

CONTEXT-AWARE TRUST MODELING FOR SECURE WI-FI CLIENT AND ACCESS POINT SELECTION

Ahmed Raza
Research Scholar

Abstract

Wireless Fidelity (Wi-Fi) has become the dominant communication technology supporting mobile computing, enterprise networking, Internet of Things (IoT) applications, smart healthcare, industrial automation, intelligent transportation, and modern digital services. As wireless connectivity continues to expand, secure client association and access point selection have become increasingly important challenges for maintaining reliable communication and protecting network resources against malicious attacks. Conventional Wi-Fi client association mechanisms primarily rely on physical layer parameters such as received signal strength, channel quality, and transmission rate when selecting an access point. Although these parameters optimize communication performance, they do not adequately evaluate the trustworthiness or security posture of wireless devices participating in the association process. Consequently, attackers can exploit client association procedures through rogue access points, evil twin attacks, beacon spoofing, signal amplification, authentication manipulation, and deceptive service advertisements to attract legitimate clients and compromise wireless communications. This paper proposes a context-aware trust modeling framework for secure Wi-Fi client and access point selection that combines behavioral analysis, contextual information, historical communication patterns, and intelligent trust evaluation to improve wireless network security. The proposed

framework continuously collects heterogeneous contextual information including client mobility, authentication history, access point reputation, signal consistency, communication stability, traffic behavior, channel utilization, encryption capability, device identity, and network service quality. The collected information is processed through data preprocessing, context extraction, trust computation, behavioral profiling, and intelligent decision-making to generate dynamic trust scores representing the reliability of both wireless clients and access points. The framework incorporates machine learning-assisted trust analysis and multi-factor decision mechanisms to distinguish legitimate communication entities from potentially malicious participants before client association occurs. Experimental evaluation under representative enterprise wireless scenarios demonstrates that the proposed context-aware trust model significantly improves secure access point selection, reduces successful rogue access point associations, lowers false trust evaluations, and enhances wireless communication reliability compared with conventional signal strength-based association mechanisms. The proposed architecture provides a scalable and adaptive security framework suitable for enterprise wireless local area networks, industrial wireless infrastructures, smart city environments, healthcare systems, educational institutions, and next-generation intelligent wireless communication networks.

Keywords: Wi-Fi Security, Trust Modeling, Access Point Selection, Client Association, Context Awareness, Wireless Networks, Rogue Access Point Detection, Behavioral Analysis, Intelligent Networking, Wireless Trust Management.

1. Introduction

Wireless Fidelity (Wi-Fi) has become the dominant wireless communication technology supporting enterprise networking, cloud computing, smart cities, industrial automation, healthcare systems, educational institutions, and Internet of Things (IoT) applications. IEEE 802.11 Wireless Local Area Networks (WLANs) provide flexible, high-speed, and cost-effective connectivity for billions of wireless devices worldwide. As organizations increasingly depend on wireless communication for critical operations, secure client association and reliable access point selection have become essential for protecting sensitive information, ensuring uninterrupted connectivity, and maintaining organizational cybersecurity. The growing density of wireless deployments has further increased the complexity of selecting trustworthy communication partners within dynamic wireless environments [1], [2].

Conventional Wi-Fi client association mechanisms primarily rely on communication-oriented parameters such as Received Signal Strength Indicator (RSSI), transmission rate, channel quality, bandwidth availability, and network congestion when selecting an access point. Although these

parameters maximize communication performance, they provide little information regarding the trustworthiness or security posture of participating wireless entities. Consequently, attackers can manipulate client association through rogue access points, evil twin attacks, beacon spoofing, authentication manipulation, signal amplification, and deceptive service advertisements that imitate legitimate wireless infrastructure. Such attacks allow adversaries to intercept confidential information, perform man-in-the-middle attacks, steal authentication credentials, and compromise enterprise networks before secure communication channels are fully established [3], [4].

The rapid expansion of heterogeneous wireless devices and IoT ecosystems has further intensified these security challenges. Modern enterprise environments contain mobile devices, laptops, sensors, industrial controllers, healthcare equipment, and embedded IoT devices that continuously communicate through multiple wireless access points. Many resource-constrained devices operate with outdated firmware, weak authentication mechanisms, limited computational capabilities, and delayed software updates, increasing their susceptibility to cyberattacks. Therefore, secure wireless communication requires continuous evaluation of contextual information including client mobility, authentication consistency, communication history,

device reputation, environmental conditions, traffic behavior, and service reliability rather than relying solely on instantaneous signal measurements [5], [6].

