International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 16, No.1 (Sep-24)

http://dx.doi.org/10.12785/ijcds/160196

Securing the Airwaves:
A Survey on De-authentication Attacks and Mitigation Strategies

Adwait Gulab Gaikwad[1] **and Balaji Patil**[2]

[1]*Department of Computer Engineering and Technology, MIT-World Peace University, Kothrud, India*
[2]*Department of Computer Engineering and Technology, MIT-World Peace University, Kothrud, India*

Received 2 Feb. 2024, Revised 28 May 2024, Accepted 31 May 2024, Published 15 Sep. 2024

Abstract: Wi-Fi networks, crucial for modern communication, are confronted with an escalating array of security challenges. Notably, de-authentication attacks emerge as formidable threats, involving the unauthorized expulsion of legitimate users from a Wi-Fi network. These attacks disrupt communication and may lead to unauthorized access by exploiting vulnerabilities in the communication protocols governing Wi-Fi networks. The susceptibility of these networks to malicious interference extends beyond disrupting communication; it poses a significant risk to the integrity of authentication methodologies, potentially facilitating unauthorized access. In the context of the Internet of Things (IoT), where seamless and secure connectivity is paramount, the implications of de-authentication attacks become particularly severe. This paper delves into a comprehensive analysis of de-authentication attacks, meticulously dissecting their various types and the resultant impact on wireless communication protocols, authentication methodologies, and the overall security posture of IoT devices. The study aims to analyze the growing threat of de-authentication attacks on Wi-Fi networks and their implications for the security of Internet of Things (IoT) devices. By employing a comprehensive methodology, we conducted an in-depth examination of various types of de-authentication attacks and their impact on wireless communication protocols and authentication methodologies.

Keywords: De-authentication, Mitigation Techniques, Wireless Networking, IoT Security

1. INTRODUCTION

In the intricate landscape of wireless communication, de-authentication attacks present a discreet yet significant threat to the stability and security of Wi-Fi networks. These attacks, exploiting vulnerabilities in how devices communicate wirelessly, can have far-reaching consequences. This paper aims to shed light on de-authentication attacks to understand their intricacies, recognize their importance, and grasp the potential impacts they can have on the reliability of Wi-Fi networks. Understanding why de-authentication attacks matter is crucial. These attacks go beyond mere interruptions in service; they have the potential to compromise the confidentiality and availability of data. As cyber adversaries exploit weaknesses in the rules that govern wireless communication, the stakes for secure Wi-Fi connectivity rise. The fallout from de-authentication attacks is varied, ranging from temporary disruptions in service to more severe compromises in the overall security of Wi-Fi networks. In an age where Internet of Things (IoT) devices are seamlessly integrated into our daily lives, the susceptibility of these interconnected devices to de-authentication attacks adds complexity and requires careful consideration of their potential impact. This paper seeks to demystify de-authentication attacks. Its primary goals are twofold: firstly, to offer a systematic analysis of these attacks, exploring their different types, methods, and where they might exploit weaknesses in wireless communication protocols. Secondly, it aims to provide practical guidance on effective mitigation techniques, serving as a resource for fortifying Wi-Fi networks against these specific threats. This survey paper examines de-authentication attacks on Wi-Fi networks, exploring their disruptive nature and security implications. By dissecting these attacks, it merges theoretical understanding with practical insights, presenting actionable strategies for mitigation. The paper seeks to enrich Wi-Fi security discourse, empowering stakeholders to fortify against evolving cyber threats within our dynamic digital ecosystem.

2. ORGANIZATION OF PAPER

The paper follows a logical sequence, commencing with an Introduction that outlines its objectives. Table 1 presents list of abbreviation. The Background section provides essential context, laying the groundwork for a deeper understanding of de-authentication attacks. The exploration continues with the De-authentication Attacks section, where various attack techniques and their potential consequences are discussed. Table 2 presents comparison of different contributions among existing survey papers.

E-mail address: adwait420gaikwad@gmail.com, balaji.patil@mitwpu.edu.in

Mitigation Techniques are then examined, offering insights into strategies for countering these attacks. The Evaluation Metrics section focuses on assessing the effectiveness of mitigation strategies without delving into specific tools. This segment adds a crucial dimension to the discussion by presenting criteria for gauging the success of mitigation efforts. The narrative advances with real-world implications of de- authentication attacks and the efficacy of mitigation strategies. Challenges and Future Directions follow, addressing current obstacles and proposing potential avenues for future research. The paper concludes by summarizing key findings in the Conclusion, providing a cohesive journey through the complexities of wireless network security.

