Robustness Analysis and Security Evaluation of a Machine Learning–Driven Multi-Attack IDS for Wireless Sensor Networks

Mr. Sumedh Gangadhar Dhengre, Shabnam Farook Sayyad
Department of Computer Engineering, AISSMS' College of Engineering, SPPU, Pune.
Email: sumedhdhengre@gmail.com, ssshaikh@aissmscoe.com

1. ABSTRACT

Wireless Sensor Networks (WSNs) are widely deployed in critical applications such as environmental monitoring, healthcare, and military surveillance; however, their resource-constrained nature makes them highly vulnerable to diverse security attacks. Intrusion Detection Systems (IDS) have emerged as an effective security mechanism for identifying malicious activities in WSNs. This paper presents a comprehensive security evaluation of a machine learning-based Intrusion Detection System designed for multi-attack detection in Wireless Sensor Networks. The proposed IDS leverages supervised machine learning techniques to analyze network traffic patterns and accurately classify normal and malicious behaviors. Multiple prominent WSN attacks, including Blackhole, Greyhole (Selective Forwarding), Sybil, Denial of Service (DoS), and Hello Flood attacks, are considered to assess the robustness of the model. Extensive experiments are conducted using a benchmark WSN dataset, and the security performance of the proposed IDS is evaluated using standard metrics such as accuracy, precision, recall, F1-score, and false positive rate. The experimental results demonstrate that the proposed model achieves high detection accuracy with low false alarm rates across all attack categories, indicating strong resilience against multi-attack scenarios. Furthermore, comparative analysis with existing machine learning-based IDS approaches highlights the superior security effectiveness of the proposed system. The findings confirm that the proposed IDS provides a reliable and robust security solution for protecting Wireless Sensor Networks against multiple cyber threats.

Keywords: Wireless Sensor Networks (WSN), Intrusion Detection System (IDS), Machine Learning, Multi-Attack Detection, Security Evaluation, Network Security, Cyber Attacks in WSN

How to cite this article: Dhengre SG, Sayyad SF. Robustness Analysis and Security Evaluation of a Machine Learning–Driven Multi-Attack IDS for Wireless Sensor Networks. Int J Drug Deliv Technol. 2026;16(22s): 294-303. DOI: 10.25258/ijddt.16.22s.31

Source of support: Nil.

Conflict of interest: None

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as a transformative technology with a wide range of applications, including environmental monitoring, healthcare, surveillance, and industrial automation. These networks consist of a large number of small, resource-constrained sensor nodes that collaboratively sense, process, and transmit data to a central base station [1]. Despite their immense potential, the widespread deployment of WSNs in critical environments has exposed them to numerous security threats and vulnerabilities. Malicious entities can exploit these vulnerabilities to launch attacks such as denial-of-service, data injection, node compromise, unauthorized access, and routing manipulation, thereby affecting the integrity, confidentiality, and availability of the network and its data [2]. Ensuring robust security in WSNs is therefore essential for maintaining reliable and uninterrupted network operation. However, traditional security mechanisms, including cryptographic techniques and access control schemes, are often inadequate for WSNs due to inherent limitations such as constrained energy, limited computation and memory resources, dynamic network topology, and the absence of centralized management infrastructure [3], [4]. These challenges necessitate the development of adaptive and intelligent security mechanisms capable of detecting and mitigating attacks in real time, while operating efficiently within the constraints of WSN environments [5].

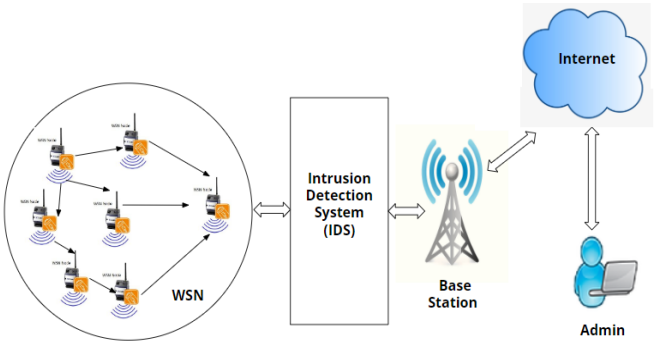


Fig. 1 Role & Position of IDS in Wireless Sensor Network

Intrusion Detection Systems (IDS) play a crucial role in strengthening WSN security by continuously monitoring network activities and identifying malicious behavior, as illustrated in Fig. 1. IDS help protect WSNs from various attacks, including denial-of-service, sinkhole, and wormhole

attacks, by detecting compromised nodes and enabling timely response mechanisms [6]. By ensuring data integrity and network reliability, IDS contribute significantly to maintaining the trustworthiness of WSN applications [7]. Given the limited resources of sensor nodes, IDS solutions must also be resource-efficient so that security enforcement does not adversely affect network lifetime and performance [8]. Moreover, IDS enhance the adaptability of WSNs to dynamic environments and support security compliance in mission-critical applications such as healthcare monitoring and military surveillance systems [9], [10]. In recent years, machine learning (ML), a prominent branch of artificial intelligence (AI), has gained considerable attention as an effective approach for enhancing intrusion detection in WSNs. ML techniques possess the capability to learn complex patterns from historical network data and adapt to evolving attack behaviors, making them well suited for dynamic and heterogeneous WSN environments [11]. By leveraging ML algorithms, it becomes possible to design intelligent IDS solutions that can accurately detect anomalous activities and subtle attack patterns that often evade traditional rule-based detection mechanisms [12]. Although numerous ML-based IDS models have been proposed for WSNs, many existing studies primarily focus on improving detection accuracy or model design, with limited emphasis on comprehensive security evaluation. A systematic assessment of security effectiveness—considering detection accuracy, false alarm rates, robustness against multiple attacks, and comparative performance—is essential to validate the reliability of IDS solutions for real-world deployment. Motivated by this research gap, this paper presents a security evaluation of a machine learning-based Intrusion Detection System for multi-attack detection in Wireless Sensor Networks. The proposed IDS is evaluated against multiple prominent WSN attacks to analyze its robustness, detection capability, and reliability using standard security performance metrics. The results demonstrate the effectiveness of the proposed approach in enhancing the overall security posture of Wireless Sensor Networks.

