Machine Learning Based IDS for WSNs: A Review

Manu Devi
Department of Computer Science and Enginnering
University Institute of Engineering and Technology, Maharshi Dayanand University
Rohtak, Haryana, India
manughanghas26@gmail.com

Priyanka Nandal
Department of Computer Science and Enginnering
Maharaja Surajmal Institute of Technology
New Delhi, India
priyankanandal@msit.in

Harkesh Senrawat
Department of Computer Science and Enginnering
University Institute of Engineering and Technology, Maharshi Dayanand University
Rohtak, Haryana, India
sehrawat_harkesh@yahoo.com

***Abstract*—A vital role is played by Wireless Sensor Networks (WSNs) in modern applications, ranging from environmental monitoring to healthcare and industrial automation. Nevertheless, WSNs are susceptible to various security threats, such as resource constraints, limited power supply, and vulnerability to attacks due to their inherent characteristics. A promising solution for enhancing WSN security by detecting anomalies and identifying malicious activities within the network are provided by the Machine Learning (ML)-based Intrusion Detection Systems (IDSs). A comprehensive examination of recent advancements in ML-based IDSs for WSNs, highlighting various techniques, including supervised, unsupervised, and deep learning approaches is provided in this review. Each approach's strengths and limitations are discussed, evaluating their applicability in addressing the unique challenges of WSN security, such as real-time processing, energy efficiency, and scalability. The paper emphasizes the necessity of hybrid models, lightweight ML techniques, and secure, resilient WSN frameworks to address evolving security threats in WSN environments. The review concludes by identifying current challenges and potential future research directions.**

Keywords—machine learning, deep learning, intrusion detection system, wireless sensor networks

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have become an integral part of numerous applications, including environmental monitoring, healthcare, industrial automation, and smart cities. These networks consist of distributed, often small and resource-constrained sensor nodes that gather and communicate data wirelessly. While WSNs offer significant benefits, they are also highly susceptible to a range of security threats due to their open wireless communication, limited computational power, and restricted energy resources. Ensuring the security of WSNs is crucial, as breaches can compromise data integrity, network functionality, and overall system reliability.

Intrusion Detection Systems (IDSs) have emerged as essential tools for protecting WSNs from malicious attacks by monitoring network traffic, identifying suspicious behaviour, and alerting network administrators to potential security breaches [1]. Traditional IDS approaches, however, are often unsuitable for WSNs due to their high computational requirements, limited adaptability, and inability to manage the unique resource constraints of WSN nodes. Machine Learning (ML) and Deep Learning (DL) -based IDSs offer a promising alternative by leveraging advanced algorithms to analyse network patterns, detect anomalies, and predict attacks more effectively and efficiently [2]. By automating the detection process, ML and DL-based IDSs reduce the need for manual monitoring, adapting over time to recognize new types of threats and enhancing overall WSN security. Various ML techniques, including supervised learning, unsupervised learning, and deep learning, have been applied in IDSs to achieve higher detection accuracy, faster response times, and lower energy consumption. Fig. 1 conceptually illustrates how an IDS within a WSN monitors and analyzes data transmission to detect any threats or anomalies that could compromise network security. This figure illustrates an IDS within a WSN, where interconnected sensor nodes transmit data to central analysis points. These analysis nodes evaluate network data flow, with subtle alert symbols indicating potential threat detection. The gradient background emphasizes a secure, digital environment, highlighting the IDS's role in monitoring for anomalies across the network pathways. The visual elements collectively represent the IDS's continuous surveillance and protective function within WSNs.

Fig. 1. Operation of an IDS within a WSN.

This review provides a comprehensive analysis of recent advancements in ML and DL-based IDSs for WSNs. We explore different ML and DL approaches, examining their applicability to the specific constraints and security needs of WSNs. In particular, we focus on techniques that improve detection accuracy, computational efficiency, and scalability. Additionally, we assess existing ML-based IDS frameworks for WSNs, comparing and analysing their strengths and limitations. The review concludes with a discussion on current challenges and potential research directions, emphasizing the need for lightweight, adaptable, and hybrid ML-based solutions tailored to the dynamic security landscape of WSNs.

II. BACKGROUNG OF WSNS

WSNs are specialized networks consisting of distributed, autonomous sensors that gather, process, and communicate data about environmental or physical conditions, such as temperature, humidity, motion, or sound. As low-power, low-cost solutions, WSNs are fundamental to various applications,

979-8-3315-3469-1/24/$31.00 ©2024 IEEE
DOI 10.1109/ICPIDS65698.2024.00043

from industrial and environmental monitoring to healthcare and smart cities. Despite their advantages, WSNs face unique challenges, particularly in maintaining security, due to their deployment in often hostile and dynamic environments with limited resources.

A. Architecture and Components of WSNs

The architecture of WSNs typically follows a layered model that includes sensor nodes, sink nodes, and a central gateway for data collection and processing [3].

- Sensor Nodes: These nodes sense physical phenomena, convert them into digital signals, and send the data to nearby nodes or the base station. Each node typically consists of sensing, processing, transceiver, and power units, which are optimized for low power consumption.
- Sink Nodes: Sink nodes act as intermediaries between sensor nodes and the central server or gateway. They aggregate and relay data from multiple sensor nodes to reduce redundancy and communication overhead.
- Gateway or Base Station: This component serves as the main point of communication between the sensor network and external applications. It collects data from sink nodes and may perform additional processing or filtering before transmitting it to the central server or end-user application.
- Power Management: Power units (typically batteries) are crucial, as WSN nodes are deployed in resource-constrained environments where replacing or recharging batteries can be challenging.