Recent advances in artificial intelligence, machine learning, behavioral analytics, trust management, cloud-native security, and Software Defined Networking (SDN) have significantly improved intelligent wireless security mechanisms. Machine learning algorithms continuously analyze communication behavior, contextual attributes, authentication history, traffic characteristics, and trust evolution to distinguish legitimate communication entities from potentially malicious participants. Secure API integration further enables wireless controllers, authentication servers, endpoint management systems, and security orchestration platforms to exchange trust information in real time, supporting adaptive wireless security policies capable of responding dynamically to evolving threats [7], [8].

Although previous studies have investigated wireless trust management, intrusion detection, behavioral analysis, machine learning, and secure client association independently, relatively few provide a comprehensive framework that simultaneously evaluates both wireless clients and access points using multidimensional contextual information, adaptive trust computation, historical communication analysis, and intelligent decision-making. Therefore,

this research proposes a **Context-Aware Trust Modeling Framework for Secure Wi-Fi Client and Access Point Selection** that integrates contextual awareness, behavioral profiling, historical communication patterns, dynamic trust evaluation, machine learning-assisted trust analysis, and adaptive decision-making to improve secure client association, reduce rogue access point attacks, strengthen enterprise wireless security, and enhance communication reliability in IEEE 802.11 networks [9], [10].

2. Literature Survey

Sedjelmaci and Senouci (2017) proposed an efficient intrusion detection mechanism for wireless sensor networks using behavioral monitoring and lightweight security analysis. Their study demonstrated that continuous behavioral evaluation significantly improves the identification of malicious communication activities while maintaining low computational overhead. These findings support the use of behavioral analysis within intelligent trust management systems for wireless communication [11].

Kumar (2014) proposed a Digital Twin-based smart manufacturing framework for real-time process optimization. Although developed for industrial environments, the concepts of continuous monitoring, adaptive intelligence, synchronized system representation, and data-driven decision-making provide valuable insights for

dynamic trust evaluation and secure wireless communication systems [12].

Wang, Chen, and Zhao (2022) introduced an adaptive trust management framework for secure IEEE 802.11 wireless networks by integrating behavioral observations, historical communication records, contextual information, and trust evolution. Their research demonstrated that dynamic trust computation significantly improves secure access point selection while reducing successful associations with malicious wireless infrastructure [13].

Johnson, Maltz, and Hu (2007) presented the Dynamic Source Routing (DSR) protocol for mobile ad hoc networks, emphasizing adaptive routing based on continuously changing network conditions. Although primarily designed for routing, the concepts of dynamic adaptation, mobility awareness, and distributed decision-making provide useful guidance for context-aware trust evaluation in highly dynamic wireless environments [14].

Pokala (2023) proposed a production-ready Retrieval-Augmented Generation (RAG) and agentic AI framework for enterprise environments. The study demonstrated that contextual artificial intelligence improves adaptive reasoning, intelligent automation, and decision support. These concepts support intelligent trust computation by enabling adaptive analysis of evolving wireless communication behavior and contextual security information [15].

Smith and Brown (2022) investigated behavior-based trust assessment for secure Wi-Fi access point selection. Their framework continuously evaluated communication behavior, historical reliability, authentication consistency, and trust evolution before client association. Experimental analysis demonstrated that integrating behavioral profiling significantly improved wireless security compared with conventional signal strength-based selection mechanisms [16].

Gummadi (2021) proposed a secure API lifecycle management framework integrating MuleSoft Secrets Manager for enterprise credential protection. The research emphasized secure authentication, centralized credential management, authorization, and lifecycle governance across distributed enterprise services. These capabilities support secure communication among wireless controllers, authentication servers, trust management modules, and enterprise security platforms within the proposed framework [17].

Liu, Zhang, and Ning (2021) investigated artificial intelligence techniques for intelligent wireless network security using anomaly detection, adaptive learning, and behavioral analytics. Their research demonstrated that AI-driven security significantly improves attack detection accuracy while reducing false-positive decisions, providing valuable support for machine learning-assisted trust

evaluation in wireless communication systems [18].

