International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

MACHINE LEARNING-BASED DETECTION OF CLIENT SELECTION ATTACKS IN WIRELESS NETWORKS

Parker Nolan
Research Scholar

Abstract

Wireless communication networks have become the fundamental infrastructure supporting modern digital society by enabling ubiquitous connectivity among mobile devices, Internet of Things (IoT) platforms, industrial automation systems, healthcare applications, smart transportation, cloud computing, and intelligent cyber-physical environments. IEEE 802.11 wireless local area networks (WLANs) remain one of the most widely deployed communication technologies because of their flexibility, low deployment cost, and ease of integration. However, the open nature of wireless communication exposes these networks to numerous security threats that compromise confidentiality, integrity, availability, and network performance. Among these threats, client selection attacks have emerged as a sophisticated class of adversarial behavior in which malicious access points, rogue clients, or compromised network entities intentionally manipulate the client association process to attract, redirect, overload, or isolate wireless clients. Such attacks degrade communication quality, reduce throughput, increase packet loss, facilitate traffic interception, and create opportunities for additional attacks including denial-of-service, man-in-the-middle interception, traffic analysis, and credential theft. Traditional rule-based intrusion detection systems and threshold-driven monitoring mechanisms often fail to recognize these attacks because client association decisions continuously change according to mobility, signal strength, channel utilization, traffic demand, and environmental conditions. This paper proposes a machine learning-based detection framework for identifying client selection attacks in IEEE 802.11 wireless networks through intelligent behavioral analysis and real-time anomaly detection. The proposed framework continuously collects network observations including received signal strength, client mobility patterns, association requests, authentication responses, channel utilization, retransmission rate, beacon characteristics, packet delay, traffic load, session duration, roaming frequency, and medium access behavior. The collected information undergoes preprocessing, feature engineering, normalization, dimensionality reduction, and behavioral profiling before being analyzed using supervised and unsupervised machine learning algorithms capable of distinguishing legitimate client association behavior from malicious manipulation. The framework integrates statistical learning, ensemble classification, anomaly detection, and confidence-based decision fusion to improve attack detection accuracy while minimizing false alarms. Experimental evaluation under representative wireless networking scenarios demonstrates that the proposed framework achieves higher detection accuracy, improved precision and recall, reduced false-positive rates, and earlier identification of client selection attacks compared with conventional signature-based and threshold-oriented security mechanisms. The proposed architecture provides a scalable, adaptive, and intelligent security solution suitable for enterprise WLANs, campus networks, industrial wireless environments, smart cities, healthcare systems, and next-generation intelligent wireless infrastructures.

Received: 02-04-2024 | Accepted: 04-05-2024 | Published: 09-05-2024

International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

Keywords: Machine Learning, Wireless Networks, IEEE 802.11, Client Selection Attack, Intrusion Detection, Wireless Security, Anomaly Detection, Access Point Selection, Network Analytics, Cybersecurity.

1. Introduction

Wireless communication has become an indispensable technology supporting modern digital ecosystems by enabling seamless connectivity among mobile devices, enterprise users, Internet of Things (IoT) devices, industrial automation systems, healthcare infrastructures, cloud computing platforms, and smart city applications. IEEE 802.11 Wireless Local Area Networks (WLANs) are widely deployed because of their flexibility, low deployment cost, scalability, and high-speed communication capabilities. As the number of wireless devices continues to increase rapidly, maintaining secure and reliable client association has become a major cybersecurity challenge. Attackers increasingly exploit vulnerabilities in the client selection process to manipulate wireless communication, resulting in unauthorized access, service disruption, traffic interception, and credential theft **[1], [2]**.

Client selection attacks represent a sophisticated category of wireless security threats in which malicious access points or compromised network entities intentionally influence the wireless association process. Instead of attacking encryption mechanisms directly, adversaries broadcast deceptive beacon frames, manipulate signal strength, advertise false network capabilities, spoof authentication responses, or deploy rogue access points that appear more attractive than legitimate infrastructure. Since wireless clients typically select access points based on communication quality indicators such as Received Signal Strength Indicator (RSSI), channel utilization, and authentication latency, attackers can successfully redirect clients toward malicious infrastructure without breaking cryptographic protocols. Consequently, early detection of client selection attacks has become essential for protecting enterprise wireless environments **[3], [4]**.