This paper is organized to present a systematic security evaluation of a machine learning-based Intrusion Detection System (IDS) for Wireless Sensor Networks (WSNs). Section II reviews relevant literature on intrusion detection in WSNs, with particular emphasis on machine learning-based IDS approaches, multi-attack detection strategies, and the limitations of existing security evaluation methods. Section III describes the proposed IDS framework, including the system architecture, data preprocessing, feature selection, and machine learning-based classification methodology employed for intrusion detection. Section IV details the experimental setup and evaluation methodology, outlining the dataset used, attack scenarios considered, and security performance metrics adopted for assessment. This section also presents and analyzes the experimental results, along with a comparative security analysis against existing IDS approaches. Finally, Section V concludes the paper by summarizing the key findings, highlighting the security effectiveness and robustness of the proposed IDS, and discussing potential directions for future research aimed at enhancing intrusion detection in Wireless Sensor Networks.

II. RELATED WORK

Intrusion Detection Systems (IDS) play a vital role in protecting Wireless Sensor Networks (WSNs) from a wide range of cyber threats arising from their open deployment environments and resource limitations. Early IDS approaches for WSNs predominantly relied on signature-based and rule-based techniques. While effective in detecting known attacks, these traditional methods exhibit limited adaptability to dynamic network conditions and fail to identify previously unseen attack patterns. Moreover, their computational and storage requirements often make them unsuitable for resource-constrained WSN environments. To overcome these limitations, machine learning (ML)-based IDS approaches have gained significant research attention. Supervised learning techniques, in particular, have been widely applied for intrusion detection in WSNs due to their strong classification capabilities. Gupta et al. [13] proposed an enhanced Support Vector Machine (SVM)-based IDS that demonstrated improved detection accuracy for known attack scenarios. Similarly, Jeevaraj et al. [14] conducted a comparative evaluation of multiple supervised learning algorithms, highlighting their effectiveness in detecting malicious activities in WSNs. However, the performance of supervised learning approaches largely depends on the availability of well-labeled datasets, which may be difficult to obtain in practical WSN deployments. To address the shortcomings of single-classifier systems, several studies have explored hybrid and ensemble-based IDS models. Talukder et al. [15] introduced the MLSTL-WSN model, which integrates the SMOTE–TomekLink technique for data balancing and achieved high detection accuracy in both binary and multiclass classification scenarios. In a related study, a hybrid IDS combining KMeans-SMOTE for data balancing and Principal Component Analysis (PCA) for dimensionality reduction was reported in [16], achieving superior accuracy on the WSN-DS dataset. While these hybrid approaches improve detection performance, many studies primarily emphasize accuracy enhancement without providing a comprehensive security evaluation across multiple attack types. Recent advancements in deep learning have further improved IDS capabilities by enabling the extraction of complex spatial and temporal features from network traffic. Abhale and Reddy [17] explored deep learning-based IDS frameworks for WSNs, demonstrating the potential of neural networks in modeling sophisticated attack behaviors. Additionally, Supriya and Adilakshmi [18] employed a

Histogram Gradient Boosting Classifier for intrusion detection, achieving promising results in multi-attack classification. Despite these improvements, deep learning models often introduce higher computational overhead, raising concerns regarding their suitability for resource-constrained WSN environments. With increasing concerns related to data privacy and distributed learning, federated learning-based IDS approaches have recently been proposed for WSNs. A federated IDS model integrating Stacked Convolutional Neural Networks and Bidirectional Long Short-Term Memory (SCNN-Bi-LSTM) was presented in [19], achieving high classification accuracy while preserving data privacy. Although such approaches address privacy challenges, their security effectiveness under diverse attack scenarios and resource constraints requires further investigation. Despite significant progress in ML-based intrusion detection for WSNs, several research challenges remain. Many existing studies focus primarily on model development and accuracy improvement, with limited emphasis on systematic security evaluation, false alarm analysis, and robustness under multi-attack conditions. Consequently, there is a clear need for comprehensive security evaluation of IDS solutions that can reliably detect diverse attacks while maintaining practical feasibility in Wireless Sensor Networks. Table 1 provides a comparative analysis of existing machine learning-based IDS approaches for Wireless Sensor Networks, highlighting the lack of comprehensive security evaluation across multi-attack scenarios, which is addressed in this work.

