transferências bancárias, utilizando redes públicas. Esse tipo de costume transforma a vulnerabilidade em um risco preocupante, pois os dados interceptados podem servir para vários objetivos maliciosos, desde fraudes bancárias até o roubo de identidade e outros crimes cibernéticos.

2.4 Ataque de desautenticação

Um ataque *Evil Twin* é muito mais efetivo quando combinado com um Ataque de Desautenticação, que é um ataque que explora uma funcionalidade do protocolo Wi-Fi e cria, através dele, uma negação de serviço temporária. Segundo Silva Neto (2021), o atacante envia pacotes de desautenticação para os dispositivos conectados a um ponto de acesso legítimo, resultando em sua desconexão imediata e os impede de reconectar-se com ele. A desconexão forçada elimina a necessidade de que o *Evil Twin* precise aguardar por vítimas se conectarem a ele de forma voluntária, pois uma vez que os dispositivos desconectados iniciam o processo de reconexão automática, quem recebe a conexão é ele ao invés da rede verdadeira, visto que a rede maliciosa é posicionada para ter maior sinal e ser prioridade para tal. Toda essa mudança entre o ponto de acesso legítimo e o ponto de acesso malicioso acontece sem gerar aviso/alarme ao smartphone do cliente, sendo assim impossível um usuário comum identificar a ação.

2.5 Padrões e protocolos

2.5.1 Padrões IEEE *Standards Association*

Os padrões *Institute of Electrical and Electronics Engineers* (IEEE) 802 são uma família de padrões para redes locais criadas pelo *Institute of Electrical and Electronics Engineers*. Cada família é destinada para um tipo de aplicação. Neste

trabalho, usamos como referência a sexta geração do 802.11: é o padrão técnico internacional para *Wireless Local Area Network* (WLAN), redes locais sem fio, amplamente conhecida como tecnologia *Wireless Fidelity* ou simplesmente Wi-Fi. O padrão 802.11ax define as especificações da *Physical Layer* (PHY), a camada física e de *Media Access Control* (MAC), o controle de acesso ao meio, permitindo a comunicação sem fio entre dispositivos através de radiofrequência em faixas como 2.4/5/6GHz, tem como características: lançado em 2019, o utiliza as frequências de 2,4GHz e 5 GHz, enquanto a versão Wi-Fi 6E também utiliza o espectro de 6 GHz. O Wi-Fi 6/6E tem velocidade máxima teórica de 9,6 Gb/s. Como abordado por Santos, Santos e Maniçoba (2024), o Wi-Fi 6 trouxe a inteligência (como o OFDMA) para lidar com a densidade, enquanto sua extensão o Wi-Fi 6E trouxe a infraestrutura (a banda de 6GHz). Ainda cita as inovações tecnológicas como MU-MIMO Bidirecional (DL/UL), Modulação 1024-QAM, Coloração BSS e *Target Wake Time* (TWT) no Wi-Fi 6 e mais espectro, canais mais largos e fim da interferência de legados no Wi-Fi 6E.

2.5.2 Protocolos de segurança Wi-Fi

Conforme publicação de Coppock e Mazal (2025), os protocolos de segurança Wi-Fi criptografam as conexões sem fio. Eles ocultam os dados e protegem as comunicações, ao mesmo tempo em que bloqueiam hackers na rede. Geralmente, o WPA3 é a melhor opção, embora não esteja disponível em todos os dispositivos. A organização Wi-Fi Alliance desenvolveu quatro protocolos de segurança de rede sem fio conforme publicado pelo mesmo autor:

- Wired *Equivalent Privacy* (WEP): protocolo de segurança Wi-Fi mais antigo e considerado obsoleto atualmente.
- Wi-Fi *Protected Access* (WPA): mais seguro que o WEP porque usa uma chave de 256 bits para criptografia.
- Wi-Fi *Protected Access* 2 (WPA2): criptografa o tráfego sem fio e limita o acesso a quem possui a senha da rede.
- Wi-Fi *Protected Access* 3 (WPA3): mais seguro do que seu antecessor o WPA2, mais novo protocolo de segurança sem fio, projetado para criptografar

dados com mais segurança e proteger sessões anteriores, mesmo que uma senha seja comprometida posteriormente, um recurso conhecido como *Perfect Forward Secrecy*. O WPA3 utiliza o *Galois/Counter Mode Protocol* (GCMP), um modo de criptografia de alto desempenho que aumenta a segurança e a velocidade. Comparado ao modo AES-CCMP usado no WPA2, o GCMP oferece melhor integridade de dados e eficiência geral.

2.5.3 Combinação do padrão 802.11ax com o protocolos modernos de segurança

A combinação do padrão 802.11ax (Wi-Fi 6) com proteções mais recentes, como o WPA3 e o padrão *Opportunistic Wireless Encryption* (OWE), representa a configuração mais robusta para a mitigação de ataques em redes sem fio de acesso público. Enquanto padrões legados apresentam falhas na proteção de quadros de gerenciamento (vulnerabilidade que viabiliza os ataques de desautenticação explorados neste estudo), a transição para o Wi-Fi 6 associada a novos protocolos altera esse cenário de forma significativa (Santos, Santos e Maniçoba, 2024).

Os principais aspectos de segurança e mitigação dessa combinação para o contexto de redes públicas são:

- Obrigatoriedade do *Protected Management Frames* (PMF): Para a obtenção da certificação WPA3, a implementação do PMF (padrão 802.11w) tornou-se um requisito obrigatório em dispositivos modernos (Dekra, 2020). O PMF adiciona proteção criptográfica aos quadros de gerenciamento da rede (como requisições de desautenticação que foram exploradas). Essa exigência neutraliza a capacidade de um atacante falsificar endereços (MAC *Spoofing*) e forçar a desconexão de clientes, eliminando o vetor inicial explorado no ataque de desautenticação.
- Proteção Transparente em Redes Abertas (*Enhanced Open* / OWE): Em ambientes públicos onde a conveniência de acesso sem senhas deve ser é essencial, a adoção do padrão *Opportunistic Wireless Encryption* (OWE) substitui o formato de rede puramente "Aberta" e desprotegida. O OWE fornece criptografia individualizada e transparente para a conexão de cada

cliente e utiliza a ativação do PMF, garantindo proteção contra interceptação dos dados e mitigando ataques de desautenticação sem degradar à experiência do usuário (Harkins, 2018).

- Modo de Transição e Dispositivos Legados: Para garantir a interoperabilidade, infraestruturas 802.11ax permitem a configuração de modos mistos. Esses modos possibilitam que os dispositivos compatíveis com WPA3 e OWE se beneficiam da proteção dos quadros de gerenciamento, enquanto os equipamentos legados continuam operando sob protocolos mais antigos, mas esses últimos continuam vulneráveis e modos de compatibilidades abrem brechas para outros ataques (Santos, Santos e Maniçoba, 2024).

2.6 Estado da arte

O aumento dos dispositivos conectados à internet e exclusivamente em redes Wi-Fi públicas, os estudos dos ataques *Evil Twin* vem crescendo como tema dos trabalhos acadêmicos. Foram pesquisados três destes relevantes no tema para a elaboração do estado da arte, eles investigam tanto a exploração dessas vulnerabilidades quanto técnicas de detecção e mitigação.

O estudo de Nascimento (2025) analisa os riscos associados ao uso de redes Wi-Fi públicas, evidenciando que usuários frequentemente desconhecem ameaças como *Evil Twin*, *Man-in-the-Middle* e roubo de credenciais. O trabalho possui caráter mais teórico e de conscientização, sem validação experimental aprofundada.

Já Alves Neto (2025) amplia essa análise ao focar em transações sensíveis, como operações bancárias em redes públicas. O autor demonstra que a ausência de criptografia adequada e a exposição em redes abertas potencializam ataques, incluindo o *Evil Twin*. No entanto, o estudo também se concentra mais em análise conceitual e não explora experimentos práticos detalhados.

Por outro lado, Silva Júnior e Nascimento (2025) propõem uma abordagem mais avançada, desenvolvendo um sistema de detecção e mitigação de ataques *Evil Twin* em ambientes industriais com *Internet of Things / Industrial Internet of Things* (IoT/IIoT). O diferencial deste trabalho está na aplicação prática de mecanismos

automatizados de defesa, embora voltado a um contexto específico (redes industriais), com maior complexidade de implementação.

Além desses, a literatura internacional recente apresenta avanços importantes. Estudos como o de Ghimiray (2023) abordam a facilidade de criação de ataques *Evil Twin* combinados com *Fake Captive Portals*, destacando o fator engenharia social como elemento crítico. Já pesquisas mais recentes, como Bücheler (2025), discutem o impacto da conexão automática em dispositivos modernos, apontando que essa funcionalidade continua sendo um vetor relevante de ataque.

Outros trabalhos focam em técnicas de detecção, utilizando aprendizado de máquina, análise de tráfego e identificação de padrões anômalos para diferenciar pontos de acesso legítimos de maliciosos. Entretanto, essas soluções ainda enfrentam desafios relacionados à implementação em larga escala e à necessidade de hardware ou infraestrutura adicional.

