INDIVIDUAL ASSIGNMENT

NAME (TP NUMBER)	**:**	Koo Wai Kit (TP081761)
INTAKE CODE	**:**	APUMF2406CYS
MODULE TITLE	**:**	Research Methodology in Computing and Engineering (102024-SIL)
MODULE LECTURER	**:**	Assoc. Prof. Dr. Shahrinaz binti Ismail
SUPERVISOR NAME	**:**	Ts. Dr. Vinesha A/P Selvarajah
PROJECT TITLE		Assignment 1: Literature Review Paper
DATE ASSIGNED	**:**	7 November 2024
DATE COMPLETED	**:**	3 January 2025

Analysis of Vulnerabilities Leading to Denial-of-Service Attacks in Wi-Fi Networks and Effective Mitigation: A Literature Review

Abstract

This literature review looks at the weaknesses of Wi-Fi networks to Denial-of-Service (DoS) attacks and studies different ways to improve their security. Wi-Fi technology is essential for global connectivity, making it a target for attackers who want to disrupt services for legitimate users. The review identifies key weaknesses in Wi-Fi networks. These weaknesses include vulnerabilities in the Wi-Fi protocols, problems with hardware and firmware, configuration mistakes, weaknesses at the physical layer, and human factors that increase the risk of DoS attacks. It also evaluates current protective measures. These measures include Protected Management Frames (PMF), stronger security protocols, 802.1X authentication with RADIUS servers, wireless intrusion detection and prevention systems (WIDS/WIPS), Wi-Fi beacon protection, and anti-jamming techniques. The discussion also addresses the need for future research, focusing on the need to study newer Wi-Fi standards and their advanced features. It is also important to consider backward compatibility for older devices and to develop lightweight intrusion detection systems for IoT environments. Overall, this review aims to offer insights into reducing risks related to Wi-Fi DoS attacks and to point out areas needing further research to improve Wi-Fi security.

Keywords: 802.11; Denial-of-service (DoS); Wi-Fi security; Wi-Fi vulnerabilities; Wi-Fi exploits; Defense mechanisms against DoS attacks; Future improvements in Wi-Fi security

1. Introduction

Wi-Fi, also known as Wireless Local Area Network (WLAN), is a technology that uses the IEEE 802.11 standard to connect devices wirelessly. Today, Wi-Fi is used to connect billions of devices to the internet. This includes devices like smartphones, laptops, and Internet of Things (IoT) devices. The technology is important for both work and personal activities as it provides easy access to online information. Wi-Fi also plays a major role in handling internet protocol (IP) traffic. This includes all forms of online communication. By

2022, Wi-Fi was expected to handle the majority of global IP traffic, which surpasses both wired Ethernet and cellular networks. This shows how Wi-Fi has shaped the way we communicate wirelessly (Pahlavan & Krishnamurthy, 2021).

However, since Wi-Fi is used by so many people, these networks are often targeted by hackers, especially those who launch Denial-of-Service (DoS) attacks. When hackers perform DoS attacks, they try to block regular users from getting online or using network services, and this may lead to serious consequences.

The main objective of this paper is to analyse how Wi-Fi networks can be attacked by DoS attacks and what can be done to reduce the risks. To achieve this, the paper will answer the following research questions:

a. What are the main weaknesses in Wi-Fi networks that allow DoS attacks to happen?
b. What methods are currently available to protect against Wi-Fi DoS attacks?
c. What should future studies focus on to improve Wi-Fi security?

The structure of the paper is divided into five sections. It starts by exploring the vulnerabilities that make Wi-Fi networks easy targets for DoS attacks. The next section covers ways to defend against these attacks. Then, it points out areas that need more research to improve the security of Wi-Fi networks. The paper finishes with a summary of findings as the conclusion.

2. Key Themes in Wi-Fi DoS Vulnerabilities

2.1 Protocol Vulnerabilities

Four-way Handshake Vulnerabilities

Several protocol-level weaknesses in Wi-Fi networks can lead to Denial-of-Service (DoS) attacks, especially during the important four-way handshake process that secures Wi-Fi connections.

One major vulnerability is the blocking of message 4 during a four-way handshake between a client and an access point (AP). This message is important because it helps complete the secure connection process between a client and the AP. Attackers can stop the handshake from completing by preventing the transmission of message 4. After the client sends message 4, it sets up a pairwise key and will only accept encrypted messages. If the AP does not receive message 4, it will resend message 3 without encryption. However, the client will reject this unencrypted message, which causes the handshake to time out (Vanhoef & Piessens, 2017). This is a significant issue in modern networks. In these networks, clients frequently move between different APs. As a result, they often need to perform the 4-way handshake repeatedly to establish a secure connection (Schepers et al, 2022).

Another problem occurs due to a race condition during the handshake. The client sets the security key after sending message 4, while the AP installs it after receiving that message. Attackers can take advantage of this timing difference by jamming the messages. This prevents the AP from receiving message 4 and setting the key, stopping the handshake (Lounis & Zulkernine, 2020).

Also, attackers can take advantage of a weakness in the message 1 of the 4-way handshake. This message does not have encryption or authentication, making it vulnerable. Attackers can exploit this vulnerability by sending a modified message with incorrect information about the key data (Schepers et al, 2022). This can cause some clients to stop the handshake and disconnect from the network if they receive message 1 with invalid data, such as an invalid PMKID (Vanhoef & Piessens, 2017).

