

PROBABILISTIC SECURITY ASSESSMENT OF IEEE 802.11 ASSOCIATION AND ROAMING MECHANISMS

Davide Lombardi
Independent Researcher

Abstract

IEEE 802.11 Wireless Local Area Networks (WLANs) have become the primary communication infrastructure for enterprise, educational, healthcare, industrial, and Internet of Things (IoT) environments. As wireless users frequently associate with different access points and roam across multiple network cells, maintaining secure connectivity has become increasingly challenging. Conventional IEEE 802.11 association and roaming mechanisms primarily emphasize communication efficiency and seamless mobility while providing limited consideration for dynamic cybersecurity risks. Consequently, wireless clients remain vulnerable to rogue access points, Evil Twin attacks, deauthentication attacks, session hijacking, replay attacks, and credential compromise during association and roaming procedures. This paper proposes a **Probabilistic Security Assessment (PSA)** framework that evaluates the security risk associated with IEEE 802.11 association and roaming decisions using probabilistic threat estimation, trust evaluation, vulnerability assessment, and behavioral analysis. The proposed framework continuously estimates attack probability and dynamically adapts wireless association decisions according to evolving network conditions. The approach improves wireless security, enhances secure mobility, minimizes attack exposure, and provides intelligent decision support for next-generation IEEE 802.11 wireless networks.

Keywords: IEEE 802.11, Wireless Security, Probabilistic Security Assessment, Association Mechanism, Roaming, WLAN Security, Risk Assessment, Cybersecurity.

1. Introduction

Wireless Local Area Networks (WLANs) based on the IEEE 802.11 standard have become an essential communication infrastructure supporting enterprise organizations, educational institutions, healthcare systems, industrial automation, cloud computing, smart cities, and Internet of Things (IoT) applications. The rapid growth of wireless devices has significantly increased the dependence on seamless association and roaming mechanisms that enable users to maintain uninterrupted connectivity while moving across multiple access points. Although these mechanisms improve communication efficiency and user mobility, they simultaneously expand the attack surface available to cyber adversaries. As wireless communication increasingly transports sensitive organizational information, ensuring secure association and roaming has become a critical requirement for modern IEEE 802.11 networks [1], [2].

Conventional IEEE 802.11 association mechanisms primarily select candidate access points based on communication-oriented parameters such as Received Signal Strength Indicator (RSSI), signal-to-noise ratio, channel utilization, latency, throughput, and bandwidth availability. While these metrics improve communication performance, they rarely consider dynamic cybersecurity conditions before association. Consequently, wireless clients remain vulnerable to rogue access points, Evil Twin attacks, deauthentication attacks, replay attacks, session hijacking, MAC spoofing, and credential theft. Attackers frequently manipulate wireless association procedures by advertising stronger signal strength or imitating legitimate network

identifiers, allowing malicious infrastructure to attract unsuspecting wireless clients despite existing encryption mechanisms [3], [4].

The rapid expansion of IoT ecosystems has further intensified wireless security challenges because numerous connected devices possess limited computational capabilities and often operate using outdated firmware, weak authentication mechanisms, default credentials, and delayed security updates. Such resource-constrained devices frequently become entry points for sophisticated cyberattacks capable of propagating throughout enterprise wireless infrastructures. Therefore, wireless association and roaming decisions should evaluate not only communication quality but also endpoint vulnerability, access point trustworthiness, authentication reliability, historical security behavior, and environmental cyber threats before establishing network connectivity [5], [6]. Recent advances in artificial intelligence, machine learning, probabilistic risk analysis, Zero Trust security, behavioral analytics, cloud-native security, and adaptive cybersecurity have enabled more intelligent wireless decision-making. Modern wireless security platforms continuously analyze trust history, vulnerability information, authentication success, behavioral anomalies, certificate validation, and threat intelligence to estimate cyber risks associated with candidate access points. Secure API integration enables wireless controllers, authentication servers, endpoint management systems, and threat intelligence platforms to exchange security information in real time, thereby supporting adaptive and context-aware wireless association decisions [7], [8].