The communication in WSNs can follow various network topologies, such as star, mesh, or hybrid, depending on the application requirements. The architecture of WSN is represented in Fig. 2. The sensor nodes in the sensor field monitor a target event and send data to cluster heads for aggregation. The cluster heads then forward the data to a sink (or base station), which acts as an intermediary, transmitting the collected information to remote users via the internet or satellite. Users can access and analyze the data through connected devices, allowing real-time monitoring and decision-making.

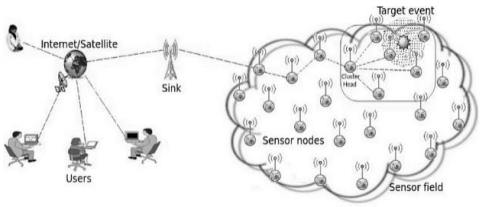

Fig. 2. Architecture of WSN.

B. Applications of WSNs

The WSNs have broad applications across multiple domains such as environmental monitoring, industrial automation, healthcare, smart cities and agriculture [4]. WSNs monitor environmental parameters in remote or hazardous areas, including forest fire detection, water quality monitoring, and wildlife tracking. In manufacturing, WSNs are used to monitor machinery, detect failures, optimize energy consumption, and maintain worker safety. Wearable or implantable WSNs track patient health metrics in real-time, enabling continuous monitoring in applications such as elder care, rehabilitation, and chronic disease management. WSNs support intelligent traffic management, energy-efficient lighting, waste management, and air quality monitoring in urban environments. In precision agriculture, WSNs are used to monitor soil moisture, weather conditions, and crop health, leading to optimized irrigation and resource use.

C. Security Challenges in WSNs

Despite their versatility, WSNs are vulnerable to a range of security threats, which can compromise the integrity, availability, and confidentiality of data. Key security challenges include resource constraints, physical vulnerability, communication security, scalability and node heterogeneity, and energy depletion attacks [5]. Limited energy, processing power, and memory in sensor nodes make it challenging to implement traditional security protocols, necessitating lightweight solutions. Sensor nodes deployed in hostile or remote environments can be physically tampered with, leading to compromised data or unauthorized network access. WSNs rely on wireless communication, making them susceptible to eavesdropping, data interception, and network manipulation. The network often requires scaling, leading to integration challenges and increased susceptibility to attacks like spoofing or jamming. Since nodes have limited power, attackers can launch battery-draining attacks, such as Denial of Service (DoS), to deplete node resources and disrupt network function [6].

In response to these challenges, WSNs require robust yet efficient security solutions. ML-based IDSs are a promising approach to address these security challenges by identifying anomalous network behavior and potential intrusions.

III. IDS FOR WSNS

IDS are critical for safeguarding WSNs from various types of attacks, including unauthorized access, data tampering, and DoS attacks. WSNs, due to their open and resource-constrained nature, are especially vulnerable to security threats, making IDS an essential layer of defense. IDS for WSNs monitor network activity to detect abnormal behavior that could indicate an intrusion or a security breach.

A. Types of IDS for WSNs

There are three types of IDS for WSNs, namely signature-based IDS, Anomaly-Based IDS, and Hybrid IDS as depicted in Fig. 3.

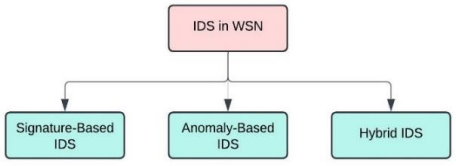

Fig. 3. Types of IDS in WSN.

1) Signature-Based IDS: Signature-based IDS operates by comparing network activity against a database of known attack patterns or signatures [7]. If the behavior matches a known signature, it is flagged as an intrusion. The main advantage of signature-based IDS is that they are efficient at detecting known attacks with low false positive rates. The limitation is that they cannot detect new or previously

unknown attacks (zero-day attacks) as it relies on predefined patterns. They are applicable in environments with well-known threat patterns, but limited in highly dynamic WSNs where new types of attacks frequently emerge.

2) Anomaly-Based IDS: Anomaly-based IDS models normal behavior of the network and flags any deviations from the expected patterns as potential intrusions [8]. This approach uses statistical methods or machine learning algorithms to detect outliers in network activity. The advantage lies in the capability of detecting unknown attacks or novel attacks since it does not rely on predefined signatures. The limitations are higher false positive rates, as not all deviations from normal behavior are necessarily intrusions. They are well-suited for dynamic WSN environments where behaviors can vary, though its resource-intensiveness may be a drawback for resource-constrained sensor nodes.

3) Hybrid IDS: Hybrid IDS combines both signature-based and anomaly-based techniques to leverage the strengths of both approaches [9]. Signature-based detection is used for known attacks, while anomaly-based techniques detect new or unknown threats. Hybrid IDS are more comprehensive and accurate, with improved detection rates and lower false positives compared to using either approach in isolation [10]. Hybrid IDS can be resource-intensive, making it more challenging to implement in WSNs with limited power and processing capabilities. Hybrid IDS can offer a balanced solution, particularly for high-risk environments where both known and unknown threats are common.

B. IDS Architectures for WSNs

There are three types of IDS architectures for WSNs, namely centralized IDS, distributed IDS, and hierarchical IDS as depicted in Fig. 4.