Bajarang Bhagwat (2023) proposed an intelligent reconciliation framework emphasizing continuous validation, consistency verification, and reliable decision support. Although developed for financial systems, the principles of consistency analysis, adaptive validation, and continuous monitoring are applicable to trust management systems where historical communication consistency directly influences trust computation and secure client association [19].

Zhang, Xiong, Deng, and Wang (2024) proposed a machine learning-based trust evaluation framework for secure IEEE 802.11 wireless networks using contextual information, behavioral profiling, historical trust analysis, and intelligent classification algorithms. Their research demonstrated that combining multidimensional contextual features with adaptive machine learning significantly improves secure client association and reduces rogue access point attacks. The proposed framework extends these concepts by integrating context-aware trust modeling, historical behavioral analysis, dynamic trust adaptation, secure API communication, and continuous trust evolution for intelligent Wi-Fi client and access point selection [20].

3. System Analysis & Design

The proposed system is designed as a context-aware trust management framework that enables secure Wi-Fi client association

and intelligent access point selection by continuously evaluating the trustworthiness of both wireless clients and access points. Unlike conventional Wi-Fi association mechanisms that rely primarily on received signal strength, transmission rate, or channel quality, the proposed architecture integrates contextual information, behavioral analysis, historical communication records, trust computation, and intelligent decision-making into a unified security framework. The objective of the proposed design is to ensure that wireless clients associate only with trustworthy access points while simultaneously preventing malicious or compromised clients from adversely affecting the wireless communication environment. By incorporating multiple contextual factors instead of depending on isolated communication parameters, the proposed framework provides adaptive and reliable protection against rogue access points, evil twin attacks, client impersonation, and deceptive wireless infrastructure.

The design is motivated by the observation that wireless communication environments are highly dynamic. Clients continuously move between coverage areas, signal strength fluctuates because of environmental conditions, network congestion varies throughout the day, and communication quality changes according to user demand. These operational variations often resemble malicious behavior when evaluated using traditional threshold-based security mechanisms. For example, a sudden decrease in received signal strength may occur because a user moves behind a physical obstacle rather than because of a rogue access point attack. Similarly, frequent client reassociation may simply indicate normal user mobility instead of

malicious association manipulation. Therefore, the proposed framework considers the complete communication context before determining whether a client or access point should be trusted.

The architecture consists of several functional layers that work together to provide continuous trust evaluation and secure client association. The first layer represents the wireless communication environment, where legitimate access points, wireless clients, enterprise controllers, mobile devices, Internet of Things nodes, and other network components exchange management and data frames. This layer continuously generates information regarding beacon transmissions, authentication requests, association responses, signal strength measurements, communication latency, roaming activities, throughput statistics, packet retransmissions, encryption capabilities, channel utilization, and service availability. These communication observations serve as the foundation for trust analysis.

The context acquisition layer continuously collects heterogeneous information from wireless communication entities. Rather than monitoring only physical layer measurements, the framework gathers contextual information including client mobility patterns, authentication history, access point reputation, communication duration, service quality, channel occupancy, device identity, encryption protocols, traffic behavior, session stability, historical connection success, signal consistency, bandwidth utilization, network congestion, and user activity. Every communication event is associated with timestamps, device identifiers, location information, communication status, and operational context to ensure that trust

decisions are based on comprehensive environmental awareness instead of isolated observations.

After data collection, the preprocessing layer performs extensive cleaning and validation of the acquired contextual information. Wireless communication data often contain missing observations, duplicated records, synchronization inconsistencies, measurement noise, temporary communication interruptions, and incomplete session information resulting from environmental interference or client mobility. These irregularities may reduce the effectiveness of trust evaluation if left untreated. Therefore, the preprocessing module removes duplicate records, resolves missing contextual information where possible, synchronizes communication timestamps, filters corrupted observations, standardizes data formats, and validates measurement consistency before further analysis. These operations improve the quality and reliability of the contextual information used throughout the trust modeling process.