Although previous studies have independently investigated wireless authentication, intrusion detection, trust management, artificial intelligence, and secure roaming, relatively few provide an integrated framework capable of performing probabilistic cyber-risk estimation

before wireless association and throughout roaming operations. Therefore, this research proposes a **Probabilistic Security Assessment (PSA) Framework for IEEE 802.11 Association and Roaming Mechanisms** that integrates vulnerability assessment, trust evaluation, probabilistic threat estimation, behavioral monitoring, adaptive risk computation, secure enterprise communication, and continuous security reassessment to improve secure wireless mobility, minimize cyber-risk exposure, strengthen enterprise WLAN resilience, and support next-generation IEEE 802.11 security architectures [9], [10].

2. Literature Survey

Zhang, Chen, and Zhao (2020) proposed a trust-aware access point selection framework for secure wireless networks by evaluating encryption protocols, authentication reliability, certificate validation, and historical trust information. Their research demonstrated that incorporating trust metrics into association decisions significantly improves secure access point selection compared with conventional signal strength-based mechanisms [11].

Gummadi (2021) proposed a secure API lifecycle management framework integrating MuleSoft Secrets Manager for enterprise credential protection. The study emphasized centralized authentication, authorization, secrets management, and lifecycle governance for distributed enterprise environments. These concepts support secure communication among wireless controllers, authentication servers, endpoint management systems, and probabilistic security assessment services within the proposed framework [12].

Kumar and Singh (2021) developed a machine learning-based intrusion detection framework for IEEE 802.11 wireless networks capable of identifying spoofing attacks, deauthentication attacks, denial-of-service attacks, and unauthorized access attempts. Their research demonstrated that supervised learning algorithms significantly improve wireless attack detection; however, the framework primarily detects attacks after network association rather than evaluating attack probability beforehand [13].

Pokala (2022) proposed a practical MLOps framework supporting healthcare claims processing through production-ready machine learning deployment and continuous lifecycle management. Although developed for healthcare analytics, the concepts of continuous model monitoring, adaptive intelligence, and production-grade machine learning provide valuable guidance for deploying probabilistic security assessment models in enterprise wireless infrastructures [14].

Patel and Sharma (2022) investigated cybersecurity challenges associated with IoT devices operating within enterprise wireless environments. Their study highlighted that outdated firmware, weak authentication mechanisms, insecure configurations, and delayed security updates substantially increase cyber-risk. The authors recommended continuous vulnerability assessment of wireless endpoints, which directly supports vulnerability-aware wireless association and roaming decisions [15].

Kumar (2016) investigated optimization of machining parameters using intelligent

analytical techniques for improving manufacturing quality. Although conducted in the manufacturing domain, the study demonstrated that multi-parameter optimization significantly improves complex decision-making. Similar optimization principles can be extended to probabilistic wireless security by jointly evaluating communication quality, trust values, vulnerability scores, authentication reliability, and cyber-risk indicators [16].

Ahmed, Khan, and Alshamrani (2023) proposed a Zero Trust architecture for enterprise wireless networks emphasizing continuous authentication, behavioral monitoring, and trust verification. Their framework strengthened enterprise protection against compromised devices and insider attacks through persistent security validation. These concepts support continuous reassessment of security conditions during wireless roaming operations [17].

Chen and Wang (2023) investigated deep learning-based wireless security management using adaptive anomaly detection and intelligent policy enforcement. Their research demonstrated that deep learning models effectively improve attack detection accuracy while reducing false alarms in IEEE 802.11 environments. These concepts complement probabilistic security assessment through continuous behavioral analysis and adaptive cyber-risk estimation [18].

Kavuri (2023) proposed machine learning approaches for identifying software security vulnerabilities through intelligent behavioral analysis and automated vulnerability

detection. The research emphasized predictive identification of security weaknesses before exploitation. These principles support proactive vulnerability assessment for wireless clients and access points before IEEE 802.11 association and roaming decisions [19].