In addition, many implementations do not follow the 802.11 standard regarding plaintext EAPOL frames. The standard says that message 4 should be sent without encryption during the initial handshake. However, some systems mistakenly send message 4 with encryption after the pairwise key is set. This causes the AP to reject the frame since it has not installed the key yet (Vanhoef & Piessens, 2017).

Attackers can also launch DoS attacks by repeatedly sending deauthentication frames to devices operating under the 802.11w standard. This attack interferes with the handshake process between the client and the AP, thus disrupting the normal connection process between the devices (Pisarev, 2020).

Key Management Vulnerability

Key Reinstallation Attacks (KRACK) exploit a flaw in the way session keys are installed. This flaw occurs when devices reset their nonce and packet counters. Attackers can use this weakness to replay broadcast and multicast UDP packets, allowing them to take control of commands in IoT networks. Attackers can use this to disrupt the normal operation of these networks (Thankappan et al, 2022).

Management Frame Vulnerability

IEEE 802.11 management frames are exchanged during the phases of network discovery, authentication, and association. They are vulnerable because they are sent before security keys are negotiated. This means these frames are not protected by security protocols. As a result, they can be easily spoofed by attackers (Thankappan et al, 2022). For example, an attacker could set up a fake AP that sends probe responses to a client. If the client receives this fake probe response before it gets the legitimate response from the real AP, it may stop the authentication process and disconnect from the network (Lounis & Zulkernine, 2020).

Networks that use Protected Management Frames (PMF) have a security feature called Security Association (SA) Query. Attackers can trick the AP into using this feature. They can send fake association or reassociation frames to make the AP issue an SA query request. If the attacker then jams the client's responses, the AP might reset the connection. This causes the AP to disconnect the device, but the device cannot reconnect (Thankappan et al, 2022).

Wi-Fi Beacon Vulnerability

Wi-Fi beacons are messages that APs send to announce their presence. These messages are not protected, which means attackers can easily create fake beacons. Attackers can use fake beacons to disrupt Wi-Fi networks in different ways. One type of attack is the Quiet Attack, where fake beacons with the "quiet" information element force clients to stop their transmissions. This can significantly impact older devices, even though it is less effective against modern ones. Attackers can also create fake beacons that tell devices to reduce their transmission power, which in turn disrupts their connections. Also, attackers can create fake beacons that change the way devices access the network. This can slow down or completely stop the network for certain devices (Vanhoef et al., 2020).

The Battery Depletion attack tricks devices into frequently checking for data, which drains their battery. Attackers can also disrupt the sleep-wake cycles of devices by sending fake timestamps. They can also create the illusion that there is no data available for devices in sleep mode, which prevents them from receiving important information. Spoofed beacons can also send out fake Channel Switch Announcements (CSAs), forcing clients to change channels and disrupting their connectivity. Attackers might also change bandwidth-related information, making clients transmit on unsupported bandwidths. This can interfere with their communication and potentially allow the attacker to intercept information (Vanhoef et al., 2020).

WPA3-SAE Protocol Vulnerability

The Simultaneous Authentication of Equals (SAE) protocol, used in WPA3-Personal, has weaknesses that can be exploited by attackers. In a clogging attack, an attacker floods the AP with many fake SAE frames that have fake source MAC addresses. This flood of invalid frames can overwhelm the AP, preventing it from serving legitimate clients trying to connect to the network (Chatzoglou et al., 2022).

Additionally, there is a vulnerability called "bad-token" that targets the WPA3-SAE handshake. This problem happens when the AP stops the authentication process after getting a bad token during the message exchange for establishing a shared key. Attackers can exploit this by sending a fake "commit" message with a bad token between the client and the AP. If this fake message arrives first, the AP ends the real authentication attempt. The client then has to start the process again. By repeatedly sending bad token messages, attackers can block the client's ability to authenticate, preventing it from connecting to the network. This is an effective attack because the AP trusts the first message it receives. Attackers only need a slight advantage in timing to succeed. This causes the client to have constant connection problems (Lounis & Zulkernine, 2019).

Vendor-Specific Vulnerabilities

Attacks can also target weaknesses in how different manufacturers implement the 802.11 standard. These attacks usually involve sending frames with errors to the AP. This causes the AP to respond in an unexpected way and disconnect legitimate users from the network. For example, an attacker can send a fake authentication frame to a WPA2 AP. This frame has a specific value in the "authentication algorithm" field. This can cause the AP to disconnect the targeted client. Similarly, sending a fake SAE Confirm frame with a specific value can also disconnect the client from a WPA3 AP. Additionally, sending a fake Authentication or SAE frame with a specific sequence number can disconnect the client from an AP made by Qualcomm (Chatzoglou et al., 2022).

2.2 Hardware and Firmware Weaknesses

Weaknesses in APs

APs have several weaknesses that can be exploited for DoS attacks. Low-end APs often have limited processing power and memory. This limitation makes them easy targets for flooding attacks, like those that exploit the SAE handshake. Attacks like "Cookie Guzzler" and "Memory Omnivore" show how these weaknesses can successfully disrupt low-end devices (Chatzoglou et al., 2022).