3. BACKGROUND

Wireless communication relies on the transmission of data through radio frequency signals, enabling devices to connect and exchange information without physical cables. This mode of communication is integral to various technologies, including Wi-Fi, Bluetooth, and cellular networks. Authentication protocols play a pivotal role in securing wireless communication by verifying the identity of devices or users before granting access to a network. These protocols ensure that only authorized entities can connect, mitigating the risk of unauthorized access and potential security breaches.

A. Common wireless communication protocols include:

- Wi-Fi (Wireless Fidelity): Wi-Fi is widely used for local wireless networking, providing connectivity to devices such as smartphones, laptops, and IoT devices. The IEEE 802.11 family of standards governs Wi-Fi communication, with security features like WPA3 (Wi-Fi Protected Access 3) enhancing data protection.

- Bluetooth: Bluetooth enables short-range wireless communication between devices, such as headphones, speakers, and smartwatches.Bluetooth devices employ pairing mechanisms and authentication to establish secure connections.

- Cellular Networks: Mobile communication relies on cellular networks, such as 4G LTE and 5G. These networks use authentication protocols to secure user identity and protect data during transmission.

B. Authentication Protocols in Communication Includes:

- WPA/WPA2/WPA3: Wi-Fi networks commonly employ WPA (Wi-Fi Protected Access) protocols to authenticate users and encrypt data. WPA3, the latest iteration, introduces enhanced security features, including stronger encryption and protection against brute-force attacks.

- EAP (Extensible Authentication Protocol): EAP is a framework that supports various authentication methods for wireless networks. It facilitates secure authentication, commonly used in enterprise Wi-Fi setups.

- Bluetooth Pairing: Bluetooth devices use pairing mechanisms, such as PIN codes or numeric passkeys, to authenticate and establish secure connections. Bluetooth also supports Secure Simple Pairing (SSP) for more robust authentication.

- SIM Authentication: Cellular networks authenticate devices using SIM (Subscriber Identity Module) cards. The SIM card stores unique identifiers and cryptographic keys, ensuring secure authentication and access to the mobile network.

De-authentication plays a disruptive role in wireless communication by intentionally severing the connection between a device and a wireless network. This activity is typically employed as a form of cyber-attack, exploiting vulnerabilities in the communication protocol. Role of de-authentication in disrupting communication as follows:

- Forced De-authentication: De-authentication involves sending forged de-authentication frames to the targeted device or devices within a wireless network. These frames mimic legitimate disconnection messages from the network's access point. Consequently, the targeted devices interpret these fake frames as genuine requests to disconnect, leading to an abrupt termination of their connection to the network.

- Service Interruption: The primary consequence of de-authentication attacks is the immediate interruption of services for the affected devices. As the devices disconnect, they lose access to the network, disrupting ongoing communication, data transfers, and any active processes that rely on continuous connectivity.

- Denial of Service (DoS): De-authentication attacks are a form of Denial of Service (DoS) attack, as they deny legitimate users access to the network. By flooding the target with de- authentication frames, an attacker can overwhelm the network, causing widespread service disruptions and rendering it temporarily inaccessible to authorized users.

- Potential Impact on IoT Devices: Internet of Things (IoT) devices, which rely heavily on wireless communication, can be particularly vulnerable to de-authentication attacks. Disrupting the connectivity of IoT devices may compromise critical functions such as home automation, industrial processes, or healthcare monitoring systems.

- Exploitation of Vulnerabilities: De- authentication attacks exploit inherent vulnerabilities in wireless communication protocols, such as the IEEE 802.11 standard. The attacker does not need to know the network's security key; instead, they manipulate the communication process itself to force disconnections.

- Social Engineering and Espionage: In some cases,

TABLE I. List of Abbreviations

Abbreviations	Full Form
Wi-Fi	Wireless Fidelity
IoT	Internet of Things
WPA	Wi-Fi Protected Access
LTE	Long Term Evolution
WPA3	Wi-Fi Protected Access 3
EAP	Extensible Authentication Protocol
PIN	Personal Identification Number
SSP	Secure Simple Pairing
SIM	Subscriber Identity Module
DoS	Denial of Service
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MFA	Multi-Factor Authentication
CPU	Central Processing Unit

TABLE II. Comparison of Different Contributions Among Existing Survey Papers

Authors	Year	Contributions
Farhad Mehdipour [1]	2020	By highlighting the inapplicability of conventional security and privacy approaches to IoT due to its decentralized topology and resource constraints, the paper raises awareness about the unique challenges faced in securing IoT systems.
Aswin Raghuprasad, Suraj Padmanabhan, Arjun Babu M, and Binu P. K [2]	2020	The paper's conclusion suggests that the proposed system has the potential to significantly contribute to creating a safer IoT ecosystem by addressing specific security vulnerabilities and paving the way for further research and innovation in IoT security.
Mathy Vanhoef, Prasant Adhikari, Christina Pöpper [3]	2020	By identifying the vulnerability of Wi-Fi beacon frames to spoofing attacks, the paper brings attention to a significant security issue within Wi-Fi networks. This awareness is crucial for understanding the potential risks associated with Wi-Fi communication.
Zachary Neal and Kewei Sha [4]	2023	The authors recommend that vendors conduct thorough testing of their products before releasing them to the market and develop efficient mechanisms for applying patches to mitigate attacks if reported. This proactive approach can help prevent security breaches and protect users from potential risks associated with Wi-Fi camera vulnerabilities.