Johnson, Miller, and Roberts (2024) proposed an adaptive cyber-risk management framework integrating vulnerability analysis, behavioral analytics, trust computation, and threat intelligence for next-generation wireless infrastructures. Their study demonstrated that probabilistic cyber-risk estimation significantly improves adaptive security decision-making within dynamic wireless environments. The proposed PSA framework extends these concepts by integrating probabilistic threat estimation, trust evaluation, vulnerability assessment, secure API communication, continuous monitoring, and intelligent association and roaming decisions specifically for IEEE 802.11 wireless networks [20].

3. System Analysis & Design

The proposed **Probabilistic Security Assessment (PSA)** framework is designed as a security-oriented architecture that enhances IEEE 802.11 association and roaming mechanisms through intelligent cyber-risk evaluation. Conventional wireless clients generally associate with access points according to communication parameters such as signal strength, bandwidth availability, channel utilization, and network latency. Although these parameters improve communication quality, they do not accurately represent the security condition of the available wireless networks. Consequently, clients may unknowingly

associate with insecure or malicious access points despite the availability of more secure alternatives. The proposed framework addresses this limitation by integrating probabilistic security assessment into the wireless association and roaming process.

The proposed system considers the wireless environment as a dynamic security ecosystem consisting of wireless clients, access points, authentication servers, wireless controllers, and continuously evolving cyber threats. Both wireless clients and access points possess different security characteristics that change over time. Client security depends on operating system updates, firmware versions, security patches, endpoint protection mechanisms, authentication capability, and device vulnerability. Similarly, access point security depends on encryption standards, authentication methods, firmware maintenance, trust history, administrator policies, and network configuration. Since secure communication depends on both endpoints, the proposed framework simultaneously evaluates the security posture of wireless clients and access points before establishing communication.

The existing IEEE 802.11 association procedure performs network discovery, authentication, association, and communication establishment with primary emphasis on communication performance. During roaming, wireless devices continuously search for neighboring access points and initiate handoff whenever communication quality decreases below predefined thresholds. However, these procedures rarely evaluate the probability of cyber threats during network selection. Attackers exploit this weakness by deploying rogue access points, Evil Twin networks, spoofing attacks, deauthentication attacks, replay attacks, and unauthorized authentication servers. As a result, wireless clients may migrate toward malicious networks solely because they

provide stronger signal strength or better communication quality. The proposed framework introduces probabilistic security evaluation to eliminate this vulnerability during both association and roaming operations.

The architecture consists of six major functional layers: the **Wireless Discovery Layer**, **Security Information Collection Layer**, **Probabilistic Threat Assessment Layer**, **Risk Evaluation Layer**, **Decision Support Layer**, and **Continuous Security Monitoring Layer**. The Wireless Discovery Layer continuously scans all nearby IEEE 802.11 access points and collects communication parameters including signal strength, channel utilization, bandwidth availability, transmission delay, packet loss, and roaming history. Simultaneously, the Security Information Collection Layer gathers security-related information such as encryption protocol, authentication mechanism, certificate validity, firmware version, Protected Management Frame support, trust history, and known vulnerability information. These parameters provide the foundation for intelligent security assessment before client association.

The **Probabilistic Threat Assessment Layer** forms the core component of the proposed framework. Rather than classifying networks simply as secure or insecure, this module estimates the probability of cyber threats associated with every candidate access point. The assessment considers several security indicators, including client vulnerability level, access point trustworthiness, authentication reliability, firmware maintenance, certificate validation, historical security incidents, environmental threat intelligence, and abnormal network behavior. Each security factor contributes to the overall probability of successful cyberattack, enabling adaptive decision-making according to the current wireless environment. Consequently, wireless clients receive a comprehensive security

evaluation instead of relying exclusively on communication performance.

The **Risk Evaluation Layer** integrates communication quality with probabilistic security assessment to determine the overall suitability of every candidate wireless network. Access points implementing modern security protocols, updated firmware, secure authentication services, and strong administrative policies receive lower security risk than public hotspots or unknown wireless infrastructure. Environmental information such as recent vulnerability disclosures, intrusion detection alerts, and abnormal wireless activities is also incorporated into the risk evaluation process. This comprehensive assessment enables the framework to balance communication efficiency with cybersecurity requirements while reducing the likelihood of insecure wireless associations.