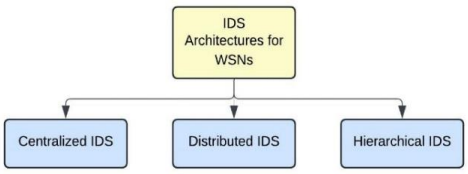

Fig. 4. Types of IDS architectures in WSN.

1) Centralized IDS: In this architecture, a central base station or sink node collects data from sensor nodes and analyzes it for potential intrusions [11]. The IDS resides at a single point of control. This architecture simplifies detection and management as all data is processed at one location, allowing for more complex IDS algorithms. The limitation is that the centralized approach creates a single point of failure and can introduce significant communication overhead, leading to energy depletion in sensor nodes. It is suitable for small-scale WSNs where the energy and resource limitations are less severe, or when the WSN is deployed in a controlled environment.

2) Distributed IDS: In distributed architectures, each sensor node or cluster of nodes independently monitors local traffic and performs intrusion detection [12]. These nodes may collaborate to detect attacks in the entire network. The advantage of distributed IDS is that there is no single point of failure, more scalable, and reduces the burden on the central node by distributing the detection process. The distributed IDS requires additional processing power at the sensor nodes, which could drain their already limited energy supplies. This type of architecture is preferred for large-scale WSNs or networks deployed in hostile or dynamic environments, where centralized approaches are impractical.

3) Hierarchical IDS: This architecture combines elements of centralized and distributed systems by organizing nodes into clusters, with cluster heads responsible for monitoring traffic within their clusters [13, 14]. The cluster heads forward suspicious data to a central base station for further analysis. Load and energy consumption is balanced between the nodes and cluster heads, offering scalability while reducing the communication overhead. This type of architecture is more complex to implement and may still be vulnerable if a cluster head is compromised. It is suitable for large-scale networks with hierarchical organization, such as WSNs used for environmental monitoring or industrial automation.

C. Challenges in Implementing IDS for WSNs

There major challenges in implementing IDS for WSNs [15, 16] are illustrated in Fig. 5.

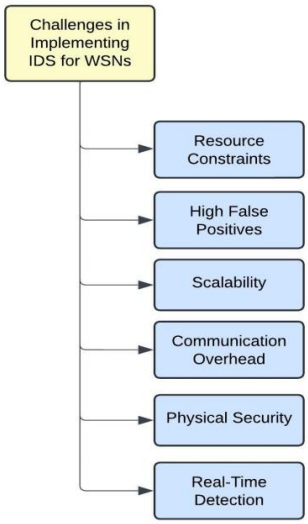

Fig. 5. Challenges in implementing IDS in WSNs.

1) Resource Constraints: WSN nodes have limited computational power, memory, and battery life. IDS algorithms, especially those involving machine learning or anomaly detection, can be resource-intensive, making it difficult to balance security with resource preservation. The possible solution is to use lightweight IDS algorithms designed specifically for low-power environments, and optimize communication protocols to reduce energy consumption during data transmission.

2) High False Positives: Anomaly-based IDS in particular may suffer from high false positive rates, where

benign behavior is flagged as an intrusion. This not only creates unnecessary alarms but also drains the limited resources of sensor nodes. The possible solution is to improve IDS accuracy through hybrid detection techniques, fine-tuning thresholds, or applying advanced machine learning models that can better differentiate between normal and abnormal behavior.

3) Scalability: As WSNs grow in size, IDS must scale accordingly. Centralized IDS architectures may struggle to handle large amounts of data in large-scale WSNs, leading to bottlenecks and inefficiencies. The possible solution is to use distributed or hierarchical IDS architectures to distribute the load and make the system more scalable. Additionally, adaptive IDS models that adjust based on network conditions can improve performance in large networks.

4) Communication Overhead: Frequent communication between sensor nodes for IDS purposes can increase the overall communication overhead, draining energy and reducing the network's lifespan. The possible solution is to implement techniques such as data aggregation and in-network processing to minimize the amount of data that needs to be transmitted, thus reducing communication overhead.

5) Physical Security: Sensor nodes in WSNs are often deployed in open, unattended environments, making them vulnerable to physical tampering. Attackers can physically access the nodes, modify them, or extract sensitive information. Possible solution is to incorporate tamper-resistant hardware, encryption, and physical security measures where possible, and monitor the physical state of nodes to detect tampering.

6) Real-Time Detection: WSNs often operate in real-time applications (e.g., military or healthcare settings), so IDS must detect and respond to threats quickly. However, real-time detection can be challenging in resource-constrained networks. Possible solution is to optimize IDS algorithms to ensure fast detection while minimizing resource consumption, potentially using heuristic or machine learning approaches designed for low-latency processing.

Therefore, while IDS is crucial for securing WSNs, implementing effective and efficient IDS in these networks presents several unique challenges. The trade-offs between detection accuracy, resource consumption, and scalability must be carefully balanced to protect WSNs from intrusions without compromising their primary functions.

D. IDS process in WSNs

The general process of an IDS in WSNs is depicted in Fig. 6. The IDS begin by collecting data from various sensor nodes within the WSN. This data may include network traffic, communication patterns, node behavior, and other relevant metrics. The data is gathered in real time and is often pre-processed to remove noise or irrelevant information. Relevant features to identify intrusions are extracted from the collected data. These features could include packet size, transmission rate, energy consumption, signal strength, and node location. Then ML or DL detection algorithm is applied to identify attacks. Based on the detection results, the IDS classify activities as normal or suspicious. If suspicious activity is detected, the system raises an alert or flags the potential intrusion. Upon detecting an intrusion, the IDS can initiate a response. This may involve isolating the compromised node, rerouting data, adjusting network configurations, or sending alerts to administrators. Modern IDSs may incorporate adaptive learning to refine their detection models over time. For instance, ML and DL-based IDSs can be retrained on new data to improve detection accuracy and adapt to evolving threats in the network.

