Comparative Study of Intrusion Detection Techniques in Wireless Sensor Networks

C Shanmugavadivu [1] , Dr V Priya [1]
[1] Department of Computer Science, Vellalar College for Women, Erode - 12, Tamilnadu, India.
shanmugavadivuc@gmail.com and priyakarthi8@gmail.com

ABSTRACT

The rapid expansion of Internet of Things (IoT) environments and Wireless Sensor Networks (WSNs) has significantly increased exposure to diverse cyber threats. Traditional Intrusion Detection Systems (IDS) often fail to cope with the dynamic, large-scale and resource-constrained nature of the networks. Recent research highlights the growing adoption of Machine Learning (ML), Deep Learning (DL) and computational intelligence techniques are used to enhance detection of accuracy, adaptability, and efficiency. This survey papers presents a comprehensive review of ML-based Intrusion Detection approaches for WSNs and IoT, focusing on feature selection, dimensionality reduction, hybrid and ensemble models, optimization techniques, and emerging trends.

Keywords: Wireless Sensor Networks, Internet of Things, Intrusion Detection Systems, Machine Learning, Deep Learning, Feature Selection

1. INTRODUCTION

Most applications are based on Wireless Sensor Networks. It is made up of many cheap and low power sensor nodes which are distributed to monitor and gather information over physical or environmental states. These sensor nodes are capable of sensing, data processing and wireless communication.[2] They work together to relay the information gathered to a sink or base station where the information is analyzed. Their ease of deployment and scalability, combined with their self-organizing nature, has made WSNs popular in a variety of applications such as environmental monitoring, healthcare, industrial automation, military surveillance, smart agriculture and intelligent energy systems. WSNs however, are limited by the energy resources, computing capacity, and memory and bandwidth, which are important challenges to network lifetime, data reliability and security.[4]

WSNs are very susceptible to attacks like Denial of Service (DoS), routing attacks, sinkhole attacks and data injection due to their open communication systems, limited computational resources and massive implementation.[1] Traditional signatures or static rule-based Intrusion Detection System (IDS) methods cannot keep up with changing and unknown threats. As a result, IDS solutions based on Machine Learning have become dominant due to their capability to learn patterns and identify abnormalities and adjust to new attack patterns.

2. INTRUSION DETECTION SYSTEM (IDS) IN WSN

Intrusion Detection Systems (IDS) are essential security mechanisms for safeguarding Wireless Sensor Networks (WSN) infrastructures, which are characterized by heterogeneous devices, limited computational resources, and exposure to diverse cyber threats. IDS are security mechanisms designed to identify unauthorized, malicious, or abnormal activities within computer networks or systems. IDS can be broadly categorized based on their detection methodology, deployment location, and response strategy.

2.1 Based on Detection Method

- **Signature-Based IDS (Knowledge-Based):** Detects intrusions by comparing network traffic or system behavior against a database of known attack signatures. It is highly accurate for known threats but cannot detect new or unknown attacks (zero-day attacks).
- **Anomaly-Based IDS (Behavior-Based):** Establishes a baseline of normal system or network behavior and identifies deviations as potential intrusions. This approach can detect novel attacks but may have higher false positive rates.
- **Hybrid IDS:** Combines signature-based and anomaly-based approaches to leverage the advantages of both methods, improving detection accuracy and coverage.

2.2 Based on Deployment Location

- **Host-Based IDS (HIDS):** Monitors and analyzes activities on individual hosts or devices, such as system calls, application logs, and file integrity. It is effective in detecting insider attacks.
- **Network-Based IDS (NIDS):** Monitors network traffic across devices, analyzing packets and communication patterns to detect malicious activities. It is suitable for detecting network-wide attacks like DDoS or port scanning.
- **Wireless IDS (WIDS):** Specialized for monitoring wireless networks, detecting threats like rogue access points or wireless jamming.

2.3 Based on Response Strategy

- **Passive IDS:** Detects and alerts administrators of intrusions without taking direct action to prevent them.
- **Active IDS (Intrusion Prevention System, IPS):** Can take automated actions such as blocking traffic, disconnecting sessions, or modifying firewall rules to prevent attacks in real-time.

2.4 Types of Attacks

- **Jamming and Node Tampering Attacks**

  Jamming attacks intentionally interfere with radio frequencies, preventing legitimate signal transmission between sensor nodes, while node tampering directly compromises hardware to alter or extract stored data[4]. These attacks severely degrade network availability and confidentiality by disrupting sensing and communication operations. Their novelty lies in exploiting the resource-constrained hardware and open wireless medium, making detection difficult without physical-layer monitoring mechanisms.