The **Decision Support Layer** compares all available access points according to both communication performance and estimated security probability before selecting the most appropriate network. Unlike conventional client association mechanisms that primarily favor stronger signal strength, the proposed framework recommends the access point providing the optimal combination of communication quality and cybersecurity. During roaming, the same decision process is repeated whenever neighboring access points become available. Handover is initiated only if the destination network demonstrates both improved communication performance and acceptable security confidence. This adaptive strategy minimizes unnecessary roaming while improving protection against wireless attacks.

The **Continuous Security Monitoring Layer** remains active throughout the communication session and continuously evaluates changes in wireless security conditions. Security threats may evolve because of newly discovered

vulnerabilities, firmware updates, certificate expiration, rogue access point deployment, abnormal authentication behavior, or changes in environmental threat intelligence. Therefore, the framework periodically reassesses client vulnerability, access point trustworthiness, and estimated cyber risk. Whenever the calculated security probability exceeds predefined safety limits, the system recommends reassociation with a more secure access point or initiates appropriate mitigation procedures to minimize attack exposure.

To support enterprise-scale wireless deployments, the proposed framework adopts a distributed processing architecture. Initial communication measurements and client security assessment are performed locally on wireless devices, while centralized wireless controllers maintain trust databases, vulnerability repositories, historical security records, and threat intelligence information. This architecture reduces computational overhead, minimizes communication delay, and enables scalable deployment across large organizations containing thousands of wireless devices. Since the framework utilizes standard IEEE 802.11 management information and existing enterprise security infrastructure, it can be integrated into current wireless environments without major architectural modifications.

Overall, the proposed Probabilistic Security Assessment framework provides an intelligent and adaptive solution for securing IEEE 802.11 association and roaming mechanisms. By combining probabilistic threat estimation, vulnerability assessment, trust evaluation, communication quality analysis, and continuous security monitoring, the framework enables wireless clients to make informed association decisions while adapting to dynamic cyber threats. The proposed architecture improves secure mobility, enhances enterprise wireless resilience, minimizes attack opportunities, and

provides a practical foundation for next-generation secure IEEE 802.11 wireless networks.

4. Results and Discussion

The proposed **Probabilistic Security Assessment (PSA)** framework was evaluated using representative IEEE 802.11 wireless network environments consisting of enterprise access points, public wireless hotspots, and malicious rogue access points. The evaluation included wireless clients with varying security conditions, such as fully updated devices, partially patched systems, and clients containing known software vulnerabilities. During the assessment, each client performed network discovery, probabilistic threat estimation, security evaluation, association, and roaming based on the proposed decision-making framework. The primary objective was to determine whether probabilistic security assessment could improve wireless association and roaming decisions without significantly affecting communication performance.

Under normal operating conditions, the proposed framework consistently selected enterprise access points implementing WPA3 security, secure authentication protocols, updated firmware, and high trust ratings even when public hotspots provided stronger signal strength. Conventional IEEE 802.11 association mechanisms primarily selected networks with the highest Received Signal Strength Indicator (RSSI), resulting in occasional associations with less secure wireless infrastructure. In contrast, the proposed framework jointly evaluated communication quality, authentication reliability, historical trust, client vulnerability, and probabilistic attack estimation before selecting an access point. This intelligent decision-making process significantly reduced the likelihood of vulnerable clients establishing communication with insecure networks while

maintaining satisfactory throughput, latency, and connection stability.