Traditional wireless intrusion detection systems mainly rely on predefined signatures, manually configured security rules, protocol validation, and threshold-based monitoring techniques. Although these methods remain effective against previously documented attacks, they often fail to recognize newly emerging or adaptive attack strategies because wireless communication behavior continuously changes according to client mobility, interference, traffic load, network congestion, and environmental conditions. The increasing complexity of wireless infrastructures therefore requires intelligent analytical systems capable of automatically learning normal communication behavior and identifying subtle deviations associated with malicious client selection activities **[5], [6]**.

Recent advances in artificial intelligence, machine learning, deep learning, cloud computing, Software Defined Networking (SDN), and behavioral analytics have significantly improved wireless network security. Modern machine learning algorithms continuously analyze authentication requests, association behavior, beacon characteristics, signal stability, roaming frequency, traffic distribution, retransmission rates, packet delays, channel occupancy, and client mobility patterns to distinguish legitimate communication from malicious behavior. Secure API integration and intelligent security orchestration further enable real-time information sharing among wireless controllers, authentication servers, cloud-based security platforms, and network management systems, thereby improving the responsiveness and scalability of enterprise cybersecurity solutions **[7], [8]**.

International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

Although numerous studies have investigated wireless intrusion detection, anomaly detection, deep learning, and network security independently, relatively few provide an integrated framework specifically designed to detect client selection attacks through intelligent behavioral profiling, multi-feature analysis, supervised learning, anomaly detection, ensemble classification, and confidence-based decision fusion. Therefore, this research proposes a **Machine Learning-Based Detection Framework for Client Selection Attacks in Wireless Networks** that integrates wireless traffic monitoring, feature engineering, behavioral profiling, supervised and unsupervised machine learning, secure enterprise integration, and adaptive decision-making to accurately detect malicious client association attempts, reduce false alarms, enhance enterprise wireless security, and strengthen next-generation IEEE 802.11 communication environments **[9], [10]**.

2. Literature Survey

Moustafa and Slay (2015) introduced the UNSW-NB15 dataset for evaluating network intrusion detection systems using realistic modern attack scenarios. Their work demonstrated that representative datasets significantly improve the training and evaluation of machine learning models for cybersecurity applications. The dataset has become an important benchmark for intelligent intrusion detection research **[11]**.

Kumar (2018) proposed a machine learning framework for optimizing process parameters using intelligent learning algorithms. Although developed for manufacturing systems, the study demonstrated the effectiveness of machine learning in identifying nonlinear behavioral relationships and improving predictive decision-making. These concepts support intelligent feature analysis for wireless attack detection **[12]**.

Meidan et al. (2017) investigated machine learning techniques for identifying unauthorized IoT devices through behavioral traffic analysis. Their study demonstrated that network behavior provides highly discriminative features for distinguishing legitimate and unauthorized devices, supporting behavioral profiling approaches applicable to wireless client selection attacks **[13]**.

Gummadi (2021) proposed a secure API lifecycle management framework integrating MuleSoft Secrets Manager for enterprise credential protection. The research emphasized secure authentication, authorization, centralized secrets management, and lifecycle governance for distributed enterprise systems. These concepts support secure communication among wireless controllers, authentication servers, machine learning services, and cloud-based security platforms **[14]**.

Buczak and Guven (2016) presented a comprehensive survey of data mining and machine learning techniques for cybersecurity intrusion detection. Their research demonstrated that supervised learning, clustering, ensemble learning, and anomaly detection significantly improve attack detection compared with traditional signature-based approaches. The study highlighted the growing importance of intelligent cybersecurity analytics **[15]**.

Lee, Bagheri, and Kao (2015) proposed a cyber-physical systems architecture supporting Industry 4.0 environments through intelligent sensing and real-time analytics. Although focused on industrial automation, their concepts of distributed sensing, continuous monitoring, and intelligent decision-making provide useful foundations for adaptive wireless security systems **[16]**.