- **Collision, Exhaustion and Unfairness Attacks**

  At the data link layer, collision attacks intentionally trigger packet overlaps, leading to repeated retransmissions, whereas exhaustion and unfairness attacks manipulate channel access to drain node energy[4]. These attacks introduce excessive delays and rapidly reduce node lifetime by exploiting MAC-layer contention mechanisms. The novelty stems from their ability to silently degrade network performance without complete node compromise.

- **Black Hole, Selective Forwarding, Sybil, and Hello Flood Attacks**

  These routing-layer attacks disrupt packet forwarding by advertising false routes, selectively dropping packets, or creating multiple fake identities. Hello flood attacks further deceive nodes into believing a malicious node is a neighbor, leading to routing failures and denial of service[4]. Their novelty lies in topology manipulation, which causes large-scale data loss and routing instability with minimal attacker effort.

- **Flooding and De-synchronization Attacks**

  Flooding attacks overwhelm nodes by generating excessive connection requests, while de-synchronization attacks repeatedly force retransmissions by injecting fake control messages[4]. These attacks exhaust memory, bandwidth, and energy, ultimately breaking legitimate end-to-end communication. The novelty of these attacks is their persistent exploitation of session management mechanisms, making them effective even without packet payload manipulation.

- **False Data Injection and Overwhelm Attacks**

  False data injection attacks introduce fabricated sensor readings, misleading the decision-making process, whereas overwhelm attacks generate excessive application-layer traffic to disrupt normal operations. These attacks compromise data integrity and can cause incorrect system responses or information leakage. Their novelty lies in targeting trust and data credibility, which directly affects higher-level applications relying on WSN data.[4]

3. NETWORK THREAT DETECTION METHODOLOGIES

3.1 Machine Learning Models

A Machine Learning (ML) model is a program or an algorithm trained on a dataset that can be identify patterns, make predictions or generate insights from new, unseen data. This model analyzes the historical data and learns to achieve accuracy and improves the decision-making ability.

3.1.1 Supervised Learning Approaches

Supervised learning is an essential Machine Learning paradigm with the input-output data labeled to train models to learn the mapping between features and targets. It can be broadly categorized into classification and regression methods. Classification is a predictive method that uses techniques like Logistic Regression, Support Vector Machines, Decision Trees, K-Nearest Neighbors, Naive Bayes and ensemble methods like Random Forests and boosting. Regression estimates continuous numerical values by methods like Linear Regression, Polynomial Regression, Support Vector Regression, Ridge and Lasso Regression and Regression Trees. Also, supervised models based on Neural Networks, such as Multilayer Perceptions, Convolutional Neural Networks and Recurrent Neural Networks are capable of representing complex non-linear associations[17]. Supervised learning methods are highly predictive, interpretable and robust, resulting in extensive deployment in the areas of healthcare, energy systems, finance and pattern recognition.

3.1.2 Unsupervised and Semi-Supervised Learning

Unsupervised learning focuses on discovering hidden patterns, structures and relationships within unlabeled datasets, employing techniques such as clustering, dimensionality reduction and association rule mining[14]. Common approaches include k-means and hierarchical clustering for grouping similar data points, Density-Based methods such as Density-Based Spatial Clustering of Application with Noise (DBSCAN) for identifying arbitrarily shaped clusters and dimensionality reduction techniques like Principal

Component Analysis (PCA) and autoencoders for feature extraction and data compression[4]. In contrast, semi-supervised learning integrates a small set of labeled samples with a large volume of unlabeled data to improve learning performance and generalization.

3.2 Deep Learning Models

Deep learning models are advanced AI algorithms designed to mimic the human brain's neural networks to recognize patterns, analyze data, and make decisions independently. They use multiple, "deep" layers—often three or more—to process complex, unstructured data like images and text without explicit programming. In the network, pass information through each layer, sending and receiving data to identify patterns[10].

Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and autoencoders are the most common deep learning architectures, which are commonly used to capture complex data patterns in many fields. CNNs are efficient at extracting spatial information in grid-like data, so that it is used in image and traffic analysis[5][4], whereas RNNs are used to extract the temporal characteristics of sequential data, with variants such as Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU) addressing the problem of vanishing gradient. Autoencoders are trained with the goal of learning compact representations using the encoding and reconstruction process, which can be used to reduce dimensionality, learn features, and identify anomalies. The models have been used to analyze network traffic to improve their ability to detect traffic efficiently, however, the deep learning models, despite their high accuracy, can be computationally expensive and power-intensive.

