An In-Depth Evaluation of Security Challenges in Modern Wi-Fi Networks

Teg Singh[1], Dr Rajesh Chauhan[2]
[1]*Ph.D. Scholar, Department of Computer Application & Technology, Career point university kota Rajasthan*
[2]*Department of Computer Application & Technology, Career point university Kota, Rajasthan*

Abstract **-** The modern Wi Fi networks have now become an essential element of digital communication within digital communication, allowing users, companies, and vital infrastructure to connect without any disruptions. The pace at which wireless technologies have evolved is however coming with sophisticated security challenges that are threatening confidentiality, integrity, and availability. The given paper introduces the balanced analysis of security problems in modern Wi Fi settings, analyzing the weaknesses in protocols, authentication methods, operating system and devices settings, and user actions. It further talks about the new vectors of attack and offers mitigation efforts in line with the existing security requirements. The research will equip the studies, teachers, and practitioners with an orderly perception of the contemporary Wi Fi security threats and protection methods.

Keywords **-** Wi Fi security, WLAN vulnerabilities, WPA3, wireless attacks, network protection, cybersecurity.

I. INTRODUCTION

Wi-Fi or Wireless Local Area Networks (WLANs) are networks that have radically changed the pattern of digital communication and access to data in the contemporary society. Wi-Fi technology is also mobile, flexible, scalable, and economical to implement unlike traditional wired networks which require physical cabling as well as fixed infrastructure and users can access network services at literally any point within signal reach. This has enabled wireless networking to become part and parcel of modern information and communication infrastructure.

Nowadays, Wi-Fi connectivity is incorporated in a broad spectrum of settings, such as residential, educational, healthcare, corporate business, transportation, smart cities, and industrial automation locations. The fast use of smartphones, laptops, cloud computing services and the Internet of Things (IoT) gadgets have further enhanced the dependency on wireless connectivity to offer real-time communication, remote collaboration, online learning, telemedicine, and smart monitoring systems. Consequently, there is a need to have a secure and reliable Wi-Fi infrastructure, both to everyday users and mission critical operations of an organization.

Wireless communication has a lot of benefits; however, it comes with some unique security issues not widely encountered in the wired networks. Since Wi-Fi signals are transmitted over the air by using radio frequencies, attackers have the possibility of trying to gain access to the network without necessarily having to touch routers or the internal infrastructure. Malicious actors may:

- Hack wireless signals to retrieve valuable data like logins, email or bank accounts.
- Fake legitimate access points (e.g. rogue or evil twin hotspots) to lure users to use malicious networks.
- Abuse flaws in authentication, encryption, or protocol architecture to obtain unauthorized access.
- Défense denial-of-service or traffic-manipulation attacks, which interfere with network availability or integrity.

To deal with these threats, the level of Wi-Fi security systems has also developed. Early security was based on Wired Equivalent Privacy (WEP), but it was subsequently succeeded by Wi-Fi Protected Access (WPA and WPA2) and, more recently, WPA3, with each successive generation having a more robust encryption, enhanced authentication, and better resistance to attacks. Nonetheless, the never-ending release of vulnerabilities, configuration mistakes, compatibility with old devices, and human factor flaws, will ensure that wireless security is not a closed issue.

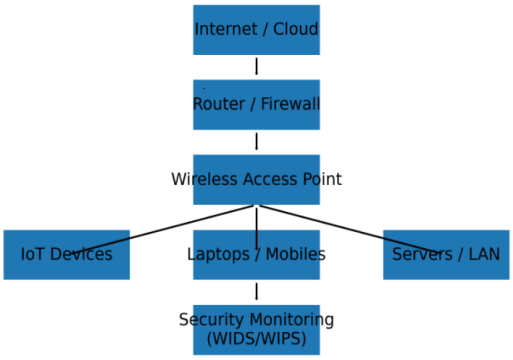

Figure-1 A more detailed architecture diagram

Since the reliance on wireless networking is growing, and cyber threats are becoming more advanced, it is time- and necessity-based to undertake a critical and thorough review of the contemporary Wi-Fi security issues. It is essential to know how vulnerabilities are created, how attackers use them and how defensive mechanisms can be enhanced to secure

sensitive data, ensure service availability and trust of the users.