Para consolidar a comparação com outros trabalhos no assunto e justificar a relevância deste trabalho, foi realizado um levantamento comparativo com outros trabalhos brasileiros que abordam a segurança em redes Wi-Fi e a exploração de pontos de acesso maliciosos (*Evil Twin / Rogue AP*). O Quadro 2 traz essas abordagens, evidenciando os cenários avaliados e as lacunas que o presente trabalho objetiva preencher.

Quadro 1 – Comparativo de estudos brasileiros sobre Evil Twin / Rogue AP

Autor(es) / Ano	**Foco Principal**	**Cenário / Ambiente de Estudo**	**Abordagem (Teórica / Prática)**	**Contraste com este trabalho**
Gomes (2018)	Análise do ataque Rogue AP para roubo de credenciais usando equipamentos dedicados.	Corporativo/Militar (Marinha do Brasil).	Prática e Teórica.	Foca em redes corporativas com restrições severas, diferentemente do cenário aberto de redes públicas.
Serafim (2020)	Testes de Penetração (*Pentest*) avaliando a vulnerabilidade de protocolos (WEP, WPA, WPA2).	Redes domésticas e empresariais.	Prática (Uso de Kali Linux, Airbase-ng).	Não avalia o comportamento de equipamentos Wi-Fi 6 nem a proteção PMF do cliente durante o ataque.
Cerqueira Jr. et al. (2024)	Propõe um sistema de detecção (UETADS) focado no cliente usando *Machine Learning* (OCSVM).	Redes IEEE 802.11 em ambiente acadêmico controlado.	Prática (Criação de dataset próprio).	Foca exclusivamente na detecção algorítmica, sem focar na mecânica de conexão automática do usuário.
Nascimento (2025)	Mapeamento de redes Wi-Fi públicas, suas criptografias (WPA/WPA2) e canais.	Redes públicas (Cuité de Mamanguape - PB).	Prática (Mapeamento) e Teórica (Ataques).	Discute o *Evil Twin* apenas conceitualmente, sem testes práticos de exploração da vulnerabilidade em laboratório.
Este TCC (2026)	Impacto da conexão automática combinada com desautenticação na transição para um *Evil Twin*.	Redes públicas abertas e modo misto.	Prática (Avaliação de hardware Wi-Fi 4 e Wi-Fi 6).	Preenche a lacuna combinando testes práticos de ataque em cenários de comodidade (redes abertas) e avaliando defesas modernas (Wi-Fi 6/PMF).

Fonte: Elaborado pelos autores (2026)

Conforme ilustrado no Quadro 2, embora existam pesquisas relevantes no cenário nacional, grande parte se divide entre análises de mapeamento em redes públicas ou testes práticos voltados para ambientes corporativos, domésticos e desenvolvimento de sistemas de detecção. Neste contexto, o presente trabalho se diferencia ao combinar abordagem teórica e validação experimental prática, demonstrando de forma objetiva: a facilidade de execução do ataque *Evil Twin*, o impacto da combinação com ataque de desautenticação, o comportamento real de dispositivos clientes e a transparência do ataque para o usuário.

Enquanto grande parte dos estudos se limita à análise conceitual ou à proposta de soluções complexas, este trabalho evidencia, por meio de experimentação controlada, que ataques podem ser realizados com ferramentas amplamente disponíveis, sem necessidade de infraestrutura avançada.

Dessa forma, contribui-se para a literatura ao reforçar que o problema não está apenas na ausência de mecanismos de detecção, mas também em limitações do protocolo IEEE 802.11 quando lidando com hardware não atual e no comportamento padrão dos dispositivos, indicando a necessidade de evolução tanto tecnológica quanto de conscientização dos usuários.

3 METODOLOGIA

Foi adotada uma abordagem mista no desenvolvimento do trabalho, combinando pesquisa bibliográfica com pesquisa experimental em ambiente de laboratório. A fundamentação bibliográfica utilizou-se de artigos científicos sobre redes sem-fio e sobre as vulnerabilidades descritas, destacando os riscos de cada uma e quando combinados. Já a fase experimental foi realizada para demonstrar de forma prática quão fácil e simples é explorar dois ataques que facilitam os demais em um cenário de redes públicas, que é o *Evil Twin* combinado com ataque de desautenticação.

3.1 Ambiente Experimental

O ambiente de laboratório utilizado, aplicou hardware e software de fácil acesso para simular um cenário de ataque. O Quadro 1 demonstra a especificação de hardware e software.

Quadro 2 – Relação de software, hardware e configuração utilizados

Cenário	Dispositivo	Hardware	Software	Configuração
Cenário 1 (Rede Aberta / TP-Link)	Computador atacante	Notebook (Intel Core i7-2630m / 8 GB RAM / Adaptador WiFi 6E AX210)	Kali Linux 2025.2	Padrão
	AP Legítimo	TP-Link Archer C6 (v2 USA)	Firmware padrão do fabricante	Rede WiFi 4 na frequência 2.4 Ghz com um SSID específico, operando como uma rede aberta (sem autenticação)
	AP *Evil Twin*	Smartphone Samsung Galaxy M35 5G	OneUI 7	Utilizou-se o recurso nativo de roteador do Android para criar um ponto de acesso com o mesmo SSID e frequência da rede legítima, mas com o canal de operação em modo automático
	Dispositivo cliente principal	Smartphone Asus Zenfone Max Plus M2	Android 9 + APP WiFiman	Padrão
	Dispositivo cliente (Validação)	Notebook Lenovo ThinkPad T480 (Adaptador original Intel AC 8265)	Windows 11	Funcionalidade "conectar-se automaticamente" desabilitada para o SSID
Cenário 2 (Modo Misto / MitraStar)	AP Legítimo	MitraStart GPT-2742	Padrão	Rede WiFi em modo misto (WIFI 5 e 6) na frequência 5 Ghz (PMF ativo)
	Dispositivos clientes (WiFi 5 e 6)	Smartphone Asus Zenfone Max Plus M2 e Smartphone Samsung Galaxy M35 5G	Padrão	Padrão
	Dispositivo cliente legado	Tablet Apple iPad de 3ª geração (2012)	iOS 9 (Legado)	Padrão

Fonte: Elaborado pelos autores (2026)

O aplicativo WiFiMan da Ubiquiti, instalado no dispositivo cliente, foi utilizado para monitorar em tempo real a conexão com a rede sem fio, permitindo verificar a intensidade do sinal, a distância estimada e o endereço MAC, que identifica o

hardware do ponto de acesso ao qual o dispositivo estava conectado, permitindo identificar, nesse caso que o ponto de acesso malicioso não utilizava estratégia de clonagem de MAC, a qual ponto de acesso o dispositivo estava conectado e quando se conectava em outro. Essa ferramenta é voltada para diagnóstico e descoberta de redes sem fio, incluindo monitoramento em tempo real de métricas de conectividades.

O ambiente físico consistiu no ponto de acesso legítimo em um cômodo, enquanto o notebook que representava o atacante foi posicionado a dois cômodos de distância, assim como o ponto de acesso malicioso, permitindo verificarmos a influência do alcance e da intensidade dos sinais com a troca de conexão entre os pontos de acesso. O computador atacante utilizou o Kali Linux como sistema operacional, que é uma distribuição Linux baseada no Debian e focada justamente para testes de intrusão e de segurança de redes, já trazendo de forma nativa ferramentas necessárias para o experimento voltado a redes sem fio.

No cenário utilizando o roteador TP-Link Archer C6 focado na banda de 2.4 GHz (WiFi 4), demonstramos a vulnerabilidade que se estende até o protocolo WiFi 802.11 ac (também conhecido como WiFi 5), que é o estado atual de grande parte dos equipamentos de rede pública e até residências no Brasil e outros países. Mesmo se considerarmos equipamentos modernos com WiFi 6, 6E e 7, quando usando as frequências clássicas de 2.4 Ghz ou 5 Ghz, massivamente são pré-configurados para o modo de compatibilidade (mixed) tanto no protocolo Wireless quanto em protocolo de criptografia (atualmente WPA2/WPA3, sendo o WPA2 vulnerável). Na rede em frequência mais moderna de 6 Ghz, os dispositivos conectados são forçados a suportarem protocolo mais moderno de comunicação e criptografia eliminando tanto o problema de sofrerem um ataque de desautenticação quanto outro ataque aqui não explorado que é o de “*downgrade*”, que faz com que em redes em modo de compatibilidade se possa forçar os dispositivos a assumirem protocolos de conectividade e/ou criptografia mais vulneráveis.

O cenário com o roteador MitraStar permite a demonstração da proteção fornecida pelo dispositivo mais moderno quando em modo misto entre WiFi 5 e WiFi 6, aplicando a proteção de pacotes de gerenciamento (*Protected Management*

Frames, PMF) quanto utilizando criptografia WPA2 e a proteção já citada no parágrafo anterior quanto ao WPA3.

3.2 Procedimentos Experimentais

O ataque experimental foi realizado utilizando ferramentas já disponíveis por padrão em uma instalação do Kali Linux, demonstrando o quão fácil um agente malicioso com informação pode ter êxito em um ambiente real no ataque de desautenticação, que é quase que essencial em ser combinado com um *Evil Twin*. As ferramentas utilizadas integram a suíte de ferramentas Aircrack-ng, que são voltadas à análise, interceptação e exploração voltadas a rede sem fio (802.11).