Many APs have outdated firmware. This outdated firmware can contain security flaws that attackers can exploit for DoS attacks. Even though these flaws are often fixed with updates, many devices remain unpatched. In addition, modern APs often support different security modes, like WPA2 and WPA3. This can introduce additional vulnerabilities. For instance, attackers may exploit the transition mode of WPA3 to execute dictionary attacks against WPA2 clients. This could allow them to steal passwords and compromise the WPA3 network (Chatzoglou et al., 2022).

Weaknesses in Clients

Many Wi-Fi clients have security flaws in their firmware. One major concern is unpatched firmware flaws, similar to those found in APs. These flaws can be used by attackers to compromise security. For example, one serious vulnerability can cause a Wi-Fi client to install an all-zero encryption key instead of a valid key during the 4-way handshake, allowing attackers to easily decrypt sensitive information. This exposes the client to further attacks and weakens the overall security of the network (Thankappan et al., 2022).

2.3 Configuration Vulnerabilities

Insecure Configuration of 802.1x and WPA-Enterprise

The way 802.1x and WPA-Enterprise are set up can create security problems in Wi-Fi networks. Eduroam is a common Wi-Fi network used in universities. It uses 802.1x with TLS tunnels for authentication. However, if devices are not configured correctly or users are careless, attackers can exploit this by setting up rogue APs. A major concern is that users are responsible for configuring their own devices. This is different from corporate networks where IT teams manage these settings. This often leads to outdated or incorrect configuration guides and pre-configured profiles, which results in security risks.

Lack of PMF Support

The absence of Protected Management Frames (PMF) support is a significant configuration weakness in Wi-Fi networks. PMF is designed to protect important management frames from being exploited in DoS attacks. These management frames are essential for starting and ending network sessions (Kwon & Choi. 2020). However, PMF is optional in WPA2, and many devices, especially IoT devices, do not support it. This is partly because PMF was initially implemented differently by different vendors, which led to inconsistent support across different devices. A survey found that about 87% of routers do not fully comply with PMF standards (Thankappan et al, 2022).

2.4 Physical Layer Weaknesses

Constant jamming attacks are a simple and effective way to launch DoS attacks. These attacks involve continuously sending strong signals over Wi-Fi channels. This brute-force method overwhelms real signals, making it hard for Wi-Fi devices to decode packets and access the channel. Some jamming attacks target a specific part of the Wi-Fi communication process called the Request to Send/Clear to Send (RTS/CTS) handshake. Attackers can interfere with this process by corrupting messages. This causes devices to retransmit data, which wastes network resources and can lead to DoS. Jammers can also take advantage of weaknesses in rate adaptation algorithms, making the network run at lower data rates. This change reduces throughput and further impacts network performance (Pirayesh & Heng, 2022).

In addition, modern Wi-Fi standards like 802.11ac and 802.11ax use a technology called MU-MIMO. This technology allows multiple devices to communicate simultaneously. Jammers can disrupt this technology by interfering with the signals used to determine the best way to transmit data. This reduces the speed of the network and can cause DoS. Some jammers can also send fake signals that mimic real traffic. This tricks APs into using resources for these false signals, which takes away bandwidth from legitimate users. These attacks are easier to carry out because Wi-Fi channels are not always protected, letting malicious devices send disruptive traffic without following access control rules (Pirayesh & Heng, 2022). Furthermore, smart jamming techniques that have been created and shown to work effectively while also avoiding detection. However, these attacks require the attacker to be physically close to the target. They also typically target only a single cell in a network (Pelechrinis et al., 2010, as cited in Xin & Starobinski, 2021).

2.5 Human Factors

Human error and a lack of security awareness significantly impact the security of Wi-Fi networks. One common issue is that users often connect to Wi-Fi networks simply based on the SSID without checking if it is legitimate. Attackers exploit this by setting up fake APs that mimic real networks. Once connected, users become vulnerable to having their information stolen, their internet traffic intercepted, and their network access disrupted by the rogue AP (Palamà et al, 2023). Another problem is that users often ignore or dismiss certificate warnings, especially on devices like Android phones. When users do not check these warnings, it allows attackers to create malicious connections (Palamà et al, 2023).

Many users also use weak passwords for their networks. These passwords are easy to guess, making it easier for attackers to gain unauthorised access and exploit network resources, potentially causing service disruptions (Kwon & Choi, 2020). Additionally, many users lack awareness about the risks of using unsecured networks and do not follow safe practices. This lack of knowledge makes them more vulnerable to social engineering attacks, which can give attackers access to the networks (Palamà et al, 2023).

3. Key Themes in Defense Mechanisms Against Wi-Fi DoS Attacks

3.1 Protected Management Frames (PMF)

PMFs are critical defense against Wi-Fi DoS attacks. It was introduced in the IEEE 802.11w standard, and it improves the security of management frames by adding authentication, encryption, and data integrity checks (Lounis & Zulkernine, 2020). Starting in 2018, PMF became a requirement for devices certified under the WPA2 and WPA3 standards, significantly boosting the security of modern Wi-Fi networks (Thankappan et al., 2022).