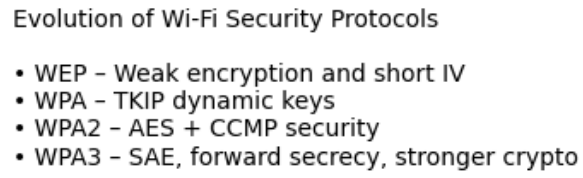

Figure-2 Evolution of Protocol Techniques

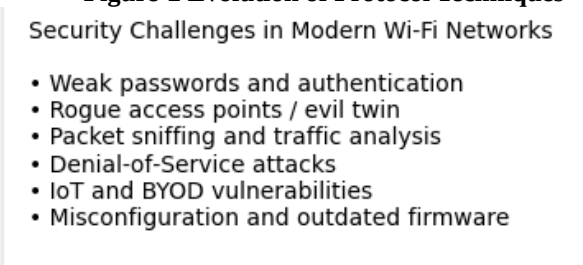

Figure-3 Security Challenges in Modern Wi-fi Networks

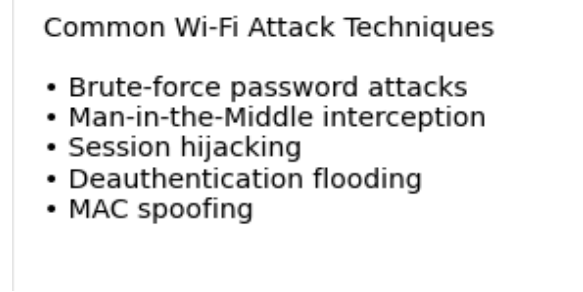

Figure 4 Common Wi-fi Attack Techniques

The paper will offer an in-depth look at security challenges in the recent Wi-Fi networks through the analysis of technological development, the threat environment, and protective measures. In particular, the research is based on:

- The development of Wi-Fi security system, such as WEP, WPA/WPA2, and WPA3.
- Typical attacks that can occur when deploying a WLAN.

Types of wireless attacks and threat actors, as well as the methods of their operation.

- Mechanisms and mitigation strategies of enhancing wireless security, as well as best practices.
- A new wave of Wi-Fi security and future research directions.

This organized discussion aims to aid researchers, cybersecurity specialists, educators, and network managers to learn more about the intricacies of wireless security and create more robust Wi-Fi spaces.

II. WI-FI-SECURITY-PROTO-EVOLUTION.

Wi-Fi wireless security architecture has gone through numerous generations of protocols with each new standard aimed at rectifying the shortcomings of the old one. Such an evolutionary direction, i.e. WEP to WPA/WPA2, and eventually WPA3, is based on the continuous work on enhancing confidentiality, integrity, authentication, and resistance to new cyber-attacks. Such a development is fundamental to the understanding of the design principles and safeguards that are installed in the contemporary wireless security systems.

2.1 Wired Equivalent Privacy (WEP): The first security protocol that was introduced with the original IEEE 802.11 wireless networking standard was Wired Equivalent Privacy (WEP). It was mainly aimed at offering a degree of privacy that is similar to the conventional wired Ethernet networks through the encryption of the wireless data transmission. WEP employed a shared secret key with the RC4 stream encoder, a 24-bit Initialization Vector (IV) and encrypted packets before transmission. Ideally, such a strategy was supposed to stop rogue access to wireless traffic. But practically, WEP was not very effective as it had a number of conceptual flaws that made it useless.

2.1.1 Significant Weaknesses of WEP.

1. **Small Initialization Vectors (IVs):** The IV space is 24-bit; it is very small and as a result, IVs replicate significantly in high traffic networks. The attackers were able to steal numerous packets and use them to de-encrypt the encryption key using statistical cryptanalysis.

2. **Weak Key Management:** WEP was based on shared keys which were manually set and hardly ever changed. Attackers might keep having an unauthorized access to the network on a long-term basis once compromised.

3. **Weak Protection of Integrity:** WEP had a primitive integrity component that was checksum based and may be forged to enable packets to be altered and injected without being noticed. Due to these weaknesses, automated tools would break the encryption of WEP in minutes and therefore it would not be at all suitable in communication involving security. WEP is therefore obsolete and is deemed to be totally insecure.