de-authentication attacks may be employed for more nefarious purposes, such as facilitating social engineering or espionage. By disrupting communications at strategic times, attackers can create opportunities to manipulate individuals or gain unauthorized access to sensitive information.

4. DE-AUTHENTICATION ATTACKS

De-authentication attacks come in various forms, each exploiting different aspects of wireless communication protocols. Two broad categories of de-authentication attacks are passive attacks and active attacks. Here is an overview of various types within these categories:

A. Active De-Authentication Attacks:

- Basic De-Authentication Attack: In a basic de- authentication attack, an attacker sends forged de-authentication frames to target device, causing it to disconnect from the network. Figure 1 presents working of basic de-authentication attack.
  Methodology: The attacker typically uses tools that allow the injection of de-authentication frames into the wireless network.
  Example: An attacker uses a tool like Air playing to send de-authentication frames to specific device, causing it to disconnect from a Wi-Fi network.

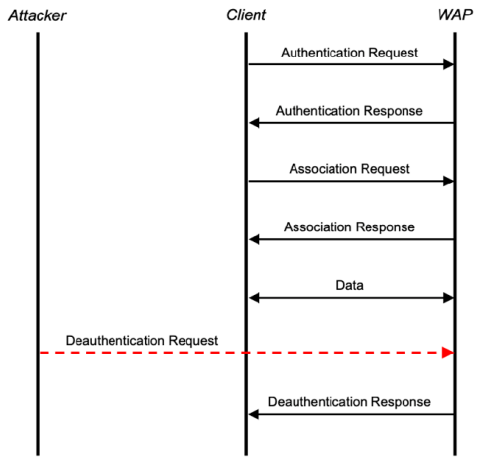

Figure 1. Basic De-authentication Attack

- Broadcast De-authentication Attack: This attack targets all devices within the range of the attacker, broadcasting de-authentication frames to force multiple devices to disconnect simultaneously. Figure

2 presents working of broadcasted de-authentication attack.
Methodology: The attacker sends de- authentication frames with broadcast addresses, affecting all devices within the network's proximity.
Example: A malicious actor utilizes tools like MDK3 to flood a wireless network with de- authentication frames, disconnecting all devices within range.

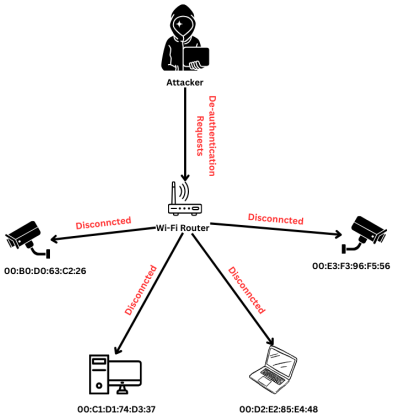

Figure 2. Broadcasted De-authentication Attack

- Directed De-Authentication Attack: In a directed de-authentication attack, the attacker specifically targets a particular device or a group of devices, disconnecting them from the network. Figure 3 presents working of directed de-authentication attack.
  Methodology: The attacker sends de- authentication frames with the address of the targeted device or devices.
  Example: An attacker targets a specific user by sending de-authentication frames directly to their device using tools like air playing.

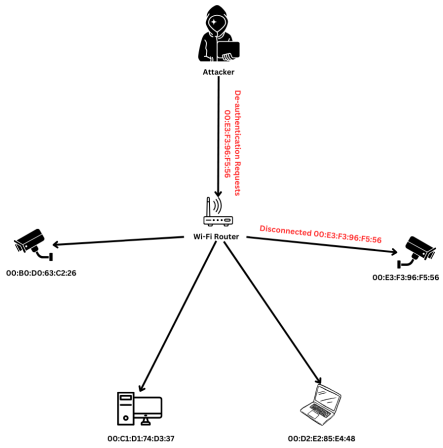

Figure 3. Directed De-authentication Attack

- De-Authentication Flood Attack: This attack involves overwhelming the target with a flood of de-authentication frames, causing widespread disruption, and making it challenging for the network to function normally.
  Methodology: The attacker floods the network with a high volume of de-authentication frames, saturating its communication channels.
  Example: A large-scale de-authentication attack is orchestrated during a public event, disrupting Wi-Fi connectivity for attendees and overwhelming network resources.