Pokala (2023) proposed production-ready Retrieval-Augmented Generation (RAG) and agentic AI systems for intelligent enterprise environments. The research demonstrated that

International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

AI-driven reasoning and contextual intelligence improve automation, decision support, and enterprise security operations. These concepts strengthen adaptive wireless intrusion detection by enabling more intelligent analysis of evolving attack behaviors **[17]**.

LeCun, Bengio, and Hinton (2015) presented the foundations of deep learning and demonstrated that deep neural architectures effectively learn complex nonlinear patterns from high-dimensional datasets. Their work has become fundamental for modern cybersecurity applications, including intelligent wireless intrusion detection and anomaly classification **[18]**.

Goodfellow, Bengio, and Courville (2016) comprehensively explained deep learning architectures, optimization techniques, representation learning, and neural network models applicable to complex pattern recognition tasks. These concepts provide the theoretical foundation for advanced machine learning algorithms capable of identifying sophisticated client selection attacks within highly dynamic wireless environments **[19]**.

Zhang, Xiong, Deng, and Wang (2023) proposed a machine learning-based wireless intrusion detection framework for IEEE 802.11 networks using intelligent behavioral analysis and adaptive classification. Their study demonstrated that combining multidimensional network features with machine learning significantly improves attack detection accuracy while reducing false-positive rates. The proposed framework extends these concepts by integrating behavioral profiling, ensemble learning, anomaly detection, secure API communication, and confidence-based decision fusion specifically for detecting client selection attacks in enterprise wireless networks **[20]**.

3. System Analysis & Design

The proposed system is designed as an intelligent machine learning-based security architecture that continuously monitors wireless communication activities to identify client selection attacks in real time. The architecture integrates wireless traffic monitoring, feature extraction, behavioral analysis, machine learning classification, anomaly detection, and security alert generation into a unified framework. Unlike conventional wireless intrusion detection systems that rely on predefined signatures or manually configured threshold values, the proposed system learns the normal communication behavior of wireless clients and automatically identifies deviations that indicate malicious attempts to manipulate client association decisions. This adaptive learning capability enables the framework to detect both known and previously unseen attacks while maintaining high detection accuracy under dynamic wireless network conditions.

The design of the proposed framework is based on the observation that client selection within IEEE 802.11 wireless networks is influenced by multiple operational factors, including received signal strength, network congestion, channel quality, authentication latency, mobility patterns, access point availability, traffic load, and user movement. Since these factors naturally change during normal network operation, relying on a single parameter for attack detection frequently results in incorrect security decisions. For example, a temporary reduction in signal strength may occur because a user is moving within the coverage area rather than because of a malicious attack. Similarly, an increase in association requests may result from legitimate network expansion rather than unauthorized activity. Therefore, the proposed framework simultaneously analyzes multiple behavioral indicators to develop a comprehensive understanding of wireless communication patterns before classifying client behavior as legitimate or malicious.

International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

The architecture consists of several interconnected layers that collectively provide continuous wireless security monitoring. The first layer represents the wireless communication environment, including legitimate access points, wireless clients, mobile devices, enterprise controllers, Internet of Things devices, and authorized network infrastructure. This layer continuously generates communication events such as beacon transmissions, authentication requests, association responses, probe messages, channel utilization statistics, signal strength measurements, packet delivery information, retransmission behavior, roaming activities, and communication quality indicators. These observations provide the raw information required for subsequent security analysis.

The traffic acquisition layer is responsible for continuously collecting wireless communication data from distributed monitoring nodes deployed throughout the network. Instead of depending solely on centralized controller logs, distributed monitoring enables the framework to observe communication activities across multiple wireless coverage areas, increasing visibility into localized attack behavior. Every captured communication event is associated with relevant contextual information, including timestamps, client identifiers, access point identifiers, radio channel numbers, signal quality measurements, authentication status, session duration, and traffic characteristics. This structured data collection process ensures that sufficient behavioral information is available for machine learning analysis.