This is the Wi-Fi Protected Access (WPA and WPA2). In addressing the number of glaring flaws of WEP, the Wi-Fi Alliance came up with Wi-Fi Protected Access (WPA) as a temporary security improvement until an actual IEEE standard was developed. WPA has substituted the inert WEP encryption with Temporal Key Integrity Protocol (TKIP), which added:

- Dynamic per-packet keying, limiting the reuse of keys.
- Checking of the integrity of messages, avoiding tampering of packets.
- Better key distribution systems, which increase authentication security.

Although WPA was much better protection than WEP, TKIP still used the older cipher RC4 and was viewed as a stop-gap measure. WPA2 was the actualization of the IEEE 802.11i standard of security and provided significant breakthroughs to cryptography:

1. It is called the Advanced Encryption Standard (AES).

WPA2 substituted RC4 with AES which is much stronger and world trusted encryption algorithm.

2. CCMP Protocol

The Counter Mode Cipher Block Chaining Controlled Message Authentication code (CCMP) was as follows:

o Data confidentiality
o Message integrity
o Source authentication

3. Enterprise-Level Authentication

WPA2 was compatible with the 802.1X authentication with RADIUS servers allowing secure and central identity management within the organization setup.

These enhancements caused WPA2 to be the leading Wi-Fi security protocol over a period of ten years.

Vulnerabilities of WPA2 Vulnerability to KRACK Attack.

WPA2 was not a fortress even though it was powerful. KRACK (Key Reinstallation Attack) has shown the vulnerabilities of the four-way handshake of setting encryption keys between a client and an access point.

Using KRACK, attackers were able to:

- Replay handshake messages
- Reuse of encryption keys by force.
- Alter or decrypt some transmitted data.

Despite software patches to address KRACK, the vulnerability has shown that the vulnerability occurs because of protocol architecture defects, which led to the WPA3 development.

2.2 Wi-Fi Protected Access 3 (WPA3)

The newest generation of Wi-Fi security is WPA3 which has been developed to counter contemporary cyber-threats and offer greater privacy, authentication, and cryptographic strength.

Important Protection Improvements of WPA3.

1. Equal Authentication between equals (SAE).

The traditional pre-shared key handshake is substituted by password authenticated key exchange in SAE that eliminates offline dictionary attacks, even after attackers obtain handshake data.

2. Forward Secrecy

WPA3 will guarantee that encrypted past traffic will be safe even in the case where the network password is found out.

3. Greater Cryptographic security.

The WPA3 Enterprise mode allows 192-bit security, which is consistent with the high-assurance government and enterprise security needs.

Still outstanding issues in WPA3 deployment.

Even though WPA3 has enhanced security on wireless connections, there are still some challenges that are encountered when deploying it practically, which include:

- Early firmware or software bugs.
- Backward compatibility downgrade attacks WPA2 |human|>Downgrade attacks (based on backward compatibility with WPA2)
- Inability to fully adopt legacy devices.

As such, secure configuration, firmware updates, and sound network administration are mandatory even in WPA3 enabled environments. Following is the summary of Protocol Evolution.

Protocol	Key Features	Major Weakness
WEP	RC4 encryption, shared key	Easily cracked, no integrity protection
WPA	TKIP, dynamic keys	Transitional, still RC4-based
WPA2	AES-CCMP, 802.1X	KRACK vulnerability
WPA3	SAE, forward secrecy, 192-bit security	Deployment and compatibility issues

Table -1 Summary of Protocol Evolution

This development demonstrates the ever-escalating arms race between security design and cyber-attack methods and why current research and ad hoc wireless security measures are necessary.

III. SECURITY THREATS IN THE WI-FI NETWORK OF THE PRESENT DAY

Regardless of the great progress in the field of wireless security protocols, including WPA2 and WPA3, contemporary Wi-Fi settings are still exposed to a plethora of technical, configuration-based, and human-factor security threats. Such risks are not only due to technological weaknesses but also due to inefficient user practices, differentiations of devices, high growth in network, and changes in cyber-attack methods. With wireless connectivity integrated into the critical infrastructure, healthcare, education, and industrial systems, these challenges should be learned to design robust and secure WLAN implementations.

