Análise Experimental de Ataques de Desautenticação em Redes WiFi e Estratégias de Mitigação com WPA3

Rafael A. Lima[1], **Paulo R.S.L. Coelho**[1], **Rafael Pasquini**[1], **Luís F. Faina**[1]

[1]Faculdade de Computação – Universidade Federal de Uberlândia (UFU)
Caixa Postal 592 – 38.400-902 – Uberlândia – MG – Brazil

{rafael.alv334,paulocoelho,rafael.pasquini,luisfaina}@ufu.br

Abstract. *Wireless networks based on the IEEE 802.11 standard are widely used in residential and enterprise environments, but remain vulnerable to deauthentication attacks. These attacks exploit the lack of protection in management frames, allowing attackers to disrupt communication between legitimate devices. This work presents an experimental analysis of deauthentication attacks in WiFi networks, considering different protocol versions (IEEE 802.11n and 802.11ac) and security mechanisms (WPA2 and WPA3). A controlled testbed was implemented to evaluate the effectiveness and impact of these attacks. Results show that WPA2 networks are highly vulnerable, while WPA3 combined with management frame protection (IEEE 802.11w) significantly mitigates them. Additionally, legacy and IoT devices introduce security gaps even in modern networks. As a contribution, this work provides an experimental comparison of security mechanisms and practical recommendations to improve the resilience of WiFi networks against deauthentication attacks.*

Resumo. *Redes sem fio baseadas no padrão IEEE 802.11 são amplamente utilizadas em ambientes residenciais e corporativos, porém permanecem vulneráveis a ataques de desautenticação, que exploram a ausência de proteção em quadros de gerenciamento. Este trabalho apresenta uma análise experimental desses ataques em redes WiFi, considerando as versões IEEE 802.11n e 802.11ac e os mecanismos de segurança WPA2 e WPA3. Foi implementado um ambiente controlado para avaliar seu impacto. Os resultados demonstram que redes WPA2 são altamente vulneráveis, enquanto o WPA3, com proteção de quadros de gerenciamento (IEEE 802.11w), mitiga significativamente o problema. Além disso, dispositivos legados e IoT introduzem lacunas de segurança mesmo em redes modernas. Como contribuição, este trabalho apresenta uma análise comparativa experimental e recomendações práticas para aumentar a resiliência de redes WiFi frente a esses ataques.*

1. Introdução

A crescente disseminação de redes WiFi em ambientes residenciais, corporativos e públicos tem impulsionado a conectividade de dispositivos e serviços digitais. No entanto, essa ampla adoção também amplia a superfície de ataque, tornando as redes sem fio alvos frequentes de ameaças cibernéticas. Dentre essas ameaças, destacam-se os ataques de desautenticação (*deauthentication attacks*), que exploram vulnerabilidades inerentes ao padrão IEEE 802.11 [Cheema et al. 2018, Gast 2005].

O ataque de desautenticação consiste na injeção de quadros falsificados de gerenciamento, com o objetivo de forçar a desconexão entre um Celular e um *Access Point* (AP). Esse tipo de ataque explora o fato de que, em versões legadas do padrão IEEE 802.11, os quadros de gerenciamento não possuem mecanismos de autenticação ou criptografia [Perahia and Stacey 2008]. Como consequência, dispositivos podem ser repetidamente desconectados da rede, caracterizando um cenário de negação de serviço (*Denial of Service* – DoS), além de viabilizar ataques subsequentes, como a captura de *handshakes* e a criação de pontos de acesso maliciosos.

A relevância desse problema é ampliada pelo crescimento do número de dispositivos conectados, especialmente em redes domésticas. No Brasil, a maioria das residências possui acesso à Internet, muitas delas com múltiplos dispositivos conectados simultaneamente [Camargo 2023]. Adicionalmente, o aumento expressivo de dispositivos IoT, frequentemente com limitações de segurança, contribui para a ampliação das vulnerabilidades [IT Forum 2023].

Apesar da evolução dos mecanismos de segurança, como o WPA2 e o WPA3, e da introdução de extensões como o IEEE 802.11w, que prevê a proteção de quadros de gerenciamento [Cisco 2015], ainda existem lacunas na efetiva mitigação desses ataques, especialmente em ambientes heterogêneos com dispositivos legados.

Diante desse contexto, este trabalho tem como objetivo analisar as vulnerabilidades associadas a ataques de desautenticação em redes WiFi, considerando diferentes versões do padrão IEEE 802.11, em especial o IEEE 802.11n (WiFi 4) e o IEEE 802.11ac (WiFi 5), sob os mecanismos de segurança WPA2 e WPA3.

Como contribuição, este trabalho apresenta uma análise comparativa do comportamento de redes WiFi frente a ataques de desautenticação, além de propor recomendações práticas para mitigação desses ataques.

2. Metodologia

Esta seção descreve o ambiente experimental, os procedimentos adotados e as configurações utilizadas para a realização dos testes de ataques de desautenticação em redes WiFi.