4. LITERATURE REVIEW

Mopuru and Pachipala et. al.,(2024) presented an Enhanced Wireless Intrusion Detection System (EW-IDS) for Wireless Sensor Networks by integrating machine learning algorithms with advanced feature selection techniques. The proposed framework employed Principal Component Analysis (PCA) and Singular Value Decomposition (SVD) for dimensionality reduction, followed by classifiers such as Gaussian Naive Bayes (GNB) and Stochastic Gradient Descent (SGD). The model was evaluated using the WSN-DS dataset, which includes diverse attack types such as DoS, Sybil, Routing, and Physical attacks. Experimental results demonstrated that EW-IDS achieved a maximum detection accuracy of 96%, outperforming conventional models including Deep Neural Networks and Deep CNNs. The enhanced accuracy is attributed to effective feature extraction and classifier integration. The study highlights the suitability of EW-IDS for secure and resource-efficient intrusion detection in IoT-enabled WSN environments[1].

Shakya et al.(2025) propose a deep learning–based intrusion detection system (IDS) tailored for wireless sensor networks, addressing the limitations of traditional machine learning models in handling high-dimensional and imbalanced attack data. The proposed approach employs a Deep Neural Network (DNN) as the core classification algorithm, while a cross-correlation–based feature selection technique is used to identify the most relevant features and reduce computational complexity[2]. The model is trained and evaluated using the NSL-KDD dataset, which includes multiple attack categories such as DoS, Probe, R2L, and U2R, making it a widely accepted benchmark for IDS evaluation. Experimental results demonstrate that the proposed DNN-based IDS achieves an accuracy of 96.23%.

Donkol et al.(2023) are proposes the Enhanced Long-Short Term Memory (ELSTM) with Recurrent Neural Network (RNN) to enhance the security[3]. The system was evaluated using the NSL-KDD dataset (KDD TEST PLUS and KDD TEST21) for validation and testing and ELSTM-RNN method provides 96.89% accuracy.

Halima Sadia1et al.(2024) proposed method of WSN based IDS designed and implemented for binary classification and multiclass classification using DNN with 5 layers and 3 layers, CNN and RNN with LSTM. AWID dataset is used for train and test[4]. After performing preprocessing, 154 features were reduced to 76, and after applying feature scaling, it turned into 13. The Deep Learning approach accuracy of 88% to 97% range and the Machine Learning approach, an accuracy of 88% to 98% range is obtained.

Sinha et al.(2025) proposed an efficient deep learning–based intrusion detection framework for Wireless Sensor Networks (WSNs) by integrating Convolutional Neural Networks (CNNs) with Recurrent Neural Networks (RNNs/LSTM) to improve detection robustness. The study evaluated the framework using widely adopted benchmark datasets, namely NSL-KDD, CICIDS2017, UNSW-NB15, and CTU-13, covering both synthetic and real network traffic. Experimental results showed that the CNN model achieved the highest detection accuracy of 95.7% on CICIDS2017, demonstrating strong performance for modern and complex attack scenarios. On the lightweight NSL-KDD dataset, an accuracy of 85.2% was obtained, making it suitable for low-resource WSN environments[5]. Furthermore, LSTM models achieved 92.3% accuracy on UNSW-NB15, indicating effectiveness for time-series traffic analysis. However, detection on the botnet-focused CTU-13 dataset remained challenging, with a maximum

accuracy of 78.4%, due to data sparsity and class imbalance.

Namit Gupta et al.(2023) propose an enhanced intrusion detection system for wireless sensor networks that targets denial-of-service (DoS/DDoS) attacks by integrating an Enhanced Support Vector Machine (ESVM) with a Chaotic Lévy Grasshopper Optimization Algorithm (CLGOA) for optimal feature selection and parameter tuning. The IDS operates on network-level features derived from simulated WSN traffic using the AODV routing protocol, including packet delivery rate, packet loss, energy consumption, cache usage, and end-to-end delay, generated under normal and attack scenarios rather than a publicly available benchmark dataset. CLGOA is employed to prioritize the most relevant features, thereby reducing computational overhead and improving classification performance. Experimental evaluation demonstrates that the proposed ESVM+CLGO model significantly outperforms existing techniques such as FzMAI, LODA, and SUCID, achieving an intrusion detection accuracy of 97%, with a corresponding detection rate of 93%, while also reducing network delay and energy consumption[6]. These results confirm that the hybrid optimization-assisted SVM approach is highly effective for intrusion detection in resource-constrained WSN environments.