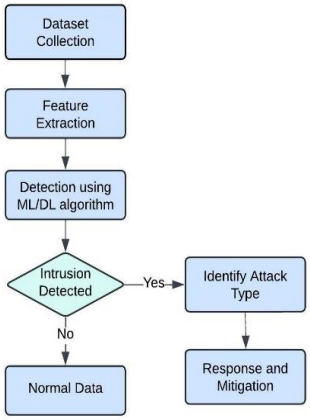

Fig. 6. IDS process in WSNs.

IV. ML AND DL TECHNIQUES FOR IDS IN WSNS

ML and DL techniques have become prominent in developing IDS for WSNs due to their capability to detect patterns, analyze large amounts of data, and adapt to evolving threats. Given the resource constraints and dynamic nature of WSNs, ML and DL offer powerful solutions to identify intrusion detection in WSNs while balancing computational efficiency and analysing complex patterns, high-level features, and temporal relationships in network traffic.

A. ML Techniques for IDS in WSNs

Fig. 7. represents the significant ML techniques used for IDS in WSNs. The explanation is given as follows.

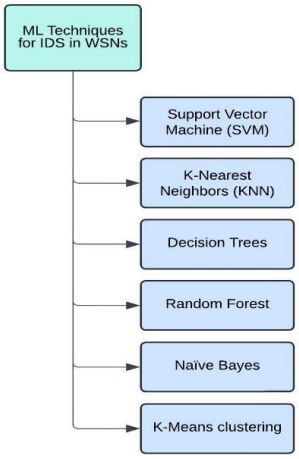

Fig. 7. ML Techniques for IDS in WSNs.

1) Support Vector Machines (SVM): SVM is a supervised learning technique that works well with small datasets and is

effective at classifying data by finding the optimal hyperplane to separate normal and malicious behavior. The major advantage is the high accuracy in binary classification problems and effective even with limited training data. The main limitation is that it is computationally expensive when dealing with large datasets, making it challenging for real-time IDS in WSNs. However, it is useful in distinguishing between normal and abnormal network traffic patterns in small-scale WSN deployments [17,18].

2) K-Nearest Neighbors (KNN): KNN is a simple, supervised ML algorithm that classifies instances based on the majority label of their nearest neighbors, where new types of attacks frequently emerge. It has high detection accuracy and is easy to implement but it requires storing a large number of samples, leading to higher memory consumption and slower performance. KNN can be used to classify network behaviors as benign or malicious, but its high memory demand makes it more suitable for specific use cases where resources are less constrained [19].

3) Decision Trees and Random Forests: Decision trees create a model of decisions based on features in the dataset, while random forest is an ensemble method that uses multiple decision trees to improve accuracy. Both are interpretable and handle non-linear data well, with Random Forest providing robustness against overfitting. Decision trees alone can overfit and be unstable, while random forests can be computationally intensive for large datasets. Random forest can detect intrusions by analyzing traffic patterns and anomalies but may need optimizations for energy efficiency [20].

4) Naïve Bayes: Naïve Bayes classifiers use Bayes' theorem and assume feature independence to classify data. It is fast and computationally efficient, suitable for WSNs with limited resources. The limitation lies in handling complex relationships between features, which can affect accuracy. It is often used in simple IDS setups to classify events in small WSNs where computational resources are minimal [21].

5) K-Means Clustering: K-Means is an unsupervised ML algorithm that clusters data points into groups based on their features, detecting anomalies as outliers. It is effective for anomaly detection in large datasets without labeled data. It is sensitive to initial settings and may struggle with complex, non-spherical data. K-Means can help in identifying anomalous behavior, particularly when labeled data is unavailable in WSN environments [22].

B. DL Techniques for IDS in WSNs

The Fig. 8. represents the significant DL techniques used for IDS in WSNs.

1) Artificial Neural Networks (ANN): ANNs are composed of interconnected layers of nodes (neurons) and can learn complex relationships between inputs and outputs. ANNs are highly flexible and capable to capture non-linear relationships in data. It requires significant computational resources, which can limit its application in resource-constrained WSNs. ANN-based IDS can identify sophisticated intrusion patterns in WSNs but may require lightweight configurations or cloud integration for practical use [23].

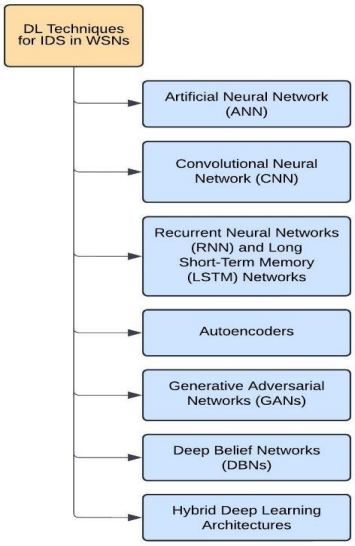

Fig. 8. ML Techniques for IDS in WSNs.