However, PMF is not a perfect solution and faces some challenges in real-world use. One major issue is compatibility. PMF only protects against DoS or man-in-the-middle (MitM) attacks if all APs and client devices in the network fully support it. Networks with older devices that do not support PMF can create security gaps (Thankappan et al., 2022).

PMF also has its own vulnerabilities. For example, it is affected by key reinstallation attacks (KRACK), such as the one identified in CVE-2017-13081. This weakens its ability to secure communication. Additionally, PMF cannot prevent certain DoS attacks like Wi-Fi jamming or beacon spoofing. These attacks disrupt network availability or trick devices into connecting to fake APs. Another limitation is its ineffectiveness against insider threats. Even with PMF enabled, authorised users with malicious intent can exploit weaknesses to carry out deauthentication or disassociation attacks, bypassing PMF's protections (Thankappan et al., 2022).

3.2 Stronger Security Protocols

The transition from WEP to WPA, and then to WPA2 and WPA3, shows a strong effort to improve wireless security. Each new version brings important upgrades in encryption methods, key management, and authentication processes (Moissinac et al, 2021).

The WPA2 security mechanism included a new key called Pairwise Transient Key (PTK). This key was used to protect messages sent to individual devices. Similarly, the IEEE 802.11w standard added a key called Integrity Group Transient Key (IGTK) to protect broadcast management frames. These encryption keys block attackers from exploiting management frames, which is a common tactic in Wi-Fi DoS attacks (Pisarev, 2020).

Moreover, the IEEE 802.11w standard also added a security feature called Security Association Query (SA Query). This feature checks if a device is allowed to connect to the network. The device and the AP exchange messages to verify the connection request. If the messages are incorrect, the connection is blocked. This helps prevent attacks that try to overload the network with fake connection requests. Another significant change is Timeout Information Element (TIE), which helps reduce DoS risks. It allows the AP to set a time limit for devices to respond during the connection process. This prevents the AP from being overloaded by fake connection requests from malicious devices (Pisarev, 2020).

Additionally, WPA2-Enterprise is a version of WPA2 that provides better security features, which can help reduce risks related to DoS attacks. One important change is the use of unique per-session keys for each connection. Unlike WPA2-PSK, which depends on a shared key, WPA2-Enterprise creates keys from random numbers given by both the client and the RADIUS server. This method lowers the risks linked to shared keys and improves overall network security (Moissinac et al, 2021).

WPA2-Enterprise uses a RADIUS server to check user logins. This means all logins are handled in one place, and this makes it harder for unauthorised people to get in. Another important feature of WPA2-Enterprise is AP authentication. It uses special digital certificates so devices can be sure they are talking to the right AP, which can help to stop evil twin attacks (Moissinac et al, 2021).

Furthermore, WPA3 has several advancements that greatly boost protection against Wi-Fi DoS attacks. It focuses on secure authentication and encryption methods. One key change is the move from the PSK exchange used in WPA2 to the SAE protocol. This new protocol is designed to resist offline dictionary attacks. This makes it much harder for attackers to figure out passwords from captured network traffic. By making it harder to crack passwords, WPA3 significantly reduces the risk of unauthorised network access, which is often the first step in launching DoS attacks. Another key feature of WPA3 is the mandatory use of Protected Management Frames (PMF), which has been discussed under Section 3.1 (Kwon & Choi. 2020).

WPA3 also enhances security for open Wi-Fi networks. It introduces Opportunistic Wireless Encryption (OWE). This feature provides a basic level of encryption and protection, this helps even when passwords are not used. This helps reduce the risks of open networks facing simple DoS attacks. This helps reduce the risks of open networks facing simple DoS attacks. This improvement is especially important in public places where users often connect to unprotected networks. OWE helps protect sensitive information and keeps the network safe (Moissinac et al, 2021). Moreover, WPA3 addresses vulnerabilities in device provisioning. It replaces the weak Wi-Fi Protected Setup (WPS) with the more secure Device Provisioning Protocol (DPP). This change makes defenses stronger against DoS attacks that target weaknesses in the device provisioning process. It ensures that devices can be added to the network safely without exposing it to possible threats (Kwon & Choi. 2020).

3.3 802.1X Authentication with RADIUS servers

Implementing 802.1X authentication with Remote Authentication Dial-In User Service (RADIUS) servers improves Wi-Fi security by providing strong authentication and centralised control. This system replaces basic pre-shared keys (PSK) with individual user authentication using unique credentials. This makes it harder for attackers to get unauthorised access to the network. This extra layer of security helps prevent DoS attacks that target weaker authentication systems (Palamà et al, 2023).

In addition, 802.1X with RADIUS allows for flexible implementation of advanced security features. This helps protect against DoS attacks. Protocols like EAP-TTLS and PEAP create secure tunnels between the user and the authentication server. This keeps user credentials safe during transmission and lowers the risk of credential theft that attackers can use for DoS attacks. EAP-TLS uses digital certificates for mutual authentication between the user and the authentication server. This makes it much harder for attackers to pretend to be legitimate entities and carry out DoS attacks (Palamà et al, 2023).

3.4 Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS)

WIDS/WIPS watch the wireless network for signs of unauthorised activity. These systems can help defend against Wi-Fi DoS attacks. They do this by alerting administrators to potential security problems and taking automatic steps to reduce threats (Mughal, 2022). These systems also consider the human element in security. However, intruders can exploit human weaknesses to bypass WIDS defenses. For example, attackers can intentionally trigger a series of alerts. This confuses security personnel and makes it difficult to respond effectively to genuine threats (Pisarev, 2020).