B. Passive De-Authentication Attacks:

- Beacon Frame De-Authentication Attack: In this attack, the attacker leverages vulnerabilities in the handling of beacon frames to de-authenticate devices without actively injecting de- authentication frames.
  Methodology: Exploiting weaknesses in the beacon frame handling process, the attacker disrupts communication between devices and the access point.
  Example: Exploiting vulnerabilities in beacon frames, an attacker disrupts the communication between devices and the access point, causing intermittent disconnections

- Power Save De-Authentication Attack: Power Save Mode allows devices to enter a low- power state to conserve energy. This attack exploits this mode to de-authenticate devices by manipulating their power-saving behavior.
  Methodology: The attacker induces targeted devices to enter power save mode, disrupting their communication with the network.
  Example: A threat actor manipulates the power save behavior of devices in a network, forcing them into power save mode and causing periodic disconnections.

- Probe Request Response De-authentication Attack: Attackers exploit the exchange of probe requests and responses between devices and access points to de-authenticate devices, impacting their ability to connect to the network.
  Methodology: By manipulating or injecting false probe requests or responses, the attacker disrupts the connection process.
  Example: By injecting false probe requests or responses, an attacker disrupts the connection process between a device and an access point, leading to intermittent disconnections.

Table 3 presents a comprehensive overview of de- authentication techniques in wireless networks. It includes key attributes such as the technique description, target scope, authentication method, network layer, attack vector, authentication protocol, intention behind the attacks, mitigation techniques, and the wireless environment affected.

This compilation serves as a valuable resource for understanding the landscape of de-authentication attacks, aiding researchers and practitioners in developing robust security measures for wireless environments

C. Real World Scenarios:

- Coffee Shop Network Disruption: Scenario: An attacker at a crowded coffee shop uses a broadcast de-authentication attack to disconnect multiple users from the public Wi-Fi network, causing frustration and potential data exposure.
- Targeted User Disconnection in Office: Scenario: A disgruntled employee uses a directed de-authentication attack to disconnect a specific coworker from the corporate Wi-Fi network, causing disruption to their work.
- Conference Wi-Fi Overload: Scenario: During a tech conference, an adversary launches a de-authentication flood attack, disrupting the conference Wi-Fi network and affecting the connectivity of attendees.
- Power Save Mode Exploitation in Smart Home: Scenario: In a smart home environment, an attacker exploits power saves de-authentication, intermittently disconnecting IoT devices and disrupting the functionality of automated systems.

Understanding these real-world scenarios helps highlight the practical implications of de-authentication attacks and underscores the importance of implementing robust security measures to protect against such threats.

5. MITIGATION TECHNIQUES

Mitigating de-authentication attacks involves implementing a combination of technical measures, security best practices, and user awareness. Here are several mitigation techniques to protect against de- authentication attacks:

- Use Strong Encryption: Employ robust encryption protocols, such as WPA3 for Wi-Fi networks, to secure the communication between devices and access points. Encryption helps prevent attackers from easily intercepting and manipulating data, including de-authentication frames.
- Implement Intrusion Detection Systems (IDS): Set up IDS to monitor network traffic and detect anomalous patterns associated with de- authentication attacks. IDS can identify and alert administrators to unusual activity, enabling timely responses.
- Network Segmentation: Segment the network to isolate critical infrastructure and sensitive devices from potential attackers. This way, even if a de-authentication attack occurs in one segment, it will not affect the entire network.
- Intrusion Prevention Systems (IPS): Deploy IPS solutions to automatically detect and block de-authentication attacks in real-time. IPS can actively prevent malicious traffic from reaching its target, enhancing the overall security posture.
- Use Multi-Factor Authentication (MFA): Implement multi-factor authentication to add an additional layer of security. Even if an attacker manages to disconnect a device, MFA ensures that unauthorized access remains challenging.
- Regularly Update Firmware and Software: Keep all network devices, including routers, access points, and IoT devices, updated with the latest firmware and security patches. Updates often include fixes for known vulnerabilities that could be exploited in de-authentication attacks.
- Monitor Network Traffic: Continuously monitor network traffic for unusual patterns or spikes in de-authentication frames. Establish baselines for normal network behavior, enabling quick detection of anomalous activities.
- Disable Unnecessary Services: Disable unnecessary services and features on devices and network equipment to reduce the potential attack surface. This limits the avenues that attackers can exploit during de-authentication attacks.
- User Education and Awareness: Educate users and administrators about the risks of de-authentication attacks and encourage best practices, such as avoiding connecting to open or unsecured networks. Awareness can prevent users from unknowingly falling victim to these attacks.
- Implement Rate Limiting: Apply rate limiting for de-authentication frames to restrict the number of frames that can be sent within a specific time frame. This can help mitigate the impact of de-authentication flood attacks.
- Authentication Protocol Enhancements: Enhance authentication protocols to include mechanisms that can detect and mitigate de- authentication attacks. For example, the implementation of countermeasures in the form of re-authentication mechanisms can enhance overall security.
- Physical Security Measures: Implement physical security measures, such as surveillance cameras and access controls, to prevent unauthorized individuals from gaining physical access to network infrastructure.
- Behavioral Analysis: Employ behavioral analysis tools that can detect unusual patterns in device behavior. This can help identify potential signs of com-

