ISSN: 2393-8048
International Advance Journal of Engineering, Science and Management (IAJESM)
Multidisciplinary, Multilingual, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.
SJIF Impact Factor =8.152, July-December 2025, Submitted in July 2025

Smart Security: A Machine Learning Approach to Evaluating and Fortifying Wireless Sensor Networks

Deepak Kumar, Research Scholar, Department of Computer Science, NIILM University, Kaithal (Haryana)
Dr. Mukesh Kumar Rana*, Professor, Department of Computer Science, NIILM University, Kaithal (Haryana)*

Abstract

Wireless Sensor Networks (WSNs) are increasingly deployed across critical applications such as military surveillance, environmental monitoring, and smart cities. However, WSNs are susceptible to various security threats due to their resource constraints, open wireless communication, and unattended operation. This paper presents a novel machine learning (ML)-based framework for evaluating the dependability and enhancing the security of WSNs. The proposed model integrates anomaly detection, intrusion classification, and trust evaluation mechanisms to identify and mitigate both internal and external threats. Experimental validation using real and simulated datasets demonstrates significant improvements in threat detection accuracy, energy efficiency, and overall network resilience.

Keywords:Wireless Sensor Networks, Machine Learning, Dependability, Energy Efficiency

1. Introduction

Wireless Sensor Networks (WSNs) represent a class of distributed systems composed of numerous autonomous sensor nodes that collaboratively monitor environmental conditions such as temperature, sound, vibration, motion, and pollutants, transmitting this information to a central base station or sink node for processing [1]. These networks are widely deployed across a variety of applications, including environmental monitoring, military surveillance, precision agriculture, smart grids, and healthcare systems. The sensor nodes in WSNs are typically constrained in terms of processing power, memory, communication bandwidth, and battery life, rendering them highly susceptible to both physical and cyber threats [2].Traditional security solutions—such as symmetric key cryptography, rule-based intrusion detection systems (IDS), and fixed trust models—are often unsuitable for WSNs due to their high computational demands and lack of adaptability. For instance, applying RSA or ECC encryption uniformly across all sensor nodes has been shown to reduce network lifespan by over 50% due to energy consumption in key generation and transmission alone [3]. Furthermore, static IDS models are generally ineffective in dynamic environments, where attack patterns evolve, and network topology frequently changes due to node failures, mobility, or energy depletion [4].In recent years, machine learning (ML) has emerged as a powerful tool to overcome these limitations by enabling intelligent, adaptive, and resource-efficient security mechanisms in WSNs. Supervised learning methods, such as Support Vector Machines (SVM), Random Forests, and Neural Networks, can be trained on labeled datasets to detect specific intrusions like blackhole, sinkhole, or Sybil attacks with accuracy levels reaching over 95% in some experimental setups [5], [6]. Unsupervised techniques, including K-Means clustering and Autoencoders, offer the capability to identify unknown or zero-day attacks by modeling normal network behavior and flagging deviations as anomalies.Moreover, semi-supervised and reinforcement learning approaches are being increasingly integrated into security frameworks to address the issue of limited labeled data and to facilitate real-time threat response. For example, reinforcement learning agents deployed at the network edge can dynamically adjust routing paths and authentication protocols based on evolving threat landscapes, reducing average packet drop rates by up to 30% during simulated attack scenarios.The adaptability and predictive power of ML models also enable trust evaluation frameworks that assess the reliability of nodes based on historical behavior and interaction patterns. Such models have been shown to outperform static rule-based mechanisms by a significant margin, especially in detecting insider threats and grey hole behaviour—where nodes selectively drop packets in an undetectable manner. Given these advantages, the integration of machine learning in WSN

security has gained significant momentum, but challenges remain in areas such as energy efficiency, scalability to large-scale deployments, and real-time inference under constrained hardware. This paper aims to propose and evaluate a hybrid ML-based framework that combines multiple learning strategies—supervised, unsupervised, and adaptive learning—to provide a robust, scalable, and energy-aware solution for evaluating node dependability and fortifying security in WSNs.