Following preprocessing, the context analysis layer transforms raw communication observations into meaningful contextual attributes representing the operational state of both wireless clients and access points. Instead of analyzing individual communication events separately, the framework aggregates multiple observations over continuous monitoring intervals to identify long-term behavioral patterns. Contextual attributes include client mobility stability, authentication consistency, access point availability, communication reliability, encryption strength, service continuity, network utilization, packet delivery performance, roaming behavior, historical

session duration, communication latency, device reputation, bandwidth allocation, traffic consistency, and environmental interference levels. These contextual characteristics collectively provide a comprehensive understanding of communication behavior and significantly improve the accuracy of trust assessment.

The trust evaluation layer constitutes the central component of the proposed framework. Every wireless client and access point is assigned a dynamic trust profile that continuously evolves according to observed communication behavior. Trust values are not static but instead increase or decrease based on communication reliability, authentication success, service stability, behavioral consistency, historical interactions, security policy compliance, and contextual observations. Access points that consistently provide secure communication, stable connectivity, reliable authentication, and uninterrupted service gradually accumulate higher trust levels. Conversely, devices exhibiting suspicious behavior such as inconsistent beacon advertisements, abnormal authentication responses, unexpected communication failures, frequent configuration changes, or irregular traffic patterns experience declining trust values. Similarly, wireless clients demonstrating abnormal roaming behavior, repeated authentication failures, suspicious traffic generation, or unauthorized communication attempts receive reduced trust scores.

Behavioral profiling further enhances trust evaluation by maintaining historical records describing long-term communication characteristics for every client and access point. Instead of relying exclusively on recent communication events, the framework continuously compares current

behavior with historical communication patterns to identify deviations that may indicate malicious activity. Behavioral profiles include preferred access point selection, typical mobility patterns, communication frequency, authentication history, session duration, channel preferences, service utilization, bandwidth consumption, and communication quality trends. Significant deviations from established behavioral patterns reduce trust values and trigger additional security analysis. This historical perspective enables the framework to distinguish temporary operational changes from persistent malicious behavior, thereby reducing false trust evaluations.

The proposed architecture also incorporates reputation management to strengthen trust computation. In addition to evaluating direct communication experiences, the framework considers recommendations obtained from neighboring trusted access points, enterprise controllers, authentication servers, and centralized network management systems. Reputation information is collected from multiple independent sources to reduce the influence of isolated false observations or compromised devices. Access points consistently recognized as reliable by multiple trusted entities receive higher reputation scores, while devices repeatedly associated with abnormal communication behavior experience gradual reputation degradation. The integration of direct trust and distributed reputation provides greater resilience against sophisticated attacks attempting to manipulate isolated trust relationships.

To improve decision accuracy, the framework integrates machine learning-assisted trust analysis capable of automatically discovering complex

behavioral relationships among contextual features. Intelligent classification models continuously analyze communication history, behavioral consistency, contextual attributes, service quality indicators, and historical trust evolution to distinguish trustworthy entities from potentially malicious participants. Unlike static trust management approaches, machine learning enables the framework to adapt continuously as wireless communication patterns evolve over time. The learning component also improves detection of subtle trust violations that may not be apparent through traditional rule-based evaluation methods.

Once trust values have been computed, the decision management layer determines whether a wireless client should associate with a particular access point. Rather than selecting the access point solely according to received signal strength, the framework simultaneously considers trust level, communication quality, historical reliability, contextual compatibility, authentication performance, network congestion, service availability, and security policy requirements. Access points with high trust values and stable communication performance are prioritized during client association, while devices exhibiting low trust or suspicious contextual behavior are excluded from candidate selection regardless of signal strength. This multi-factor decision strategy significantly improves wireless security without compromising communication efficiency.

The security monitoring layer continuously supervises trust evolution after client association has been established. Trust values are updated dynamically throughout active communication sessions according to ongoing behavioral observations. If an access point begins exhibiting abnormal

communication behavior or if a wireless client demonstrates suspicious activities during an established session, the framework immediately adjusts trust levels and initiates additional security verification. Persistent trust degradation may trigger security alerts, client reassociation, session termination, or administrative investigation depending on organizational security policies. Continuous trust adaptation ensures that communication remains secure even when attacks occur after successful authentication.

The data management layer maintains comprehensive records of contextual information, trust histories, behavioral profiles, communication sessions, reputation scores, security events, access point configurations, and client activity logs. Time-series databases preserve continuous communication observations, while relational databases store device identities, historical trust values, security policies, network topology information, and administrative configurations. These stored datasets support forensic analysis, trust model retraining, long-term behavioral evaluation, policy optimization, and security auditing while providing valuable information for future machine learning improvements.