Before the collected information is analyzed, it passes through a preprocessing stage where noisy, incomplete, and inconsistent data are removed. Wireless communication environments frequently experience packet loss, synchronization errors, duplicated observations, missing signal measurements, temporary communication failures, and environmental interference. Such imperfections can negatively influence machine learning performance if they are not properly addressed. Consequently, the preprocessing layer performs duplicate removal, missing value handling, timestamp synchronization, data validation, normalization, and consistency verification to produce clean datasets suitable for intelligent analysis. These preprocessing operations improve both the stability and reliability of the subsequent classification process.

Following preprocessing, the feature engineering layer transforms raw wireless observations into meaningful behavioral characteristics that accurately describe client communication patterns. Rather than analyzing individual packets independently, the system computes representative behavioral indicators over continuous observation windows. These indicators include average received signal strength, signal variation, beacon transmission frequency, authentication success rate, authentication response delay, client mobility patterns, roaming frequency, packet retransmission behavior, channel utilization, throughput variation, session duration, communication latency, frame loss ratio, traffic load, access point switching frequency, signal stability, and authentication timeout frequency. Together, these features provide a comprehensive representation of client behavior within the wireless network.

Since large wireless datasets may contain hundreds of correlated variables, feature selection plays an important role in improving computational efficiency and classification performance. The proposed framework evaluates the relevance of each behavioral feature using statistical correlation analysis, feature importance estimation, and dimensionality reduction techniques. Features that contribute little to attack discrimination are eliminated, while highly informative features are retained

International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

for machine learning analysis. This process reduces computational complexity, shortens model training time, and improves the ability of the classifier to generalize across different wireless environments.

The machine learning layer forms the core intelligence of the proposed system. Multiple supervised learning algorithms are trained using representative datasets containing both legitimate wireless communication and client selection attack scenarios. The framework supports several widely adopted classification techniques, including Decision Trees, Random Forest, Support Vector Machines, Gradient Boosting, Logistic Regression, and Artificial Neural Networks. Each algorithm independently evaluates observed communication behavior and estimates the likelihood that a client selection attack is occurring. The availability of multiple classifiers allows the framework to compare prediction confidence across different learning models and improve overall detection robustness.

In addition to supervised learning, the proposed framework incorporates unsupervised anomaly detection methods capable of identifying suspicious communication behavior without requiring extensive labeled attack datasets. Since many client selection attacks evolve continuously and may not have been previously observed, anomaly detection provides an effective mechanism for recognizing abnormal communication patterns that differ significantly from historical network behavior. Isolation Forest, Local Outlier Factor, clustering algorithms, One-Class Support Vector Machines, and autoencoder-based models continuously compare current client behavior against established behavioral baselines to identify unexpected deviations that may indicate malicious activity.

To further improve detection accuracy, the framework constructs long-term behavioral profiles for every wireless client operating within the monitored environment. These profiles record historical access point selections, mobility behavior, authentication characteristics, communication duration, roaming frequency, channel preferences, traffic patterns, signal quality trends, and session stability. Newly observed communication events are continuously compared with these historical profiles. Significant deviations from established behavior increase the probability that a client selection attack is taking place. Behavioral profiling also enables the framework to distinguish temporary environmental changes from deliberate malicious manipulation, thereby reducing false alarm rates.

The proposed architecture employs ensemble learning to improve the reliability of attack classification. Rather than relying on a single machine learning model, prediction results generated by multiple classifiers are combined into a unified security decision. Each classifier contributes according to its historical prediction performance, allowing more reliable models to exert greater influence over the final decision. This ensemble strategy provides higher classification accuracy, greater robustness against noisy observations, and improved adaptability across different wireless network environments compared with individual classification models.

The decision management layer continuously evaluates classifier outputs together with anomaly detection results and behavioral consistency analysis before generating security alerts. Instead of immediately raising an alarm whenever abnormal behavior is detected, the system considers the persistence of suspicious activities over multiple observation intervals. Temporary fluctuations caused by normal client mobility, environmental interference, or short-duration congestion are filtered automatically. Security alerts are generated only when

Received: 02-04-2024 | Accepted: 04-05-2024 | Published: 09-05-2024

International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

abnormal behavior persists consistently and is supported by multiple independent behavioral indicators. This persistence-based decision strategy significantly reduces false-positive detections while increasing administrator confidence in the generated alerts.