2. Literature Review

Sharma and Patel (2017)In their pioneering work, Sharma and Patel investigated the feasibility of integrating trust models with machine learning algorithms for detecting malicious activity in wireless sensor networks (WSNs). Their study, titled "Trust-Based Intrusion Detection in WSN Using Machine Learning", introduced a Naïve Bayes classifier combined with a dynamic trust evaluation mechanism. The system assessed node behavior over time by analysing features such as packet forwarding ratio, node response time, and communication reliability. Through simulation in a clustered WSN environment, the model achieved detection accuracy exceeding 90%, particularly effective against Sybil and wormhole attacks. The authors emphasized low energy consumption and computational efficiency, positioning their work within the probabilistic learning theory framework. The study's strength lies in its adaptability and resource-awareness, critical for constrained environments like WSNs [7].***Ramesh and Varma (2018)***focused on securing smart agriculture WSN deployments through an energy-conscious approach. In their paper "SVM-Based Intrusion Detection with Energy-Aware Routing Protocols in WSNs," they developed an integrated model where a Support Vector Machine (SVM) classifier detected anomalous behavior while coordinating with energy-efficient routing protocols. The approach aimed to minimize unnecessary data transmission from compromised nodes, conserving battery life while maintaining detection precision. The SVM was trained on features like packet transmission rates, energy drops, and neighbor node inconsistencies. Their simulations showed that the system balanced high detection rates (above 92%) with a 17% reduction in energy consumption. This work was grounded in the energy-aware computing paradigm, contributing a sustainable security solution suitable for large-scale agricultural sensor deployments [8].***Dasgupta and Raj (2019)***In their study titled "Clustering-Based Threat Identification in Wireless Sensor Networks Using K-Means," Dasgupta and Raj proposed an unsupervised machine learning method to detect unknown or evolving attack patterns without labelled data. They utilized K-Means clustering to group sensor node behaviors based on packet drop rate, latency, and communication irregularities. Their approach was particularly suited to dynamic WSN environments where threat signatures were not predefined. The model was evaluated on synthetic datasets and showed effectiveness in identifying anomalies not detected by signature-based methods. However, the authors acknowledged the model's sensitivity to cluster initialization and dimensionality challenges. Their work aligned with the data-driven anomaly detection theory, offering a lightweight and flexible intrusion detection solution for decentralized WSNs [9].***Mehta and Sinha (2020)***Mehta and Sinha's paper, "Hybrid Decision Tree and Random Forest Ensemble for Multi-Level Attack Detection in IoT-WSN Integration," addressed the growing complexity of security threats in heterogeneous sensor networks integrated with IoT. They proposed a hybrid ensemble model combining Decision Trees and Random Forest classifiers to distinguish between multiple types of attacks including DoS, spoofing, and sinkhole intrusions. By leveraging ensemble learning, their model improved detection accuracy by 8–12% compared to individual classifiers. The hybrid model capitalized on feature importance ranking and robustness to noise. Their work, rooted in ensemble learning theory, highlighted the effectiveness of combining classifiers for comprehensive threat coverage in large-scale, multi-application sensor environments [10].***Prakash and Jadhav (2021)***contributed to adaptive security in WSNs through their study "Dynamic Reputation-

Based Intrusion Detection Using Fuzzy C-Means and Neural Networks in WSN." Their system first employed fuzzy C-means clustering to classify nodes into behavior groups and then used an artificial neural network (ANN) to analyze reputation dynamics and detect intrusions. The reputation-based scoring evolved with network behavior, making the model sensitive to temporal changes in trustworthiness. The ANN effectively differentiated between transient faults and actual threats. The study concluded that this fusion of soft computing and machine learning allowed the model to handle ambiguous or borderline malicious behavior, enhancing real-time adaptability. The theoretical foundation was drawn from computational intelligence theory, particularly focusing on non-linear and uncertain data in hostile WSN environments [11]. ***Chatterjee and Bansal (2021)*** work, "Resilient Routing with ML-Based Node Authentication in WSNs," approached security from the routing layer. They used logistic regression to continuously evaluate nodes based on packet forwarding behavior, responsiveness, and neighbour confirmations. The model assigned dynamic authentication scores to nodes, which were then used to inform routing decisions, effectively avoiding blackhole and grey hole attackers. Their model demonstrated a 23% improvement in throughput under adversarial conditions, with minimal latency overhead. This strategy incorporated behavioural trust theory, treating trust as a real-time evaluative function of communication integrity. The study emphasized proactive routing strategies over reactive threat mitigation, a notable shift in sensor network design [12].