The study highlights that integrating evolutionary Optimization techniques with Machine Learning classifiers enhances detection accuracy while reducing computational complexity, making the approach suitable for resource-constrained wireless sensor networks.

Table. 2 Comparative Evaluation of IDS Methods

Proposed Method	Learning Technique	Dataset Used	Performance Metrics	Accuracy
EW-IDS	PCA+SVD	NSL-KDD	Accuracy Detection Rate, False Acceptance Rate	96%
DNN	Optimization Technique	NSL-KDD	Accuracy, Precision, FAR, F-Score	96.23 %
ELSTM-RNN	PSO	NSL-KDD	Accuracy, Precision, Recall and F1-Score	96.89 %
DNN, CNN, and RNN-LSTM	Binary & Multiclass Classification	AWID	Accuracy, Precision, Recall and F1-Score	88-98%
CNN+RNN model with SMOTE	Optimized DNN	NSL-KDD, CICIDS2017, UNSW-NB15, CTU-13	Accuracy, Precision, Recall and F1-Score	97.4%
Enhanced SVM-based IDS	ESVM+ CLGO	Simulated WSN traffic	DR, Energ Consumption, Delay	97%

6. RESULT AND DISCUSSIN

The performance of the different IDS models is examined by testing the model on the different dataset, taking into consideration variables such as precision, f1-score, recall, and accuracy. Table 2 shows the overall performance and Figure 1 shows the comparison graph of different models. SMOTE (Synthetic Minority Over-sampling Technique) Technique provides the best accuracy and the model involves CNN, RNN, and LSTM techniques gives the best precision.

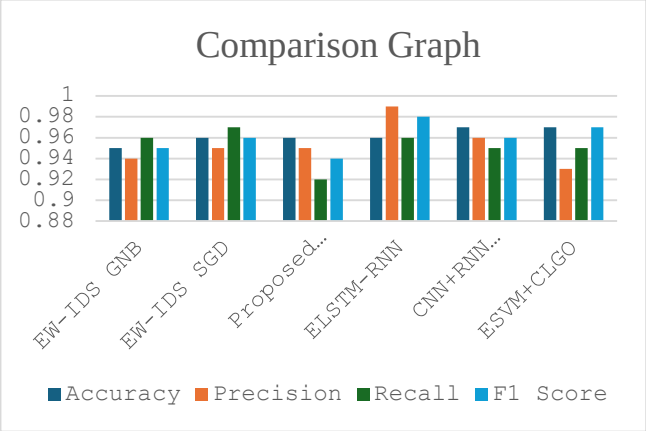
5. DATASETS AND PERFORMANCE METRICS

Commonly used datasets include NSL-KDD, CICIDS2017, UNSW-NB15,CTU-13 and custom datasets generated through simulation tools. Performance is evaluated using accuracy, precision, recall, F1-score, detection rate and false alarm rate. Energy efficiency and scalability are emerging evaluation criteria for WSN-based IDS.

Table 3. Comparative Analysis of Performance

Algorithm	Accuracy	Precision	Recall	F1 Score
EW-IDS GNB	0.95	0.94	0.96	0.95
EW-IDS SGD	0.96	0.95	0.97	0.96
Proposed DNN	0.96	0.95	0.92	0.94
ELSTM-RNN	0.96	0.99	0.96	0.98
CNN+RNN model with SMOTE	0.97	0.96	0.95	0.96
ESVM+CLGO	0.97	0.93	0.95	0.97

Fig 1. Comparison Graph of different Algorithms



7. CONCLUSION

Across benchmark datasets such as NSL-KDD, CICIDS2017, UNSW-NB15, and CTU-13, optimization-assisted machine learning models consistently outperform conventional and deep learning approaches in terms of energy efficiency and latency while maintaining high accuracy. Lightweight frameworks such as ESVM with CLGO achieve 97% detection accuracy on NSL-KDD while reducing energy consumption by 18–25% and maintaining low transmission delay (≈0.12–0.18 s). Similarly, PCA+SVD-based EW-IDS evaluated on NSL-KDD report 96% accuracy, though explicit energy and latency values are not numerically quantified. In contrast, The Deep Learning approach accuracy of 88% to 97% range and the Machine Learning approach, an accuracy of 88% to 98% range is obtained in WSN environments.

