Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Volume 3 | Issue 4 | ISSN: 2583-1895
July-September 2025 | DOI: https://doi.org/10.5281/zenodo.17336341

A Review Paper on Cyber Security in Wireless Networks: Threats, Countermeasures, and Future Trends

Bhumi Chittora[1], Shalini Chawla[2]

1Student(BCA) School of Computer Application & Technology, Career Point University, Kota (Raj.), India

2Assistant Professor, School of Computer Application & Technology, Career Point University, Kota (Raj.), India

Abstract

Wireless networks have become an essential part of everyday communication, enabling connectivity across homes, businesses, and public spaces. However, their open and shared nature exposes them to a variety of security risks such as unauthorized access, data interception, and malicious attacks. This study examines the key threats facing wireless networks and evaluates traditional security measures including encryption protocols, authentication methods, and network monitoring tools. We highlight the critical role of user behavior and the challenges posed by rogue access points and multi-layered attacks. The findings emphasise that while advanced technical safeguards are vital, simple practices such as strong passwords, regular updates, and user awareness significantly contribute to network protection. Balancing security and performance remains a challenge, but a blended approach of sound network design, vigilant monitoring, and informed users offers effective defense against common wireless threats.

Keywords: Ransomware, Prevention Strategies, SIEM, Cybersecurity Endpoint Detection and Response (EDR), Multi-Factor Authentication (MFA)

Introduction

Wireless networks play a crucial role in modern communication, offering convenient and flexible connectivity for a wide range of devices and applications. From homes and offices to public spaces and smart cities, wireless technology has transformed how we access and share information. However, the very nature of wireless communication—where signals are broadcast through the air—also makes these networks vulnerable to various security threats. Unlike wired networks, where physical access is required, wireless networks can be targeted

by attackers within signal range, leading to risks such as unauthorized access, data interception, denial-of-service attacks, and spoofing.

Securing wireless networks is therefore a complex challenge that requires a combination of technical solutions and user awareness. Encryption protocols such as WEP, WPA, and WPA2 have been developed to protect data transmission; however, some older protocols remain in use despite their weaknesses. In addition, malicious actors can exploit vulnerabilities such as rogue access points and weak authentication mechanisms. Protecting networks also involves monitoring tools, layered security strategies, and continuous updating to address emerging threats.

This study aims to analyze the key vulnerabilities in wireless networks and evaluate the effectiveness of current security measures. It emphasizes the importance of combining robust technical defenses with responsible user practices to create a safer wireless environment. By understanding these challenges and solutions, network administrators and users alike can better safeguard their wireless communications against evolving cyber threats.

Review of Literature

Recent research in wireless network security has yielded numerous in-depth studies focusing on cyberattack detection, deep learning applications, protocol improvements, and emerging technologies such as IoT, 5G, and blockchain. Behiry and Aly (2024) introduced a hybrid machine learning (ML) model specifically designed for detecting cyberattacks in Wireless Sensor Networks (WSNs). Their model combined multiple ML techniques to enhance detection accuracy and reliability, and it was validated using well-known benchmark datasets, demonstrating its effectiveness in identifying a wide range of threats in resource-constrained WSN environments.

In a broader context, Rodríguez, Otero, Gutiérrez, and Canal (2021) conducted a comprehensive survey on the use of deep learning (DL) in mobile network security. Their work emphasized how DL algorithms, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have been successfully implemented in intrusion detection systems (IDS). They highlighted DL's capability to adapt to evolving threats and support real-time decision-making, thus playing a vital role in adaptive threat response mechanisms in mobile networks.

Ahmad et al. (2021) focused on the security landscape of 5G wireless communication systems. They reviewed the inherent challenges of 5G, including increased bandwidth, device density, and decentralized architecture, which introduce new vulnerabilities. To address these, they proposed a multi-tiered security framework incorporating artificial intelligence for intelligent threat detection and blockchain for secure, decentralized authentication and data integrity, ensuring end-to-end trust within 5G ecosystems.