O ataque de desautenticação se inicia configurando a interface de rede sem fio para o modo de monitoramento utilizando o comando sudo airmon-ng start wlan0 (no caso de apenas um adaptador *Wireless* conectado).

Após configurado o adaptador de rede para o modo monitoramento, o comando sudo airodump-ng wlan0mon permite escanear as redes disponíveis (descoberta de redes), gerando uma lista no console que permite identificar informações das redes no alcance, tal como SSID (nome da rede), endereço MAC e canal de operação. Na lista o foco é identificar o ponto de acesso alvo do ataque que é necessário anotar ou copiar seu endereço MAC e o canal da rede. A variação sudo airodump-ng --band abg wlan0mon permite uma captura mais abrangente, incluindo todas as frequências suportadas pelo adaptador WiFi do equipamento que faz a varredura.

O ataque de desautenticação é tão simples, que nesse parágrafo já chegamos ao comando que o realiza, que é o sudo aireplay-ng --deauth 0 -a [ENDEREÇO_MAC_DO_ROTEADOR] wlan0mon, sendo a ferramenta aireplay-ng responsável por injetar os pacotes no ataque. O parâmetro --deauth 0 faz com que a ferramenta nativa do sistema operacional Kali Linux envie um fluxo contínuo de pacotes de desautenticação, forçando a desconexão de todos os clientes conectados ao ponto de acesso legítimo. Antes de executar o envio dos pacotes, é necessário configurar o adaptador de rede para transmitir no canal exato do alvo,

que pode ser realizado através do comando sudo airodump-ng -c [canal] --bssid [endereço MAC alvo] wlan0mon.

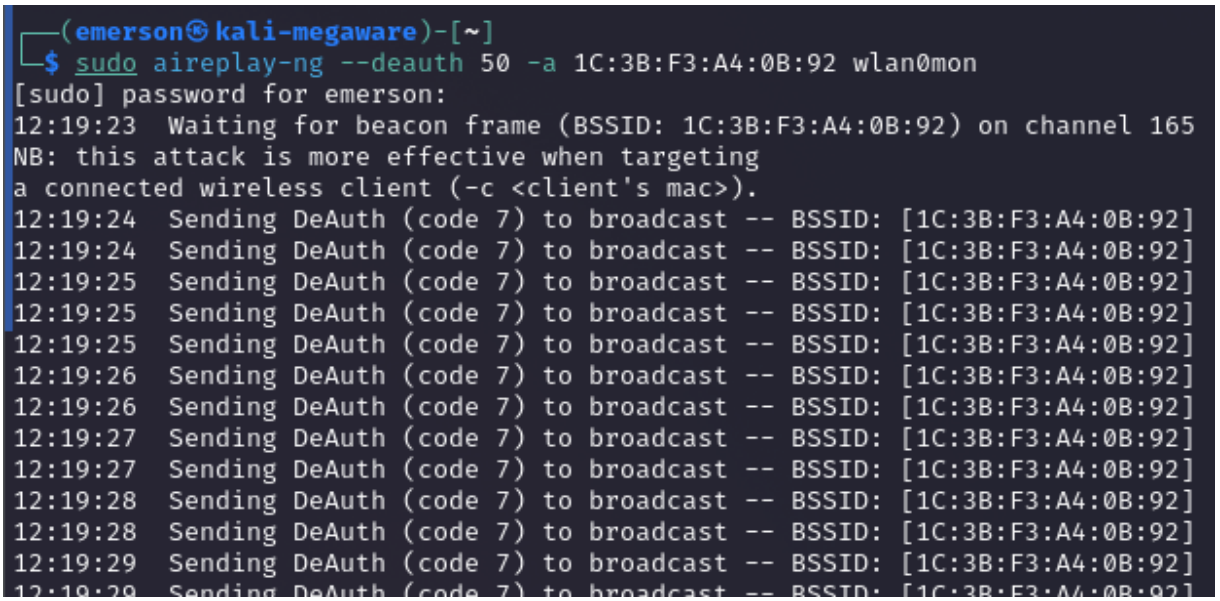
Para melhor explorarmos a composição desse ataque, utilizou-se, em um terminal separado na mesma máquina comando para coletarmos o tráfego e podermos analisar utilizando o software Wireshark em momento posterior, que é o comando sudo airodump-ng wlan0mon -c [CANAL_DO_TPLINK] --bssid [MAC_DO_TPLINK] -w captura_tcc, o qual após disparados os pacotes de desautenticação devemos interromper manualmente (CTRL+C) para não continuar coletando tráfego, como mostra a Figura 1.

Figura 1 – Comando para coleta do tráfego e pacotes de desautenticação

Fonte: Elaborado pelos autores (2026)

Em vista de não termos um arquivo muito extenso, na coleta de tráfego realizada na Figura 1, vamos utilizar uma variação do comando que envia os pacotes de desautenticação para o alvo, utilizando sudo aireplay-ng --deauth 50 -a [MAC_DO_TPLINK] wlan0mon, que limita a 50 pacotes enviados, conforme mostra a Figura 2.

Figura 2 – Ataque com envio de pacotes de desautenticação

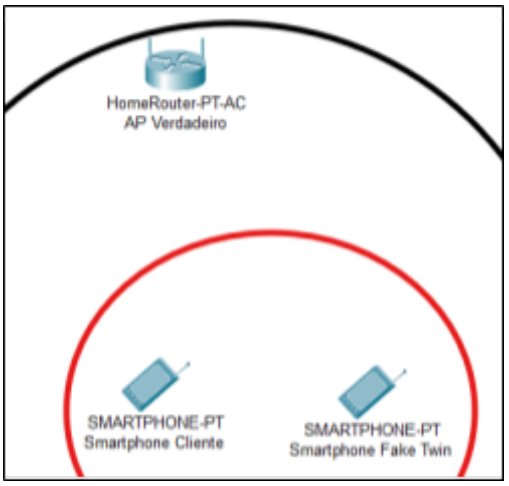


Fonte: Elaborado pelos autores (2026)

Além do ataque de desautenticação para podermos experimentar como ocorre a desconexão e conexão aos pontos de acessos no ambiente, testamos o comportamento em cenários no qual um dispositivo cliente simplesmente está presente em um ambiente que possui um *Evil Twin*, mas não há o vetor de desautenticação em execução.

Primeiro testamos a conexão por proximidade, ilustrada na Figura 3, como foco em verificar se o dispositivo cliente, com a rede salva para conexão automática, iria se conectar automaticamente ao *Evil Twin* em vez do AP legítimo, pelo primeiro estar fisicamente mais próximo e com mais sinal.

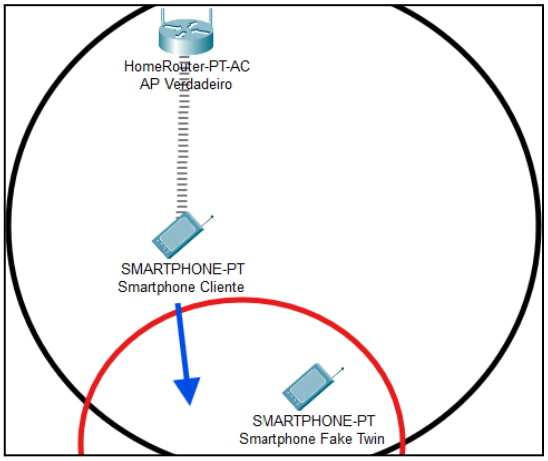
Figura 3 – Ambiente de testes *Evil Twin* para testar conexão automática



Fonte: Elaborado pelos autores (2026)

Depois testamos, como exemplifica a Figura 4, se quando o dispositivo cliente já está conectado ao AP verdadeiro, quando fisicamente distanciado do AP legítimo perdendo intensidade de sinal enquanto sempre próximo do *Evil Twin,* iria alterar a conexão para o ponto de acesso com o sinal mais forte que seria o malicioso e em qual condição o faria.

Figura 4 – Ambiente de testes *Evil Twin* para testar conexão por qualidade de sinal



Fonte: Elaborado pelos autores (2026)

3.3 Coleta e Análise de Dados

A coleta de dados se baseou na observação das informações exibidas no aplicativo WiFiMan no dispositivo cliente, que indicava qual AP o dispositivo estava conectado e estatísticas da rede, como intensidade do sinal e distância aproximada.

Também conduzimos uma análise do pacote de desautenticação capturado através de monitoramento da interface *Wireless* utilizando ferramenta nativa do sistema operacional do dispositivo atacante e analisando através do software Wireshark para entendimento do efeito causado. O Wireshark é um analisador de protocolos de rede gratuito, permitindo tanto trabalhar com dados em tempo real ou, como em nosso cenário, dados armazenados em arquivos com extensão “.cap”.

A análise aplicada foi de natureza descritiva e qualitativa. Analisamos a ocorrência da transição de rede com as mudanças executadas no ambiente, tal como a proximidade física entre os hardwares presentes no experimento e a própria execução do ataque de desautenticação, descrevendo o resultado de cada cenário.