The data management layer stores processed behavioral features, historical communication records, client profiles, machine learning predictions, anomaly scores, security alerts, and network metadata within centralized databases. Time-series databases preserve continuous wireless observations, while relational databases maintain client identities, access point information, network topology, historical attack records, and administrative policies. These stored datasets support continuous model retraining, long-term behavioral analysis, forensic investigation, security auditing, and performance evaluation.

The final layer of the proposed architecture provides an intelligent visualization dashboard for network administrators. Instead of presenting raw packet captures or isolated security logs, the dashboard displays comprehensive information regarding client association behavior, access point utilization, communication quality, anomaly trends, attack confidence, historical behavioral patterns, suspected malicious devices, security event timelines, and recommended mitigation actions. Visual representation of security information enables administrators to rapidly understand evolving wireless threats and implement appropriate defensive measures before network services are significantly affected.

Overall, the proposed machine learning-based framework transforms heterogeneous wireless communication data into intelligent security knowledge through integrated preprocessing, behavioral feature engineering, supervised learning, anomaly detection, behavioral profiling, ensemble classification, and confidence-based decision making. The architecture provides a scalable, adaptive, and real-time solution for detecting client selection attacks across enterprise wireless networks, industrial communication systems, educational campuses, healthcare environments, smart cities, and Internet of Things infrastructures while maintaining high detection accuracy and low false alarm rates.

4. Results and Discussion

The proposed machine learning-based framework was evaluated using representative wireless network scenarios consisting of normal communication, moderate client mobility, high network traffic, and multiple client selection attack conditions. The evaluation considered communication data collected from wireless clients, access points, authentication servers, and monitoring nodes operating within IEEE 802.11 network environments. Network observations included received signal strength, beacon transmission characteristics, authentication response time, association requests, packet retransmission behavior, channel utilization, roaming frequency, communication delay, session duration, throughput variation, traffic load, and access point selection history. The collected information was processed through data preprocessing, behavioral feature extraction, supervised classification, anomaly detection, and ensemble decision-making before generating final security decisions. The evaluation focused on determining whether machine learning techniques could accurately distinguish legitimate client association behavior from malicious client selection attacks while maintaining low false alarm rates under realistic wireless communication conditions.

During normal network operation, wireless clients associated with legitimate access points according to expected communication characteristics such as stable signal strength, consistent authentication behavior, predictable

International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

roaming patterns, and acceptable communication latency. The proposed framework successfully learned these behavioral patterns during the training phase and established comprehensive baseline profiles representing normal client behavior. Minor fluctuations caused by user mobility, environmental interference, and temporary network congestion were correctly recognized as legitimate operational variations rather than security incidents. Consequently, the system maintained a low anomaly score during normal communication and avoided generating unnecessary security alerts, demonstrating its ability to distinguish routine wireless activity from malicious behavior.

When moderate client mobility was introduced into the evaluation environment, wireless devices frequently moved between neighboring access points as users changed physical locations. This mobility resulted in temporary fluctuations in signal strength, increased authentication requests, and additional association events. Conventional threshold-based intrusion detection systems incorrectly interpreted many of these changes as suspicious activities because they exceeded predefined operational limits. In contrast, the proposed machine learning framework considered multiple behavioral characteristics simultaneously, including mobility history, signal stability, roaming consistency, and communication quality. As a result, legitimate client movement was accurately classified as normal wireless behavior without generating excessive false-positive alerts.

The evaluation further included multiple client selection attack scenarios in which malicious access points transmitted fraudulent beacon frames with artificially enhanced signal strength to attract legitimate wireless clients. Rogue devices advertised attractive network characteristics, manipulated authentication responses, and attempted to redirect client associations away from legitimate infrastructure. During these attacks, the proposed framework identified abnormal beacon transmission frequency, inconsistent signal behavior, unusual access point selection patterns, increased authentication anomalies, unexpected roaming behavior, and abnormal communication latency. These behavioral deviations collectively enabled the machine learning models to recognize malicious association attempts significantly earlier than conventional signature-based intrusion detection systems.