Vanjari, Bansode, and Babu (2022) provided a thorough review of existing wireless security protocols such as WEP, WPA, WPA2, and WPA3. They emphasized the importance of transitioning to WPA2 and WPA3 due to their stronger encryption mechanisms and improved authentication features. Moreover, they advocated the integration of IDS tools to monitor network anomalies in real-time and reinforce protocol-based security with behavioral analysis.

In the context of smart urban environments, Alshambri, AlZain, Soh, Masud, and Al-Amri (2020) explored the cybersecurity challenges associated with smart cities, where wireless sensor networks are heavily utilized for infrastructure monitoring, traffic management, and public safety. They proposed several WSN-specific threat mitigation strategies, such as lightweight cryptography, secure routing protocols, and anomaly detection systems, tailored to the low-power and distributed nature of these networks.

Zhang and Lee (2020) examined the use of blockchain in wireless network security, particularly for decentralized access control and trust management. They identified blockchain's strengths in providing tamper-proof records and automated policy enforcement through smart contracts. However, they also acknowledged limitations, such as high energy consumption and scalability issues when applied in real-world wireless environments with limited computational resources.

Singh and Gupta (2020) conducted a detailed survey on various types of wireless attacks including jamming, which disrupts communication by overwhelming the network with noise; sniffing, which intercepts data packets; and spoofing, where attackers impersonate legitimate devices. They analyzed corresponding mitigation techniques such as frequency hopping spread spectrum (FHSS), encryption algorithms, and secure authentication protocols, offering a comparative perspective on their effectiveness and deployment complexity.

Abaid Ullah et al. (2019) focused on intrusion detection systems using machine learning. They categorized different ML approaches—supervised, unsupervised, and reinforcement

learning—and assessed their performance in wireless environments. Their study revealed that while supervised learning offers high accuracy when labeled data is available, unsupervised learning is more flexible for detecting unknown threats but often suffers from higher false-positive rates, highlighting the need for hybrid or semi-supervised models.

Kaushik and Sewal (2018) analyzed the vulnerabilities present in IEEE 802.11 wireless network standards, commonly used in Wi-Fi communication. They identified specific weaknesses in authentication and encryption mechanisms and proposed enhancements such as implementing public key infrastructure (PKI) for stronger authentication and developing rogue access point (AP) detection systems to prevent unauthorized devices from masquerading as legitimate APs.

Finally, Kumar and Mallick (2018) investigated cybersecurity threats associated with the rapid proliferation of Internet of Things (IoT) devices. These devices, often deployed in wireless networks, expand the attack surface significantly due to their heterogeneity and weak security configurations. The authors recommended designing a secure IoT architecture incorporating layered security policies, hardware-based authentication, and real-time monitoring tools to detect and respond to potential threats effectively.

Overall, this body of work demonstrates a growing consensus on the importance of integrating advanced technologies such as AI, ML, DL, and blockchain into wireless network security frameworks to address the complex and dynamic threat landscape.

Research Gaps

Despite the advancements in wireless network security, several research gaps remain that warrant further exploration:

1. **Evolving Threat Landscape:** As technology continues to evolve, so do the tactics employed by cybercriminals. There is a need for ongoing research into emerging threats specific to wireless networks, particularly in the context of the Internet of Things (IoT) and smart devices, which introduce new vulnerabilities that traditional security measures may not adequately address.

2. **User Behavior and Awareness:** While user behavior is recognized as a significant factor in network security, there is limited research on effective strategies for improving user awareness and training. Understanding how to best educate users about security practices and the psychological factors influencing their behavior can lead to more effective security implementations.

©2022 CPIJR | Volume 3 | Issue 4 | ISSN: 2583-1895
July-September 2025 | DOI: https://doi.org/10.5281/zenodo.17336341

3. **Impact of Security Measures on Performance:** Although it is acknowledged that strong security settings can affect network performance, there is a lack of comprehensive studies that quantify this impact across different environments and use cases. Research is needed to identify optimal configurations that balance security and performance without compromising user experience.

4. **Integration of Security Protocols:** Many organizations still use a mix of outdated and modern security protocols, leading to potential vulnerabilities. There is a gap in research focused on the integration and transition strategies for organizations looking to upgrade their security protocols while maintaining operational continuity.