2) Convolutional Neural Networks (CNN): CNNs are primarily used for image or spatial data but have been adapted to identify patterns in sequential data by capturing local dependencies. It has high accuracy and ability to process large amounts of data efficiently, high computational demand and power consumption, which can be challenging for real-time IDS in WSNs. CNNs can detect network intrusions by analyzing data patterns, though they are more suitable for WSNs connected to more powerful processing nodes [24].

3) Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) Networks: RNNs and LSTMs are specialized in handling sequential data by capturing temporal dependencies. LSTMs, in particular, are adept at learning long-term dependencies. They are ideal for detecting patterns in time-series data, making them effective for IDS in monitoring network traffic over time. However, they are computationally heavy, requiring optimization for real-time use in WSNs. LSTM-based IDS can identify evolving attack patterns by analyzing historical traffic data, suitable for complex WSN applications with a higher power budget [25].

4) Autoencoders: Autoencoders are unsupervised learning models that learn to encode data in a reduced form and can detect anomalies by reconstructing data with minimal error for normal events. They are effective at anomaly detection, as intrusions typically show high reconstruction error. Significant processing power is required, limiting its applicability in low-power WSN nodes. Autoencoders are useful for anomaly-based IDS, where sensor nodes perform minimal processing and rely on a central node for data reconstruction and anomaly detection [26].

5) Generative Adversarial Networks (GANs): GANs consist of two neural networks (generator and discriminator) that compete to improve their respective outputs, useful for generating synthetic data and anomaly detection. GANs are effective in detecting outliers by modeling normal data

distribution. High computational and energy requirements are the limitations, often impractical for WSNs without significant optimizations. GANs can detect intrusions by comparing actual data patterns to generated patterns of normal behavior, though they are generally more suitable for WSNs with external processing capabilities [27].

6) Deep Belief Networks (DBNs): DBNs are a type of deep neural network composed of multiple layers of Restricted Boltzmann Machines (RBMs) stacked on top of each other. DBNs can learn complex, hierarchical representations of data, making them suitable for intrusion detection. DBNs can capture high-level features in data, which enhances the IDS's ability to detect sophisticated attacks. Training DBNs is computationally intensive, and the network is resource-hungry, making it more suitable for high-powered devices in the WSN. DBNs can be used in IDS for feature extraction and anomaly detection in WSNs, particularly in cases where high-level representation is needed. However, given the computational demands, they are typically deployed on central nodes or external servers [28].

7) Hybrid Deep Learning Architectures: Hybrid models combine multiple deep learning architectures to leverage the strengths of each. For example, a CNN-LSTM model uses CNN layers to extract spatial features and LSTM layers to analyze temporal dependencies. Thereby capturing both spatial and temporal patterns, which is beneficial for comprehensive intrusion detection. Hybrid architectures are more complex and require significant computational resources, which can limit their use in resource-constrained WSN nodes. Hybrid CNN-LSTM or CNN-RNN models are useful for analyzing complex intrusion patterns that have both spatial and temporal characteristics, such as identifying coordinated attacks across different parts of the network over time. They are suitable for centralized or high-capacity nodes [29].

V. Recent Survey of ML/DL-based IDS for WSNs

ML and DL techniques have emerged as a powerful tools to develop IDS in WSNs. These techniques offer advanced analytical capabilities over traditional methods by automatically building detection models from training data, reducing the need for manual signature writing or behavior specification that improve intrusion detection accuracy and efficiency. Several studies have explored the application of ML and DL techniques for intrusion detection in WSNs, including logistic regression, naïve Bayes, K-Nearest Neighbors (KNN), CNN, decision trees, random forests, and SVM [30-32] .

Recent studies continue to employ classic ML algorithms like SVM and decision trees for IDS in WSNs due to their relatively low computational cost. For example, [33] combined SVM with feature selection methods to optimize intrusion detection performance with minimal resource consumption, making it suitable for deployment in energy-constrained WSNs.

Ensemble methods, such as LSTM & Multilayer Perceptron (MLP), have been explored for WSN-based IDS, as they combine the strengths of multiple algorithms to improve detection accuracy. For instance, [34] proposed an ensemble model integrating multiple classifiers, achieving high detection rates and low false-positive rates. The model was designed to adapt to WSN environments by minimizing the computational overhead typically associated with ensemble models.

Clustering-based methods, especially K-means and Density-Based Spatial Clustering (DBSCAN), have gained attention for their ability to detect anomalies without labeled data. In 2024, [35] employed a clustering-based anomaly detection model for WSNs, where K-means clustering helped identify abnormal patterns in network traffic, enhancing IDS performance in detecting unknown attacks. However, the model required optimization to reduce resource usage, a common challenge in WSN applications.

CNNs have been widely adopted in IDS for WSNs due to their strong feature extraction capabilities. Abed et al. [36] used a CNN-based IDS to analyze packet headers as image-like structures, achieving accurate intrusion detection by capturing spatial patterns in network data. CNNs are particularly effective at recognizing known intrusion patterns, though they require optimization when deployed on resource-limited sensor nodes. This has led to research on lightweight CNN variants specifically tailored for WSN applications.

The ability of RNNs, particularly LSTM networks, to capture temporal dependencies in data has proven valuable in IDS for WSNs. Halbouni et al. [37] employed an LSTM-based model to monitor WSN traffic for signs of sequential anomalies, identifying multi-stage attacks over time. LSTM networks, a type of RNN, have demonstrated effectiveness in capturing temporal dependencies and detecting nuanced sequential patterns in network traffic. LSTMs are useful in detecting complex attacks like Distributed Denial of Service (DDoS) attacks. However, due to the high computational demand, LSTM models in WSNs often require optimization, such as pruning or quantization, to reduce memory and energy consumption.