WIDS utilises a variety of analytical methods, including advanced machine learning techniques. These techniques automate the detection of attacks and identify malicious activities within the network. This automation significantly enhances the system's ability to recognize and respond to potential DoS attacks. Additionally, WIDS makes use of a mix of traditional algorithms and modern approaches for traffic analysis. These include clustering and anomaly-based detection. Conventional algorithms like Random Forest and AdaBoost work alongside Artificial Neural Networks (ANN), which are effective at examining network traffic flow. This combination of techniques helps WIDS find unusual patterns that might signal a DoS attack (Pisarev, 2020).

3.5 Wi-Fi Beacon Protection

Wi-Fi networks can be made more secure by authenticating beacon frames, which helps reduce various DoS attacks. Each beacon frame includes a special code called a Message Integrity Code (MIC). The AP generates this code using a secret key and a unique number. Clients receive this secret key when they connect to the network. They use this key to verify the MIC in each beacon frame. If the MIC is incorrect, the client ignores the beacon. This protects the client from potential attacks. This mechanism helps prevent several types of attacks. Clients can verify the authenticity of beacons, which prevents attacks that force them to stop transmitting. It also prevents attacks that try to change the device's transmission power. This mechanism also helps devices maintain their normal network speed by rejecting fake parameters. In addition, clients can also avoid attacks that drain their battery and ensure they stay connected to the network. Beacon protection guards against fake bandwidth information that could disrupt connections. The system also allows devices to report any suspicious APs. This helps network administrators quickly identify and address potential threats (Vanhoef et al, 2020).

3.6 Anti-Jamming Techniques

According to Pirayesh and Heng (2022), several anti-jamming techniques can defense against Wi-Fi jamming attacks:

i. **Channel Hopping**: This method quickly switches between available Wi-Fi channels. It makes it harder for jammers to keep attacking. It works well against narrow-band and reactive jammers that need to target one channel.
ii. **Spread Spectrum Techniques**: These techniques spread the Wi-Fi signal across a wider range of frequencies. This makes it more difficult for narrowband jammers to interfere with the signal. However, these techniques can reduce the speed of the network.
iii. **MIMO-Based Mitigation**: This technique multiple-input and multiple-output technology. It uses multiple antennas to separate the desired signal from interference. This is effective but requires accurate information about the channel and is limited by the number of antennas.
iv. **Rate Adaptation and Power Control**: These techniques adjust the transmission speed and power based on the quality of the channel. They can help reduce the effects of low-power jamming. Transmission strength can be increased to fight low-power jamming, but it must follow regulations.
v. **Jamming Detection Mechanisms**: These techniques are used to identify jamming attacks. They analyse signal patterns, channel activity, and error rates to differentiate jamming from other types of interference. Machine learning algorithms are being developed to improve the accuracy of these techniques.

4. Implications for Future Research

Future research on DoS attacks in Wi-Fi networks should look at newer standards like 802.11ac, 802.11ad, and 802.11ax. These standards include advanced features such as beamforming and multi-user multiple-input multiple-output (MU-MIMO) technology. Researchers should investigate how attacks on one network can affect other networks. This research will help to improve the resilience of Wi-Fi networks (Xin & Starobinski, 2021). Additionally, MIMO technology shows promise in reducing jamming attacks. Most modern Wi-Fi devices also use MIMO, making it an important area for further study. Developing effective jamming mitigation techniques for MIMO networks will significantly improve their resistance to interference (Pirayesh & Heng, 2022).

Many devices still use older Wi-Fi standards like WPA-TKIP. Therefore, future defense measures should ensure backward compatibility. This is important because it may not always be possible to update the security of older devices. Finally, developing lightweight and effective systems for detecting intrusions for IoT environments should be a priority. A good intrusion detection strategy is likely the best way to reduce DoS attacks in these resource-limited settings (Thankappan et al, 2022).

5. Conclusion

This literature review highlights key advancements in defending against Wi-Fi DoS attacks. Key measures include Protected Management Frames (PMF), improved encryption protocols like WPA3, 802.1X authentication with RADIUS, and Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS). Features such as Opportunistic Wireless Encryption (OWE), Device Provisioning Protocol (DPP), and advanced anti-jamming methods provide targeted ways to reduce vulnerabilities. However, challenges still exist. These challenges include compatibility issues with legacy devices, limitations in countering advanced threats like jamming, and the growing complexity of attack methods.

Future research should prioritise lightweight and scalable intrusion detection systems for resource-limited IoT environments. It is also important to ensure that these systems work with older devices. Researchers should also investigate vulnerabilities in modern Wi-Fi standards. Refining MIMO-based jamming mitigation techniques will further strengthen defenses. Combining advanced technologies with strong security protocols is essential to addressing evolving Wi-Fi DoS threats and ensuring the reliability of wireless communication networks.

References

Chatzoglou, E., Kambourakis, G., & Kolias, C. (2022). How is your Wi-Fi connection today? DoS attacks on WPA3-SAE. *Journal of Information Security and Applications, 64*, 103058.