TABLE III. De-Authentication Techniques Overview

De-authentication Technique	Description	Target Scope	Authentication Method	Network Layer	Attack Vector	Authentication Protocol	Intention	Mitigation Techniques	Wireless Environment
Global De-authentication	Targets all devices on network	Global	Password-based	Link-layer	Active	WPA/WPA2	Malicious	Prevention-based	Wi-Fi
Individual De-authentication	Targets a specific device	Individual	Certificate-based	Network-layer	Passive	WEP	Security Testing	Detection-based	Bluetooth
Jamming-Based De-authentication	Overloads Wi-Fi channels with noise, disrupting communication	Global	N/A	Link-layer	Active	WPA/WPA2	Malicious	Frequency hopping, Channel diversity	Wi-Fi
Spoofed De-authentication	Sends de-authentication frames with forged source addresses	Global	N/A	Link-layer	Active	WPA/WPA2	Malicious	Packet-filtering, Intrusion Detection Systems	Wi-Fi
Disassociation Flood Attack	Floods the network with disassociation frames to disconnect devices	Global	N/A	Link-layer	Active	WPA/WPA2	Malicious	Rate limiting, Anomaly detection	Wi-Fi
Rogue Access Point De-authentication	Pretends to be a legitimate access point, leading devices to disconnect	Global	N/A	Link-layer	Active	WPA/WPA2	Malicious	Wireless Intrusion Prevention System (WIPS)	Wi-Fi
Beacon Flood De-authentication	Floods the network with beacon frames, causing devices to de-authenticate	Global	N/A	Link-layer	Active	WPA/WPA2	Malicious	Beacon frame filtering, Beacon rate limiting	Wi-Fi
EAPOL Manipulation	Exploits weaknesses in the EAPOL (Extensible Authentication Protocol over LAN)	Global	Password-based	Link-layer	Active	WPA/WPA2	Malicious	Use strong EAP methods, Regular monitoring	Wi-Fi
Security Assessment De-authentication	Simulates de-authentication attacks to identify vulnerabilities	Global	N/A	Link-layer	Active	WPA/WPA2	Security Testing	Security awareness, Regular audits	Wi-Fi
Controlled De-authentication	Ethical testing with proper authorization to assess network security	Global	Password-based	Link-layer	Active	WPA/WPA2	Security Testing	Coordination with network administrators	Wi-Fi

promise or ongoing de-authentication attacks.

- Regular Security Audits: Conduct regular security audits and penetration testing to identify vulnerabilities in the network. This proactive approach allows organizations to address potential weaknesses before they can be exploited.

Implementing a combination of these mitigation techniques creates a layered defense against de- authentication attacks, enhancing the overall security of wireless networks and the connected devices. Regularly reassess and update these measures to adapt to evolving threats and technologies. Table 4 categorizes de- authentication mitigation techniques according to Effectiveness, Applicability, and Implementation.

6. EVALUATION METRICS

To evaluate the efficacy of de-authentication mitigation techniques, researchers commonly rely on specific metrics to gauge their performance. These metrics serve as key indicators, allowing for a comprehensive assessment of the techniques' effectiveness.

- False Positive Rate: This metric measures the frequency with which legitimate users are mistakenly flagged as attackers. Lower false positive rates indicate a more accurate identification process, minimizing disruptions to normal network activities.

- False Negative Rate: The false negative rate signifies instances where actual de-authentication attacks go undetected. A lower false negative rate is indicative