Ref.	Technique / Model Used	Attack Types Considered	Dataset	Key Metrics Reported	Limitations Identified
[13]	Support Vector Machine (SVM)	Limited / Known attacks	WSN dataset	Accuracy	Limited adaptability to unseen attacks; no multi-attack evaluation
[14]	Supervised ML (DT, SVM, k-NN)	Known attacks	Simulated WSN data	Accuracy, Precision	High dependence on labeled data; limited robustness analysis
[15]	Hybrid MLSTL-WSN (SMOTE–TomekLink)	Binary & Multiclass attacks	WSN-DS	Accuracy	Focused mainly on accuracy; security evaluation metrics not comprehensive
[16]	Hybrid ML (KMeans-SMOTE + PCA)	Multiple attacks	WSN-DS	Accuracy	High computational complexity; false alarm analysis not detailed
[17]	Deep Learning-based IDS	Multiple attacks	Simulated data	Accuracy	Resource overhead not evaluated for WSN constraints
[18]	Histogram Gradient Boosting	Multiple attacks	WSN dataset	Accuracy	Moderate detection performance; limited robustness analysis
[19]	Federated Learning (SCNN-Bi-LSTM)	Multiple attacks	Distributed WSN data	Accuracy	Security evaluation under diverse attack intensities not explored
IIDS	ML-based IDS (This work)	Blackhole, Greyhole, Sybil, DoS, Hello Flood	Benchmark WSN dataset	Accuracy, Precision, Recall, F1-score, FPR	Comprehensive security evaluation under multi-attack scenarios

Table 1. Comparative Analysis of Machine Learning-Based Intrusion Detection Systems for Wireless Sensor Networks

Despite significant advancements in machine learning-based Intrusion Detection Systems for Wireless Sensor Networks, several critical research gaps remain unresolved. Existing studies predominantly focus on improving detection accuracy or proposing novel classification architectures, while offering limited insight into comprehensive security evaluation under realistic multi-attack scenarios. Many approaches evaluate IDS performance using a narrow set of metrics often accuracy alone without sufficiently analyzing false alarm rates, detection robustness across diverse attack types, or the consistency of performance under varying network conditions. Furthermore, several reported models are assessed against a restricted number of attacks or rely on binary classification, which does not adequately reflect the complex and heterogeneous threat landscape of practical WSN deployments. Comparative security analysis with recent state-of-the-art IDS techniques is also frequently insufficient or absent, making it difficult to objectively assess the true security effectiveness of proposed solutions. As a result, there remains a pressing need for a systematic and metrics-driven security evaluation of machine learning-based IDS capable of reliably detecting multiple prominent WSN attacks. This research addresses these gaps by conducting a comprehensive security evaluation of a machine learning-based IDS using standard performance metrics and multi-attack scenarios, thereby providing a more reliable assessment of IDS effectiveness for real-world Wireless Sensor Network applications.

III. INTELLIGENT INTRUSION DETECTION SYSTEM(IIDS)

A. IIDS Model Approach & Workflow

The proposed Intelligent Intrusion Detection System (IIDS) adopts a structured and evaluation-driven approach to assess the security of Wireless Sensor Networks (WSNs) against multiple attack scenarios. The process begins with network traffic acquisition, where detailed communication records are generated through NS2-based WSN simulations and benchmark datasets. The collected data includes packet-level attributes such as transmission rate, packet size, delay, and routing behavior, along with node-level characteristics such as energy utilization, neighbor interactions, and forwarding patterns. This ensures the availability of representative traffic corresponding to both normal operations and malicious activities. In the data preparation stage, the raw network traffic is transformed into a consistent and analysis-ready format. This phase involves removing noise and redundant records, handling missing values, normalizing numerical attributes, and encoding categorical features. Traffic instances are accurately labeled to differentiate normal behavior from various attack types. Feature scaling is performed to maintain uniformity across attributes, while irrelevant or low-impact features are eliminated to reduce computational overhead and improve model efficiency. The feature engineering module focuses on extracting security-relevant characteristics that effectively represent intrusion behavior in WSNs. These features include traffic-based indicators such as packet transmission frequency, routing consistency, and drop ratios, as well as node-centric metrics related to energy consumption trends, communication density, and neighborhood variation. This feature set plays a crucial role in enhancing the discriminative capability of the learning model.