Autoencoders have been widely used for unsupervised anomaly detection in IDS for WSNs. In 2022, [26] applied an autoencoder-based model that learns patterns of normal network traffic, detecting deviations as potential intrusions. By comparing the reconstruction error, the model effectively identified anomalies without requiring labeled data. Autoencoders are particularly useful in WSNs where labeled attack data is scarce, though they require centralized deployment due to computational demands.

GANs have emerged as a promising technique for IDS, primarily for generating synthetic attack data to train other models. Hemalatha and Amanullah [38] developed a GAN-based IDS to generate synthetic intrusion samples, which were used to train a CNN-based model to improve detection accuracy. GANs address the challenge of limited labeled intrusion data in WSNs, but their high computational requirements limit their deployment to more powerful nodes, such as base stations or cloud resources.

Hybrid architectures combining multiple deep learning models, such as CNN-LSTM, have shown promise in balancing the strengths of various techniques. For example, [39] implemented a CNN-LSTM hybrid IDS for WSNs, where the CNN component handled spatial feature extraction while the LSTM processed temporal patterns. This model demonstrated high accuracy in detecting complex intrusion patterns, making it suitable for dynamic WSN environments. Hybrid architectures often require computational offloading,

where processing is shifted from sensor nodes to base stations or edge servers to manage resource constraints effectively.

Interestingly, some research has focused on optimizing ML and DL models for improved performance. For instance, a nature-inspired whale optimization algorithm has been used to optimize CNN parameters, resulting in enhanced intrusion detection accuracy compared to conventional Deep Neural Networks (DNN), random forests, and decision trees [40]. Another study proposed an intelligent differential evolution-based feature selection technique combined with a deep neural network (IDEFS-DNN) to select optimal features and classify intrusions, reducing complexity and improving classifier outcomes [41].

Lightweight approaches for IDS in WSNs have been used recently. These approach focuses on minimizing resource usage while maintaining effective detection capabilities [42-44].

Recent literature underscores the potential of ML and DL models to enhance IDS effectiveness in WSNs. While traditional ML approaches such as SVM and ensemble models remain popular for their low computational cost, DL architectures, including CNNs, LSTMs, autoencoders, and GANs, offer higher detection accuracy and adaptability to complex attack patterns. Thus, ML and DL-based IDSs for WSNs have shown great potential in improving detection accuracy, efficiency, and adaptability to evolving threats.

Table 1 summarizes the recent studies on various ML and DL techniques for intrusion detection in WSNs in tabular form. The recent literature presented in the table highlights the strengths and limitations of the models in adapting to the constraints of WSN environments.

TABLE I. TABULAR FORM REPRESENTING THE MODEL USED, ITS ADVANTAGES AND LIMITATIONS

Method	Approach Used	Advantages	Limitations
Support Vector Machine (SVM)	SVM combined with feature selection [33]	Low computational cost, suitable for energy-constrained WSNs	Limited to linear classification; may struggle with complex patterns
Decision Trees	Used in hybrid architectures [32]	Efficient and interpretable; balances accuracy and computational efficiency	Prone to overfitting; performance may degrade with complex intrusion patterns
LSTM & Multilayer Perceptron (MLP)	Ensemble of classifiers [34]	High detection accuracy, low false-positive rate; robust in diverse WSN environments	Higher computational overhead, requires optimization for resource-limited WSN nodes
K-means & DBSCAN	Clustering for anomaly detection [35]	Detects anomalies without labeled data, useful for unknown attack patterns	Resource-intensive; often requires optimization to fit WSN constraints
Convolutional Neural Network (CNN)	CNN for spatial pattern analysis [36]	High accuracy in detecting known intrusion patterns; strong feature extraction	Requires optimization for resource-limited nodes; computationally demanding
Long Short-Term Memory (LSTM)	Temporal anomaly detection [37]	Captures temporal dependencies, effective for multi-stage attack detection	High computational demand; needs pruning or quantization for WSN deployment
Autoencoders	Unsupervised anomaly detection [26]	Effective in detecting deviations without labeled data; adaptable to anomaly patterns	Requires centralized deployment due to computational needs; may be inefficient in resource-limited WSN
Generative Adversarial Networks (GANs)	Synthetic data generation for IDS training [38]	Addresses limited labeled data; improves detection accuracy in CNN-based IDS	High computational requirements; typically limited to base stations or cloud resources
CNN-LSTM Hybrid	Combines spatial and temporal analysis [39]	High accuracy, effective in dynamic environments; leverages strengths of CNN and LSTM	Requires offloading to manage computational constraints in WSN
Whale Optimization Algorithm with CNN	CNN optimization for intrusion detection [40]	Enhances CNN accuracy, outperforming traditional ML models	May add complexity in optimization process; requires specialized tuning
IDEFS-DNN	Differential evolution feature selection with DNN [41]	Reduces complexity, improves classifier performance, optimized feature selection	Complexity in feature selection process; may require extensive data preprocessing
Lightweight approach based on Decision Tree	Gini feature selection method [42]	Processing time reduced	Trained on only one unbalanced dataset
Ensemble Feature Selection	Ensemble Feature Selection (EFS) technique [43]	Reduced resource consumption, improved detection accuracy	Dependency on feature selection techniques, complexity in ensemble design
Received Signal Strength Indicator (RSSI)	Received Signal Strength Indicator (RSSI) values of packets to detect attacks [44]	Lightweight and efficient, real-time detection, easy deployment	Sensitivity to environmental factors, vulnerability to RSSI spoofing