TABLE IV. De-Authentication Mitigation Techniques Categorization

Effectiveness	High Effectiveness	1) Mitigations that are proven to significantly reduce or eliminate the risk. 2) Supported by strong evidence and widely acknowledged in the field. 3) Examples: Encryption of sensitive data, Regular security audits, multi-factor authentication.
	Moderate Effectiveness	1) Mitigations that provide a reasonable level of risk reduction. 2) Effective in specific contexts or against certain types of threats. 3) Examples: Firewalls, intrusion detection systems, employee training programs.
	Low Effectiveness	1) Mitigations that offer limited risk reduction. 2) Might be more of a deterrent than a complete solution. 3) Examples: Warning signs, basic password policies, perimeter fencing.
Applicability	Broad Applicability	1) Mitigations suitable for a wide range of scenarios and industries. 2) Versatile and adaptable to different contexts. 3) Examples: Regular software updates, employee awareness programs, access controls.
	Moderate Applicability	1) Mitigations effective in specific situations or against certain types of threats. 2) Tailored to address risks or vulnerabilities. 3) Examples: Biometric access controls, network segmentation, specific malware protection tools.
	Limited Applicability	1) Mitigations relevant only in certain cases or industries. 2) Address niche risks and may not be universally applicable. 3) Examples: Industry-specific compliance measures, specialized security protocols.
Implementation	Easy Implementation	1) Mitigations that can be put in place with minimal effort and resources. 2) Often involve straightforward configurations or policy changes. 3) Examples: Enforcing strong password policies, regular data backups, employee awareness training.
	Moderate Implementation	1) Mitigations requiring a reasonable investment of time and resources. 2) Implementation may involve deploying specific technologies or conducting comprehensive training programs. 3) Examples: Installing and configuring advanced firewalls, developing incident response plans, periodic security assessments.
	Complex Implementation	1) Mitigations demanding significant time, resources, and expertise. 2) Often involve complex technical solutions or major organizational changes. 3) Examples: Full-scale network redesign, implementing advanced threat intelligence systems, comprehensive security awareness programs.

of a system's capability to effectively identify and respond to malicious activities.

- Detection Time: Detection time is the duration taken to identify and acknowledge a de-authentication attack. Swift detection times are imperative in reducing the impact of attacks and preventing unauthorized access.
- Mitigation Time: This metric gauge the time required to implement countermeasures and halt a de-authentication attack. Efficient mitigation times are crucial in minimizing network disruption durations.
- Resource Utilization: Resource utilization measures the impact of the mitigation technique on system resources, such as CPU and memory. Efficient resource usage is essential to prevent adverse effects on overall network performance.
- Robustness: The robustness metric evaluates a technique's ability to withstand various attack scenarios and adapt to emerging threats. A robust solution is vital for sustained security in the face of evolving cyber threats.
- Compatibility: Compatibility assesses how seamlessly the mitigation technique integrates with existing network infrastructure and security systems. Smooth integration ensures that the solution works harmoniously with other components.
- Usability and Manageability: Usability and manageability consider how easily the mitigation technique can be configured, monitored, and managed. User-friendly interfaces and effective management tools contribute to the practicality of the solution.
- Cost-Effectiveness: Cost-effectiveness encompasses the overall expenses associated with implementing and maintaining the de-authentication mitigation technique. Evaluating cost-effectiveness is essential to determine the practicality of the solution in relation to the security benefits it provides.

7. CHALLENGES AND FUTURE DIRECTIONS

In addressing the multifaceted landscape of de- authentication attacks and their mitigation, several prominent challenges emerge. The adaptability to evolving attacks is paramount, given that threat vectors are in a constant state of evolution. As attackers refine their techniques, mitigation strategies must equally evolve to keep pace with

new de-authentication attack methods. This necessitates a continuous commitment to research, ensuring the identification and effective counteraction of emerging threats. Another critical challenge lies in the potential exploitation of cryptographic weaknesses within wireless communication protocols by de-authentication attacks. The security implications of such vulnerabilities are far-reaching, demanding researchers' attention to address and fortify cryptographic aspects. Strengthening these foundations is integral to enhancing the overall security of the system against de-authentication threats. Insider threats introduce an additional layer of complexity to the landscape of de-authentication attacks. The possibility of attacks orchestrated by individuals with insider knowledge highlights the need for dedicated research in detecting and preventing such threats. Effectively countering insider threats should thus be a focal point, requiring innovative strategies to safeguard against unauthorized network access. The resource- intensive nature of some mitigation techniques poses a consequential challenge, potentially impacting overall network performance. This challenge prompts the exploration of optimization strategies – a crucial area of research that seeks to enhance the efficiency of mitigation techniques without compromising the fundamental security they provide.

The delicate balance between minimizing false positives and false negatives in detection systems presents a nuanced challenge. Achieving this equilibrium is inherently challenging but underscores the need for ongoing research to refine detection algorithms. This refinement process aims to reduce errors on both fronts, ensuring accurate and reliable identification of de- authentication attacks. Looking towards future directions in research, the integration of machine learning and artificial intelligence emerges as a promising avenue. The rationale lies in the adaptive capabilities of these technologies, allowing for enhanced de-authentication detection and mitigation systems. Machine learning algorithms, capable of learning and adapting to evolving attack patterns, contribute significantly to improving overall system resilience. Behavioral analysis represents another future direction, offering insights into identifying anomalies in network behavior. By analyzing normal network behavior, this approach aids in the early detection of de- authentication attacks based on deviations from established patterns. Quantum-safe cryptography becomes increasingly relevant as a research direction to safeguard against potential threats from quantum computing. Recognizing the need for long-term security in wireless networks, exploring cryptographic algorithms resistant to quantum threats is imperative.