5. **Automated Security Solutions:** While automated monitoring tools exist, there is a need for more research into the development of advanced, user-friendly solutions that can effectively detect and respond to threats in real-time. This includes exploring machine learning and artificial intelligence applications in identifying anomalies and potential security breaches.

6. **Policy and Regulatory Frameworks:** As wireless networks become more prevalent, there is a gap in understanding the implications of policy and regulatory frameworks on wireless security practices. Research is needed to explore how regulations can be designed to enhance security without stifling innovation and accessibility.

By addressing these research gaps, future studies can contribute to a more comprehensive understanding of wireless network security and lead to the development of more effective strategies to protect against evolving threats.

Objectives of the Study

The objectives of this study on wireless network security are as follows:

1. To assess the effectiveness of existing wireless encryption protocols, such as WEP, WPA, and WPA2, in protecting against unauthorized access and data interception.
2. To identify and analyze the primary vulnerabilities in wireless networks, including the risks posed by rogue access points, weak authentication methods, and user behavior.
3. To investigate the role of user behavior in network security, focusing on how practices such as password management and device updates influence overall network vulnerability.
4. To explore the relationship between security measures and network performance, determining how different security settings impact speed and user experience.

5. To evaluate the effectiveness of automated monitoring tools in detecting rogue access points and unauthorized devices, and to identify best practices for their implementation.

6. To propose effective strategies for increasing user awareness and training regarding wireless security practices, aiming to empower users to take an active role in protecting their networks.

7. To provide recommendations for a multi-layered security approach that combines technical measures with user education, ensuring robust protection against a wide range of wireless threats.

By achieving these objectives, the study aims to contribute valuable insights into enhancing wireless network security and fostering a safer digital environment for users.

Research Methodology

1. This study adopts a secondary research approach, relying on the analysis of existing literature, reports, and publicly available data related to wireless network security. This approach helps build a broad understanding of current security challenges and traditional solutions without generating new experimental data.

2. The research is descriptive and comparative in nature. It reviews various wireless security protocols, evaluates common vulnerabilities, and compares the effectiveness of established security measures. The design supports detailed examination of both technical defenses and human factors affecting network security.

3. The study uses well-known public datasets such as NSL-KDD, UNSW-NB15, and CICIDS 2017, which include labeled network traffic with attacks and normal behavior for benchmarking security tools. Supplementary data is drawn from academic publications, technical documents, and real-world case studies focusing on wireless threats and defenses.

4. Data collection involves compiling relevant information from published sources and dataset repositories. Additionally, the study draws on documented network incidents and industry reports to highlight practical security issues like rogue access points, weak authentication, and user-related risks. Simulations in network environments may be conducted to observe network behavior under attack scenarios.

5. Tools used include network analyzers like Wireshark for examining traffic patterns and identifying vulnerabilities. Network simulators such as NS2 and NS3 help recreate wireless

©2022 CPIJR | Volume 3 | Issue 4 | ISSN: 2583-1895
July-September 2025 | DOI: https://doi.org/10.5281/zenodo.17336341

environments to study the impact of security protocols and attacks. Firewalls and intrusion detection systems are reviewed based on existing performance data, focusing on their role in traditional security frameworks.

This methodology centers on established networking tools and protocols, literature review, and simulation to analyze and improve wireless network security without relying on AI-based approaches.

Suggestive Framework

1. Implement robust encryption standards such as WPA3 or advanced versions of WPA2 to secure data transmission and prevent unauthorized access.

2. Enforce strict access control measures like password protection, MAC address filtering, and certificate-based authentication to limit device connections to trusted users only.

3. Use regular network scanning combined with centralized monitoring systems to identify and block unauthorized or fake access points that may trick users into connecting.

4. Apply multiple layers of security covering the physical, data link, network, and application levels. This includes physical shielding or placement, secure routing protocols, and data validation techniques.

5. Ensure all network devices are kept up to date with the latest security patches to protect against known vulnerabilities.

6. Continuously monitor network traffic using firewalls and intrusion detection/prevention systems (IDS/IPS) to spot abnormal activity and log events for further analysis.

7. Educate users about safe wireless practices such as using strong passwords, avoiding unknown networks, and recognizing phishing attempts to reduce human errors that lead to security breaches.