Kwon, S., & Choi, H. K. (2020). Evolution of Wi-Fi protected access: security challenges. *IEEE Consumer Electronics Magazine, 10*(1), 74-81.

Lounis, K., & Zulkernine, M. (2019, September). Bad-token: denial of service attacks on WPA3. In *Proceedings of the 12th International Conference on Security of Information and Networks* (pp. 1-8).

Lounis, K., & Zulkernine, M. (2020, November). Exploiting race condition for Wi-Fi denial of service attacks. In *13th International Conference on Security of Information and Networks* (pp. 1-8).

Moissinac, K., Ramos, D., Rendon, G., & Elleithy, A. (2021, January). Wireless encryption and WPA2 weaknesses. In *2021 IEEE 11th Annual computing and communication workshop and conference (CCWC)* (pp. 1007-1015). IEEE.

Mughal, A. A. (2022). Well-architected wireless network security. *Journal of Humanities and Applied Science Research*, *5*(1), 32-42.

Pahlavan, K., & Krishnamurthy, P. (2021). Evolution and impact of Wi-Fi technology and applications: A historical perspective. *International Journal of Wireless Information Networks, 28*, 3-19.

Palamà, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F., & Bianchi, G. (2023). Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments. *Computer Communications, 212*, 129-140.

Pisarev, D. (2020). Overview of wireless connection security standards in company's digital infrastructure and their weaknesses. In *CEUR Workshop Proceedings (CEUR-WS. org)* (pp. 1-13).

Pirayesh, H., & Zeng, H. (2022). Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE communications surveys & tutorials, 24(2)*, 767-809.

Schepers, D., Ranganathan, A., & Vanhoef, M. (2022, May). On the robustness of Wi-Fi deauthentication countermeasures. In *Proceedings of the 15th ACM conference on security and privacy in wireless and mobile networks* (pp. 245-256).

Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2022). Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. *Expert Systems with Applications, 210*, 118401.

Vanhoef, M., & Piessens, F. (2017, November). Denial-of-service attacks against the 4-way wi-fi handshake. In *9th International Conference on Network and Communications Security (NCS)*.

Vanhoef, M., Adhikari, P., & Pöpper, C. (2020, July). Protecting wi-fi beacons from outsider forgeries. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 155-160).

Xin, L., & Starobinski, D. (2021). Countering cascading denial of service attacks on Wi-Fi networks. *IEEE/ACM Transactions on Networking, 29*(3), 1335-1348.

Appendix A. Literature Review Matrix

Author / Article Title, Journal Title, and Publication Details	Research Question(s) / Hypotheses	Methodology	Analysis and Results	Conclusions	Implications for Future Research / Practice
Chatzoglou, E., Kambourakis, G., & Kolias, C. (2022). How is your Wi-Fi connection today? DoS attacks on WPA3-SAE. Journal of Information Security and Applications, 64, 103058.	Examine if WPA3-SAE implementation flaws can enable DoS attacks.	Conducted manual fuzz testing on WPA3-capable devices to uncover vulnerabilities.	Discovered 7 generic DoS techniques that exploit WPA3-SAE flaws, disrupting AP-STA communication.	Multiple vulnerabilities in WPA3-SAE result from improper implementation and outdated standards.	Advocate for stateless Anti-Clogging Mechanism (ACM) to strengthen WPA3-SAE against DoS attacks.
Kwon, S., & Choi, H. K. (2020). Evolution of Wi-Fi protected access: security challenges.	Identify vulnerabilities in older WPA versions and see how WPA3 improves security.	Review the development of security features in different WPA versions to find weaknesses.	Explain how WPA3 features like Dragonfly protect against offline password guessing attacks.	State that WPA3 fixes many issues from WPA2 but still needs improvements against DoS attacks and better	Emphasise the need for ongoing updates to Wi-Fi security protocols to keep up with new threats.

IEEE Consumer Electronics Magazine, 10(1), 74-81.				security validation.	
Lounis, K., & Zulkernine, M. (2019, September). Bad-token: denial of service attacks on WPA3. In Proceedings of the 12th International Conference on Security of Information and Networks (pp. 1-8).	Find and study weaknesses in the WPA3-SAE protocol, focusing on the "bad-token" vulnerability and WPA2-related DoS attacks.	Analyse the WPA3-SAE protocol and create attack scenarios using Raspberry Pi to show how these weaknesses can be exploited.	Looks at how attackers can use the "bad-token" vulnerability and WPA2-related attacks to disrupt network connections.	Shows that the identified vulnerabilities can be used to launch DoS attacks on WPA3 networks, blocking legitimate clients and disconnecting existing ones.	Device manufacturers need to implement countermeasures against these vulnerabilities, and more research is needed to find other potential attack methods and their effects on Wi-Fi IoT applications.
Lounis, K., & Zulkernine, M. (2020, November). Exploiting race condition for Wi-Fi denial of service attacks. In 13th International Conference on	Aim to show three new attack scenarios that use a race condition vulnerability to stop users from connecting to real Wi-Fi networks and suggest ways	Set up an experimental environment with laptops, smartphones, tablets, a Wi-Fi AP, and a desktop for monitoring to test and analyze the attacks using an evil twin	The attacks take advantage of weaknesses in Wi-Fi authentication protocols, where devices act on the first message received without proper verification.	DoS attacks are a serious threat to Wi-Fi networks, especially as Wi-Fi use grows in IoT applications. They highlight that the attack scenarios are easy to carry	Add intelligence to the authentication process so devices evaluate multiple messages before proceeding.