3.4 Limitações do Estudo

Pela limitação na execução do estudo em um ambiente controlado e simplificado, visto que havia apenas ponto de acesso legítimo e um dispositivo cliente, sem complexidade de redes públicas com múltiplos APs e vários usuários simultâneos. Também podemos incluir na limitação a própria configuração realizada no AP legítimo que utilizamos, que não utilizava-se de nenhuma configuração diferente do padrão do dispositivo sem habilitar alguma autenticação ou explorar mitigações adicionais. Uma das configurações que pode impactar no cenário explorado no WiFi 5 usando WPA2, como mitigação, é a ativação em dispositivo suportado do 802.11w ou mais conhecido como PMF (*Protected Management Frames*) que adiciona criptografia e verifica a autenticidade do pacote de desautenticação, mas no WiFi 5 é conhecido que ele foi implementado tardiamente sendo incompatível com diversos adaptadores Wireless e há certa instabilidade que gera desconexões. No teste conduzido há a exploração do cenário, mas em um roteador moderno com WiFi 6 que em modo misto oferece a proteção habilitando

PMF, porém em dispositivos com suporte limitado a WiFi 5, como o que utilizamos (TP-Link) não há disponível no software do fabricante a opção de ativar o PMF e não é ativa por padrão para equipamentos domésticos.

Também por limitação de equipamentos disponíveis para os testes práticos, esse trabalho não aplicou testes com base em redes abertas protegidas, padrão *Enhanced Open* (OWE), que foi introduzido para fornecer criptografia em redes sem senhas e exigem PMF para mitigar ataques de desautenticação (Harkins, 2018).

Focamos no comportamento de conexão ao *Evil Twin* em variáveis controladas e um simples ataque de desautenticação, não explorando outros ataques que poderiam ser executados posteriormente tal como *Man-in-the-Middle* ou *Fake Captive Portal*.

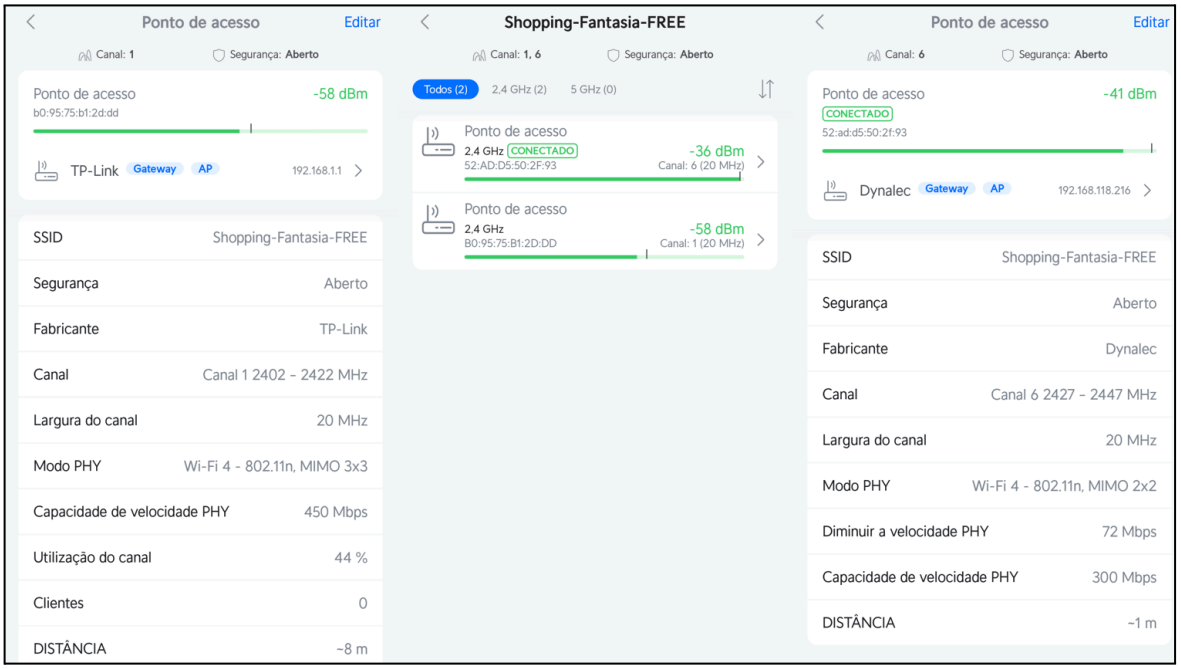
Por se tratar de um estudo para rede não guiada, a intensidade do sinal é uma limitação, pois na maioria dos cenários, o AP ofensor foi intencionalmente posicionado mais próximo do cliente e assim entregava uma maior intensidade de sinal, o que é uma condição favorável ao ataque.

Há também a limitação do tipo de hardware que tivemos acesso para a condução das simulações, na qual nos limitamos a pontos de acesso até WiFi 6 e dispositivo cliente que até possuía capacidade WiFi 6E, mas não explorado devido a compatibilidade do ponto de acesso.

4 RESULTADOS

Os testes experimentais em laboratório (ambiente controlado) permitiram uma análise prática da vulnerabilidade associadas à comodidade de conexão automática e o cenário comum em redes Wi-Fi públicas. Observamos que o dispositivo cliente, ao ter o SSID da rede previamente salvo, conecta-se automaticamente ao ponto de acesso que tinha maior intensidade de sinal, que conforme mostra a Figura 5, era o Evil Twin, que por estar fisicamente mais próximo do cliente recebeu a conexão do dispositivo cliente, demonstrando como essa convivência faz com que o ataque tenha êxito, uma vez que os dispositivos cliente priorizaram o sinal mais intenso para redes conhecidas e conectaram o usuário a rede maliciosa.

Figura 5 – Lista de pontos de acesso no *SSID* criado para teste no WiFiman

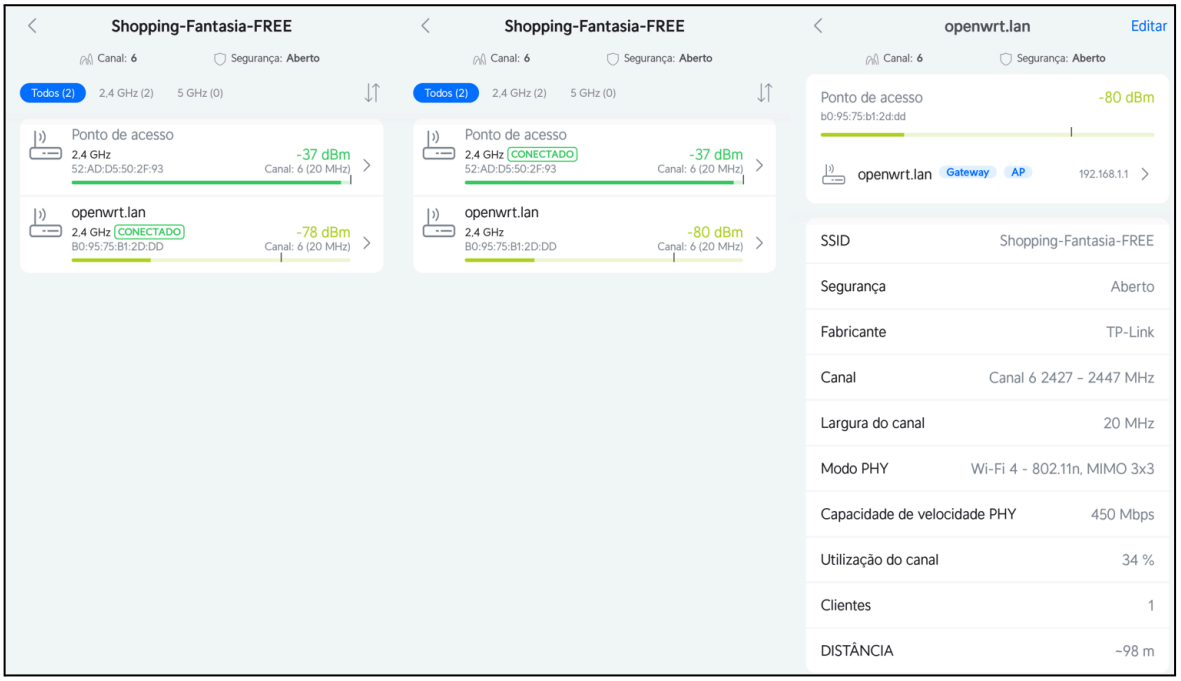


Fonte: Elaborado pelos autores (2026)

Ao testarmos o comportamento do dispositivo já conectado ao ponto de acesso verdadeiro e com um sinal em boa intensidade, a presença do *Evil Twin* mais próximo e com maior intensidade de sinal não foi suficiente para que acontecesse uma troca de rede. Mesmo quando afastamos o dispositivo cliente do ponto de acesso legítimo sempre o mantendo próximo do *Evil Twin*, o algoritmo de roaming de

rede do cliente foi conservador, mantendo a conexão estabelecida mesmo com quando a intensidade de sinal seria tecnicamente muito mais fraca. Foi necessário um distanciamento físico de aproximadamente 90 metros do AP legítimo para que a degradação do sinal fizesse com que o dispositivo trocasse a conexão automaticamente para o *Evil Twin*, como ilustrado na Figura 6. Assim entendemos que a transição por sinal de rede depende de uma variação de sinal significativa, condição difícil em ambientes como shoppings ou aeroportos que investem em boa cobertura de rede.