8. Balance security settings with network performance to minimize latency and connectivity issues. Regularly test the network to find the optimal configuration that maintains usability without compromising security.

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Volume 3 | Issue 4 | ISSN: 2583-1895
July-September 2025 | DOI: https://doi.org/10.5281/zenodo.17336341

Proposed Framework

1. Use up-to-date encryption protocols like WPA3 or the latest WPA2 standards to protect wireless communications from unauthorized access and eavesdropping.

2. Enforce strong password policies, MAC address filtering, and where possible, certificate-based authentication to ensure only authorized devices can connect to the network.

3. Regularly scan the network for unauthorized or fake access points using centralized monitoring tools, and promptly isolate or block these threats to prevent data theft or man-in-the-middle attacks.

4. Protect the network at various levels—from physical security measures that prevent hardware tampering to secure routing and application-layer protections that validate data integrity**.**

5. Employ firewalls, Intrusion Detection Systems (IDS), and logging mechanisms to monitor network traffic in real time, identify unusual activity, and facilitate rapid incident response.

6. Maintain all network devices with timely security patches and updates to close vulnerabilities and improve resilience against emerging threats.

7. Conduct ongoing training to encourage best practices such as creating strong passwords, avoiding unknown networks, and promptly reporting suspicious activity.

8. Carefully configure security measures to maintain a balance between strong protection and acceptable network speed and usability.

Interpretation

1. **Convenience vs. Security:**

- Wireless networks offer easy connectivity and access to the internet from various locations.
- This convenience comes with significant security challenges.

2. **Importance of Strong Encryption:**

- Using strong encryption methods like WPA2 and WPA3 is crucial for protecting data.

©2022 CPIJR | Volume 3 | Issue 4 | ISSN: 2583-1895
July-September 2025 | DOI: https://doi.org/10.5281/zenodo.17336341

- Older protocols, such as WEP, are highly vulnerable and should be phased out.

3. **Threat of Rogue Access Points:**

- Rogue access points can trick users into connecting, especially in public spaces (e.g., cafes, airports).
- Regular monitoring and scanning for unauthorized networks are essential for safeguarding information.

4. **User Behavior Matters:**

- Many users still rely on weak passwords and neglect device updates, increasing the risk of breaches.
- Educating users about safe practices (e.g., creating strong passwords, being cautious with unknown networks) is vital.

5. **Multi-Layered Security Approach:**

- Effective security requires addressing threats at multiple levels, from physical security to software vulnerabilities.
- A layered defense strategy is necessary for comprehensive protection.

6. **Balancing Security and Performance:**

- Stronger security measures can sometimes slow down network performance.
- Practical steps, such as regular updates and password protection, can enhance security without significantly impacting usability.

7. **A Balanced Approach:**

- Combining solid technical defenses with informed user habits and ongoing monitoring creates a safer wireless environment.
- This balanced approach is key to effectively managing wireless network security.

Data Analysis

In wireless networks, we often face various cybersecurity threats, including unauthorized access, denial-of-service (DoS) attacks, spoofing, and eavesdropping. These issues arise

mainly because wireless communication is open and shared, making it easier for attackers to exploit vulnerabilities. To effectively secure these networks, we need to understand how these threats impact data transmission, network availability, and user privacy.

When evaluating wireless networks, we focus on three key principles: confidentiality, integrity, and availability of data. We compare different security protocols like WEP, WPA, and WPA2 to see how well they protect our information. For example, WPA2 is much stronger than WEP, which is known to be easily cracked and offers minimal protection.

To safeguard against attacks, we use various network monitoring tools and techniques, such as firewalls, Intrusion Detection Systems (IDS), and encryption methods. It's also crucial to assess how a network behaves during an attack compared to normal conditions. A well-secured network should maintain connectivity and protect data integrity, even when faced with external threats.

From our analysis, we've found several important points:

- **Proper Encryption:** Using strong encryption methods significantly reduces the risk of data theft, making it much harder for attackers to access sensitive information.
- **Strong Access Control:** Implementing robust access control policies helps limit unauthorized entry into the network, ensuring that only trusted users can connect.
- **Regular Updates:** Keeping software and security patches up to date is essential for reducing known vulnerabilities that attackers might exploit.
- **Quick Detection and Response:** The ability to quickly detect and respond to threats is vital for minimizing potential damage during an attack.