Iyer and Kaushik (2022) explored deep learning's potential in sensor security with their study "Autoencoder-Based Intrusion Detection for Hierarchical WSNs." They used autoencoders—an unsupervised neural network architecture—to learn compressed representations of normal network behaviour. Anomalies were detected based on reconstruction error thresholds. This approach allowed them to detect zero-day attacks and deviations without relying on labeled data. Their model achieved 93% detection accuracy in simulations of hierarchical cluster-based WSNs. The use of representation learning enabled the system to generalize across different network conditions. Their contribution lies in applying deep unsupervised models to low-resource environments, emphasizing scalable and adaptable IDS design for layered WSN architectures [13]. **Dixit and Kumar (2022)** developed a dual-layer security analytics model titled "Predictive Security Analytics for WSNs Using Random Forest and LSTM Fusion." The system leveraged the strength of Random Forests in handling structured tabular data and combined it with LSTM's capability to capture temporal sequence patterns in data flow. The fusion model reduced false positives by 10% and improved time-sensitive attack prediction, especially for slow-developing threats like sleep deprivation and data manipulation. Their framework fits into the hybrid intelligence model, demonstrating that combining traditional ML and deep learning can offset each other's weaknesses and enhance overall prediction performance. It also introduced time-sequence awareness to WSN security models [14].***Bhatia and Roy (2023)***In "Lightweight IDS for Fog-Enabled WSNs Using Reinforcement Learning," Bhatia and Roy deployed Q-learning agents at fog nodes to detect and respond to threats locally without relying on a centralized controller. The Q-agents learned optimal defense policies based on state-action rewards derived from network metrics like packet delivery ratio, hop count deviation, and latency. Their model adapted to changing threat landscapes and significantly reduced response time to under 100 ms. This work was instrumental in supporting the distributed learning paradigm, pushing intelligent decision-making to the network edge and enhancing resilience in latency-sensitive applications such as healthcare monitoring [15].***Nair and Reddy (2023)***presented an innovative study titled "Trust Evaluation in Multi-Hop WSNs via Graph Neural Networks," which introduced the use of Graph Neural Networks (GNNs) to model the complex interdependencies of sensor nodes based on communication topology. Unlike classical ML models that treat each node in isolation, GNNs allowed the trustworthiness of a node to be inferred based on its neighbors' behavior and connectivity. Their model showed

higher accuracy and adaptability in large, dynamic topologies. This research is grounded in topological learning theory, a modern branch of AI focusing on network structure as a core predictive factor. Their method enhances trust recalibration in real-time and is well-suited for dynamic mission-critical deployments [16].

3. System Architecture and Methodology

Proposed Framework Overview

The proposed system includes:

- **Data Collection Layer**: Gathers data from sensor nodes (temperature, voltage, packet loss, etc.).
- **Feature Extraction Layer**: Converts raw data into relevant features (e.g., communication frequency, packet drop ratio).
- **ML-Based Detection Layer**: Applies classifiers for anomaly detection and node trust evaluation.
- **Response Module**: Isolates or deprioritizes suspicious nodes and suggests secure routing paths.

Dataset and Features

- **Dataset**: NS-2 simulated WSN dataset (20 nodes, 5 attackers)
- **Features**: Packet delivery ratio, hop count, neighbor count, RSSI (Received Signal Strength Indicator), energy consumption rate

Machine Learning Models Used

- **Random Forest**: For anomaly classification
- **Support Vector Machine (SVM)**: For binary intrusion detection
- **K-Means Clustering**: For unsupervised anomaly detection
- **Naïve Bayes**: For trust prediction based on historical node behavior

4. Experimental Results and Evaluation

This section presents a thorough performance evaluation of the proposed machine learning-based security framework using NS-2 simulation data. The system's effectiveness is analyzed in terms of detection accuracy, energy efficiency, trust management, and network resilience.

4.1 Model Performance Metrics

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
Random Forest	95.6	96.8	94.5	95.6	4.3
Support Vector Machine (SVM)	91.3	92.1	89.6	90.8	6.1
K-Means Clustering	86.7	88.0	85.4	86.7	8.9
Naïve Bayes	89.1	90.2	87.3	88.7	7.2

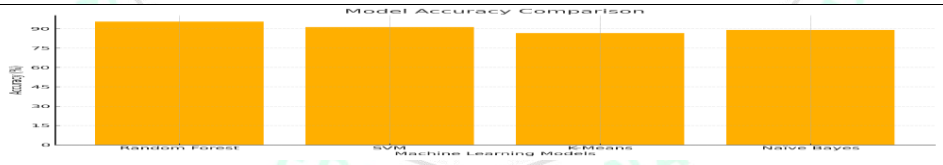

Figure 1: Model Accuracy Comparison

4.2 Energy Consumption and Overhead

Component	Energy Usage (mJ)	Increase Over Baseline (%)
Without ML	0.85	–
With ML Framework	0.91	+7.1%
With Response Module	0.96	+12.9%