3.1 Low Authentication and password practices

Poor password hygiene is one of the biggest factors that lead to compromise of Wi-Fi. Many users select:

- Easy to guess passwords or short passwords.

Common words or foreseeable patterns in the dictionary.

- Existing passwords to use in multiple services or networks.

The attackers take advantage of these vulnerabilities with:

Brute-force attacks are considered to be- Brute-force attacks are methods that systematically employ all possible combinations.

- Dictionary attacks are those that attempt to use popular passwords.
- Credential-stuffing attacks, in which the reuse of credentials due to other breaches is reused.

Since Wi-Fi pre-shared keys can be used to secure whole networks, a single weak password will allow a network to be compromised, intercept data, and gain access to devices.

3.2 Evil Twin Attacks 3.2 Rogue Access Points

Rogue access point are illegitimate wireless devices attached or pretending to be an authentic network. One of the most perilous ones is the evil twin attack, in which an attacker establishes a rogue hotspot with a similar network name (SSID) to a trusted Wi-Fi network.

By default, unsuspecting users can join such fake networks, and the attackers can:

- Steal customer names and passwords.
- Steal session cookies to hijack an account.
- Inoculate with malicious or phishing pages.
- Surveillance of sensitive communications.

The attacks mostly occur in places of mass gathering like airports, cafes, and hotels where people are supposed to have unrestricted wireless access.

3.3 Packet Sniffing and Traffic Analysis

Since Wi-Fi sends information over radio frequency signals over the air, individuals within the range can intercept wireless packets through sniffing or monitoring devices.

Without a good encryption or with incorrectly configured or no encryption, attackers can easily access:

- Login credentials
- Emails and private messages
- Monetary or personal data.

Despite the strong encryption (e.g., WPA2/WPA3), attackers can still do traffic analysis and check:

- Communication timing
- Packet sizes
- Connection patterns

This type of metadata leak can give the information about the behavior that can be used to do surveillance, profiling or targeted attacks.

3.4 Denial-of-Service (DoS) Attacks

The wireless networks are particularly susceptible to attacks based on availability where the communication is disrupted as opposed to data being stolen. Popular Wi-Fi DoS methods are:

- DE authentication floods, which makes devices disconnect.
- Jamming of signals, disruption of radio frequency.
- Resource depletion, bombarding access points.

Such attacks may result in network downtime, service or operational failure which is particularly disastrous in:

- Healthcare monitoring systems and hospitals.
- Smart manufacturing and industrial automation.

Emergency response and public safety networks

|human|>• Emergency response and public safety networks.

Therefore, DoS attacks are not only a cybersecurity threat, but they are also potentially life-threatening and malfunctioning.

3.5 IoT and BYOD Risks

Wi-Fi networks have become much more vulnerable to attacks due to the rapid proliferation of Internet of Things (IoT) devices and Bring Your Own Device (BYOD) policy.

The problems that affect many IoT and personal devices include:

- Obsolete or unupgradable firmware.
- Weak or hard-coded passwords
- Incident of lack of encryption or secure authentication.
- Low level security surveillance.

Having been compromised, these devices have the potential to be used to:

- Introduce network attacks internally.
- Belong to botnets to attack the distributed mode.
- Offer unauthorized access persistently.

Thus, one of the key contemporary wireless security challenges is uncontrollable device diversity.

3.6 Misconfiguration and Incompatible Firmware

Much of the Wi-Fi security breache is not caused due to sophisticated hacking but due to inappropriate setting up and inadequate maintenance. Common issues include:

- Crippled or poor encryption options.
- Default usernames and passwords of administrators.
- Open distant administration interfaces.
- Lack of installation of firmware and security patches.

Automated scanning, used by attackers on a regular basis, is to find out such vulnerabilities and use them to gain unauthorized access, steal data, or take control of the network.

This emphasizes the fact that administrative negligence and human error can be as harmful as a technical weakness.