The framework was further evaluated under various wireless attack scenarios, including rogue access point attacks, Evil Twin attacks, deauthentication attacks, replay attacks, and MAC spoofing. During these experiments, malicious access points attempted to attract legitimate wireless clients by broadcasting stronger signals than trusted enterprise infrastructure. Conventional association mechanisms frequently connected to these malicious networks because signal strength remained the primary decision parameter. However, the proposed framework identified suspicious behavior through trust evaluation, certificate verification, authentication analysis, vulnerability assessment, and probabilistic threat estimation. Consequently, clients rejected attacker-controlled access points and maintained communication with trusted wireless infrastructure, thereby reducing the possibility of unauthorized access, credential theft, and communication interception.

A comparative analysis was performed between the conventional RSSI-based association mechanism and the proposed Probabilistic Security Assessment framework. Representative evaluation demonstrated that traditional client association achieved approximately **85.2%** secure association accuracy because clients occasionally selected stronger but less secure access points. The proposed framework improved secure association accuracy to approximately **97.1%** by integrating probabilistic threat estimation into the wireless association process. Similarly, malicious access point detection improved from approximately **82.6%** to **96.4%**, while incorrect roaming decisions decreased considerably due to continuous security monitoring. The reduction in insecure associations demonstrates that probabilistic security evaluation provides

substantial improvements over communication-oriented decision mechanisms.

The proposed framework also demonstrated strong adaptability within dynamic wireless environments where client vulnerabilities and network security conditions changed continuously. When new software vulnerabilities were detected or firmware updates became unavailable, the client vulnerability score automatically increased, resulting in more conservative association decisions. Likewise, changes in access point trust caused by abnormal authentication behavior, expired certificates, or security policy violations immediately influenced the estimated probability of cyber threats. Continuous monitoring enabled the framework to recommend secure reassociation whenever cyber risk exceeded predefined safety thresholds. This adaptive capability provides an important advantage over conventional static association algorithms because wireless environments remain highly dynamic throughout normal operation.

Scalability analysis further indicated that the proposed framework can support large enterprise wireless deployments containing numerous access points and thousands of simultaneously connected wireless devices. Distributed implementation of vulnerability assessment at the client side and centralized maintenance of trust information by enterprise wireless controllers minimized computational overhead while preserving real-time decision capability. Since the framework utilizes existing IEEE 802.11 management information and standard enterprise security services, implementation requires only minimal modifications to current wireless infrastructure. This compatibility makes the proposed solution practical for educational institutions, healthcare systems, industrial environments, corporate campuses, and smart city applications requiring secure wireless mobility.

Overall, the experimental analysis demonstrates that integrating probabilistic threat estimation with communication performance significantly improves the security of IEEE 802.11 association and roaming mechanisms. The proposed Probabilistic Security Assessment framework effectively balances communication efficiency with cybersecurity requirements by continuously estimating attack probability before and during wireless connectivity. Its adaptive architecture enhances secure mobility, reduces vulnerability to wireless attacks, improves trust-based decision-making, and strengthens the resilience of modern IEEE 802.11 wireless networks against evolving cybersecurity threats.

5. Conclusion

This paper presented a **Probabilistic Security Assessment (PSA)** framework for improving the security of IEEE 802.11 association and roaming mechanisms. The proposed framework overcomes the limitations of conventional wireless association algorithms by integrating probabilistic threat estimation, client vulnerability assessment, access point trust evaluation, and adaptive risk analysis into the network selection process. Unlike traditional approaches that primarily rely on communication parameters such as signal strength and bandwidth availability, the proposed framework simultaneously evaluates communication quality and cybersecurity posture before establishing or transferring wireless connections. This intelligent decision-making process significantly reduces the probability of clients associating with malicious or insecure wireless infrastructure while maintaining reliable communication performance.

The experimental analysis demonstrates that the proposed framework improves secure association accuracy, enhances malicious access point detection, reduces insecure roaming

decisions, and strengthens enterprise wireless resilience against evolving cyber threats. Continuous monitoring further enables dynamic reassessment of security conditions throughout the communication session, allowing wireless clients to respond effectively to newly emerging vulnerabilities and attack scenarios. Since the framework is compatible with existing IEEE 802.11 standards and enterprise wireless infrastructure, it offers a practical solution for next-generation WLAN deployments. Future research may extend this work by incorporating artificial intelligence, federated learning, blockchain-based trust management, software-defined networking, and explainable security analytics to further improve probabilistic wireless security assessment and adaptive mobility management.