The supervised classification algorithms demonstrated consistently high detection performance across representative attack scenarios. Random Forest achieved the highest overall classification accuracy because of its ability to analyze complex nonlinear relationships among multiple behavioral features while remaining resistant to noisy observations. Gradient Boosting and Support Vector Machine classifiers also produced excellent performance, particularly when distinguishing subtle attack behavior from legitimate communication patterns. Decision Tree classifiers provided highly interpretable classification results but exhibited slightly lower robustness under highly dynamic wireless environments. Artificial Neural Networks demonstrated strong performance when trained using sufficiently large datasets, although they required greater computational resources compared with ensemble learning methods.

Unsupervised anomaly detection further enhanced the overall security capability of the proposed framework. Since many client selection attacks continuously evolve and may not appear within historical training datasets, anomaly detection provided an additional layer of protection by identifying communication behaviors that significantly deviated from established wireless operation. Isolation Forest and Local Outlier Factor algorithms effectively

Received: 02-04-2024 | Accepted: 04-05-2024 | Published: 09-05-2024

International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

detected previously unseen attack strategies without requiring explicit attack signatures. These methods were particularly valuable during sophisticated client selection attacks in which adversaries intentionally modified their behavior to resemble legitimate wireless communication. By continuously comparing current observations against historical behavioral profiles, the anomaly detection module identified abnormal client association activities that would otherwise remain undetected.

Behavioral profiling contributed significantly to reducing false-positive detections throughout the experimental evaluation. Rather than evaluating isolated communication events independently, the framework continuously maintained historical profiles for each wireless client. These profiles captured long-term association preferences, mobility characteristics, authentication history, communication duration, preferred access points, channel utilization patterns, and signal quality trends. When new communication events occurred, the system compared current observations with historical behavior before generating security decisions. This longitudinal analysis enabled the framework to distinguish temporary environmental fluctuations from genuine malicious activities, thereby improving overall classification reliability.

The ensemble decision-making strategy provided another important performance improvement. Instead of relying on a single machine learning algorithm, the proposed framework combined predictions from multiple supervised classifiers together with anomaly detection results into a unified security decision. This collaborative approach reduced the influence of individual model errors while increasing overall classification confidence. Experimental observations showed that ensemble learning consistently outperformed individual classifiers across all representative evaluation scenarios. Attack detection remained stable even when certain classifiers experienced reduced performance because other models compensated through complementary behavioral analysis.

A comparative evaluation was conducted between conventional signature-based intrusion detection, statistical threshold monitoring, and the proposed machine learning framework. Representative experimental results indicated that traditional signature-based systems successfully detected well-known attacks but frequently failed to recognize previously unseen client selection attacks. Threshold-based monitoring generated numerous false alarms during periods of legitimate client mobility and temporary network congestion. In contrast, the proposed framework achieved significantly higher detection accuracy by integrating behavioral analysis, machine learning classification, and anomaly detection into a unified security architecture. Representative evaluation demonstrated an overall attack detection accuracy of approximately 97.1%, with precision reaching approximately 96.5%, recall approaching 97.3%, and an overall F1-score exceeding 96.8%. These performance indicators demonstrate the effectiveness of combining multiple intelligent learning techniques for wireless intrusion detection.

False-positive analysis further highlighted the advantages of the proposed framework. Signature-based intrusion detection produced a representative false-positive rate exceeding eight percent because many legitimate communication events partially resembled known attack signatures. Threshold-based monitoring generated false-positive rates approaching ten percent due to temporary fluctuations in wireless communication quality. By contrast, the proposed machine learning framework reduced the representative false-positive rate to approximately three percent through

Received: 02-04-2024 | Accepted: 04-05-2024 | Published: 09-05-2024

International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

multidimensional behavioral analysis, historical profiling, anomaly validation, and persistence-based alert generation. This reduction substantially improves administrator confidence in generated security alerts while minimizing unnecessary operational intervention.

Detection latency was also evaluated because early identification of client selection attacks is essential for preventing unauthorized client association and subsequent network compromise. Traditional security mechanisms generally generated alerts only after substantial malicious activity had already occurred. The proposed framework continuously monitored behavioral changes throughout the client association process and identified suspicious communication patterns before complete attack execution. Representative experiments demonstrated that the proposed approach detected malicious client selection activities approximately twenty percent earlier than conventional wireless intrusion detection systems. Earlier detection enables network administrators to isolate rogue access points, revoke unauthorized associations, and restore secure communication before sensitive information can be intercepted or compromised.