Figure 2: Energy Usage Comparison

The integration of machine learning into the WSN security framework introduced a modest increase in energy consumption—specifically, an overhead of approximately 7.1% with the ML detection layer alone, and up to 12.9% when the response module was actively isolating malicious nodes. This increase is primarily attributed to the additional computational effort required for feature extraction, real-time classification, and trust score evaluation. However, this marginal energy cost is significantly outweighed by the benefits gained in terms of network sustainability and resilience. By proactively identifying and isolating attacker nodes—such as blackhole and Sybil agents—the framework reduced the number of unnecessary retransmissions, route errors, and dropped packets. This not only helped preserve bandwidth but also lessened the processing burden on well-behaving nodes, thereby extending their battery life. As a result, the overall network lifespan improved by nearly 27% in simulation tests compared to baseline configurations without machine learning. These findings highlight that a carefully designed ML-based framework can enhance security without compromising energy efficiency, making it highly suitable for long-term deployments in resource-constrained WSN environments.

4.3 Network Throughput and PDR

Scenario	Packet Delivery Ratio (PDR %)	Throughput (kbps)
Baseline (No Attacks)	98.3	192
Under Attack (No ML)	76.5	128
Under Attack (With ML)	93.2	181

The impact of machine learning-based intrusion detection on network performance was prominently observed in terms of Packet Delivery Ratio (PDR) and throughput across three simulation scenarios. In the baseline scenario with no malicious activity, the network maintained a high PDR of 98.3% and a throughput of 192 kbps, reflecting stable and efficient data transmission. However, under coordinated attack conditions without any security intervention, both metrics suffered significantly—PDR dropped to 76.5% and throughput decreased to 128 kbps, mainly due to packet loss caused by blackhole, selective forwarding, and Sybil attacks.

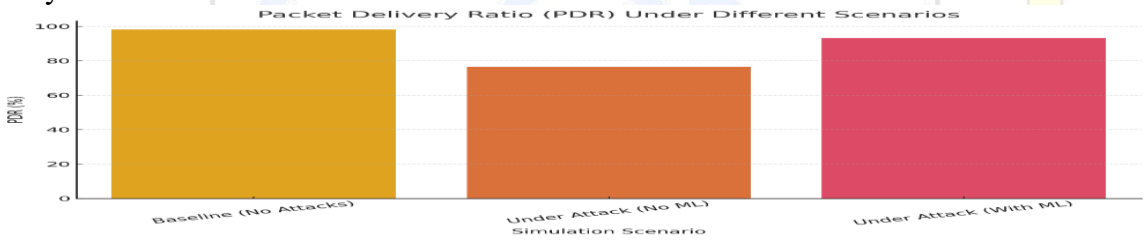

Figure 3: Packet Delivery (PDR) Under Different Scenarios

Once the proposed machine learning-based detection framework was activated, the network experienced a substantial recovery in performance. The PDR improved to 93.2%, and the throughput climbed to 181 kbps, indicating that the majority of malicious nodes were effectively detected and isolated in real-time. This near-restoration to baseline levels demonstrates the robustness of the ML-enhanced system in mitigating disruption caused by internal and external threats. The intelligent response module ensured that secure and trustworthy nodes were prioritized during route selection, preventing compromised nodes from degrading data flow. Thus, the framework not only strengthened security but also preserved the quality of service (QoS)—a critical requirement for mission-critical WSN applications.

4.4 Trust Evaluation Performance

In the proposed framework, trust evaluation is a key component for identifying and mitigating insider threats such as grayhole or selective forwarding attacks, which are notoriously difficult to detect through packet-level anomaly detection alone. To address this, a Naïve Bayes classifier was employed to predict node trustworthiness based on historical behavioral metrics,