Figura 6 – Troca automática de ponto de acesso quando já conectado



Fonte: Elaborado pelos autores (2026)

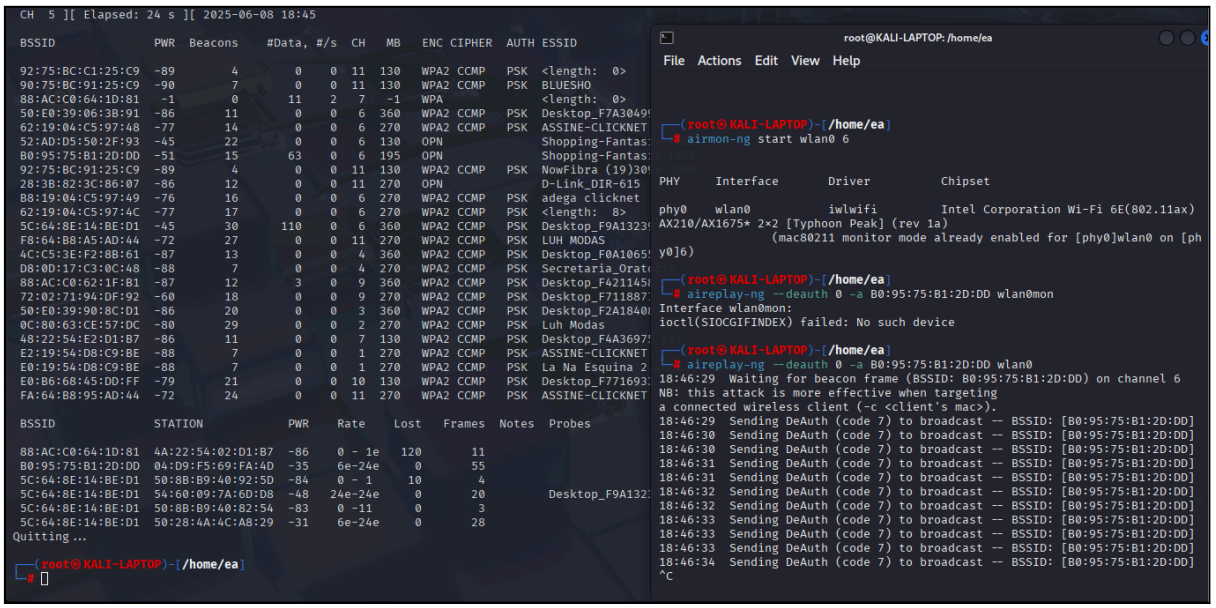
Partindo do ponto que com a conexão já estabelecida foi observado o comportamento do dispositivo quando em um ambiente com um *Evil Twin*, avançamos para um cenário que utiliza uma estratégia ativa, sendo o *Evil Twin* combinado com o ataque de desautenticação. Nesse teste o dispositivo cliente estava conectado ao ponto de acesso verdadeiro, conforme demonstrado na Figura 7.

Figura 7 – Cliente associado ao ponto de acesso sem fio verdadeiro

Fonte: Elaborado pelos autores (2026)

Com o dispositivo cliente conectado ao ponto de acesso legítimo e parado no espaço físico para não ocorrer influência pela variação de sinal, o ataque de desautenticação foi realizado utilizando o notebook com Kali Linux e ferramenta pré-instalada, conforme processo detalhado na metodologia deste trabalho. A execução do ataque, com o envio de pacotes em broadcast para o AP legítimo como desautenticação, é evidenciada na Figura 8.

Figura 8 – Ataque de desautenticação sendo executado

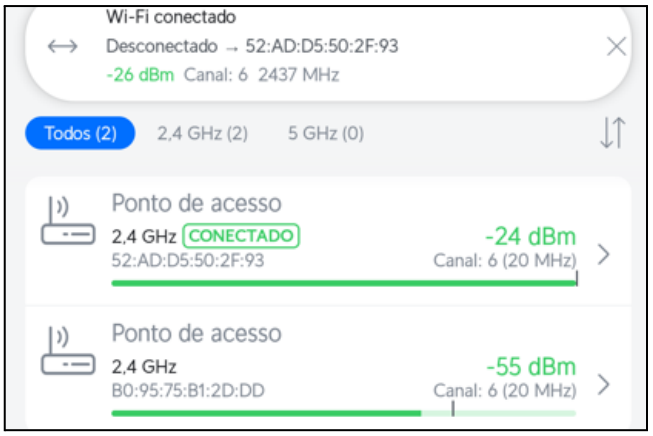


Fonte: Elaborado pelos autores (2026)

Assim que os primeiros pacotes de desautenticação são transmitidos há um efeito imediato de o dispositivo cliente de forma forçada ter se desconectado da rede legítima e automaticamente se conectado ao *Evil Twin*. Este resultado expõe a falha no padrão 802.11 anterior a especificação ax (WiFi 6), que para os quadros de gerenciamento, como os de desautenticação, não há autenticação ou criptografia e assim permitem que um atacante os use para interromper a comunicação da rede.

Essa transição da conexão automática em na rede maliciosa ocorreu de forma completamente transparente para o usuário, sendo visível apenas utilizando o software de análise de rede, como o WIFIman, que permitiu ver a mudança do valor de MAC *Address* para o do ponto de acesso malicioso, como demonstrado na Figura 9. A eficácia e a discrição deste ataque combinado entre *Evil Twin* e desautenticação representam o maior risco dos abordados neste trabalho, pois o atacante não depende de um cenário com condições passivas, como a posição do dispositivo do usuário, assumindo o controle ativo forçando a conexão a uma rede que detém controle.

Figura 9 – Cliente conectado no *Evil Twin* após ataque de desautenticação



Fonte: Elaborado pelos autores (2026)

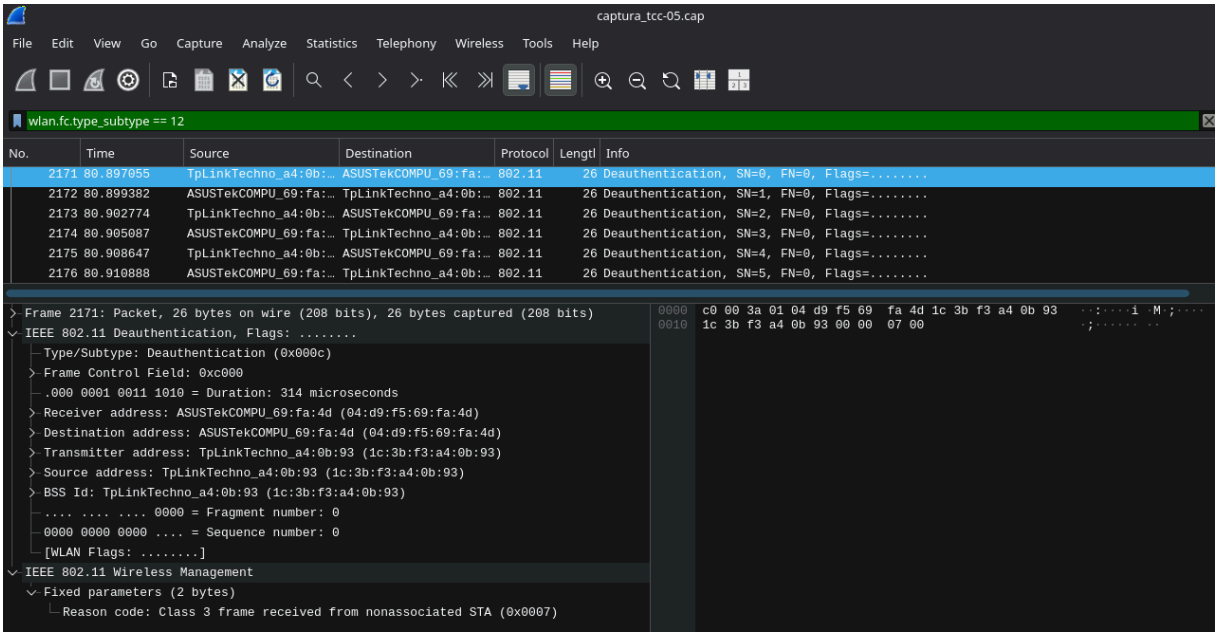
Direcionando o ataque de desautenticação ao dispositivo cliente de teste, foi possível coletar pacotes entre o ponto de acesso e o cliente, que não são criptografados (*Management Frames*). Analisando o arquivo do tráfego no Wireshark, como mostra a Figura 10, o pacote capturado é classificado logo em seu

cabeçalho como um quadro de desautenticação (*Type/Subtype: Deauthentication* - 0x000c).

A captura evidencia a característica fundamental do ataque, que é o MAC *Spoofing* (falsificação de endereço MAC *Address*). Os pacotes forjados injetados pelo atacante não tem o endereço físico da interface de rede dele, em vez disso, a ferramenta de ataque falsifica o endereço de origem (*Source Address*), se passando pelo ponto de acesso legítimo (TP-Link) ou pelo dispositivo cliente (ASUS).

Essa falsificação faz com que o dispositivo alvo acredite que a solicitação partiu de uma fonte confiável. Ao observarmos o *payload* na parte inferior da Figura 10 (na seção IEEE 802.11 *Wireless Management*), vemos o exato envio do parâmetro *Reason code*: 7 (*Class 3 frame received from nonassociated STA*). É este campo que instrui a desconexão imediata da rede ao dispositivo, tendo sucesso tanto direcionado a um cliente específico alvo ou quando transmitido em forma de broadcast (direcionado a qualquer dispositivo conectado ao ponto de acesso).