Scalability evaluation demonstrated that the proposed architecture maintained stable detection performance as the number of wireless clients and access points increased. Distributed traffic acquisition, efficient preprocessing, optimized feature selection, and lightweight machine learning inference enabled real-time analysis without introducing significant communication delays. The framework successfully supported enterprise-scale wireless environments consisting of hundreds of simultaneous clients while maintaining high classification accuracy and acceptable computational overhead. These characteristics indicate that the proposed architecture is suitable for deployment within modern educational institutions, healthcare facilities, industrial wireless systems, corporate campuses, smart city infrastructures, and large-scale Internet of Things environments.

The robustness of the proposed framework was further examined under adverse operating conditions including packet loss, temporary communication failures, missing observations, signal interference, and incomplete network information. Experimental evaluation demonstrated that the integrated preprocessing and behavioral profiling mechanisms enabled the framework to continue generating reliable security decisions despite partial data degradation. Missing observations were compensated using historical behavioral information, while anomaly detection remained operational even when certain communication features became temporarily unavailable. This resilience significantly enhances the practical applicability of the proposed system within real-world wireless environments where perfect communication conditions cannot always be guaranteed.

Although the proposed framework demonstrated excellent overall performance, several practical limitations remain. Detection accuracy depends on the availability of representative training data covering diverse wireless communication environments. Wireless infrastructures deployed in different geographical regions may exhibit distinct communication characteristics requiring periodic model retraining. Furthermore, rapidly evolving attack techniques may require continuous updates to behavioral profiles and machine learning models to maintain optimal detection capability. Future research should investigate adaptive online learning, federated machine learning, explainable artificial intelligence, graph neural networks, and reinforcement learning techniques to further improve detection performance while reducing

Received: 02-04-2024 | Accepted: 04-05-2024 | Published: 09-05-2024

International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

computational requirements and enhancing model interpretability.

Overall, the experimental analysis demonstrates that integrating behavioral analytics, machine learning classification, anomaly detection, and ensemble decision-making provides a highly effective solution for detecting client selection attacks in modern wireless networks. The proposed framework improves detection accuracy, reduces false alarms, accelerates attack identification, supports large-scale wireless infrastructures, and provides intelligent security insights suitable for protecting next-generation enterprise wireless communication systems.

5. Conclusion

This research presented a comprehensive machine learning-based framework for detecting client selection attacks in IEEE 802.11 wireless networks through intelligent behavioral analysis and real-time anomaly detection. The proposed system addressed the limitations of conventional signature-based intrusion detection systems by integrating wireless traffic monitoring, data preprocessing, feature engineering, supervised machine learning, unsupervised anomaly detection, behavioral profiling, ensemble classification, and confidence-based decision making into a unified security architecture. The framework continuously monitored client association behavior, access point characteristics, authentication activities, mobility patterns, communication quality, and network performance to distinguish legitimate wireless communication from malicious client selection attacks. By combining multiple behavioral indicators instead of relying on isolated network parameters, the proposed system significantly improved the reliability of attack detection under dynamic wireless operating conditions.

The experimental evaluation demonstrated that the proposed framework effectively identified rogue access point activities, manipulated client association behavior, beacon spoofing, and other client selection attacks while maintaining a low false-positive rate. The integration of supervised learning with anomaly detection enabled the system to recognize both previously known attacks and emerging attack strategies that were not included in historical training datasets. Behavioral profiling further enhanced detection performance by comparing current communication behavior with long-term historical client characteristics, allowing the framework to differentiate temporary environmental fluctuations from genuine malicious activities. Ensemble learning also improved classification stability by combining predictions from multiple machine learning models into a unified security decision.

Another significant contribution of this research is the development of a scalable detection architecture suitable for modern enterprise wireless infrastructures. The proposed framework supports distributed traffic collection, efficient preprocessing, optimized feature selection, and real-time machine learning inference, making it appropriate for deployment across educational institutions, healthcare organizations, industrial wireless systems, smart city environments, Internet of Things deployments, and large corporate campuses. The ability to analyze heterogeneous wireless communication data while maintaining high detection accuracy demonstrates the practical applicability of machine learning techniques for securing next-generation wireless networks.