VI. Conclusion

This review highlights the significant advancements in ML and DL-based IDS for WSNs. ML and DL techniques provide promising approaches to enhance the detection of malicious activities and anomalies in WSNs, especially given their ability to handle large amounts of data and adapt to complex attack patterns. Traditional ML algorithms, such as SVM, decision trees, and ensemble methods, have shown effectiveness in balancing detection accuracy and computational efficiency, making them suitable for resource-constrained WSN environments. Meanwhile, DL models, including CNNs, RNNs, and hybrid architectures like CNN-LSTM, have demonstrated superior accuracy in detecting sophisticated intrusions, albeit with higher computational demands.

Despite the progress, several challenges remain in implementing IDS in WSNs. Resource constraints, limited labeled data, and the need for real-time processing continue to pose obstacles to practical deployment. To address these issues, ongoing research is focusing on lightweight models, optimization techniques, and hybrid architectures that can adapt to the dynamic nature of WSNs. Future directions may involve the integration of edge computing, transfer learning, and unsupervised learning methods to create IDS solutions that are both scalable and efficient for diverse WSN applications.

Overall, ML and DL-based IDS models have the potential to significantly enhance the security of WSNs, contributing to robust defense mechanisms that protect these networks against a wide array of threats. Continued research and development in this field will be critical for achieving secure, resilient, and sustainable WSNs in an increasingly connected world.

References

1. I. Butun, S.D.Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," IEEE communications surveys & tutorials, vol. 16, no.1, pp. 266-282, 2013.
2. S. Otoum, B. Kantarci, and T.H. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," IEEE Networking Letters, vol. 1, no. 2, pp. 68-71, 2019.
3. H. Karl, and A.Willig, "Protocols and architectures for wireless sensor networks," John Wiley & Sons, 2007.
4. H. M. A. Fahmy, "WSNs applications. In Concepts, applications, experimentation and analysis of wireless sensor networks," Cham: Springer Nature Switzerland., pp. 67-242, 2023.
5. S. A. Salehi, M.A. Razzaque, P. Naraei and A. Farrokhtala, "Security in wireless sensor networks: Issues and challenges," In 2013 IEEE International Conference on Space Science and Communication, pp. 356-360, 2013.
6. M. Devi, P. Nandal and H. Sehrawat, "DDOS Attack in WSN Using Machine Learning," International Conference on Innovative Computing and communication, Singapore: Springer Nature Singapore, pp. 859-872, 2023.
7. S.Einy., C.Oz and Y.D. Navaei, "The anomaly-and signature-based IDS for network security using hybrid inference systems," Mathematical Problems in Engineering, pp. 6639714, 2021.
8. K. Devika, R. Rajakumar, R. Manikandan, K. Dineshand M. Sreedevi, "A review on Machine Learning based IDS approaches in Wireless sensor networks," In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Vol. 1, pp. 1238-1243, 2023.
9. D. W. Huang, F. Luo, J. Biand M. Sun, "An efficient hybrid IDS deployment architecture for multi-hop clustered wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2688-2702, 2022.
10. Ansam Khraisat et al., "Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine," Electronics, vol. 9. No. 1, pp. 173, 2020.
11. D. W.Huang, F. Luo, J. Biand M. Sun, "An efficient hybrid IDS deployment architecture for multi-hop clustered wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2688-2702, 2022.
12. K. Medhat, R.A. Ramadan and I. Talkhan, "Distributed intrusion detection system for wireless sensor networks," 9th International Conference on Next Generation Mobile Applications, Services and Technologies, IEEE, pp. 234-239, 2015.
13. S.Shin, T. Kwon, G.Y.Jo, Y. Park and H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks," IEEE transactions on industrial informatics, vol. 6, no. 4, pp 744-757, 2010.
14. G. G. Gebremariam, J., Panda and S. Indu, "Design of advanced intrusion detection systems based on hybrid machine learning techniques in hierarchically wireless sensor networks," Connection Science, vol. 35, no. 1, pp. 2246703, 2023.
15. M.H. Behiry and M. Aly, "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods,"Journal of Big Data, vol. 11, no. 1, pp. 16, 2024.
16. D.S. Ibrahim, A.F. Mahdi and Q.M. Yas, "Challenges and issues for wireless sensor networks: A survey," J. Glob. Sci. Res, vol. 6, no. 1, pp. 1079-1097, 2021.
17. M. Safaldin, M. Otair and L. Abualigah, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks,"Journal of ambient intelligence and humanized computing, vol. 12, pp. 1559-1576, 2021.
18. E. A. Shams and A. Rizaner, "A novel support vector machine-based intrusion detection system for mobile ad hoc networks," Wireless Networks, vol. 24, pp. 1821-1829, 2018.
19. G. Liu, H. Zhao, F. Fan, Q. Xu and S. Nazir, "An enhanced intrusion detection model based on improved kNN in WSNs," Sensors, vol. 22 no. 4, pp. 1407, 2022.
20. I. Domor Mienye, N. Jere, "A Survey of Decision Trees: Concepts, Algorithms, and Applications," IEEE Access , Vol. 12, pp. 86716-86727, 2024.
21. D. Jeevaraj, "Feature selection model using naive bayes ML algorithm for WSN intrusion detection system," International journal of electrical and computer engineering systems, Vol. 14, no. 2, pp. 179-185, 2023.
22. S. Tabbassum and R.K. Pathak, "Effective data transmission through energy-efficient clustering and Fuzzy-Based IDS routing approach in WSNs," Virtual Reality & Intelligent Hardware, vol. 6(1), pp. 1-16. 2024.
23. S. Alzahrani, L. Hong, "Detection of distributed denial of service (ddos) attacks using artificial intelligence on cloud," 2018 IEEE World Congress on Services, pp. 35-36, 2018.
24. M. Zhu, K. Ye, C.Z. Xu, "Network anomaly detection and identification based on deep learning methods," Cloud Computing – CLOUD 2018, Springer, Springer International Publishing, Cham (2018), pp. 219-234, 2018.
25. S. M. S. Bukhari, M. H. Zafar, M. Abou 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, pp. 103407, 2024.
26. R. Zhao, J. Yin, Z. Xue, G.Gui, B. Adebisi, T. Ohtsuki, & H. Sari, H "An efficient intrusion detection method based on dynamic autoencoder," IEEE Wireless Communications Letters, Vol. 10, no. 8, pp. 1707-1711, 2021.
27. K. Hemalatha, and M. Amanullah, "Deep Learning Model of GRU Based Energy Effective Clustering and GAN Based Intrusion Detection in WSN," International Conference on Artificial Intelligence and Smart Energy. pp. 337-354, 2024.