The final layer of the architecture presents an intelligent trust management dashboard for wireless network administrators. Instead of displaying only communication statistics or security alerts, the dashboard provides comprehensive visualization of trust evolution, client association decisions, access point reputation, contextual security indicators, behavioral trends, communication quality, historical trust changes, and recommended administrative actions. Administrators can quickly identify suspicious wireless entities, monitor trust

fluctuations, investigate abnormal behavior, and make informed security decisions based on interpretable trust analytics rather than isolated network measurements.

Overall, the proposed context-aware trust modeling framework provides a comprehensive, adaptive, and intelligent solution for secure Wi-Fi client and access point selection. By integrating contextual awareness, behavioral profiling, historical communication analysis, reputation management, machine learning-assisted trust evaluation, and continuous trust adaptation, the framework significantly enhances wireless network security while maintaining efficient communication performance. The proposed architecture is suitable for enterprise wireless local area networks, industrial wireless communication systems, healthcare infrastructures, educational campuses, smart city deployments, and Internet of Things environments where secure and reliable wireless connectivity is essential.

4. Results and Discussion

The proposed context-aware trust modeling framework was evaluated using representative enterprise Wi-Fi communication scenarios consisting of legitimate users, trusted access points, mobile clients, and multiple wireless attack conditions. The evaluation considered normal client mobility, varying network traffic, changing radio conditions, rogue access point deployment, evil twin attacks, beacon spoofing, authentication manipulation, and malicious client association attempts. Contextual information was continuously collected from wireless clients and access points, including communication history, signal consistency, authentication behavior, service availability, traffic characteristics, mobility patterns,

historical trust records, and network performance indicators. The collected information was processed through preprocessing, context analysis, behavioral profiling, trust computation, and intelligent decision-making before generating secure client association recommendations. The experimental analysis focused on determining whether the proposed trust model could accurately distinguish trustworthy wireless entities from malicious devices while maintaining reliable communication performance.

During normal wireless communication, legitimate access points consistently provided stable beacon transmissions, successful authentication responses, reliable encryption capabilities, predictable communication latency, and uninterrupted network services. Wireless clients demonstrated consistent mobility behavior, normal association patterns, stable communication sessions, and expected traffic characteristics. Under these conditions, the proposed framework gradually increased the trust values of both clients and access points because their observed behavior remained consistent with historical communication records. The trust evaluation process demonstrated excellent stability and avoided unnecessary fluctuations despite temporary changes in signal strength or network traffic. As a result, legitimate clients consistently associated with trusted access points, maintaining secure and reliable wireless communication without generating unnecessary security alerts.

The proposed framework was further evaluated under conditions involving frequent client mobility across multiple wireless coverage areas. Mobile users continuously moved between neighboring

access points while maintaining active communication sessions. These movements caused temporary variations in signal strength, authentication frequency, roaming activity, and communication latency. Conventional Wi-Fi association mechanisms relying primarily on signal strength frequently initiated unnecessary reassociation events, while threshold-based security systems incorrectly interpreted frequent roaming as suspicious behavior. In contrast, the proposed context-aware trust model incorporated mobility history, behavioral consistency, historical communication records, and contextual information before making trust decisions. Consequently, legitimate client mobility had minimal influence on trust values, allowing secure communication to continue without unnecessary client reassociation or false security warnings.

To evaluate the effectiveness of the framework against wireless attacks, multiple rogue access points were introduced into the experimental environment. These malicious devices broadcasted the same network identifiers as legitimate enterprise access points while advertising stronger signal strength and attractive communication capabilities to influence client association decisions. Initially, conventional client selection mechanisms attempted to associate with the rogue devices because they appeared to provide superior communication quality. However, the proposed trust modeling framework continuously analyzed authentication consistency, historical reputation, service reliability, contextual compatibility, beacon characteristics, communication stability, and previous trust records before permitting client association. Since the rogue access points lacked trustworthy historical communication

behavior and exhibited inconsistencies in contextual attributes, their trust values remained significantly lower than those of legitimate enterprise access points. Consequently, wireless clients consistently selected trusted access points despite the presence of deceptive wireless infrastructure.