IV. WI-FI ATTACK WI-FI TECHNIQUES

The Wireless Local Area Networks (WLANs) work on open radio-frequency networks which is the main difference with the wired networks where interception cannot be achieved without accessing the physical cable. Since Wi-Fi signals are not restricted to organizational boundaries, attackers can monitor, intercept, or manipulate communications by other nearby locations with low-cost hardware and other publicly available tools. As a result, many real-world strategies of attack have developed that take advantage of vulnerabilities in the authentication, encryption, session processing, and wireless protocols management. These threats must be understood to come up with safe wireless infrastructures and effective defensive measures.

4.1 Dictionary Attacks and Brute-Force

Wi-Fi networks that use pre-shared keys (PSKs) (including WPA2-Personal or weak WPA3 passphrase deployments) are the main victims of brutal and dictionary attacks. These attacks are designed so as to find the network password through repeated attempts to guess the key combinations.

Attack Procedure

1. The hacker records the four-way handshake that transpires when a legitimate user is connected to the Wi-Fi network.
2. The attacker uses offline cracking tools to come up with password guesses.
3. Individual passwords are guessed and converted into a cryptographic key and matched with the handshake data captured.
4. On finding a match the correct password is displayed.

It employs two enormous techniques:

- Dictionary attacks: Use a list of common passwords, credentials that have been leaked, or pre-determined word patterns.
- Brute-force attacks: Linearly try all possible combinations of characters, which are less efficient, but which ensure the success of a weak enough password.

Reasons for Success

- Short, simple or reused passwords are usually chosen by the users.

Hackers can easily use weak pass phrases on many routers.

- Offline cracking can have unlimited attempts without alarming.

Security Impact

Attackers can steal the password and do:

- Get access to a network legitimately.
- Surveillance of internal communication.
- Carry out sideways attacks on interconnected devices.
- Install malware or spy.

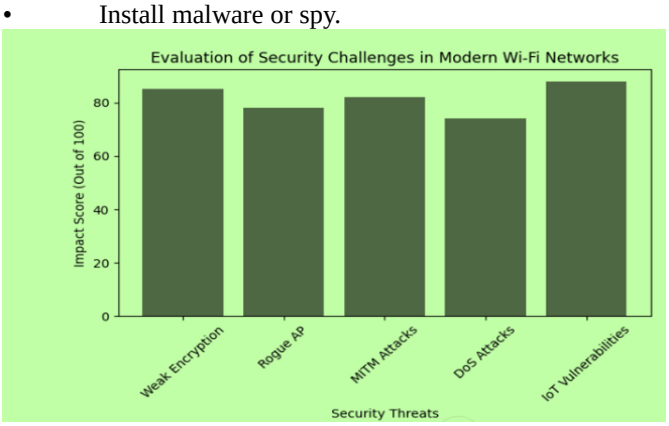

Figure-5 Comparative Impact Analysis of Security Challenges in Modern Wi-Fi Networks

The figure displays a comparative study of how serious security threats have affected modern Wi-Fi networks. The Y-axis is the Impact Score (between 0 and 100) that describes the seriousness and potential harm that each threat can cause. These security challenges have been evaluated as listed in the X-axis.

4.2 Man-in-the-Middle (MITM) Attacks

A Man-in-the-Middle attack is defined as an attack in which a malicious party intercepts communication between a wireless client and the authentic access point, and possibly changes it. Attackers will install rogue access points that are attached to a different network or a gateway that is under control, in order to monitor all traffic of the victim.

Evil Twin Attacks

The attacker sets up a replicated access point which replicates:

- Network name (SSID)
- MAC address
- Security configuration

The faked AP can often send a stronger signal and therefore devices connect automatically.

The capabilities following connection can be classified into three categories: physical capabilities, technical capabilities, and managerial capabilities.

Attackers may:

- Obtain usernames and passwords.
- Refer the victims to phishing sites.
- Inject malicious downloads
- Monitor browsing activity
- Secrecy of unprotected connections.

Consequences

MITM attacks enable:

- Identity theft
- Financial fraud
- Corporate espionage
- Malware distribution
- Privacy violations

4.3 Session Hijacking

Session hijacking is concerned with the stealing of user sessions that have been authenticated and not with passwords. Upon a successful connection, web servers provide session tokens or cookies which are used to preserve authentication.