Collaborative defense mechanisms, emphasizing the sharing of threat intelligence and coordinated responses, present an avenue for more robust and efficient mitigation strategies. Collective efforts across multiple entities can significantly enhance the overall resilience of networks against de-authentication threats. The integration of de- authentication mitigation techniques into the security frameworks of Internet of Things (IoT) devices is a proactive research direction. As the adoption of IoT devices grows, securing communication channels becomes paramount, making this area of investigation crucial for overall network security. Addressing standardization and interoperability concerns is pivotal for the widespread adoption of de- authentication mitigation techniques. Working towards establishing standards and ensuring compatibility with diverse network environments enhances the overall effectiveness of these strategies. Lastly, emphasizing research on user education and awareness is crucial in preventing social engineering attacks that may lead to de- authentication vulnerabilities. Recognizing the role users play in preventing unauthorized access, educational initiatives contribute significantly to overall network security. In conclusion, navigating the challenges and embracing these future research directions presents a comprehensive approach to fortifying wireless networks against the evolving landscape of de-authentication attacks.

8. CONCLUSION

In conclusion, this survey paper has provided a thorough examination of the intricate landscape surrounding de- authentication attacks, mitigation techniques, and the evaluation metrics essential for assessing their efficacy. Exploring the realm of de-authentication attacks, we delved into the various threat vectors that undermine the integrity of wireless networks. Understanding the nuanced tactics employed by attackers is crucial for developing robust mitigation strategies that can stand up to evolving challenges.

Our scrutiny of de-authentication mitigation techniques underscored the importance of a multifaceted approach. Proactive measures, including the implementation of robust encryption protocols and secure authentication mechanisms, serve as critical foundations. Meanwhile, reactive strategies, empowered by effective network monitoring tools, are pivotal for swift detection and response to potential threats. The evaluation metrics discussed throughout this paper serve as a compass for navigating the effectiveness of mitigation strategies. From false positives and negatives to detection times and resource utilization, these metrics provide a comprehensive framework for researchers and practitioners to gauge the real-world performance of de-authentication countermeasures in diverse scenarios.

As we reflect on the implications of our findings, it is evident that the arms race between attackers and defenders in the realm of de-authentication attacks persists. To stay ahead, continuous research is imperative, especially given the ever-evolving nature of cyber threats. The adaptive integration of machine learning and artificial intelligence, as well as the exploration of behavioral analysis techniques, present promising avenues for enhancing detection capabilities and fortifying network security.

Moreover, standardization efforts and interoperability considerations are essential for the seamless integration of de-authentication mitigation techniques across varied network environments. Collaborative defense mechanisms that leverage shared threat intelligence also offer a compelling

prospect for a collective and resilient response to emerging threats. In contemplating the future of de- authentication security, the integration of these insights into a cohesive strategy will be paramount. The synergy between robust mitigation techniques, thorough evaluation metrics, and innovative research directions will shape the landscape of wireless network security. As we navigate this dynamic terrain, our collective efforts will undoubtedly contribute to a more secure and resilient wireless ecosystem.

References

[1] F. Mehdipour, "A review of iot security challenges and solutions," *Proceedings of the 8th International Japan-Africa Conference on Electronics*, 2020.

[2] A. B. P. K. B. A. Raghuprasad, S. Padmanabhan, "Security analysis and prevention of attacks on iot devices," *International Conference on Communication and Signal Processing*, pp. 0876–0880, 2020.

[3] C. P. M. Vanhoef, P. Adhikari, "Protecting wi-fi beacons from outsider forgeries," *WiSec 2020 - Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 155–160, 2020.

[4] K. S. Z. Neal, "Analysis of evil twin, deauthentication, and disassociation attacks on wi-fi cameras," *Proceedings - International Conference on Computer Communications and Networks*, 2023.

[5] V. V. S. C. Sethuraman, S. Dhamodara, "Intrusion detection system for detecting wireless attacks in ieee 802.11 networks," *IET Networks*, pp. 219–232, 2019.

[6] I. A. J. O. Agyemang, J. J. Kponyo, "Lightweight man-in- the-middle (mitm) detection and defense algorithm for wifi- enabled internet of things (iot) gateways," *Information Security and Computer Fraud*, vol. 7, pp. 1–6, 2019.

[7] A. A. C. A. K. Z. Belghazi, N. Benamar, "Secure wifi-direct using key exchange for iot device-to-device communications in a smart environment," *Future Internet*, vol. 11, 2019.