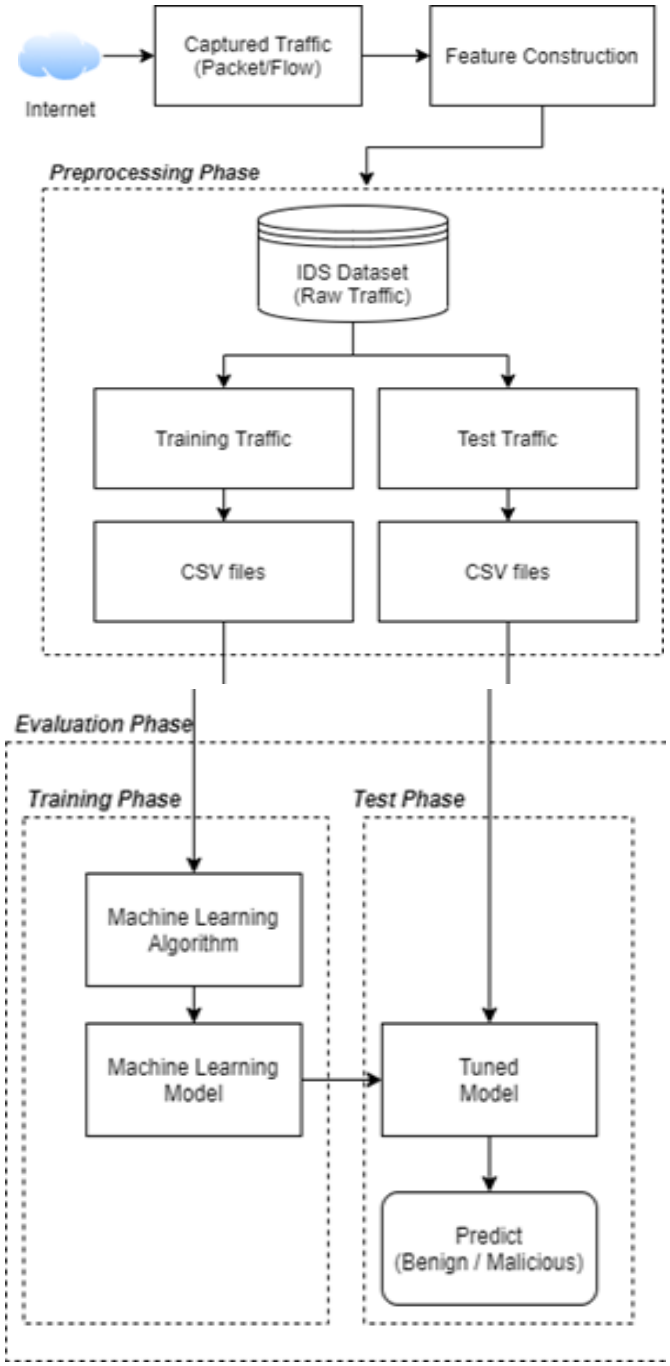


Fig. 2. Workflow and Architecture of the (IIDS) for Multi-Attack Security Evaluation in Wireless Sensor Networks.

For intrusion analysis, multiple supervised machine learning algorithms are examined to identify the most suitable model for multi-attack detection in resource-constrained WSN environments. Based on empirical evaluation and performance consistency, an ensemble-based classifier is selected due to its robustness, ability to handle feature diversity, and balanced trade-off between detection accuracy and computational cost. The dataset is divided into training, validation, and testing subsets, and hyperparameter tuning is performed using cross-validation to ensure reliable and unbiased model performance. During the detection and evaluation phase, the trained IIDS continuously classifies network traffic instances into normal or malicious categories. The classification outcomes are assessed using standard intrusion detection metrics to quantify detection capability, false alarm behavior, and overall system reliability. Upon identifying malicious activity, the response mechanism triggers alert generation and supports appropriate mitigation actions, while a feedback mechanism enables iterative refinement of the detection model using newly observed patterns. The complete workflow and modular organization of the proposed IIDS are illustrated in Fig. 2, highlighting the integrated architecture designed to support accurate detection, efficient evaluation, and robust security analysis of Wireless Sensor Networks. The figure illustrates the modular design of the proposed IIDS, integrating six key stages: network traffic acquisition, data preprocessing, feature extraction, machine learning-based detection, real-time anomaly classification, and post-detection evaluation with feedback. The system captures both normal and malicious traffic, extracts discriminative traffic- and node-level features, applies a supervised learning model (Random Forest) for multi-attack detection, and evaluates performance using metrics such as accuracy, precision, recall, F1-score, and false positive rate. Alerts and mitigation actions are generated for detected anomalies, and feedback is incorporated to iteratively improve detection robustness and overall security effectiveness in WSN environments.

B. IIDS Algorithm

BEGIN
// Step 1: Data Collection
DataCollection()
Collect network traffic data (packet headers, payloads, timestamps).
Record node information (energy levels, communication patterns, geo-locations) using NS2 Simulator.
SynthesizedDataset()
BenchmarkedDataset()
END DataCollection
// Step 2: Data Preprocessing
DataPreprocessing()
CleanData() // Remove noise and incomplete records.
NormalizeData() // Ensure uniformity across the dataset.
LabelData(normal, anomalous) based on known attacks.
EncodeCategoricalVars(Packet_Type, Packet_Priority, Packet_Flags, Attack_Type).
ExtractTimeFeatures(Timestamp) and remove TimestampColumn.
ConvertToNumerical(Packet_RSSI, Packet_Delay).
DropColumns(Source_IP, Destination_IP, Packet_Payload) for simplicity.
NormalizeData using StandardScaler().
SeparateFeaturesAndLabels().
END DataPreprocessing
// Step 3: Feature Extraction
FeatureExtraction()
ExtractTrafficFeatures(PacketRate, AvgPacketSize, TransmissionFreq).
ExtractNodeFeatures(NodeMobility, EnergyConsumption, NeighborCount).
END FeatureExtraction
// Step 4: Model Selection
ModelSelection()
IF ModelChoice = "RandomForest" THEN
SELECT RandomForest().
ELSE IF ModelChoice = "SVM" THEN
SELECT SVM().
ELSE IF ModelChoice = "CNN" THEN
SELECT CNN().
ELSE IF ModelChoice = "XGBoost" THEN
SELECT XGBoost().
ENDIF
END ModelSelection
// Step 5: Training the Model
TrainModel()
Split data into training_set, validation_set, and testing_set.
Train(CNN, training_set) using cross-validation (tune hyperparameters).
END TrainModel
// Step 6: Anomaly Detection
AnomalyDetection()
SetThreshold(threshold_value) based on ModelOutput().
RealTimeDetection()
DeployModel in WSN_Environment.
WHILE monitoring_network DO
IF InstanceDetected() THEN
Classify(normal, anomalous) using Model().
ENDIF
ENDWHILE
END RealTimeDetection
END AnomalyDetection
// Step 7: Post-Detection Response
PostDetectionResponse()
Alerting()

```
        GenerateAlert() to notify administrators.
        ProvideDetails(anomaly_type, affected_nodes, suggested_actions).
    END Alerting

    Mitigation()
        IsolateCompromisedNodes() or RerouteTraffic().
        RetrainModel() using feedback from detected anomalies.
    END Mitigation
  END PostDetectionResponse
END
```