Figura 10 – Pacote de desautenticação com endereço MAC falsificado

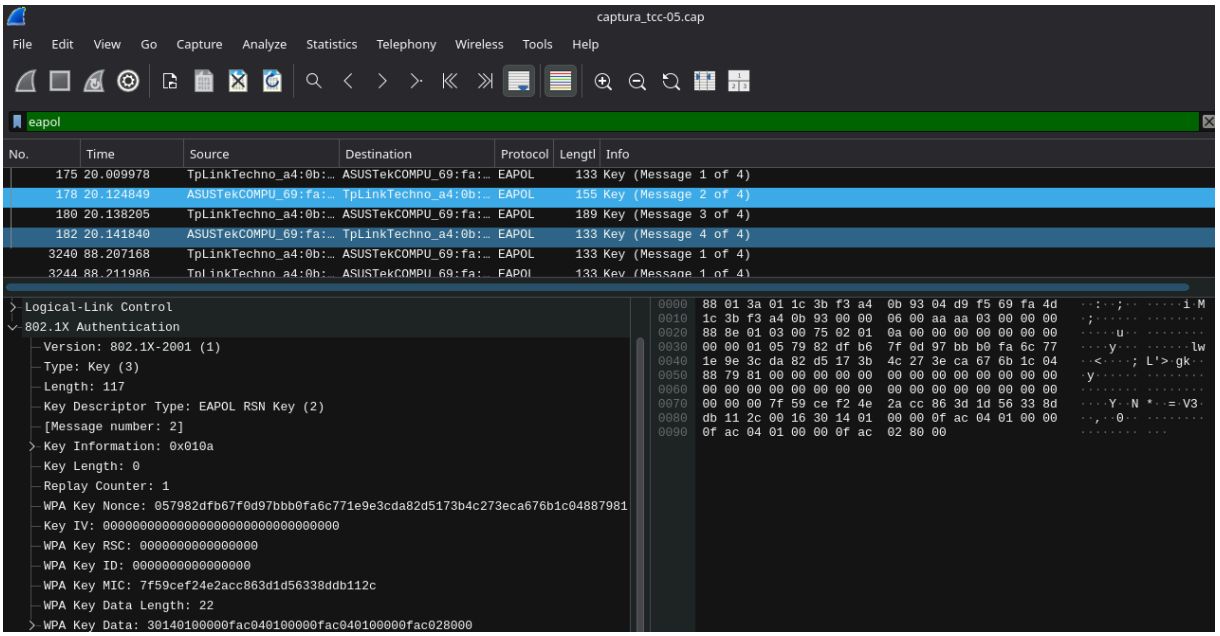


Fonte: Elaborado pelos autores (2026)

Além do cenário principal com a rede aberta, como mostra a Figura 11 em redes protegidas com WPA2 é possível capturar o 4-*Way Handshake* (protocolo *Extensible Authentication Protocol over LAN* (EAPOL)), que como visível na lista de

pacotes, o ataque de desautenticação forçou o dispositivo cliente a se reconectar e isso permitiria ao atacante interceptar todas as quatro mensagens de troca de chaves. Com a troca de chaves completa, as 4 mensagens, reúne-se material criptográfico necessário do processo de associação a rede protegida para realizar ataques de força bruta ou de dicionário offline (utilizando ferramentas como Aircrack-ng ou Hashcat), como esforço de descobrir a senha da rede, sendo essas ferramentas focadas em quebra de hashes e senhas utilizando alto processamento computacional (força bruta).

Figura 11 – Captura de *handshake* após desautenticação em rede protegida



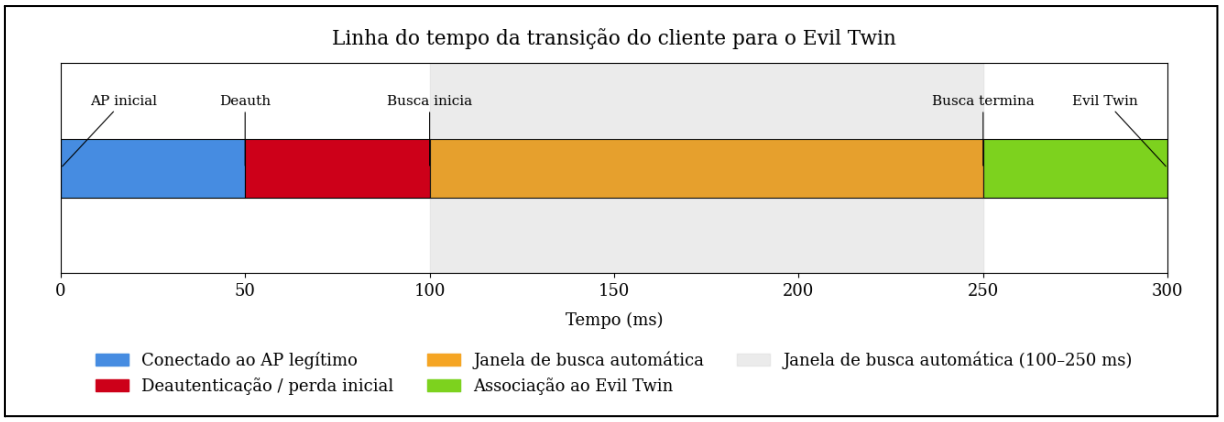
Fonte: Elaborado pelos autores (2026)

Para fortalecer a afirmação de transação transparente ao usuário, um teste adicional foi realizado com um laptop executando Microsoft Windows 11, que estava com a funcionalidade de "conectar-se automaticamente" desabilitada para o SSID da rede legítima. Mesmo com essa configuração, a execução do ataque de desautenticação contra o ponto de acesso legítimo também fez o dispositivo cliente se conectar ao Evil Twin automaticamente, sem qualquer notificação no dispositivo ou comportamento reconhecível, indicando que as contramedidas utilizando hábitos simples no nível do sistema operacional são insuficientes para proteger contra esse tipo de ataque combinado, pois uma desconexão total que resulta na conexão a

única rede disponível com o mesmo SSID pelo sistema operacional que é a rede maliciosa.

A transação ser transparente acontece devido ao tempo curto entre a desconexão do ponto de acesso legítimo e a reconexão automática ao ponto de acesso malicioso. Para ter uma amostragem desse intervalo, realizamos a análise dos pacotes capturados usando o Wireshark e, conforme ilustra a Figura 12, identificamos dois marcos principais, sendo o envio do quadro de desautenticação ao cliente, registrado aos 50 milissegundos, e a associação automática ao ponto de acesso malicioso que se segue, observada aos 300 milissegundos. O tempo de transição é calculado pela diferença entre esses dois eventos, sendo um intervalo de 250 milissegundos (300 ms − 50 ms). Esse valor ilustra que por todo o processo ocorrer em menos de um terço de segundo, para o usuário final seria invisível mesmo que o ícone de rede sofresse uma alteração em tempo real ou durante consumo de serviço de rede.

Figura 12 – Tempo de transição entre o AP legítimo e o Evil Twin



Fonte: Elaborado pelos autores (2026)

Quanto ao cenário utilizando ponto de acesso WiFi 6 (MitraStar), mesmo com a contínua transmissão de pacotes do ataque de desautenticação, utilizando protocolo de criptografía WPA2 em modo misto de WiFI 5 e 6, é possível verificar que não há desconexão do dispositivo cliente compatível com WIFI 6. Devido ao nosso dispositivo também habilitar por padrão PMF quando em modo misto, dispositivos conectados em WIFI 5 também não são desconectados, mas

dispositivos antigos como Apple iPad de terceira geração (2012) deixam de conseguir se conectar.

Em resumo, os resultados demonstram o claro risco da exploração da rede pública, especialmente no cenário de pontos de acesso WiFi 5 e anteriores. A vulnerabilidade inicial da conveniência da conexão automática baseada em sinal é muito maior quando há a manipulação ativa da vulnerabilidade do protocolo da rede Wi-Fi, que ignora a resiliência de uma conexão já estabelecida tanto quanto as configurações mais básicas de preferência em relação a rede, como de conexão automática. Principalmente a facilidade com que esses ataques podem ser realizados, além da transparência para a vítima, expõe a fragilidade da segurança em redes abertas e a necessidade de soluções que protejam os usuários delas junto de conscientização dos riscos.

5 CONSIDERAÇÕES FINAIS

As redes sem fio revolucionaram a conectividade, tornando-se predominantes em ambientes públicos e privados. Este trabalho demonstra que a operação das redes sem fio abertas ou criptografadas, baseada no protocolo IEEE 802.11ac e anteriores, expõe os usuários a riscos de segurança diversos através de vulnerabilidades, uma vez que a busca por conveniência e acesso simplificado faz com que a segurança seja uma questão em segundo plano especialmente para decisões de implementação, criando um ambiente de rede propício para ataques.

Conforme evidenciado pela fase experimental, um ponto de acesso malicioso (*Evil Twin*) pode receber a conexão e passar a roteador o tráfego de um dispositivo com facilidade. Essa facilidade é criada pela vulnerabilidade gerada pelo comportamento padrão dos sistemas operacionais clientes, que para redes conhecidas realiza conexão automática apenas com base no nome da rede (SSID) e prioriza a conexão com o ponto de acesso de maior intensidade de sinal.