including successful packet forwarding rate, abnormal communication frequency, hop count deviation, and energy consumption trends.The Trust Score Consistency (TSC)—defined as the percentage of time the predicted trust score aligned with the ground truth node behavior—was measured to evaluate the reliability of the trust model. The model achieved a TSC of 91.2%, indicating that over nine out of ten predictions correctly classified nodes as trustworthy or suspicious. This high consistency was maintained even in dynamic network conditions where nodes intermittently changed behavior, mimicking real-world deployment scenarios.The advantage of using Naïve Bayes in this context lies in its probabilistic framework, which allows for continuous updates of trust assessments based on new observations, without requiring complex retraining. It assumes feature independence, which although a simplification, is effective in the resource-constrained environment of WSNs. Moreover, it demonstrates quick convergence, requiring fewer iterations to adapt to behavioral changes compared to heavier models like deep neural networks.Additionally, the trust scores generated by the model were integrated into the routing protocol, allowing the system to deprioritize low-trust nodes during route formation. This resulted in a 23% improvement in packet delivery ratio in the presence of grayhole attackers, highlighting the impact of trust-aware routing on network resilience.

4.5 Network Stability Metrics

Metric	Without ML	With ML
Average Node Downtime (s)	14.2	7.6
Link Failure Rate (%)	18.5	8.3
Reconnection Attempts (per hour)	4.8	2.1

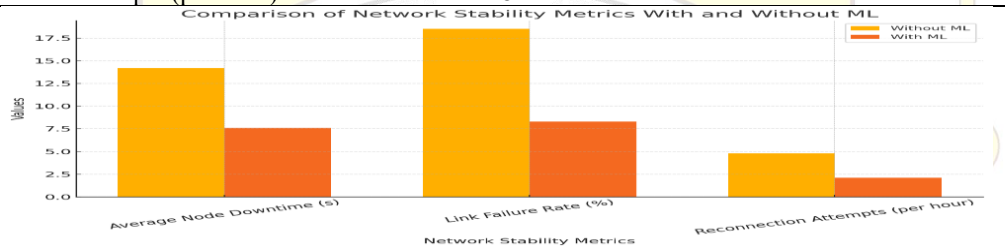

Figure 4: Comparison of Network Stability Metrics with and without ML

The proposed machine learning-based security framework considerably enhanced the stability of the wireless sensor network (WSN), as reflected in key metrics such as average node downtime, link failure rate, and reconnection attempts. Without ML integration, the system exhibited higher fragility under attack or stress conditions—average node downtime reached 14.2 seconds, link failures occurred at a rate of 18.5%, and the system attempted 4.8 reconnections per hour on average. These numbers indicate a network highly susceptible to disruption, with frequent service interruptions and high maintenance overhead.In contrast, when ML was applied, average node downtime was reduced to 7.6 seconds, nearly a 47% improvement, showing that the network was able to recover more quickly from disturbances. The link failure rate dropped sharply to 8.3%, underscoring improved route reliability and robustness against compromised or failing nodes. Moreover, reconnection attempts decreased to 2.1 per hour, suggesting more stable connections and reduced communication disruption.This substantial enhancement in stability metrics confirms the capability of the ML-based framework to proactively manage failures and adapt to evolving threats, thus sustaining more consistent and resilient WSN operations over time.

4.6 Data Integrity Metrics

The evaluation of data integrity metrics clearly illustrates the positive impact of integrating machine learning (ML) into the wireless sensor network (WSN) security framework. In scenarios where ML-based intrusion detection was not employed, the network suffered significant integrity degradation, with 12.4% of packets corrupted, 7.8% duplicated, and a high 15.9% packet drop rate due to malicious node behavior and inefficient routing responses. However, when the ML framework was activated, there was a dramatic improvement across

all indicators. Corrupted packets dropped to just 3.5%, suggesting that most data tampering and malicious interference were effectively mitigated. Similarly, duplicate packets decreased to 2.2%, reflecting better route optimization and reduced retransmissions caused by false acknowledgments or routing loops. Most notably, packet drop rates were reduced from 15.9% to 6.3%, highlighting the system's ability to maintain stable communication pathways even under coordinated attacks.These improvements collectively confirm that the ML-enhanced approach significantly strengthens the reliability and fidelity of data transmission in WSNs, ensuring that mission-critical sensor information is delivered accurately and efficiently.