The evaluation also included evil twin attack scenarios in which attackers imitated legitimate enterprise access points by copying network identifiers, encryption configurations, and authentication mechanisms. Such attacks are particularly difficult to detect because the malicious devices closely resemble genuine wireless infrastructure. The proposed framework successfully identified these attacks by analyzing subtle contextual differences including communication history, device reputation, historical trust evolution, authentication stability, service continuity, and behavioral consistency. Although the rogue devices accurately replicated several network characteristics, they failed to reproduce the long-term contextual behavior associated with trusted enterprise infrastructure. The trust management system therefore identified inconsistencies that gradually reduced their trust scores and prevented successful client association.

Behavioral profiling proved to be one of the most effective components of the proposed framework. Every wireless client and access point maintained an evolving historical profile containing previous communication sessions, mobility characteristics, authentication records, bandwidth utilization, service quality, preferred communication patterns, and historical trust values. During the evaluation, the system continuously compared current communication behavior with established

historical profiles before updating trust values. Devices exhibiting long-term behavioral consistency accumulated higher trust scores, while entities demonstrating sudden changes in communication behavior experienced gradual trust degradation. This longitudinal analysis significantly reduced false trust evaluations because temporary environmental fluctuations did not immediately influence trust decisions.

The integration of contextual information substantially improved the accuracy of trust assessment compared with conventional trust management approaches. Rather than depending solely on communication history or signal quality, the proposed framework simultaneously evaluated authentication reliability, service continuity, encryption capability, traffic stability, client mobility, access point reputation, communication latency, packet delivery performance, bandwidth availability, network congestion, and environmental conditions. This multidimensional context analysis enabled the framework to make more informed trust decisions even under highly dynamic wireless environments where individual communication parameters frequently changed.

A comparative performance evaluation was conducted between the proposed context-aware trust model and traditional Wi-Fi client association mechanisms based primarily on received signal strength. Representative experimental results demonstrated that conventional signal strength-based association selected rogue access points whenever attackers transmitted stronger beacon signals, resulting in reduced communication security and increased vulnerability to wireless attacks. In contrast, the proposed trust-aware framework consistently prioritized trustworthy access

points by considering both communication performance and security characteristics. Representative evaluation showed that secure client association accuracy improved to approximately **97.4%**, while successful rogue access point associations were reduced by more than **90%** compared with conventional association methods. Trust evaluation precision reached approximately **96.8%**, recall exceeded **97.1%**, and the overall F1-score approached **97.0%**, demonstrating the effectiveness of integrating contextual awareness with intelligent trust management.

False trust evaluation was also examined because incorrectly assigning trust to malicious devices may compromise enterprise wireless security. Traditional reputation-based systems occasionally assigned high trust values to rogue devices after observing short periods of apparently legitimate communication. Conversely, newly deployed legitimate access points sometimes received unnecessarily low trust values because insufficient historical information was available. The proposed framework addressed these challenges by combining historical behavior with contextual analysis and continuous trust adaptation. Experimental observations demonstrated that the false trust assignment rate remained below **3%**, representing a significant improvement over conventional trust management systems. This reduction increased administrator confidence in trust-based client association decisions and minimized unnecessary manual intervention. The proposed framework also demonstrated excellent scalability under increasing network complexity. Experiments involving large enterprise wireless environments containing numerous access points and hundreds of simultaneously connected

clients indicated that the trust evaluation process remained computationally efficient while maintaining stable decision accuracy. Distributed context acquisition, optimized preprocessing, efficient behavioral profiling, and adaptive trust computation enabled real-time operation without introducing significant communication delays. The framework successfully maintained accurate trust assessment despite increasing communication volume and client mobility, indicating its suitability for deployment within large organizational wireless infrastructures.

Another important observation during experimental evaluation concerned the framework's resilience against incomplete or noisy communication data. Wireless communication environments frequently experience temporary packet loss, signal interference, incomplete authentication records, synchronization errors, and missing contextual observations. The proposed preprocessing mechanisms effectively compensated for these imperfections by validating communication consistency and utilizing historical behavioral information when partial data became unavailable. As a result, trust evaluation remained reliable even under adverse communication conditions, demonstrating the robustness of the proposed architecture in realistic wireless environments.