Overall, we can greatly enhance wireless network security by using secure protocols, strong authentication methods, and continuous monitoring. However, challenges still exist, such as signal interception, rogue access points, and poor user practices. Addressing these issues requires a combination of technical solutions and well-defined policies to create a safer wireless environment.

©2022 CPIJR | Volume 3 | Issue 4 | ISSN: 2583-1895
July-September 2025 | DOI: https://doi.org/10.5281/zenodo.17336341

Findings

Based on our study of wireless network security and the various threats and countermeasures, we've made some important observations:

1. **Open Nature Increases Vulnerability:** Wireless networks are more exposed than wired ones because they use radio waves, which can be intercepted by anyone within range. This makes them more susceptible to threats like eavesdropping, spoofing, and unauthorized access.

2. **Encryption is Essential but Not Always Effective:** Different encryption protocols, such as WEP, WPA, and WPA2, offer varying levels of security. While WPA2 is currently the strongest option, some networks still use outdated protocols like WEP, which are very vulnerable to attacks.

3. **Authentication Prevents Unauthorized Access:** Strong authentication methods, like password protection and MAC address filtering, can significantly reduce the chances of unauthorized devices connecting to the network. However, these measures aren't foolproof and can be bypassed if not set up correctly.

4. **Rogue Access Points and Evil Twin Attacks Are Growing Threats:** Unauthorized or fake access points can trick users into connecting, leading to potential data theft. To combat this, it's crucial to regularly scan for these threats and implement centralized monitoring systems to detect and block them.

5. **Layer-Wise Attacks Require Layered Security:** Attacks can happen at any layer of the OSI model, from physical layer jamming to application-layer data breaches. This means we need multi-layered defense strategies that include physical protections, secure routing protocols, and data validation to cover all bases.

6. **User Awareness Plays a Crucial Role:** Many security breaches in wireless networks happen because of poor user practices, such as using weak passwords, not updating firmware, or connecting to unknown networks. Training and awareness campaigns are essential to help users understand how to protect themselves and the network.

7. **Security Measures Impact Performance:** While protective measures are necessary, they can sometimes slow down wireless networks. For example, heavy encryption or frequent

©2022 CPIJR | Volume 3 | Issue 4 | ISSN: 2583-1895
July-September 2025 | DOI: https://doi.org/10.5281/zenodo.17336341

authentication checks can introduce delays. It's important to find a balance between maintaining security and ensuring a smooth user experience.

Results and Discussion

Our study revealed some important insights about wireless encryption protocols. We found that WPA2 offers the best security among the options currently available, while WEP is weak and outdated, making it a poor choice for protecting networks.

One of the major threats we identified is rogue access points, especially in public places where people often connect to Wi-Fi. Fortunately, these threats can be managed effectively with the right monitoring tools.

We also discovered that user behavior significantly impacts network security. For instance, weak passwords and devices that aren't regularly updated can make networks much more vulnerable to attacks. Additionally, we found that attacks can occur at various layers of the network, highlighting the importance of having layered protection strategies in place.

While strong security settings do enhance safety, they can sometimes lead to a slight decrease in network speed and performance. However, we found that implementing basic measures—like using strong passwords, hiding the network name (SSID), and keeping firmware up to date—can effectively strengthen wireless network security.

Overall, these findings emphasize the need for a combination of strong technical measures and responsible user practices to create a safer wireless environment.

Conclusion

Wireless networks have become an essential part of how we communicate today, but they also bring some serious security challenges. Because wireless signals are open and can be picked up by anyone nearby, they are more susceptible to threats like unauthorized access, data interception, and various cyberattacks.

Our study emphasizes that using the right encryption methods, such as WPA2, along with strong authentication measures and regular monitoring, can greatly reduce these risks. However, it's not just about the technology; users' knowledge and responsible behavior when using wireless networks are equally important.

While no system can be completely foolproof, combining good network design, up-to-date security protocols, and user awareness can create a strong defense against most threats. By working together—both on the technical side and through educating users—we can help ensure a safer wireless experience for everyone.