2.1. Ambiente Experimental

Os experimentos foram conduzidos em um ambiente controlado, representando um cenário típico de rede doméstica com Access Point TP-Link Archer AX12 e Celular Redmi Note 11 executando Android 13. Foram considerados os padrões amplamente utilizados como IEEE 802.11n e IEEE 802.11ac [Gast 2005, Perahia and Stacey 2008].

Em relação à segurança, foram avaliadas redes configuradas com WPA2-PSK e WPA3-SAE, permitindo analisar diferentes níveis de proteção [Cisco 2015].

O cenário experimental adotado neste trabalho segue a configuração ilustrada na Figura 1, que representa um ambiente típico de rede doméstica composto por um *Access Point*, um *Desktop* de Usuário, um *Celular* (Alvo do Ataque *De-Auth*). Neste cenário, introduzimos um dispositivo atacante (*Notebook De-Auth* - Kali Linux 2025.2) e um dispositivo que captura pacotes (*Notebook Sniffer - Kali Linux 2025.2*) que não estão associados ao AP. Essa configuração permite a observação controlada do comportamento da

rede durante todas as fases do experimento, incluindo autenticação, associação e execução do ataque de desautenticação.

Figura 1. Cenário Padrão Para os Testes. Fonte: Do Autor.

2.2. Ferramentas Utilizadas

A execução dos ataques foi realizada com a suíte *Aircrack-ng* [Aircrack 2025], amplamente utilizada em testes de segurança em redes sem fio. Para análise do tráfego, utilizou-se o Wireshark, ferramenta consolidada para inspeção de protocolos e análise de pacotes em redes [Wireshark 2024].

2.3. Procedimento Experimental

O procedimento experimental seguiu três etapas principais: i) estabelecimento da conexão entre um Celular e o AP, incluindo autenticação e associação; ii) execução do ataque de desautenticação por meio da injeção de quadros forjados [Cheema et al. 2018]; e iii) coleta e análise dos quadros capturados para avaliação do impacto na comunicação.

O processo de conexão em redes WiFi inicia-se com a autenticação do cliente junto ao Access Point, seguida da associação, na qual o dispositivo é formalmente integrado à rede e recebe um identificador que permite a troca de dados. Em redes WPA2, após a associação, ocorre o *4-Way Handshake*, no qual AP e cliente trocam *nonces* e derivam a *PTK* a partir da *PSK*, garantindo a segurança da comunicação.

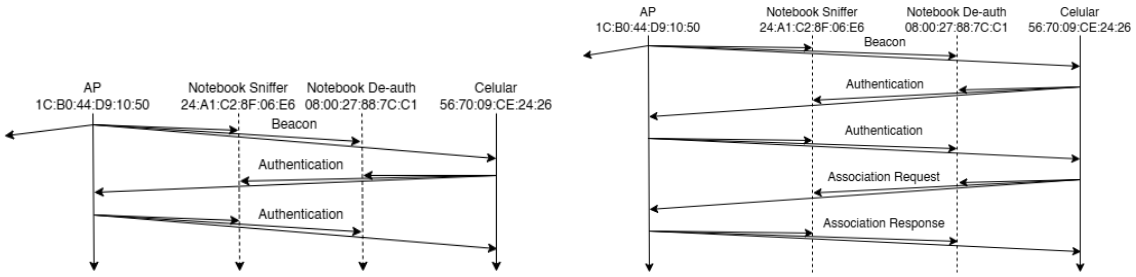
O processo de *deauthentication* encerra a conexão, mas a ausência de autenticação desses quadros em versões legadas permite que atacantes os forjem para provocar desconexões e ataques de negação de serviço. Os experimentos foram repetidos para diferentes combinações de protocolos e mecanismos de segurança, permitindo análise comparativa.

3. Resultados

A Fig. 2a descreve as mensagens trocadas entre o Celular e o AP para estabelecer a autenticação. O próximo passo no processo de conexão ao AP é a associação, na qual o Celular solicita a entrada na rede. Esse processo é fundamental para estabelecer uma conexão e garantir que o dispositivo seja reconhecido como parte da rede.

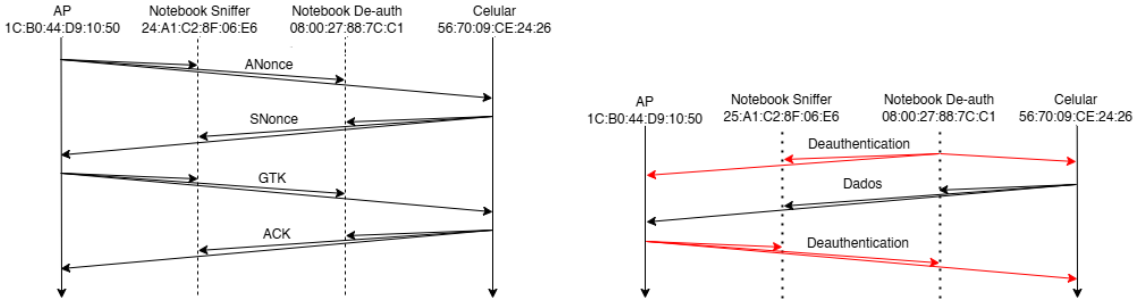
Já a Fig. 2b descreve as mensagens trocadas entre o Celular e o AP, incluindo a varredura da rede, autenticação e associação.