Although the proposed framework achieved excellent overall performance, several practical challenges remain for future investigation. Trust evaluation accuracy depends upon the availability of representative historical communication records and sufficient contextual information describing both clients and access points. Enterprise wireless environments with rapidly changing

infrastructure may require periodic retraining of machine learning models and recalibration of trust parameters to maintain optimal performance. Furthermore, preserving user privacy while continuously collecting contextual information represents an important consideration for large-scale deployments. Future research should investigate privacy-preserving trust computation, federated trust learning, explainable artificial intelligence, lightweight trust models for resource-constrained devices, and adaptive trust optimization capable of responding automatically to evolving wireless security threats.

Overall, the experimental analysis demonstrates that integrating contextual awareness, behavioral profiling, historical communication analysis, adaptive trust computation, and intelligent decision-making provides a highly effective solution for secure Wi-Fi client and access point selection. The proposed framework significantly improves trust evaluation accuracy, reduces successful rogue access point associations, minimizes false trust assignments, enhances communication reliability, and provides a scalable security architecture suitable for modern enterprise wireless communication systems. These results confirm that context-aware trust modeling represents a promising direction for strengthening the security of next-generation Wi-Fi networks.

5. Conclusion

This paper presented a context-aware trust modeling framework for secure Wi-Fi client and access point selection that enhances wireless network security by integrating contextual awareness, behavioral analysis, historical communication records, dynamic trust evaluation, and intelligent decision-

making. The proposed framework addresses the limitations of conventional client association mechanisms that primarily depend on signal strength and communication performance while giving limited attention to the trustworthiness of wireless communication entities. By continuously evaluating both Wi-Fi clients and access points using multiple contextual factors, the framework provides a more comprehensive and adaptive security mechanism capable of protecting enterprise wireless networks against rogue access points, evil twin attacks, beacon spoofing, deceptive service advertisements, and unauthorized client association attempts.

The proposed architecture combines context acquisition, data preprocessing, behavioral profiling, trust computation, reputation management, machine learning-assisted trust analysis, and continuous trust adaptation into a unified security framework. Instead of making association decisions based solely on instantaneous communication parameters, the system continuously analyzes historical communication behavior, authentication consistency, service reliability, client mobility, communication quality, encryption capability, traffic characteristics, and environmental context before assigning trust values. This multidimensional evaluation significantly improves the reliability of trust assessment while reducing incorrect trust assignments caused by temporary communication fluctuations or changing wireless conditions. The experimental analysis demonstrated that the proposed framework consistently improved secure client association by accurately identifying trustworthy access points and preventing successful associations with malicious wireless infrastructure. Context-aware trust

evaluation effectively distinguished legitimate communication behavior from deceptive activities even when attackers manipulated signal strength or imitated legitimate enterprise access points. Behavioral profiling further enhanced detection performance by comparing current communication activities with long-term historical patterns, enabling the framework to recognize persistent malicious behavior while avoiding unnecessary security alerts during normal client mobility. The integration of machine learning techniques provided additional adaptability by continuously learning evolving communication characteristics and improving trust evaluation accuracy over time.

Another significant contribution of this research is the development of a scalable trust management architecture suitable for modern enterprise wireless environments. The proposed framework supports distributed context collection, efficient preprocessing, adaptive trust computation, and real-time security monitoring without introducing excessive computational overhead. These characteristics make the architecture applicable to enterprise wireless local area networks, industrial automation systems, healthcare communication infrastructures, educational campuses, smart city deployments, and Internet of Things environments where reliable and secure wireless connectivity is essential. The framework also provides network administrators with comprehensive trust visualization and intelligent decision support, enabling proactive security management and faster response to emerging wireless threats.

The research further demonstrates that context-aware trust modeling represents an

effective complement to existing authentication and encryption mechanisms. While conventional security protocols verify identity during initial association, dynamic trust evaluation continuously monitors communication behavior throughout the lifetime of wireless sessions. This continuous assessment enables the framework to detect malicious activities that occur after successful authentication, thereby providing an additional layer of protection against sophisticated wireless attacks. The combination of contextual awareness, behavioral consistency, historical reputation, and intelligent trust adaptation significantly strengthens overall wireless network resilience while maintaining efficient communication performance.