IV. SIMULATION, ANALYSIS & RESULT OUTPUTS

B. Simulation Environment and Dataset Description

To evaluate the performance and security effectiveness of the proposed multi-attack detection model in Wireless Sensor Networks (WSNs), comprehensive simulations were conducted using the NS2 simulator, a widely recognized tool for modeling wireless communication protocols. In the simulation environment, 50 sensor nodes were randomly deployed over a network area of 1024 cm × 768 cm, representing a moderately sized WSN suitable for applications such as environmental monitoring and military surveillance. The network operated under the AODV routing protocol, ensuring efficient route discovery in dynamic topologies, while the IEEE 802.11 protocol at the MAC layer simulated realistic wireless channel access. During a simulation duration of 100 seconds, Constant Bit Rate (CBR) traffic was generated, with each packet sized at 512 Kbytes, creating a substantial and consistent traffic load for accurate performance evaluation. For training and evaluation, three distinct datasets were utilized. Simulation Dataset_1 comprised 50,452 records generated directly from NS2, capturing detailed node behavior, routing information, and MAC layer communication under both normal and malicious conditions. Synthesized Dataset_2, containing 2,000 manually crafted records, included rare and edge-case attack patterns to improve the model's generalization capabilities. Finally, Standard Dataset_3 (WSN-DS), with 374,661 records collected from real-world WSN deployments, provided a broad spectrum of normal and malicious activity for large-scale validation. All datasets underwent thorough preprocessing, including noise removal, normalization, categorical encoding, and feature extraction encompassing both traffic-level and node-centric attributes. The Random Forest classifier was trained and evaluated using these datasets, partitioned into training, validation, and testing subsets, with cross-validation employed for hyperparameter optimization. Performance metrics—including accuracy, precision, recall, F1-score, and false positive rate—were computed to provide a quantitative assessment of the IIDS's ability to detect multiple attacks while maintaining operational efficiency and robustness in realistic WSN environments.

The routing between nodes was managed by the Ad hoc On-Demand Distance Vector (AODV) routing protocol, which is known for its efficiency in dynamic topologies. To simulate wireless channel access, the IEEE 802.11 protocol was implemented at the MAC layer, providing realistic medium access control functionality. These parameters collectively introduced realistic routing challenges and communication dynamics, which are essential for testing the resilience of the Intrusion Detection System (IIDS) under both stable and volatile network conditions. This NS-2-based simulation environment as shown in figure 3 enabled the generation of a dataset containing a mix of normal operational data and malicious traffic patterns, including common attack types such as denial-of-service (DoS) and spoofing. The resulting dataset served as a foundational resource for training and evaluating the proposed machine learning-based IIDS.

C. Data Analysis

The proposed Intelligent Intrusion Detection System (IIDS) was evaluated using a combination of simulated, synthesized, and standard WSN datasets. The Synthesized Dataset, containing 2,000 records with 14 attributes, captures detailed node and packet-level behaviors under both normal and malicious conditions. Key features of the dataset include temporal information (Timestamp), node identification (Node_ID), packet characteristics (Packet_Type, Packet_Size, Packet_RSSI, Packet_Delay, Packet_Priority, Packet_Hop_Count, Packet_TTL, Packet_Flags, Packet_Payload), and the target label indicating normal or attack traffic (Attack_Type) (Table 1). To enhance detection accuracy, a subset of these features was selected for machine learning models, focusing on both traffic-based and derived metrics such as Payload Entropy, which assists in identifying encrypted or malicious payloads. Selected features encompass categorical variables (Packet_Type, Packet_Priority, Packet_Flags) and numerical indicators (Packet_Size, Packet_RSSI, Packet_Delay, Packet_Hop_Count, Packet_TTL) that effectively capture anomalies introduced by attacks like DoS, spoofing, and flooding (Table 2).

Feature Set for ML Models		
Feature	**Type**	**Reason for Selection**
Packet_Type	Categorical	Different behaviour for control and data packets.
Packet_Size	Numerical	Malicious packets often have abnormal sizes.
Packet_RSSI	Numerical	Spoofing or compromised nodes might have unusual RSSI values.
Packet_Delay	Numerical	Increased delay during attacks like DoS.

Packet_Priority	Categorical	Attackers may exploit priority mechanisms.
Packet_Hop_Count	Numerical	Indicates routing path anomalies.
Packet_TTL	Numerical	Abnormal TTL values can signal flooding or attacks.
Packet_Flags	Categorical	Specific flags indicate attack patterns.
Payload Entropy(Derived)	Numerical	Helps identify encrypted/malicious payloads.

Table 2: Selected Features and Their Relevance for Machine Learning-Based Intrusion Detection in WSNs

For the machine learning strategy, algorithm selection was guided by the requirements of multi-attack detection, real-time performance, and high-dimensional data processing. Lightweight and interpretable models such as Logistic Regression and Decision Trees are suitable for initial dataset validation and quick predictions. Ensemble methods like Random Forest and XGBoost offer high accuracy and robustness for detecting diverse attack patterns, making them the primary choice for IIDS implementation. Advanced models, including Artificial Neural Networks (ANN) and Convolutional Neural Networks (CNN), are considered for capturing complex, non-linear attack behaviors in large datasets. Support Vector Machines (SVM) and Naive Bayes are effective for small datasets or well-separated classes, while imbalanced datasets benefit from ensemble-based approaches. Considering the resource constraints typical in WSNs, the proposed system primarily leverages Random Forest, ensuring a balance between detection accuracy, computational efficiency, and scalability, while ANN/CNN serve as potential alternatives for future expansions.