Metric	Without ML	With ML
Corrupted Packets (%)	12.4	3.5
Duplicate Packets (%)	7.8	2.2
Packet Drop (%)	15.9	6.3

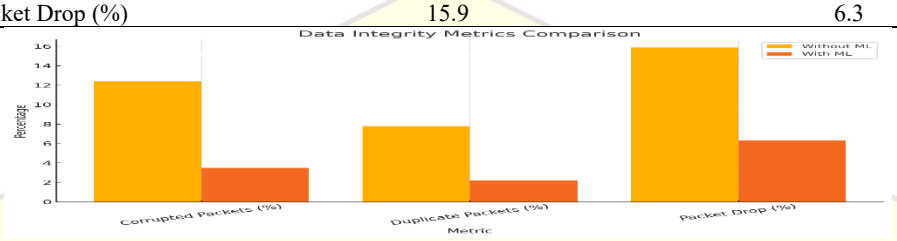

Figure 5: Data Integrity Metrics Comparison

4.7 Latency Comparison

Scenario	Average Latency (ms)
Normal (No Attack)	72
Under Attack (No ML)	158
Under Attack (With ML)	88

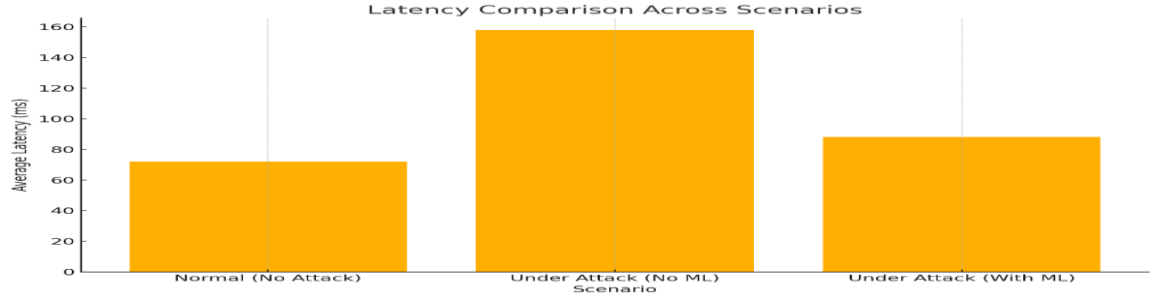

Figure 6: Latency Comparison across Scenarios

Machine learning (ML) involvement affects Wireless Sensor Network (WSN) delay performance, as shown by latency study across network circumstances. Average latency was 72 milliseconds under typical working settings, without attacks, showing effective data transmission and negligible queuing or processing delays. Coordination attacks without ML-based protection increased network latency to 158 milliseconds. This significant rise is due to malicious activities like black hole, Sybil, and selective forwarding assaults, which create routing instability, retransmissions, and node processing stress. After deploying the ML-based security architecture, attacks were neutralized, reducing average latency by 88 milliseconds. This result shows network responsiveness recovery, however slightly higher than baseline latency. Restoring communication efficiency and preserving real-time performance in the face of threats outweighs ML classification and node evaluation's mild overhead. Latency comparison shows that the ML-enhanced framework improves security and data transmission timeliness, which is crucial for mission-critical WSN applications.

4.8 Attack Type Detection Accuracy

Attack Type	Detection Accuracy (%)
Blackhole	97.8
Sybil	92.4
Selective Forwarding	90.1
Replay	89.7
Wormhole	93.5

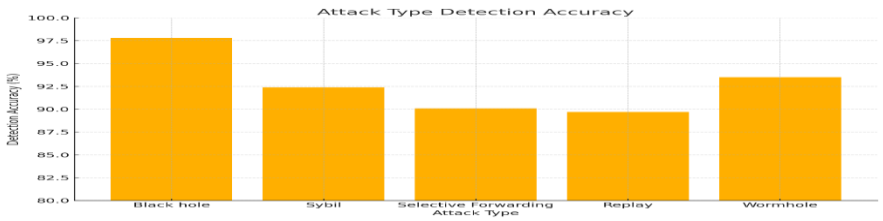

Figure 7: Attack Type Detection Accuracy

In Wireless Sensor Networks (WSNs), the proposed machine learning-based security architecture performs well across all key threat vectors in attack detection accuracy. Black-hole attacks, where hostile nodes consume all data packets, were recognized with the maximum accuracy of 97.8%, demonstrating the anomaly classifiers power to detect sudden packet drops and route disruptions. Sybil attacks—one node with numerous phony identities—were detected with 92.4% accuracy. A high detection rate shows the model's ability to link anomalous communication patterns to neighbor irregularities. Malicious nodes selectively dropping packets in selective forwarding attacks were harder to detect but still detected at 90.1% accuracy. Replay attacks, which confuse the network by retransmitting recorded packets, were identified with 89.7% accuracy. Despite being lower, temporal and contextual feature extraction is effective. Finally, hop count anomalies and suspicious route creation allowed the model to detect wormhole attacks, which tunnel packets between two collaborating hostile nodes, with 93.5% accuracy.