O diagrama de sequência da Fig. 3a detalha as etapas do processo de descoberta da rede, autenticação, associação e *4-Way Handshake* no WPA2, destacando as mensagens enviadas entre o Celular e o AP. Durante essa troca de mensagens o *Notebook Sniffer* e *Notebook DeAuth* obtem os dados necessários para montar e dispar o Ataque de *De-Authentication* ou *De-Auth*.



(a) Autenticação do Celular (*Host*). **(b) Associação do Celular (*Host*).**

Figura 2. Diagrama de Sequência Temporal para Autenticação e Associação.



(a) 4-Way Handshake do Celular (*Host*). **(b) Ataque DeAuth pelo *Notebook Sniffer*.**

Figura 3. Diagrama de Sequência do *4-Way Handshake* e Ataque *DeAuth*.

A dinâmica do ataque de desautenticação pode ser melhor compreendida por meio do diagrama de sequência apresentado na Figura 3b, que ilustra a troca de mensagens entre o atacante, o *Access Point* e o Celular. Nesse processo, o atacante injeta quadros de desautenticação forjados, simulando comunicações legítimas e induzindo o encerramento da conexão.

3.1. Comportamento em Redes com WPA2

Os experimentos demonstraram que redes protegidas com WPA2 permanecem vulneráveis a ataques de desautenticação, uma vez que os quadros de gerenciamento não são protegidos [Gast 2005, Cheema et al. 2018]. A injeção de quadros forjados resultou na interrupção imediata da comunicação.

Esse comportamento confirma limitações conhecidas do WPA2, mesmo com uso de criptografia AES-CCMP para dados [Perahia and Stacey 2008].

3.2. Comportamento em Redes com WPA3

Nos cenários com WPA3 e proteção de quadros de gerenciamento (IEEE 802.11w), observou-se que os ataques não foram efetivos, pois os quadros falsificados não foram aceitos [Cisco 2015].

Entretanto, dispositivos operando em modo de compatibilidade ainda apresentaram vulnerabilidades, evidenciando limitações práticas na adoção do WPA3.

3.3. Análise Comparativa

A comparação entre WPA2 e WPA3 evidencia que a proteção de quadros de gerenciamento é o principal fator para mitigação do ataque, e não a versão do padrão IEEE 802.11

em si [Gast 2005].

3.4. Impacto em Dispositivos IoT

Dispositivos IoT mostraram-se particularmente vulneráveis, pois frequentemente não suportam WPA3 ou IEEE 802.11w, corroborando estudos recentes sobre segurança em ambientes IoT [IT Forum 2023].

4. Conclusão

Este trabalho investigou vulnerabilidades associadas a ataques de desautenticação em redes WiFi, com base em diferentes versões do padrão IEEE 802.11 e mecanismos de segurança.

Os resultados confirmam que redes WPA2 permanecem vulneráveis devido à ausência de proteção em quadros de gerenciamento [Gast 2005], enquanto WPA3 com IEEE 802.11w oferece mitigação efetiva [Cisco 2015]. Também foi evidenciado que dispositivos legados e IoT representam um ponto crítico na segurança das redes, conforme apontado na literatura recente [IT Forum 2023].

Como contribuição, este trabalho apresenta uma análise experimental comparativa e recomenda a adoção de WPA3, a ativação da proteção de quadros de gerenciamento (IEEE 802.11w/PMF), a atualização periódica de *firmware* e a desativação de modos de compatibilidade legados quando possível, como medidas essenciais para aumentar a segurança das redes WiFi.

Como trabalhos futuros, sugere-se investigar mecanismos complementares, como sistemas de detecção de intrusão aplicados a redes WiFi.

Referências

Aircrack (2025). Aircrack-ng. https://www.aircrack-ng.org/.

Camargo, B. (2023). Cerca de 84% dos Lares Brasileiros Têm Acesso à Internet, Diz Pesquisa.

Cheema, R., Bansal, D., and Sofat, S. (2018). Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks. *Department of Computer Science and Engineering, PEC University of Technology*.

Cisco (2015). *802.11r, 802.11k, and 802.11w Deployment Guide, Cisco IOS-XE Release 3.3*.

Gast, M. S. (2005). *802.11 Wireless Networks: The Definitive Guide*. O'Reilly Media.

IT Forum (2023). Ataques Contra a Internet das Coisas Saltam 41%, Alerta Check Point.

Perahia, E. and Stacey, R. (2008). *Next Generation Wireless LANs: Throughput, Robustness, and Reliability in 802.11n*. Cambridge University Press, Cambridge, 1st edition.

Wireshark (2024). Wireshark. https://www.wireshark.org/.