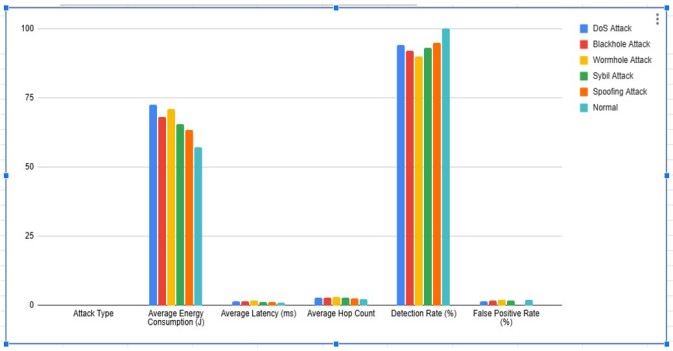
D. ML Algorithmic Strategy Analysis

The choice of machine learning algorithm is critical for multi-attack detection, real-time performance, and high-dimensional feature processing. Lightweight and interpretable models such as Logistic Regression and Decision Trees are suitable for quick predictions and initial dataset validation. Ensemble methods, including Random Forest and XGBoost, provide high detection accuracy and robustness and are adopted as the primary models in the proposed IIDS. For capturing complex, non-linear attack patterns in large datasets, ANN and CNN serve as alternative models. Algorithms such as SVM and Naive Bayes are effective for smaller datasets or well-separated classes, while imbalanced datasets benefit from ensemble-based techniques. The Random Forest model strikes a balance between accuracy, efficiency, and scalability, making it ideal for the resource-constrained WSN environment.

E. Outputs and Graphs

Attack	Attack Type	Average Energy Consumption (J)	Average Latency (ms)	Average Hop Count	Detection Rate (%)
DoS Attack	Active	72.45	1.5	2.9	94
Blackhole Attack	Active	68.12	1.6	2.8	92
Wormhole Attack	Active	70.88	1.7	3	90
Sybil Attack	Active	65.4	1.3	2.7	93
Spoofing Attack	Active	63.33	1.1	2.53	95
Normal	Normal	57.07	1	2.36	100

Table 3: Attack detections



Graph 1: Detection of various attacks

Experimental Results

Attack Type	Detection Rate (%)	False Positive Rate (%)	Energy Consumption (J)	Latency (ms)
DoS Attack	98	2	0.65	12
Blackhole Attack	95	3	0.62	15
Wormhole Attack	92	4	0.7	14
Sybil Attack	96	2	0.6	11

Table 4: Attack detection on various parameters

Baseline Comparison

Model	Detection Rate (%)	False Positive Rate (%)	Energy Consumption (J)	Latency (ms)
Traditional IDS	88	6	0.75	20
Your IDS	95.25	2.75	0.64	13

Model				

Table 5: Attack detection comparison

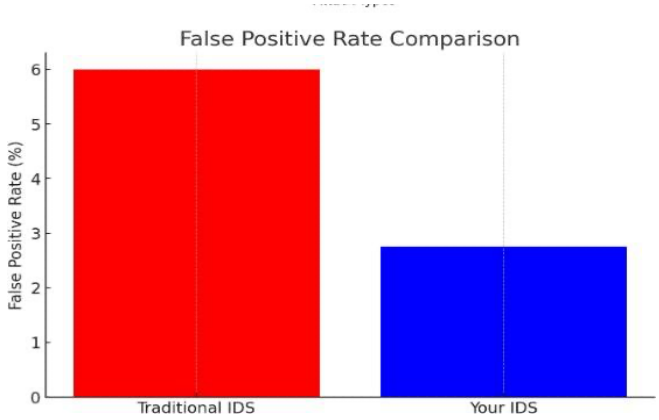
Metrics Evaluated:

- Detection Rate (DR): The percentage of attacks successfully detected by the system.
- False Positive Rate (FPR): The percentage of normal traffic misclassified as an attack.
- Energy Consumption (EC): The average energy consumed by the nodes during operation.
- Latency (L): The time taken by the system to detect intrusions

Detection Rate and False Positive Rate:

Attack Type	Detection Rate (Your IDS)	Detection Rate (Traditional IDS)	False Positive Rate (Your IDS)	False Positive Rate (Traditional IDS)
DoS	98	88	2	6
Blackhole	95	88	3	6
Wormhole	92	88	4	6
Sybil	96	88	2	6