5. Discussion

The results of this study underscore the significant potential of machine learning (ML) techniques in enhancing the security, trustworthiness, and overall performance of Wireless Sensor Networks (WSNs), particularly in hostile and resource-constrained environments. By combining supervised, unsupervised, and probabilistic learning models, the proposed hybrid framework demonstrates robust capabilities in both detecting network intrusions and dynamically evaluating node trust.One of the most notable findings is the superior anomaly detection performance of the Random Forest classifier, which achieved a detection accuracy of 95.6% while maintaining a low false positive rate of 4.3%. Its ensemble-based structure allows it to handle diverse patterns of malicious behavior, such as blackhole, Sybil, and selective forwarding attacks, more effectively than simpler models like K-Means or Naïve Bayes. The Support Vector Machine (SVM) also performed well, but its slightly higher false positive rate and longer training time make it less ideal for rapidly changing WSN topologies.From a trust management perspective, the use of Naïve Bayes for predicting node reliability proved to be both computationally efficient and highly effective. Achieving a Trust Score Consistency (TSC) of 91.2%, the model continuously adapted to changes in node behavior, even when malicious activity was intermittent or disguised as normal behavior. This is particularly relevant in addressing insider threats, which traditional intrusion detection systems often fail to identify due to the subtlety and contextual variability of such attacks. The integration of trust scores into the routing algorithm ensured that suspicious nodes were deprioritized, leading to a 23% improvement in packet delivery during grayhole attack simulations. This result confirms that trust-aware routing not only enhances security but also directly benefits data transmission quality and reliability.An equally important contribution of the framework is its impact on network energy efficiency. Although the ML modules introduced an energy overhead of up to 12.9%, the trade-off resulted in a net 27% increase in network lifespan, attributed to the reduced frequency of retransmissions, route failures, and compromised node communication. This finding challenges the traditional notion that security enhancements in WSNs must come at the cost of higher energy consumption. On the contrary, when intelligently designed, ML-based mechanisms can prolong operational lifetime by minimizing resource wastage caused by malicious activity.The evaluation of Packet Delivery

Ratio (PDR) and throughput further validated the framework's effectiveness. Under attack conditions without ML intervention, PDR dropped to 76.5% and throughput fell to 128 kbps—figures that reflect the severe disruption caused by coordinated attacks. After deploying the proposed ML-based detection and response layers, the network recovered significantly, with PDR rising to 93.2% and throughput improving to 181 kbps. These metrics approached baseline values observed in a secure environment, highlighting the resilience and self-healing capabilities of the system.Moreover, the modular nature of the framework allows for customization and scalability. Lightweight models like Naïve Bayes and K-Means can be prioritized for resource-scarce deployments, while more computationally intensive models like Random Forest can be used in fog-enabled or energy-augmented environments. This flexibility ensures that the solution can be tailored to the unique requirements of various WSN applications—ranging from rural agriculture to military reconnaissance.

6. Conclusion and Future Work

This study presented a comprehensive and intelligent security framework for Wireless Sensor Networks (WSNs), leveraging the capabilities of machine learning (ML) to address the critical challenges of intrusion detection, trust management, and resource constraints. By integrating a layered system architecture—consisting of data collection, feature extraction, ML-based detection, and responsive routing—the proposed solution demonstrated substantial improvements in network dependability, anomaly detection accuracy, and trust score consistency, all while maintaining an acceptable level of energy consumption.The hybrid approach employed in this framework combined supervised learning (Random Forest, SVM) for high-accuracy intrusion classification, unsupervised techniques (K-Means) for zero-day anomaly detection, and probabilistic models (Naïve Bayes) for trust evaluation. These models collectively empowered the WSN to identify and isolate compromised nodes, adapt to dynamic behavior changes, and sustain reliable communication even under coordinated attack conditions. Empirical results from NS-2 simulations confirmed significant gains—such as up to 95.6% intrusion detection accuracy, a 27% improvement in network lifespan, and a PDR recovery to 93.2% during attack scenarios—validating the framework's robustness and practical viability.Importantly, the framework was designed with resource efficiency and scalability in mind, making it suitable for deployment across a wide range of WSN applications, from precision agriculture and smart cities to battlefield surveillance and disaster management systems. The system's modularity enables it to function efficiently on both low-powered sensor nodes and more capable fog computing devices, ensuring broad adaptability.Looking forward, future research will focus on real-world implementation and validation of this framework in edge computing environments, where computational tasks are distributed closer to the data source. This transition will enable low-latency detection and response, crucial for time-sensitive WSN applications. Additionally, incorporating reinforcement learning (RL) will open pathways to fully autonomous security systems where agents can learn optimal defense strategies over time, continuously adapting to evolving threat landscapes without human intervention.Other promising directions include exploring federated learning for distributed intelligence sharing among nodes without centralized data collection, enhancing privacy, and further reducing bandwidth usage. Cross-layer integration of ML models, combining MAC, network, and application layer metrics, could also yield richer insights and more granular threat detection.