The comparative analysis lies in the integration of bio-inspired optimization with lightweight classifiers, which enables dataset-agnostic performance stability without imposing excessive energy or delay overhead. Unlike deep learning IDSs that rely on high-dimensional feature spaces (e.g., CICIDS2017 with 85 features), optimization-driven models effectively operate on reduced feature subsets (10–15 features) while preserving detection performance. This balance between numerical accuracy gains, measurable energy reduction, and low latency highlights a scalable and deployable IDS design paradigm for WSN-IoT systems. Consequently, the results demonstrate that hybrid optimization–ML frameworks offer a superior trade-off across all evaluated datasets, establishing a practical direction for future real-time and energy-aware intrusion detection research.

REFERENCES

1. B. Mopuru and Y. Pachipala, “Advancing IoT Security: Integrative Machine Learning Models for Enhanced Intrusion Detection in Wireless Sensor Networks,” Engineering, Technology & Applied Science Research, vol. 14, no. 4, pp. 14840–14847, 2024.
2. M. Nivaashini et al., “FEDDBN-IDS: Federated Deep Belief Network-Based Wireless Network Intrusion Detection System,” EURASIP Journal on Information Security, 2024.
3. A. Donkol, Ali G. Hafez, Aziza I. Hussein and M. Mourad Mabrook, “Optimization of Intrusion Detection Using Likely Point PSO and Enhanced LSTM-RNN Hybrid Technique in communication Networks”, IEEE Access, vol. 21, 2017
4. Halima Sadia, Saima Farhan, Yasin Ul Haq, Rabia Sana, Tariq Mahmood, Saeed Ali Omer Bahaj and Amjad Rehman Khan, “Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach”, IEEE Access, vol. 12, 2024
5. Y. Zhou, X. Li, and H. Zhang, “Dimensionality Reduction and Feature Optimization for Intrusion Detection in WSN-IoT Environments,” Sensors, vol. 24, no. 9, pp. 4211–4226, 2024.
6. K. Sharma and P. K. Singh, “Ensemble Learning-Based Intrusion Detection for Resource-Constrained Wireless Sensor Networks,” Journal of Network and Computer Applications, vol. 224, pp. 103847, 2024.
7. F. S. Alsubaei, “Smart Deep Learning Model for Enhanced IoT Intrusion Detection,” Scientific Reports, 2025.
8. [8] P. Sinha et al., “An Efficient Data Driven Framework for Intrusion Detection in Wireless Sensor Networks Using Deep Learning,” Scientific Reports, 2025.
9. A. Verma, R. Kumar, and S. Banerjee, “Lightweight Deep Learning-Based Intrusion Detection for Resource-Constrained IoT Networks,” IEEE Internet of Things Journal, vol. 12, no. 3, pp. 2145–2158, 2025.
10. H. Alqahtani and M. A. Khan, “Energy-Efficient Machine Learning Framework for Secure Wireless Sensor Networks,” IEEE Sensors Journal, vol. 25, no. 7, pp. 8891–8902, 2025.
11. J. Wang, Y. Liu, and Z. Chen, “Hybrid CNN–LSTM Model for Real-Time Intrusion Detection in IoT-Enabled WSNs,” Future Generation Computer Systems, vol. 147, pp. 112–124, 2025.
12. S. R. Patel and K. N. Patel, “Federated Learning-Based Privacy-Preserving Intrusion Detection in IoT Networks,” Computer Networks, vol. 243, pp. 110322, 2025.
13. M. Elhoseny, A. Abdelaziz, and K. Shankar, “Explainable AI-Based Intrusion Detection for Secure Industrial IoT Systems,” IEEE Transactions on Industrial Informatics, vol. 21, no. 2, pp. 1764–1775, 2025.

14. M. Hassan, T. Alshammari, and A. Jolfaei, “Lightweight Deep Learning Framework for Real-Time Intrusion Detection in IoT-Based Wireless Sensor Networks,” IEEE Internet of Things Journal, vol. 12, no. 6, pp. 5872–5884, 2025.
15. L. Chen, J. Sun, and Y. Wang, “Federated and Privacy-Aware Intrusion Detection System for Large-Scale IoT Networks,” Future Generation Computer Systems, vol. 149, pp. 341–353, 2025.
16. A. Kumar and R. Buyya, “Adaptive and Explainable Deep Learning Models for Intrusion Detection in Industrial IoT Systems,” Expert Systems with Applications, vol. 238, pp. 121812, 2025.
17. M. Karthikeyan, D. Manimegalai, and K. RajaGopal, “Firefly Algorithm Based WSN-IoT Security Enhancement with Machine Learning for Intrusion Detection,” Scientific Reports, vol. 14, 2024.