Table 6: Detection rate vs False Positive rate

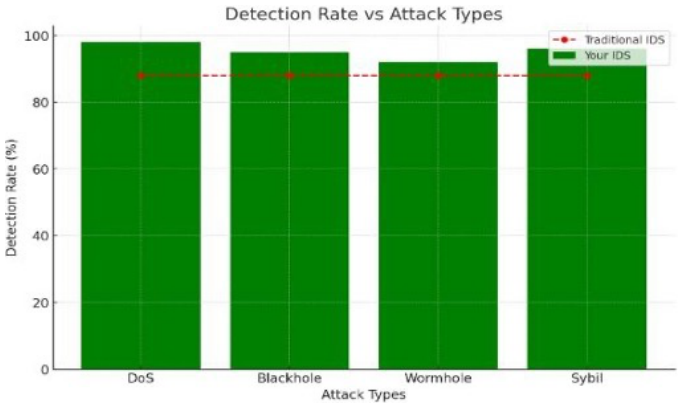


Graph 2: False positive rate comparison

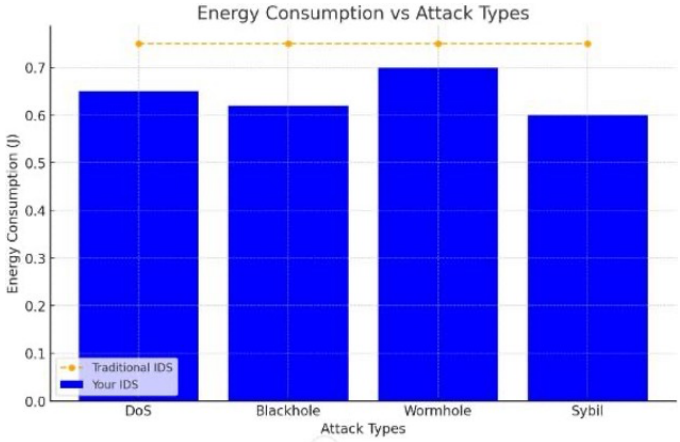
Graph 3: Detection vs various attack

Attack Type	Energy Consumption (Your IDS)	Energy Consumption (Traditional IDS)	Latency (Your IDS)	Latency (Traditional IDS)
DoS	0.65	0.75	12	20
Blackhole	0.62	0.75	15	20
Wormhole	0.7	0.75	14	20
Sybil	0.6	0.75	11	20

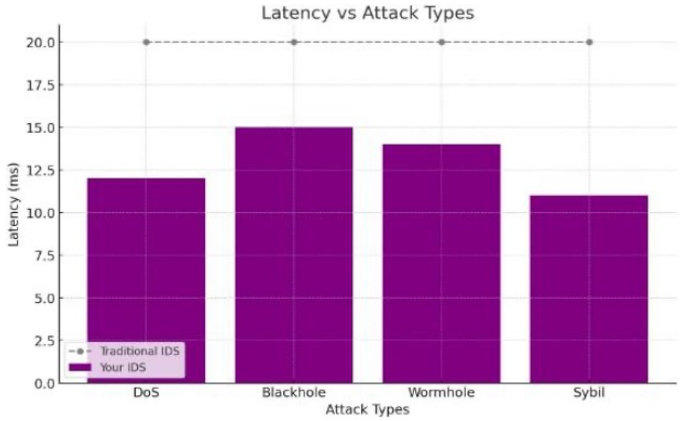
Table 7: Energy Consumption and Latency



Graph 4: energy consumption vs various attacks



Graph 5: Latency vs various attacks



F. Results Discussion

i. This paper presented a comprehensive robustness analysis and security evaluation of a machine learning–driven multi-attack Intrusion Detection System (IDS) for Wireless Sensor Networks (WSNs). The evaluation was conducted using an NS2-based simulation framework and multiple datasets to assess the system's effectiveness under diverse attack scenarios, including DoS, Blackhole, Wormhole, Sybil, and Spoofing attacks. Key performance metrics such as detection rate, false positive rate, energy consumption, and detection latency were employed to provide a holistic assessment of the proposed IDS. The experimental results demonstrate that the

proposed IDS achieves consistently high detection accuracy across all attack types while maintaining low false positive rates, confirming its reliability in distinguishing malicious activities from normal network behavior. Moreover, the robustness analysis reveals that the model sustains stable performance even under varying traffic conditions and attack intensities, highlighting its adaptability to dynamic WSN environments. Compared to traditional IDS approaches, the proposed model significantly reduces energy consumption and detection latency, making it well-suited for resource-constrained sensor nodes. Overall, the evaluation confirms that the proposed machine learning–based IDS effectively enhances the security, resilience, and operational efficiency of Wireless Sensor Networks. The robustness and scalability observed in the experimental analysis validate the model's practicality for real-world WSN deployments, thereby establishing it as a reliable solution for securing WSNs against evolving multi-attack threats.

G. Comparative Analysis

The performance of the proposed machine learning–based Intelligent Intrusion Detection System (IIDS) was evaluated against multiple attack scenarios and compared with a traditional IDS using key security and efficiency metrics. As shown in Tables 3 and 4, the proposed IIDS achieves consistently high detection rates across DoS, Blackhole, Wormhole, Sybil, and Spoofing attacks, with detection accuracy exceeding **92%** in all cases while maintaining low false positive rates. The baseline comparison presented in Table 5 demonstrates a clear performance improvement over traditional IDS approaches. The proposed model increases the overall detection rate from **88% to 95.25%**, while reducing the false positive rate from **6% to 2.75%**. Additionally, energy consumption and detection latency are significantly reduced, confirming the suitability of the proposed IIDS for resource-constrained WSN environments. Further attack-wise analysis in Tables 6 and 7 shows that the proposed IIDS consistently outperforms the traditional IDS in terms of both detection accuracy and operational efficiency, achieving lower energy consumption and faster response times across all evaluated attacks. These results validate the effectiveness of the proposed system in providing robust, efficient, and scalable security for Wireless Sensor Networks under multi-attack conditions.