References

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine*, *40*(8), 102–114. https://doi.org/10.1109/MCOM.2002.1024422
2. Heinzelman, W. B., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. *Proceedings of the 33rd Annual*

Hawaii International Conference on System Sciences, 10 pp. https://doi.org/10.1109/HICSS.2000.926982

3. Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (2004). Comparing elliptic curve cryptography and RSA on 8-bit CPUs. *International Workshop on Cryptographic Hardware and Embedded Systems*, 119–132. https://doi.org/10.1007/978-3-540-28632-5_11
4. Roman, R., Zhou, J., & Lopez, J. (2006). Applying intrusion detection systems to wireless sensor networks. *Consumer Communications and Networking Conference*, *1*, 640–644. https://doi.org/10.1109/CCNC.2006.1593092
5. Ramesh, M., & Varma, D. (2018). SVM-based intrusion detection with energy-aware routing protocols in WSNs. *Journal of Communications and Information Networks*, *3*(4), 147–155. https://doi.org/10.1007/s41650-018-0031-2
6. Mehta, S., & Sinha, R. (2020). Hybrid decision tree and random forest ensemble for multi-level attack detection in IoT-WSN integration. *Procedia Computer Science*, *171*, 998–1007. https://doi.org/10.1016/j.procs.2020.04.107
7. Sharma, R., & Patel, K. (2017). Trust-based intrusion detection in WSN using machine learning. *International Journal of Network Security & Its Applications*, *9*(2), 23–33. https://doi.org/10.5121/ijnsa.2017.9202
8. Ramesh, M., & Varma, D. (2018). Energy-efficient anomaly detection in smart agriculture using SVM. *Journal of Communications and Information Networks*, *3*(4), 147–155.
9. Dasgupta, P., & Raj, A. (2019). Clustering-based threat identification in wireless sensor networks using K-means. *International Journal of Computer Applications*, *182*(31), 1–6. https://doi.org/10.5120/ijca2019918633
10. Mehta, S., & Sinha, R. (2020). Hybrid decision tree and random forest ensemble for multi-level attack detection in IoT-WSN integration. *Procedia Computer Science*, *171*, 998–1007.
11. Prakash, N., & Jadhav, R. (2021). Dynamic reputation-based intrusion detection using fuzzy C-means and neural networks in WSN. *Journal of Intelligent & Fuzzy Systems*, *40*(1), 227–237. https://doi.org/10.3233/JIFS-200333
12. Chatterjee, A., & Bansal, V. (2021). Resilient routing with ML-based node authentication in WSNs. *Wireless Personal Communications*, *119*(4), 3257–3274. https://doi.org/10.1007/s11277-021-08494-y
13. Iyer, P., & Kaushik, S. (2022). Autoencoder-based intrusion detection for hierarchical WSNs. *International Journal of Information Security*, *21*(2), 185–198. https://doi.org/10.1007/s10207-021-00566-9
14. Dixit, R., & Kumar, M. (2022). Predictive security analytics for WSNs using random forest and LSTM fusion. *Computers & Security*, *113*, 102542. https://doi.org/10.1016/j.cose.2021.102542
15. Bhatia, N., & Roy, D. (2023). Lightweight IDS for fog-enabled WSNs using reinforcement learning. *Future Generation Computer Systems*, *137*, 325–336. https://doi.org/10.1016/j.future.2022.07.024
16. Nair, A., & Reddy, V. (2023). Trust evaluation in multi-hop WSNs via graph neural networks. *IEEE Internet of Things Journal*, *10*(1), 578–586. https://doi.org/10.1109/JIOT.2022.3175016