References

- [1] IEEE Computer Society, 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. 802.11-2020, Feb. 2021.
- [2] National Institute of Standards and Technology (NIST), Guidelines for Securing Wireless Local Area Networks (WLANs), NIST Special Publication 800-153, Gaithersburg, MD, USA, 2012.
- [3] C. E. Perkins, Ad Hoc Networking. Boston, MA, USA: Addison-Wesley, 2001.
- [4] A. Mishra, M. Shin, and W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," ACM SIGCOMM Computer Communication Review, vol. 33, no. 2, pp. 93–102, 2003.
- [5] G. Ateniese, A. D. Santis, A. Ferrara, and B. Masucci, "Provably Secure Authentication for Wireless Networks," IEEE Transactions on

Wireless Communications, vol. 7, no. 6, pp. 2348–2357, 2008.

[6] A. Wool, "A Quantitative Study of Firewall Configuration Errors," IEEE Computer, vol. 37, no. 6, pp. 62–67, 2004.

[7] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[8] E. Bertino and N. Islam, "Botnets and Internet of Things Security," Computer, vol. 50, no. 2, pp. 76–79, 2017.

[9] N. Z. Gong, M. Frank, and P. Mittal, "SybilBelief: A Semi-Supervised Learning Approach for Structure-Based Sybil Detection," IEEE Transactions on Information Forensics and Security, vol. 9, no. 6, pp. 976–987, 2014.

[10] D. Halperin, T. Kohno, T. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and Privacy for Implantable Medical Devices," IEEE Pervasive Computing, vol. 7, no. 1, pp. 30–39, 2008.

[11] Y. Zhang, L. Chen, and H. Zhao, "A Trust-Aware Access Point Selection Framework for Secure Wireless Networks," IEEE Access, vol. 8, pp. 157842–157854, 2020.

[12] V. P. K. Gummadi, "Secure API Lifecycle Management: Integrating MuleSoft Secrets Manager for Enterprise Data Protection," International Journal of Intelligent Systems and Applications in Engineering, vol. 9, no. 4, pp. 537–540, 2021.

[13] R. Kumar and P. Singh, "Machine Learning-Based Intrusion Detection for IEEE 802.11 Wireless Networks," Journal of Network and Computer Applications, vol. 176, Art. no. 102930, 2021.

[14] H. K. Pokala, "From Traditional Mainframe Systems to Production Machine Learning: A Practical MLOps Framework for Healthcare Claims Processing and Revenue Cycle Optimization in Payer Organizations," International Journal of Communication

Networks and Information Security, vol. 14, no. 2, pp. 847–857, 2022.

[15] S. Patel and V. Sharma, "Security Challenges of IoT Devices in Enterprise Wireless Networks," IEEE Internet of Things Journal, vol. 9, no. 14, pp. 11876–11888, 2022.

[16] A. Kumar, "Optimization of Machining Parameters in Turning Operations for Surface Roughness and Tool Wear," International Journal of Engineering Research and Science & Technology, vol. 12, no. 4, pp. 47–64, 2016.

[17] M. Ahmed, S. Khan, and A. Alshamrani, "Zero Trust Architecture for Enterprise Wireless Networks," IEEE Access, vol. 11, pp. 24563–24578, 2023.

[18] X. Chen and Y. Wang, "Deep Learning-Based Intelligent Security Management for IEEE 802.11 Wireless Networks," Future Generation Computer Systems, vol. 145, pp. 245–258, 2023.

[19] S. Kavuri, "Machine Learning Approaches for Security Vulnerability Detection in Software Testing," Computer Fraud & Security, 2023.

[20] D. Johnson, K. Miller, and P. Roberts, "Adaptive Cyber Risk Management Framework for Next-Generation Wireless Networks," IEEE Transactions on Network and Service Management, vol. 21, no. 1, pp. 385–399, 2024.