Também pode-se analisar que um ataque de desautenticação, quando combinado com um *Evil Twin*, reduz ainda mais a segurança, pois força o redirecionamento do tráfego de forma transparente para o usuário, que acontece pela reconexão em um ponto de acesso diferente (ponto de acesso malicioso), mesmo com o recurso de conexão automática desativada em sistemas operacionais móveis e de computadores. Uma vez que o atacante controla o fluxo de dados através do ponto de acesso, ele pode aplicar outros ataques, como os descritos no referencial teórico.

Conclui-se que a segurança em redes públicas não depende apenas da conscientização do usuário, mas de aprimoramentos tecnológicos, em vista que nossa análise indica que seriam exigidas mudanças em duas frentes em prol de maior segurança. Primeiramente, na frente do próprio usuário das redes WIFI, os sistemas operacionais dos dispositivos clientes deveriam adotar critérios de validação de rede mais rigorosos não se limitando apenas ao SSID, mas incluindo outros parâmetros como o endereço MAC de pontos de acesso que considera confiáveis ou até de uma conexão ativa. Em segundo lugar, o próprio responsável pela disponibilização de redes baseadas no protocolo 802.11 poderia adotar pontos de acesso com suporte a 802.11ax e superiores para proteger a integridade dos

quadros de gerenciamento mesmo em redes sem autenticação para impedir ataques de desautenticação e a infraestrutura de rede da organização que disponibiliza a rede poderiam incorporar mecanismos para detectar os pontos de acesso fraudulentos. A atualização para pontos de acesso mais modernos é baseada na informação pública que dispositivos fabricados a partir de julho de 2020, tem obrigatoriedade de suporte aos Quadros de Gerenciamento Protegidos (PMF) para serem certificados pela Wi-Fi Alliance. Sendo essa uma exigência aplicada aos padrões Wi-Fi 4, 5 e 6, definida como condição essencial para a implementação da segurança WPA3 (Dekra, 2020).

Diante dos cenários abordados e discutidos ao longo desse, conforme sugerido pelo CERT.BR (2026), algumas contramedidas a serem consideradas pelo usuário quando conectar nessas redes públicas: não acessar plataformas que sejam para pagamentos ou de instituições financeiras, use serviços que ofereçam criptografia como HTTPS, PGP, SSH e *Virtual Private Network* (VPN), prefira usar redes Wi-Fi que solicitem autenticação, desabilite a conexão automática. Para proprietários das redes as dicas são: alterar a senha de administração dos equipamentos, usar senha forte e trocar periodicamente, não use nome (SSID) padrão para sua rede Wi-Fi, ative criptografia na rede prefira WPA3 ou WPA2/WPA3, ative o firewall de rede e se possível crie uma rede para convidados/clientes/visitantes. Nascimento (2025) vai um pouco além sugerindo conscientização ao usuário através de títulos chamativos, dicas rápidas e chamativas e até um passo a passo com orientações sobre como configurar uma VPN ou identificar redes falsas.

Concluindo, o trabalho evidencia a lacuna entre conveniência e a segurança nas redes Wi-Fi abertas e públicas, direcionando para que pesquisas futuras explorem o desenvolvimento prático de mecanismos de mitigação ou detecção principalmente dos ponto de acesso maliciosos (*Evil Twins*) ou de tentativas de ataque de desautenticação, seja direcionado aos pontos de acesso ou aos sistemas operacionais clientes, de forma a aprimorar a segurança sem comprometer a conveniência que faz com que as redes sem fio sejam, de forma crescente, unanimidade entre os usuários. Outro foco de pesquisa a partir desse trabalho seria a exploração em campo, coletando dados expostos pelos ponto de acesso de

ambientes de grande movimento ou até de amostragem de ambientes residenciais, de forma a identificar o percentual de ponto de acesso limitados a tecnologia anterior ao WIFI 6 e pesquisas de campo para amostragem da compatibilidade de dispositivos cliente com o padrão mais seguro de WIFI, que seriam possíveis a partir de coleta de marca e modelo dos dispositivos para serem submetidos a extração posterior das especificações dos adaptadores WIFI e até a versão de sistema operacional quanto ao suporte a criptografia moderna como o WPA3.

REFERÊNCIAS

ALVES NETO, J. P. A. **Segurança e vulnerabilidades em redes wi-fi e móveis: riscos e proteção de dados em transações bancárias** - 2025. TCC (Graduação – Tecnologia em Sistema da Informação) – Instituto Federal Goiano – IFGO 2025. Disponível em: https://repositorio.ifgoiano.edu.br/bitstream/prefix/5485/1/art_tcc_Jose%20Pedro%20Alves%20Neto.pdf. Acesso em: 12 abr. 2026.

BAKER, K**. What is a Man in the Middle (MITM) Attack?**. CrowdStrike.com, 17 jan. 2025. Disponível em: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/man-in-the-middle-mitm-attack/. Acesso em: 6 jun. 2025.

BLUEPEX. **Captive Portal: Segurança e Conformidade no Wi-Fi Corporativo**. [S. l.]: BluePex, 22 jan. 2025. Disponível em: https://bluepex.com.br/noticias/captive-portal-seguranca-e-conformidade-no-wi-fi-corporativo. Acesso em: 6 jun. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 6 jun. 2025.

BÜCHELER, D**. Next-Generation Hotspots: Privacy Aspects of Wi-Fi Autoconnection**. *In*: SPRING 2025, Nuremberg, 28-29 abr. 2025. Nuremberg: [s. n.], 2025. Disponível em: https://fg-sidar.gi.de/fileadmin/FG/SIDAR/Reports/SIDAR-Report-SR-2025-01.pdf#page=9. Acesso em: 7 jun. 2025.

CERQUEIRA JÚNIOR, R. L. et al. **Um Sistema de Detecção de Ataques Evil Twin com Aprendizado de Máquina Não-Supervisionado**. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC). **Anais** [...]. Porto Alegre: SBC, 2024. Disponível em: https://sol.sbc.org.br/index.php/sbrc/article/view/29846/29649. Acesso em: 17 jan. 2025.

CERT.BR. **Redes - Cartilha de Segurança para Internet**. 16 ago. 2024. Disponível em: https://cartilha.cert.br/fasciculos/redes/fasciculo-redes-alta.pdf. Acesso em: 10 maio 2026.

COPPOCK, MAZAL. **Wi-fi security comparisons: What are WEP, WPA, WPA2, and WPA3.** Avast Academy, 01 sep. 2025. Disponível em: https://www.avast.com/c-wep-vs-wpa-or-wpa2. Acesso em: 13 abr. 2026.

DEKRA. **Wi-Fi CERTIFIED WPA3™ Will Be Mandatory from July, 2020**. [S. l.], 15 jul. 2020. Disponível em: https://cpstp.bureauveritas.com/BVInternet/News/1109;mainIDX=1109. Acesso em: 11 maio 2026.

GHIMIRAY, D**. O que é e como funciona um ataque evil twin?**. Avast Academy, 5 dez. 2023. Disponível em: https://www.avast.com/pt-br/c-evil-twin-attack. Acesso em: 6 jun. 2025.

GOMES, R. C. **Problemas de segurança em redes de computadores na Marinha do Brasil: uma análise sobre a técnica Rogue Access Point**. 2018. Monografia (Curso de Aperfeiçoamento Avançado de Segurança da Informação e Comunicações) - Centro de Instrução Almirante Wandenkolk, Marinha do Brasil, Rio de Janeiro, 2018. Disponível em: https://repositorio.marinha.mil.br/bitstream/ripcmb/845486/1/CAPA-SIC-16%201T%20Rafael%20CAVEARI%20Gomes%20-TCC.pdf. Acesso em: 25 maio 2026.

HARKINS, Dan. **Wi-Fi CERTIFIED Enhanced Open™: Transparent Wi-Fi® protections without complexity**. Wi-Fi Alliance, 2018. Disponível em: https://www.wi-fi.org/beacon/dan-harkins/wi-fi-certified-enhanced-open-transparent-wi-fi-protections-without-complexity. Acesso em: 11 maio 2026.

MORAES, A. F**. Redes sem fio: instalação, configuração e segurança: Fundamentos**. São Paulo: Érica, 2010. Disponível em: https://www.kufunda.net/publicdocs/Redes%20Sem%20Fio%20-%20Instala%C3%A7%C3%A3o%20Configura%C3%A7%C3%A3o%20e%20Seguran%C3%A7a%20-%20Fundamentos%20(ALEXANDRE%20FERNANDES%20DE%20MORAES).pdf. Acesso em: 6 jun. 2025.

NASCIMENTO, S. L. do. **Os riscos de conectar-se a uma rede wi-fi de acesso público** – 2025. TCC (Graduação – Tecnologia em Sistemas de Telecomunicações) – Instituto Federal da Paraíba – IFPB / Coordenação de Tecnologia em Sistemas de Telecomunicações, 2025. Disponível em: https://repositorio.ifpb.edu.br/handle/177683/4462. Acesso em: 12 abr. 2026.