28. Vikas, R. P. Daund, D. Kumar, P. Charan, R. S. K. Ingilela and R. Rastogi, "Intrusion Detection in Wireless Sensor Networks using Hybrid Deep Belief Networks and Harris Hawks Optimizer," 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, pp. 1631-1636, 2023.
29. M. Sajid, K.R. Malik, A. Almogren, T.S. Malik, A.H. Khan, J. Tanveer and A. U. Rehman, "Enhancing intrusion detection: a hybrid machine and deep learning approach," Journal of Cloud Computing, vol. 13 no. 1, 123, 2024.
30. V. Kathiresan, Dr.S. Karthik, P.Divya, D. Palanivel Rajan, " A Comparative Study of Diverse Intrusion Detection Methods using Machine Learning Techniques," International Conference on Computer Communication and Informatics (ICCCI -2022), Coimbatore, INDIA, Jan. 25-27, 2022.
31. B. Mahbooba, M. Timilsina, R. Sahal and W. Alosaimi, "Trust in Intrusion Detection Systems: An Investigation of Performance Analysis for Machine Learning and Deep Learning Models," Hindawi complexity, vol.2021, pp 23, 2021.
32. H. Tanveer, M. Ali Adam, M. Ahmad Khan, M. A. Ali, "Analysing the Performance and Efficiency of Machine Learning Algorithms, such as Deep Learning, Decision Trees, or Support Vector Machines, on Various Datasets and Applications," The Asian Bulletin of Big Data Management, vol. 3, no.2, pp. 126–136, 2022.
33. A. Davahli., M. Shamsi and G. Abaei, "A lightweight Anomaly detection model using SVM for WSNs in IoT through a hybrid feature selection algorithm based on GA and GWO," Journal of Computing and Security, Vol. 7, no. 1, pp 63-79, 2020.
34. V. S. Prasanth, A. Mary Posonia, and A. Parveen Akhther. "Effective ensemble-based intrusion detection and energy efficient load balancing using sunflower optimization in distributed wireless sensor network," Multimedia Systems, vol. 30, no. 4 pp. 223, 2024.
35. U. Rashid, M. F. Saleem, S. Rasool, A. Abdullah, H. Mustafa and A. Iqbal, A, "Anomaly Detection using Clustering (K-Means with DBSCAN) and SMO," Journal of Computing & Biomedical Informatics, vol. 7(02), 2024.
36. R. A. Abed, E. K. Hamza and A. J. Humaidi, "A modified CNN-IDS model for enhancing the efficacy of intrusion detection system. Measurement," Sensors, vol. 35, 101299. 2024.
37. A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," in IEEE Access, vol. 10, pp. 99837-99849, 2022.
38. K.Hemalatha and M. Amanullah, "Deep Learning Model of GRU Based Energy Effective Clustering and GAN Based Intrusion Detection in WSN," International Conference on Artificial Intelligence and Smart Energy, pp. 337-354.
39. H. C. Altunay [a], Z.Albayrak, "A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks," Engineering Science and Technology, an International Journal, Vol. 38, Feb.2023.
40. G. Vembu, D. Ramasamy, "Optimized deep learning-based intrusion detection for wireless sensor networks," International Journal of Communication Systems, 2022.
41. Ibrahim M EL-Hasnony, " Intelligent differential evolution-based feature selection with deep neural network for intrusion detection in wireless sensor networks," Journal of Intelligent Systems and Internet of Things, pp. 78-89, 2019.
42. M. A. Eadig, "Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach," IEEE Access, vol. 11, pp. 83537-83552, 2023.
43. M. Fatima, O. Rehman, I. M. Rahman, A. Ajmal, and S. J. Park, "Towards Ensemble Feature Selection for Lightweight Intrusion Detection in Resource-Constrained IoT Devices", Future Internet, vol. 16(10). 2024.
44. M. Sadeghizadeh, "A lightweight intrusion detection system based on RSSI for sybil attack detection in wireless sensor networks," International Journal of Nonlinear Analysis and Applications, vol. 13(1), pp. 305-320, 2022.