[8] V. S. D. J. B. S. V. Hassija, V. Chamola, "A survey on iot security: Application areas, security threats, and solution architectures," *IEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[9] M. Z. K. Lounis, "Bad-token: Denial of service attacks on wpa3," *ACM International Conference Proceeding Series*, 2019.

[10] R. L. J. Z. J. D. Z. Jiang, K. Zhao, "Phyalert: identity spoofing attack detection and prevention for a wireless edge network," *Journal of Cloud Computing*, vol. 9, 2020.

[11] V. B. O. Barybin, E. Zaitseva, "Testing the security esp32 internet of things devices," *2019 IEEE International Scientific- Practical Conference Problems of Infocommunications, Science and Technology*, pp. 143–146, 2019.

[12] G. S. K. J. O. B. J. O. Agyemang, J. J. Kponyo, "Lightweight rogue access point detection algorithm for wifi- enabled internet of things(iot) devices," *Internet of Things*, vol. 11, 2020.

[13] R. A. A. P. K. C. Shripriya, G. I. Mary, "Manipulation and detection of dos attacks on ieee802.11 protocol," *ViTECoN 2023 - 2nd IEEE International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies, Proceedings*, 2023.

[14] H. T. N. Xie, Z. Lie, "A survey of physical-layer authentication in wireless communications," *IEEE*, vol. 23, pp. 282–310, 2021.

[15] S. V. S. P. S. K. R. L. K. S. R. Gopal, P. R. Prasanth, "Deauthentication of ip drones and cameras that operate on 802.11 wifi standards using esp8266," *International Journal of Electronics and Communication Engineering and Technology*, vol. 10, pp. 23–30, 2019.

[16] V. C. K. R. C. T. Alladi, B. Sikdar, "Consumer iot: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, pp. 17–25, 2020.

[17] K. T. J. Shailendra, "Analysis on iot networks security : Threats, risks, esp8266 based penetration testing device and defense framework for iot infrastructure," *2023 3rd International Conference on Intelligent Technologies*, 2023.

[18] A. C. L. Naggy, "Router-based iot security using raspberry pi," *IEE*, 2019.

[19] K. M. Y. A. M. J. Milliken, V. Selis, "Impact of metric selection on wireless deauthentication dos attack performance," *IEEE Wireless Communications Letters*, vol. 2, pp. 571–574, 2013.

[20] Z. D. M. W. W. L. Y. Zhang, Y. Lin, "Monitoring and identification of wifi devices for internet of things security," *IEE*, 2019.

[21] M. T. U. R. S. P. B. I. R. Singh, R. Thakkar, "Wifi deauth and cloning using esp8266," *5th IEEE International Conference on Advances in Science and Technology*, pp. 106–110, 2022.

[22] P. K. D. Ahamadpor, "Detecting forged management frames with spoofed addresses in ieee 802.11 networks using received signal strength indicator," *Iran Journal of Computer Science*, vol. 3, pp. 137–143, 2020.

[23] N. S. D. P. L. R. D. S. Maesaroh, L. Kusumaningrum, "Wireless network security design and analysis using wireless intrusion detection system," *International Journal of Cyber and IT Service Management*, vol. 2, pp. 30–39, 2022.

[24] S. S. R. Cheema, D. Bansal, "Deauthentication/ disassociation attack: Implementation and security in wireless mesh networks," *International Journal of Computer Applications*, vol. 23, pp. 07–15, 2011.

[25] A. G. N. K. G. S. K. J. P. N. Dalal, N. Akhtar, "A wireless intrusion detection system for 802.11 wpa3 networks," *2022 14th International Conference on COMmunication Systems and NETworkS, COMSNETS 2022*, pp. 384–392, 2022.

Adwait Gulab Gaikwad is a M. Tech. student at MIT-World Peace University, Pune, Maharashtra India. His research area includes Wireless Networking Security, Wireless Devices, IoT Security, and Wireless Attack Detection. His main research topic is Enhancement of De-authentication Mitigation Technique for IoT Environment. He received his B.E (Information Technology) from Savitribai Phule Pune University, Pune, Maharashtra, India. Beside his interest in Networking and Cybersecurity, he also has an interest in Web Application and Android Application Development.

Prof. Dr. Balaji M. Patil is a Professor in Department of Computer Engineering at MIT World Peace University, Pune India. He received his PhD in Computer Science and Engineering from Uttarakhand Technical University, Dehradun, India in the year 2016. His primary research interests include Network Management, Cyber Security, Cyber Forensics and IoT. Over the years he has supervised numerous bachelors and master's students and 3 PhD Scholars. He has published 25+ papers in various National / International conferences and journals. At MIT-WPU, currently he is an Associate Head for School of Computer Engineering and Technology and acting as Secretary of CSI Pune Chapter.