Security of Information and Networks (pp. 1-8).	to prevent these attacks.	attack scheme.		out with few resources.	
Moissinac, K., Ramos, D., Rendon, G., & Elleithy, A. (2021, January). Wireless encryption and WPA2 weaknesses. In 2021 IEEE 11th Annual computing and communication workshop and conference (CCWC) (pp. 1007-1015). IEEE.	Looks at the security of wireless communication, especially WPA2 weaknesses, and suggests that WPA2-Enterprise features can improve security for home and small business users.	Use a Kali Linux virtual machine to simulate WPA2-Enterprise components with tools like Aircrack-ng, FreeRADIUS, and an Apache web server for SSL handshakes.	The simulation shows that the proposed solution would triple the AP load compared to WPA2-PSK, but the authors argue this increase is minor since authentication happens rarely.	The authors conclude their solution offers strong encryption for home and small business users without needing complex systems, making it a practical way to improve wireless security.	Future research should focus on creating a more precise model by testing the solution on devices like Raspberry Pi, integrating it with Linux APs, and managing public key certificates to prevent man-in-the-middle attacks.
Mughal, A. A. (2022). Well-architected wireless network security. Journal of Humanities and Applied Science	Aims to explore wireless network security, focusing on fundamental principles and best practices for enterprise environments.	Examines the complexities of wireless security architecture and outlines steps for designing and managing secure wireless	Real-world case studies show how security concepts apply, including a large enterprise's secure wireless network and security challenges	The article summarises key findings, emphasizing the need for a comprehensive, multi-layered approach to wireless network security.	For practitioners, the research offers a framework and guidance for secure wireless network management. For researchers, it

Research, 5(1), 32-42.		networks in businesses.	faced by small-to-medium-sized businesses.		points to areas needing further study, like new security protocols and technologies.
Pahlavan, K., & Krishnamurthy, P. (2021). Evolution and impact of Wi-Fi technology and applications: A historical perspective. International Journal of Wireless Information Networks, 28, 3-19.	Explores the growth of Wi-Fi technology and its applications, focusing on how its popularity in indoor settings drives interest in new cyberspace applications.	The authors categorize the history of Wi-Fi technology into three eras: before 1985, from 1985 to 1997, and from 1997 to now, while also discussing market evolution and applications from their perspective as researchers.	The authors found that Wi-Fi is favored for smartphones due to its high data rates, reliable indoor connections, and lower costs, and noted that the WLAN industry led the development of key wireless technologies. They also identified Wi-Fi positioning, popularized by the iPhone, as a major innovation.	The study concludes that the proliferation of Wi-Fi devices has enabled significant advancements in cyberspace applications.	The industry is looking for new applications of Wi-Fi signals to improve cyberspace intelligence, with future efforts focused on combining RSS signals with sensor data to enhance positioning accuracy and flexibility.
Palamà, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F., &	Aims to evaluate the security of 802.1x authentication	The researchers conducted two experiments:	The findings showed that many users lacked security awareness and	Although 802.1x is meant for secure authenticatio	Future work should focus on creating technologies to help users

Bianchi, G. (2023). Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments. Computer Communications, 212, 129-140.	mechanisms in Wi-Fi enterprise networks, focusing on vulnerabilities in the Eduroam service and assessing user security awareness.	one with a controlled group at the University of Rome where participants' credentials were captured using a rogue Eduroam AP, and another at the University of Brescia involving real-world attacks with rogue APs in crowded areas to evaluate user vulnerability	had vulnerable device configurations, with over one-third of participants losing credentials in the controlled experiment. The in-the-wild attack revealed that many users were at risk due to misconfigurations, and Android devices were generally more vulnerable than Apple devices.	n, it is ineffective in practice due to user behavior and device vulnerabilities, indicating a need for better security measures and user education.	recognise attacks, promote security awareness, and improve security protocols. Manufacturers should restrict forced connections when certificates change, and organizations should provide current security guides and awareness campaigns for users.
Pisarev, D. (2020). Overview of wireless connection security standards in company's digital infrastructure and their weaknesses. In	Aims to review wireless security standards, focusing on Wireless Intrusion Detection Systems (WIDS), and identify	The authors conduct a literature review to compare how well machine learning and deep learning techniques detect attacks on wireless networks.	The analysis shows that many studies have flaws, like using old data and lacking real-world testing, which affect their findings.	The researchers conclude that the 802.11 standard still has security weaknesses, even in its latest version, and a stronger WIDS is	Future studies should use updated data and practical tests to compare detection methods, while companies should improve their