Attack Mechanism

Attackers can:

- Hack cookies through packet sniffing of insecure or poorly encrypted networks.

MITM positioning is the technique used to intercept session data.

- Play stolen tokens and take the place of the authorized user.

Why It Is Dangerous

- No need to crack passwords
- Skips authentication at the log-in point.
- Gives access to active services on the spot.

Real-World Risks

- Unlicensed access or cloud access of emails.
- Banking or payment fraud
- Confidential data theft
- Takeover of account and fraudulent impersonation.

4.4 DE authentication and Disassociation Attacks.

Historically, Wi-Fi management frames do not include authentication, which can be used to forge control messages by attackers.

Attack Execution

An intruder transmits fraudulent DE authentication or disassociation frames to:

- Kick the users out of the legitimate network.
- Interrupt connectivity
- Attempts to reconnection triggered.

Victims may reconnect to:

- An evil-twin access point that is of a malevolent character.
- The identical network revealing authentication handshakes.

Security Implications

- Facilitates Denial-of-Service (DoS) attacks.
- Helps in cracking passwords.
- Assists MITM positioning

Contemporary features such as 802.11w Protected Management Frames (PMF) reduce not completely avert the risk.

4.5 MAC Address Spoofing

Background

Other networks use MAC address filtering as a form of access-control. The MAC addresses are however observable and easily altered.

Attack Steps

1. The attacker sniffs packets to get to know the MAC address of an authorized device.
2. The attacker modifies the MAC address of his or her device to coincide.
3. Access is mistakenly provided to the network.

Weakness of MAC Filtering

- No encryption or identity check.
- Can be easily circumvented with a few simple software packages.

MAC filtering must hence be a small complementary measure and not a security in its own.

4.6 Attack Scenario Combinations and Advanced.

Attackers in practice tend to combine several techniques:

1. DE authentication 1.1 capture handshake 1.2 brute-force password.

- Evil twin and injecting MITM session hijacking.
- Network access: lateral movement: data exfiltration.

These multi-stage attacks have a severe effect on compromise.

4.7 Need for Défense-in-Depth

Secure Wi-Fi environments should make use of layered protection since no single layer can ensure protection such as: WPA3 encryption and difficult to crack passphrases.

- Enterprise authentication (802.1X, RADIUS, MFA)
- Wireless intrusion monitoring and detection.
- Lockdown setups and updates of firmware.
- User enlightenment on rogue networks.

V. CONCLUSION

The new Wi-Fi networks are indispensable in communication both at home, enterprises, health, education, and smart environments as they provide the advantages of mobility, scalability, and cost-effectiveness in connecting. Nonetheless, the vulnerability of these networks to serious security risks including weak authentication, rogue access points, packet snatching, denial-of-service attacks, and IoT risks and misconfigured devices is because of the open nature of the wireless transmission. Despite the development of security measures by way of WEP to WPA2 and currently WPA3, that offers more effective encryption, authentication and forward secrecy, there are still practical threats of security breach based on human factors, compatibility issues with the environment, and other implementation flaws. Thus, to create secure wireless environments, it is necessary to implement a multi-layered defense strategy that will integrate the adoption of WPA3 and robust authentication systems, active monitoring, secure configuration, regular firmware updates, and user awareness. The security of Wi-Fi in the future will be more focused on threat detection using AI, zero-trust systems, and improved security in Wi-Fi 6/7 and IoT ecosystems. The ongoing research, proactive security control, and technological innovation are vital towards ensuring privacy of the data, availability of the services, and the trust in the next generation wireless communication systems.

VI. REFERENCES

[1]. IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11, IEEE, latest revision.

[2]. NIST, *Guidelines for Securing Wireless Local Area Networks (WLANs)*, NIST Special Publication 800-153, National Institute of Standards and Technology, USA.

[3]. Wi-Fi Alliance, *Wi-Fi Protected Access 3 (WPA3) Specification*, Wi-Fi Alliance Technical Documentation.

[4]. Vanhoef, M., and Piessens, F., Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2017.

[5]. Fluhrer, S., Mantin, I., and Shamir, A., "Weaknesses in the Key Scheduling Algorithm of RC4," *Selected Areas in Cryptography*, Springer, 2001.