PAULA FILHO, D. et al**. Ataque a redes abertas com Man in the Middle**. *In*: SALÃO DE PESQUISA E INOVAÇÃO, 8., 2022, Bragança Paulista. **Anais** [...]. Bragança Paulista: Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, 2022. p. 1-3. Disponível em: https://intra.brt.ifsp.edu.br/eventos/spi/publicacoes/spi_8/SPI22BRT09.pdf. Acesso em: 6 jun. 2025.

PEREIRA, M. V**. Implementando Segurança no Nível de Acesso Utilizando Servidor RADIUS**. 2011. Trabalho de Conclusão de Curso (Especialização em Gerência de Redes de Computadores) - Universidade Tecnológica Federal do Paraná, Curitiba, 2011. Disponível em: https://riut.utfpr.edu.br/jspui/bitstream/1/17243/2/CT_GESER_1_2011_17.pdf. Acesso em: 6 jun. 2025.

SANTOS, A. A.; SANTOS, A. F. dos; MANIÇOBA, R. H. C. **Wi-Fi 6 e Wi-Fi 6E: Uma análise comparativa dentro do novo padrão 802.11ax**. *Revista Científica Foz*, v. [s.v.], n. [s.n.], p. [s.p.], 2024. Disponível em: https://revista.ivc.br/index.php/revistafoz/article/view/306/151. Acesso em: 25 maio 2026.

SERAFIM, L. V. **Análise de segurança em redes wireless por meio do teste de penetração**. 2020. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) - Universidade do Extremo Sul Catarinense, Criciúma, 2020. Disponível em: https://repositorio.unesc.net/bitstream/1/8839/1/Lurian%20Vieira%20Serafim.pdf. Acesso em: 25 maio 2026.

SILVA JUNIOR, W. C. S; NASCIMENTO, M. H. R. **Sistema Unificado de Detecção e Mitigação de Ataques de Evil Twin em Redes Wi-Fi Industriais com IOT/IIOT**. Revista de Gestão e Secretariado – GeSec, V.16, N.6, P. 01 - 22, 2025. Disponível em: https://ojs.revistagesec.org.br/secretariado/article/view/4982/3291. Acesso em: 12 abr. 2026.

SILVA NETO, Luiz Gustavo. **Análise de vulnerabilidades em redes sem fio IEEE 802.11 com Kali Linux**. 2021. 53 f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, Votuporanga, 2021. Disponível em: https://vtp.ifsp.edu.br/images/TCC/2021/BCC/Luiz_Gustavo_Silva_Neto.pdf. Acesso em: 19 out. 2025.

VENTAS DE SEGURIDAD. **Fake Captive Portals**. [S. l.]: Ventas de Seguridad, 18 jul. 2023. Disponível em: https://www.ventasdeseguridad.com/en/more-in-depth/columns-and-opinions/21722-fake-captive-portals.html. Acesso em: 6 jun. 2025.

GLOSSÁRIO

AES-CCMP / AES-GCMP: Modos avançados de criptografia usados em redes sem fio, sendo o GCMP adotado pelo WPA3 por oferecer maior eficiência e melhor integridade de dados comparado ao antecessor CCMP.

Aircrack-ng: Suíte de softwares de código aberto voltada para a análise, interceptação e exploração de vulnerabilidades em redes sem fio.

Ataque de desautenticação: Exploração de falhas na proteção de pacotes de gerenciamento do Wi-Fi para forçar a desconexão de dispositivos de um ponto de acesso legítimo, causando uma negação de serviço temporária.

Ataque de Força Bruta / Dicionário: Técnicas que utilizam alto poder computacional para tentar adivinhar chaves de criptografia ou senhas *offline*, testando exaustivamente combinações de caracteres ou listas de palavras.

***Beacon frame*:** Quadro de gerenciamento transmitido continuamente por um ponto de acesso para anunciar a presença da rede sem fio aos dispositivos em seu raio de alcance.

***Broadcast*:** Método de envio de pacotes de dados direcionado de forma simultânea a todos os dispositivos conectados em um mesmo segmento de rede.

BSSID (*Basic Service Set Identifier*): Endereço físico (MAC Address) que identifica de forma exclusiva a interface sem fio de um roteador ou ponto de acesso alvo.

***Captive Portal*:** Página ou ferramenta de autenticação web exibida ao usuário em redes públicas para forçar uma interação (como login ou aceite de termos) e registrar o acesso à internet.

***Downgrade* (Ataque):** Técnica cibernética em que o atacante força um dispositivo a abandonar um protocolo moderno de conectividade ou criptografia para assumir um padrão mais antigo e vulnerável.

EAPOL (*Extensible Authentication Protocol over LAN*): Protocolo responsável por encapsular e transportar as mensagens de troca de chaves criptográficas (como as do *Handshake*) durante o processo de associação em redes protegidas.

***Evil Twin*:** Ponto de acesso malicioso configurado para clonar o nome (SSID) de uma rede legítima, visando assumir as conexões e interceptar o tráfego dos usuários de forma transparente.

***Fake Captive Portal*:** Versão falsificada de um portal de autenticação de rede, desenvolvida para ser visualmente idêntica à legítima, a fim de enganar o usuário e capturar dados e credenciais sensíveis.

***Handshake* (*4-Way Handshake*):** Processo estruturado em quatro etapas realizado entre o dispositivo cliente e o ponto de acesso em redes com criptografia (como o WPA2) para validar credenciais e gerar o material criptográfico da sessão.

Hashcat: Ferramenta computacional altamente avançada focada na recuperação e quebra de senhas, utilizada para reverter *hashes* criptográficos por meio de ataques locais (*offline*).

IEEE 802.11: Família de padrões técnicos globais estabelecidos pelo *Institute of Electrical and Electronics Engineers* que definem as especificações da camada física e do controle de acesso das redes locais sem fio (Wi-Fi).

IoT / IIoT (*Internet of Things / Industrial Internet of Things*): Conceito que descreve a interconexão digital massiva à internet de dispositivos do dia a dia (IoT) e de equipamentos e maquinários do setor industrial (IIoT).

Kali Linux: Sistema operacional baseado na distribuição Linux Debian, amplamente reconhecido e utilizado para auditorias e testes de intrusão por já possuir dezenas de ferramentas de segurança pré-instaladas.

MAC Address (*Media Access Control*): Endereço físico fixo que identifica o hardware de um dispositivo de rede (como a placa Wi-Fi de um celular ou computador) de forma única em uma rede local.

MAC Spoofing: Técnica que consiste em falsificar o endereço MAC de origem nos pacotes de rede, fazendo com que o dispositivo alvo acredite que os pacotes recebidos partiram de uma fonte confiável.

Man-in-the-Middle (MitM): Modalidade de ataque onde o invasor atua invisivelmente como um intermediário na comunicação entre a vítima e o serviço legítimo para espionar e interceptar o tráfego de dados.

MU-MIMO / OFDMA / 1024-QAM: Inovações e tecnologias de radiofrequência introduzidas pelo padrão Wi-Fi 6 com o objetivo de otimizar a densidade de transmissão, velocidade e estabilidade das conexões.

OWE (*Opportunistic Wireless Encryption* / Padrão *Enhanced Open*): Padrão de conectividade que aplica criptografia individualizada aos dados transmitidos pelos usuários, mesmo em redes públicas abertas sem a exigência de senhas.

***Payload*:** O corpo ou carga útil contida dentro de um pacote de rede, onde localizam-se os dados primários ou as instruções reais sendo transmitidas entre a origem e o destino.

PGP, SSH e VPN: Ferramentas, protocolos e serviços recomendados para a criação de túneis virtuais que oferecem criptografia a fim de proteger as comunicações de usuários em redes públicas ou não confiáveis.

PMF (*Protected Management Frames*): Mecanismo tecnológico que adiciona criptografia e atesta a autenticidade dos pacotes de gerenciamento de rede sem fio, protegendo a conexão contra tentativas forçadas de desconexão.

RADIUS (*Remote Authentication Dial-In User Service*): Protocolo/servidor utilizado no cenário corporativo para fornecer um gerenciamento centralizado e seguro de autenticação (frequentemente utilizado na arquitetura WPA2/WPA3 *Enterprise*).

SAE (*Simultaneous Authentication of Equals*): Avançado protocolo de segurança de troca de chaves que integra o WPA3, protegendo o procedimento de associação da rede contra ataques de adivinhação, mesmo se o usuário utilizar senhas vulneráveis.

SSID (*Service Set Identifier*): O nome público atribuído a um ponto de acesso ou roteador para identificar visualmente uma rede Wi-Fi aos clientes que buscam se conectar.

WEP (*Wired Equivalent Privacy*): Um dos primeiros padrões de segurança de rede sem fio, considerado atualmente obsoleto e vulnerável por apresentar falhas matemáticas críticas em sua proteção.

Wireshark: Analisador de protocolos de rede amplamente utilizado na academia e na indústria para inspecionar, em alto grau de detalhe, os pacotes que trafegam em conexões locais.

WLAN (*Wireless Local Area Network*): Nomenclatura técnica oficial que categoriza uma Rede Local Sem Fio, popularizada globalmente como tecnologia Wi-Fi.

WPA2 / WPA3 (*Wi-Fi Protected Access*): Gerações recentes e robustas dos protocolos de segurança da *Wi-Fi Alliance*, dedicados a garantir forte criptografia e acesso autenticado exclusivo a quem detém a senha correta da rede.