CEUR Workshop Proceedings (CEUR-WS. org) (pp. 1-13).	weaknesses to prevent cyberattacks.			needed to protect against data leaks.	security measures and stay updated on new threats.
Pirayesh, H., & Zeng, H. (2022). Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. IEEE communications surveys & tutorials, 24(2), 767-809.	Aims to provide a clear overview of jamming attacks and anti-jamming strategies in different wireless networks to encourage more research and help design better wireless systems.	Reviews existing research on jamming attacks and anti-jamming strategies across various wireless networks, organising techniques and comparing them with previous surveys.	Examine different types of jamming attacks and categorise anti-jamming techniques, providing tables that summarise both for each wireless network type.	Despite improvements in wireless technology, many systems are still at risk from jamming attacks due to limited anti-jamming techniques that are practical and effective.	More research on better anti-jamming methods, especially in areas like MIMO techniques, cross-domain designs, flexible resource allocation, and using machine learning for anti-jamming solutions.
Schepers, D., Ranganathan, A., & Vanhoef, M. (2022, May). On the robustness of Wi-Fi deauthentication countermeasur	Studies how well Wi-Fi deauthentication countermeasures work in the IEEE 802.11 standard and whether Management	Examines the IEEE 802.11 standard's rules for handling deauthentication frames and tested how MFP is implemented in different	Found problems in the standard, such as unclear rules and vulnerabilities that could lead to denial-of-service attacks. It showed that many systems,	MFP does not provide enough protection against deauthentication attacks and emphasised the need for better	Creating stronger defenses against deauthentication attacks and improving the IEEE 802.11 standard.

es. In Proceedings of the 15th ACM conference on security and privacy in wireless and mobile networks (pp. 245-256).	Frame Protection (MFP) is enough to stop deauthentication attacks.	operating systems and wireless devices, using practical experiments to find vulnerabilities.	including Linux and Apple devices, are still vulnerable to deauthentication attacks even with MFP.	security measures, including beacon frame protection.	
Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2022). Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. Expert Systems with Applications, 210, 118401.	Looks at Multi-Channel MitM attacks that alter encrypted wireless frames between two endpoints and evaluates how well current protection mechanisms work against these attacks.	Reviews existing research on Multi-Channel MitM attacks, focusing on their effects on WPA, WPA2, and WPA3 networks, as well as the difficulties in implementing protection methods.	Found that Multi-Channel MitM attacks can manipulate wireless frames on WPA3 networks, bypassing protections like PMF. They also noted that many Wi-Fi devices remain unpatched and vulnerable due to delays in releasing updates.	Multi-Channel MitM attacks are a serious threat to Wi-Fi security because they can bypass protections and exploit weaknesses in Wi-Fi protocols, highlighting that effective defense mechanisms are still needed, especially in IoT contexts.	Focus on creating lightweight wireless intrusion detection systems for real Wi-Fi-based IoT networks and improving Wi-Fi standards to prevent Multi-Channel MitM attacks from bypassing protections.
Vanhoef, M., & Piessens, F. (2017, November). Denial-of-	Studies the 4-way Wi-Fi handshake to see if there were	Tests different implementations of the 4-way	Found three new denial-of-service attacks. The first two attacks exploit	Two of the attacks can be prevented by always sending	Recommend changing implementations to send plaintext

service attacks against the 4-way wi-fi handshake. In 9th International Conference on Network and Communications Security (NCS).	vulnerabilities that could lead to denial-of-service attacks.	handshake for weaknesses and performed a jamming attack on OpenBSD's rum driver to check if the pairwise key (PTK) could be installed before the fourth message was sent.	timing issues between the client and AP, causing failed handshakes. The third attack involves sending a bad message after the handshake, which disconnects some clients from the network.	plaintext EAPOL frames during the initial handshake, while the third attack can be stopped by ignoring malformed message 1's during the handshake.	EAPOL frames during key rekeying and modifying clients to accept only authenticated messages during this process.
Vanhoef, M., Adhikari, P., & Pöpper, C. (2020, July). Protecting wi-fi beacons from outsider forgeries. In Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (pp. 155-160).	Can an attacker create fake beacons to perform various attacks, and can a low-bandwidth method be developed to authenticate beacon frames and stop these attacks?	Reviews existing attacks with fake beacons, analyses beacon information for vulnerabilities, audits code and tests their scheme on various devices.	Many devices are vulnerable to forged beacons, leading to issues like denial of service and battery drain. The proposed scheme prevents outside forgeries, is efficient, and works with older systems but does not protect against	Unprotected beacon frames pose security risks, and the researchers demonstrated attacks using them. They proposed a protective scheme for outside forgeries that is now part of the draft 802.11 standard.	Future research should address insider forgeries. Vendors should implement the protection scheme, and network administrators should enable it on their networks.

			insider forgeries.		
Xin, L., & Starobinski, D. (2021). Countering cascading denial of service attacks on Wi-Fi networks. IEEE/ACM Transactions on Networking, 29(3), 1335-1348.	Studies cascading DoS attacks on Wi-Fi networks and aims to optimise packet transmission times to reduce these attacks while boosting throughput.	The authors used analytical modeling, simulations, and experiments. They created a model to analyse neighboring nodes' utilization affected by MAC overhead and conducted tests with ns-3 and real Wi-Fi cards.	The optimal packet duration can prevent cascading DoS attacks and enhance throughput, varying with MAC overhead. Simulations and experiments confirmed that this method outperforms RTS/CTS.	Cascading DoS attacks threaten Wi-Fi networks, but optimising packet durations can effectively mitigate them and improve throughput.	Investigate cascading DoS attacks in newer Wi-Fi standards. The study emphasises considering MAC overhead and packet length for robust Wi-Fi network design.