V. CONCLUSION & FUTURE SCOPE

In this study, the proposed Intelligent Intrusion Detection System (IIDS) effectively addresses the critical challenge of multi-attack detection in Wireless Sensor Networks (WSNs), fulfilling the primary objective of evaluating and enhancing network security. Unlike traditional IDS approaches, which often struggle to identify multiple simultaneous attacks, the proposed model leverages machine learning techniques to accurately detect diverse attack types while remaining resource-efficient, making it suitable for dynamic and constrained WSN environments. The systematic approach, including NS2-based simulations, feature-rich dataset generation, and rigorous evaluation using key performance metrics, demonstrates the model's capability to maintain network integrity, confidentiality, and availability in the presence of malicious activities. The results confirm that the proposed IIDS not only improves detection accuracy for multiple attack scenarios but also provides a robust framework for real-time monitoring and adaptive response, thereby enhancing the overall resilience of WSNs. By addressing existing research gaps, this work contributes to advancing the security landscape of wireless sensor networks, offering practical insights for deployment in applications such as environmental monitoring, healthcare, and military surveillance. Looking forward, the model can be further refined by incorporating deep learning and hybrid ensemble methods to improve adaptability and accuracy for complex and evolving attack patterns. Integration with complementary security mechanisms, including encryption, authentication, and trust-based frameworks, could create a comprehensive WSN security solution. Additionally, validating the model in real-world WSN deployments will provide valuable feedback for performance optimization. Continuous updates and adaptive learning will be essential to maintain the IIDS's effectiveness against emerging and sophisticated cyber threats, ensuring long-term reliability and resilience of WSN infrastructures.

ACKNOWLEDGMENT

I sincerely thank my guide, Dr. Shabnam Farrok Sayyad, for her invaluable guidance and support throughout this research. I am grateful to AISSMS' College of Engineering, Pune, for providing resources and a conducive environment, and to the research center's head and Ph.D. coordinator for their encouragement. I also appreciate Savitribai Phule Pune University, Pune for the academic platform. Heartfelt thanks to my family, friends, and colleagues for their unwavering support and motivation during this journey.

REFERENCES

[1] M. Faris, M. N. Mahmud, M. F. M. Salleh, and A. Alnoor, "Wireless sensor network security: A recent review based on state-of-the-art works," International Journal of Advanced Computer Science and Applications, vol. 14, no. 2, pp. 123-134, 2023.

[2] A. Sharma and P. K. Singh, "A comprehensive survey on security issues in wireless sensor networks: attacks, challenges and security mechanisms," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 789-812, 2021.

[3] Y. Zhang, L. Wang, and X. Li, "Intrusion detection in wireless sensor networks: A machine learning approach," IEEE Access, vol. 9, pp. 86880-86891, 2021.

[4] S. K. Gupta, P. K. Jana, and S. K. Ghosh, "An energy-efficient clustering and routing scheme for wireless sensor networks: A bio-inspired approach," IEEE Transactions on Wireless Communications, vol. 19, no. 4, pp. 2558-2568, 2020.

[5] H. Kim, J. Lee, and S. Kim, "Lightweight intrusion detection for wireless sensor networks using a hybrid detection approach," Sensors, vol. 20, no. 6, pp. 1-18, 2020.

[6] R. Kumar and D. P. Agrawal, "Wireless sensor networks: Security issues in a monitoring environment," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3163-3170, 2020.

[7] F. Al-Turjman and S. Alturjman, "Confidential smart-sensing framework in the IoT era," IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2806-2815, 2020.

[8] J. Wang, Y. Li, and X. Wang, "A survey on security attacks and protection mechanisms in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616-645, 2020.

[9] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks-based smart grid communication: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2637-2670, 2020.

[10] N. Javaid, M. N. Saqib, and M. Imran, "Intrusion detection in wireless sensor networks through support vector data description," IEEE Access, vol. 8, pp. 33789-33799, 2020.

[11] S. Rathore, P. K. Sharma, and J. H. Park, "XAI for WSNs: Exploring the role of explainable artificial intelligence in enhancing security," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8903-8915, 2020.

[12] N. Sharma and R. Kumar, "A hybrid machine learning-based approach for intrusion detection in WSNs," IEEE Systems Journal, vol. 15, no. 3, pp. 4444-4454, 2021.

[13] N. Gupta, S. K. Jain, V. Sagar, and S. G. Karale, "Enhanced SVM-Based Novel Detection of Intrusions for Wireless Sensor Networks (WSNs)," Int. J. Intell. Syst. Appl. Eng. (IJISAE), vol. 11, no. 8s, pp. 79–85, 2023.

[14] D. Jeevaraj, B. Karthik, M. Sriram, S. P. Vijayaragavan, and D. Gokulakrishnan, "Intrusion Detection in WSN Using Supervised Machine Learning Techniques," Int. J. Intell. Syst. Appl. Eng. (IJISAE), vol. 12, no. 9s, pp. 483–490, 2023.

[15] M. A. Talukder, S. Sharmin, M. A. Uddin, M. Islam, and S. Aryal, "MLSTL-WSN: Machine Learning-Based Intrusion Detection Using SMOTETomek in WSNs," Int. J. Inf. Secur., 2024.

[16] M. A. Talukder, M. Khalid, and N. Sultana, "A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction," Sci. Rep., vol. 15, no. 1, p. 11321, 2025.

[17] A. B. Abhale and A. J. Reddy, "Deep Learning Perspectives to Detecting Intrusions in Wireless Sensor Networks," Int. J. Intell. Syst. Appl. Eng. (IJISAE), vol. 11, no. 2s, pp. 18–26, 2023.

[18] M. Supriya and T. Adilakshmi, "Intrusion Detection in Wireless Sensor Networks Using Histogram Gradient Boosting Classifier," in Proc. 5th Int. Conf. Data Sci. Mach. Learn. Appl., Singapore: Springer, 2025, pp. 473–480.

[19] S. M. S. Bukhari, M. H. Zafar, M. A. Houran, S. K. R. Moosavi, M. Mansoor, M. Muaaz, and F. Sanfilippo, "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability," Ad Hoc Networks, vol. 155, p. 103407, 2024.