[6]. He, D., Zeadally, S., Kumar, N., and Lee, J. H., "Anonymous Authentication for Wireless Body Area Networks With Provable Security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601, 2017.

[7]. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and Levkowetz, H., "Extensible Authentication Protocol (EAP)," *IETF RFC 3748*, 2004.

[8]. Bianchi, G., "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, 2000.

[9]. Alshamrani, A., Myneni, S., Chowdhary, A., and Huang, D., "A Survey on Advanced Persistent Threats: Techniques,

Solutions, Challenges, and Research Opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, 2019.
[10]. Zhang, Y., Chen, X., and Li, J., "Security and Privacy in Smart IoT-Based Wireless Networks: Challenges and Opportunities," *IEEE Internet of Things Journal*, recent issue.
[11]. Vanhoef, M., and Ronen, E., "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," *IEEE Symposium on Security and Privacy*, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," *USENIX Security Symposium*, 2003.
[12]. Wright, J., "Detecting Wireless LAN MAC Address Spoofing," *SecurityFocus*, 2003.
[13]. Mishra, A., Shin, M., and Arbaugh, W., "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," *ACM SIGCOMM Computer Communication Review*, 2003.
[14]. Gast, M., 802.11 Wireless Networks: The Definitive Guide, O'Reilly Media, latest edition.
[15]. Scarfone, K., and Padgette, J., "Guide to Enterprise Telework, Remote Access, and BYOD Security," *NIST Special Publication 800-46*, NIST.
[16]. Kolias, C., Kambourakis, G., Stavrou, A., and Voas, J., "DDoS in the IoT: Mirai and Other Botnets," *IEEE Computer*, vol. 50, no. 7, 2017.
[17]. Sicari, S., Rizzardi, A., Grieco, L. A., and Coen-Porisini, A., "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks*, vol. 76, 2015.
[18]. Humayed, A., Lin, J., Li, F., and Luo, B., "Cyber-Physical Systems Security—A Survey," *IEEE Internet of Things Journal*, 2017.
[19]. Conti, M., Dragoni, N., and Lesyk, V., "A Survey of Man-in-the-Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, 2016.
[20]. Zubair, M., et al., "Machine Learning for Wireless Network Security: A Survey," *IEEE Access*, recent publication.
[21]. Xiao, Y., "IEEE 802.11i: Enhancing Wireless LAN Security," *IEEE Wireless Communications*, vol. 12, no. 1, 2005.
[22]. Perkins, C., Ad Hoc Networking, Addison-Wesley, 2008.
[23]. Stallings, W., Network Security Essentials: Applications and Standards, Pearson, latest edition.
[24]. M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, Dallas, TX, USA, 2017, pp. 1313–1328.
[25]. A. O. Almohri, D. B. Rawat, and M. M. Parvez, "Security challenges in wireless sensor networks for smart cities," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 98–104, Feb. 2017.
[26]. A. B. M. Alotaibi and L. A. Alotaibi, "A survey of wireless security protocols (WEP, WPA and WPA2/802.11i)," in *2018 21st Saudi Computer Society National Computer Conference (NCC)*, Riyadh, Saudi Arabia, 2018, pp. 1–6.
[27]. S. Mathew and M. Al Hajj, "Wireless network security threats, vulnerabilities and their defenses," *American Journal of Operations Management and Information Systems*, vol. 2, no. 1, pp. 1–6, 2017.
[28]. D. He and S. Zeadally, "Authentication Protocols for Wireless Networks: A Survey and Open Issues," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2571–2599, Fourthquarter 2017.
[29]. N. Tippenhauer, K. Rasmussen, C. Pöpper, and S. Capkun, "On the Requirements for Successful GPS Spoofing Attacks," *ACM Conference on Computer and Communications Security*, 2017 (relevant to wireless signal spoofing concepts).
[30]. S. Morgan, "Cybercrime To Cost The World $6 Trillion Annually By 2021," *Cybersecurity Ventures Report*, 2017 (contextual relevance to wireless network threats).
[31]. Wi-Fi Alliance, "WPA3™ Specification Version 1.0," Wi-Fi Alliance Technical Specification, 2018.