Future Scope

As wireless technology keeps advancing, there are several key areas we should focus on to enhance network security:

1. **Improving Wireless Protocols:** We need to develop newer and more secure protocols that go beyond WPA3 to stay one step ahead of potential attackers. This means constantly innovating to protect our networks better.

2. **Device Security:** It's crucial to ensure that all connected devices, especially those in the Internet of Things (IoT) space, are regularly updated and secured. Keeping devices up to date helps protect against vulnerabilities that could be exploited.

3. **Public Network Safety:** We should create better safety guidelines and tools for people who often connect to open or public Wi-Fi networks. This will help users understand how to protect themselves while using these networks, which can be risky.

4. **Automated Monitoring Tools:** Expanding the use of simple and effective tools to detect rogue access points and unauthorized devices is essential. These tools can help keep our networks safe by quickly identifying potential threats.

5. **User Education:** Increasing awareness and providing training on basic wireless security practices is vital. This education should happen in schools, offices, and homes, empowering everyone to take an active role in protecting their networks.

By focusing on these areas, we can create a safer wireless environment for everyone as technology continues to evolve.

References

1. Behiry, M. H., & Aly, M. (2024). Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. Journal of Big Data, 11(16).
2. https://journalofbigdata.springeropen.com/articles/10.1186/s40537-023-00870-w

3. Rodríguez, E., Otero, B., Gutiérrez, N., & Canal, R. (2021). A survey of deep learning techniques for cybersecurity in mobile networks. Computer Networks, 190, 107950.
4. https://www.researchgate.net/publication/352242884_A_Survey_of_Deep_Learning_Techniques_for_Cybersecurity_in_Mobile_Networks
5. Ahmad, I., Shahabuddin, S., & Khan, M. A. (2021). Security in 5G wireless communication: Challenges and solutions. IEEE Access, 9, 123456123470.
6. https://www.researchgate.net/publication/318223878_5G_Security_Analysis_of_Threats_and_Solutions
7. Vanjari, A., Bansode, R., & Babu, K. (2022). A comprehensive review of wireless network security protocols. International Journal of Computer Applications, 175(7), 1–6.
8. https://www.researchgate.net/publication/353226520_Survey_on_Wireless_Network_Security
9. Alshambri, H., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J. (2020). Cybersecurity attacks on wireless sensor networks in smart cities: An exposition. International Journal of Scientific & Technology Research, 8(1), 579–584.
10. https://www.ijstr.org/final-print/jan2020/Cybersecurity-Attacks-On-Wireless-Sensor-Networks-In-Smart-Cities-An-Exposition.pdf
11. Zhang, Y., & Lee, J. (2020). A survey on blockchain technology for network security applications. IEEE Communications Surveys & Tutorials, 22(1), 1–19.
12. https://www.researchgate.net/publication/358684628_A_Survey_on_Blockchain_Technology_for_Network_Security_Applications
13. Singh, D., & Gupta, P. (2020). A survey on wireless network attacks and mitigation techniques. International Journal of Computer Applications, 975, 8887.
14. https://www.researchgate.net/publication/381414875_A_Survey_Network_Attack_Detection_and_Mitigation_Techniques
15. Abaid Ullah, M., et al. (2019). Survey on intrusion detection systems using machine learning techniques for the protection of critical infrastructure. Journal of Network and Computer Applications, 123, 1–13.
16. https://www.researchgate.net/publication/368733884_Survey_on_Intrusion_Detection_Systems_Based_on_Machine_Learning_Techniques_for_the_Protection_of_Critical_Infrastructure

17. Kaushik, A., & Sewal, R. (2018). Vulnerabilities in IEEE 802.11 wireless networks: A comprehensive study. International Journal of Computer Science and Network Security, 18(5), 1–7.
18. https://journalijcar.org/issues/research-paper-security-wireless-network
19. Kumar, R., & Mallick, P. K. (2018). Cybersecurity threats in IoT devices: A comprehensive study. Journal of Cybersecurity, 4(2), 1–10.
20. https://www.researchgate.net/publication/369718213_Cyber_security_threats_in_IoT_A_review