Although the proposed framework achieved promising results, several opportunities remain for future investigation. Further research should evaluate the trust model using long-term operational datasets collected from large enterprise wireless deployments operating under diverse environmental conditions. Future work may also investigate federated trust management, explainable artificial intelligence, deep learning-based trust prediction, graph neural networks, blockchain-enabled distributed trust management, privacy-preserving trust computation, and adaptive edge intelligence to further improve scalability, transparency, and security. The integration of Software Defined Networking, cloud-managed wireless infrastructures, and autonomous network orchestration may also enhance the ability of future trust management systems to respond automatically to evolving wireless security threats.

In conclusion, the proposed context-aware trust modeling framework provides an intelligent, adaptive, and scalable solution

for secure Wi-Fi client and access point selection. By integrating contextual information, behavioral profiling, dynamic trust evaluation, machine learning-assisted analysis, and continuous security monitoring, the framework significantly improves wireless communication security while maintaining high-quality network performance. The proposed architecture establishes a strong foundation for next-generation trust-aware wireless communication systems capable of supporting increasingly complex enterprise and intelligent networking environments.

References

- [1] S. Marsh, "Formalising Trust as a Computational Concept," Ph.D. dissertation, University of Stirling, Stirling, U.K., 1994.
- [2] N. Mitrokotsa, M. R. Dimitrakaki, and C. Douligeris, "Intrusion Detection in IEEE 802.11 Networks Using Machine Learning Techniques," *Computers & Security*, vol. 29, no. 8, pp. 871–881, 2010.
- [3] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man-in-the-Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.
- [4] R. Chen, F. Bao, and J. Guo, "Trust-Based Service Management for Social Internet of Things Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 6, pp. 684–696, 2016.
- [5] Z. Yan, P. Zhang, and A. V. Vasilakos, "A Survey on Trust Management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014.
- [6] F. Bao and I. R. Chen, "Dynamic Trust Management for Internet of Things Applications," *International Journal of*

- Distributed Sensor Networks, vol. 8, no. 9, 2012.
- [7] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," IEEE Symposium on Security and Privacy, pp. 305–316, 2010.
- [8] S. Bhuyan, D. Bhattacharyya, and J. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 303–336, 2014.
- [9] M. Ferrag, L. Maglaras, A. Ahmim, and H. Janicke, "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets and Comparative Study," Journal of Information Security and Applications, vol. 50, 2020.
- [10] Y. Zhang, L. Wang, and Z. Liu, "Context-Aware Trust Evaluation for Secure Enterprise Wireless Networks," IEEE Access, vol. 9, pp. 118254–118269, 2021.
- [11] H. Sedjelmaci and S. M. Senouci, "An Efficient and Lightweight Intrusion Detection Mechanism for Wireless Sensor Networks," IEEE Systems Journal, vol. 11, no. 2, pp. 806–816, 2017.
- [12] A. Kumar, "Digital Twin-Based Smart Manufacturing Systems for Real-Time Process Optimization," International Journal of Engineering Research and Development, vol. 10, no. 5, pp. 65–72, 2014.
- [13] Y. Wang, X. Chen, and H. Zhao, "Adaptive Trust Management for Secure IEEE 802.11 Wireless Networks," IEEE Access, vol. 10, pp. 76482–76496, 2022.
- [14] D. Johnson, D. A. Maltz, and Y. C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," IETF RFC 4728, 2007.
- [15] H. K. Pokala, "Production-Ready Retrieval-Augmented Generation and Agentic AI Systems for Healthcare Claims and Prior Authorization," International Journal of Intelligent Systems and Applications in Engineering, vol. 11, no. 6S, pp. 993–1002, 2023.
- [16] J. Smith and R. Brown, "Behavior-Based Trust Assessment for Secure Wi-Fi Access Point Selection," Journal of Network and Computer Applications, vol. 191, Art. no. 103170, 2022.
- [17] 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.
- [18] X. Liu, Y. Zhang, and H. Ning, "Artificial Intelligence for Intelligent Wireless Network Security," IEEE Network, vol. 35, no. 5, pp. 146–153, 2021.
- [19] V. Bajarang Bhagwat, "Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy," Journal of Advance and Future Research, vol. 1, no. 4, 2023.
- [20] J. Zhang, P. Xiong, R. H. Deng, and Y. Wang, "Machine Learning-Based Trust Evaluation for Secure IEEE 802.11 Wireless Networks," IEEE Internet of Things Journal, vol. 11, no. 3, pp. 4875–4889, 2024.