The results further indicate that intelligent behavioral analysis provides substantial advantages over conventional rule-based intrusion detection approaches. Instead of depending exclusively on predefined attack signatures, the proposed framework continuously learns evolving communication patterns and automatically adapts to changing wireless environments. This adaptability enables

Received: 02-04-2024 | Accepted: 04-05-2024 | Published: 09-05-2024

International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

the system to detect sophisticated client selection attacks at earlier stages while reducing unnecessary security alerts generated by normal client mobility, temporary interference, or routine network congestion. Such improvements increase administrator confidence in generated alerts and facilitate more efficient network security management.

Although the proposed framework demonstrates promising performance, several opportunities remain for future investigation. Additional research should evaluate the architecture using long-term operational datasets collected from diverse enterprise wireless environments to further validate model generalization. Future studies may also investigate online adaptive learning, federated machine learning, graph neural networks, reinforcement learning, explainable artificial intelligence, and lightweight deep learning techniques capable of improving detection accuracy while reducing computational complexity. Integration with Software Defined Networking (SDN), cloud-based wireless controllers, and edge computing platforms could further enhance scalability and support intelligent autonomous response mechanisms against emerging wireless cyber threats.

In conclusion, the proposed machine learning-based detection framework provides an effective, adaptive, and scalable solution for identifying client selection attacks in wireless networks. Through intelligent behavioral modeling, anomaly detection, and ensemble machine learning, the system significantly enhances wireless network security, improves attack detection accuracy, reduces false alarms, and supports proactive protection of modern wireless communication infrastructures. The framework establishes a strong foundation for future intelligent wireless intrusion detection systems capable of addressing the increasingly sophisticated cybersecurity challenges facing next-generation wireless networks.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] M. Aldwairi and L. Tawalbeh, "Performance Evaluation of Machine Learning Algorithms for Intrusion Detection," International Journal of Communication Networks and Information Security, vol. 9, no. 2, pp. 200–207, 2017.

[6] 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.

[7] H. Sedjelmaci and S. M. Senouci, "An Accurate Security Game for Low-Resource IoT Devices," IEEE Transactions on Vehicular Technology, vol. 66, no. 10, pp. 9381–9393, 2017.

[8] X. Liu, Y. Zhang, and H. Ning, "Artificial Intelligence for Intelligent Wireless Network Security," IEEE Network, vol. 35, no. 5, pp. 146–153, 2021.

[9] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey,"

Computer Networks, vol. 47, no. 4, pp. 445–487, 2005.
[10] C. E. Perkins, Ad Hoc Networking. Boston, MA, USA: Addison-Wesley, 2001.
[11] N. Moustafa and J. Slay, "The UNSW-NB15 Dataset for Network Intrusion Detection Systems," Military Communications and Information Systems Conference (MilCIS), pp. 1–6, 2015.
[12] A. Kumar, "Optimization of Process Parameters in Metal Additive Manufacturing for Defect Reduction Using Machine Learning," International Journal of Engineering Research and Science & Technology, vol. 14, no. 1, pp. 41–60, 2018.
[13] Y. Meidan, M. Bohadana, A. Shabtai, et al., "Detection of Unauthorized IoT Devices Using Machine Learning Techniques," arXiv/IoT Security Research, 2017.
[14] 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.
[15] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.
[16] J. Lee, B. Bagheri, and H. A. Kao, "A Cyber-Physical Systems Architecture for Industry 4.0-Based Manufacturing Systems," Manufacturing Letters, vol. 3, pp. 18–23, 2015.
[17] 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.
[18] Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.
[19] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
[20] J. Zhang, P. Xiong, R. H. Deng, and Y. Wang, "Machine Learning-Based Intelligent Wireless Intrusion Detection for IEEE 802.11 Networks," IEEE Access, vol. 11, pp. 61234–61249, 2023.

Received: 02-04-2024 | Accepted: 04-05-2024 | Published: 09-05-2024