

FORTIFYING WIRELESS SENSOR NETWORKS USING SVM FOR ADVANCED INTRUSION DETECTION AND ATTACK PREVENTION

Mohammad Taghi Sadeghi ^{1*}  , Hiba Alzubaidi ¹ 

¹ Faculty of Technical and Engineering, University of Qom, Qom, Iran

* Corresponding author E-mail: mt.sadeghi@srbiau.ac.ir (Mohammad T. Mohammed)

RESEARCH ARTICLE

ARTICLE INFORMATION	ABSTRACT
SUBMISSION HISTORY: Received: 5 February 2025 Revised: 6 April 2025 Accepted: 22 April 2025 Published: 30 June 2025 KEYWORDS: Wireless Sensor Networks; Intrusion Detection Systems; Support Vector Machine; Cybersecurity Threats; Network Attack Prevention;	WSNs have increasingly become part and parcel of the current and emerging communication systems, hence the need for solid measures to protect this critical infrastructure from evolving cyber threats. This research investigates the development of a Supervised Machine Learning-based IDS using MLP, SVM, and LR to increase the detection of network attacks for prevention purposes. A new method is proposed that entails the integration of an inter-dataset evaluation strategy that harmonizes two heterogeneous data structures and simultaneously aims to protect models and sensitive data. The conceived framework assesses the accuracy of a variety of machine learning metrics, such as accuracy, precision, recall, and the F1 score. The results stated that the detection efficiency was significantly improved with the incorporation of inter-dataset routing. MLP achieved a maximum accuracy of 99.1%. SVM demonstrated a precision of 99.4% in certain scenarios, effectively minimizing false positives and enhancing classification confidence. Logistic Regression also showed stable precision values, contributing to consistent detection performance. These analyses stress how existing techniques for machine learning algorithms used in IDS designs cover a wide variety of purposive uses. The work done consolidating the result and outcome of this study points a way forward for subsequent studies on WSN security, with the view of providing a springboard for the development of intrusion detection systems, in view of the dynamic nature of cybersecurity.

1. INTRODUCTION

In the digital environment of the contemporary world, people interact with users from different countries constantly due to the constant sharing of information. These scenarios demonstrate the preponderance of the connectedness of the users, in which case, security threats may affect scattered and diverse individuals. The availability of new WiFi devices and the evolving nature of the networks have greatly increased the possibility of a breach and unauthorized access. Regular preventive security approaches prove ineffective in countering innovation threats, thereby requiring higher visibility protection approaches like machine learning-based Intrusion Detection Systems (IDS). However, deploying a solid IDS designed for WNs is difficult, especially when relying on supervised machine-learning techniques [1], [2]. Wireless networks, by nature, possess inherent architectural weaknesses: interception, interference, and spoofing due to the open communication environment. Other challenges that add to the difficulty of discriminating between a malicious practice and legal network use include instability of signal strength, interference, and mobility. It is important to learn how to build an IDS that can track all these subtleties if a wireless network is to be effectively protected [3], [4].

A limitation in the approach to implementing supervised machine learning for IDS is the difficulty in obtaining training and calibration datasets containing these labels. Labeling real-world wireless network traffic involving both normal and intrusive activities is both computationally expensive and time-consuming. Moreover, since new forms of cyberattacks are constantly emerging, the datasets need to be updated constantly with IO patterns. Thus making it difficult to achieve the perfect representation [5], [6].

Feature selection is another critical issue in wireless network intrusion detection. In wired networks, the backbone is between only bandwidth and latency [7], and in wireless networks, this range should include the signal strength, packet loss, and channel usage, which are important to detect intrusions accurately. The selection methods [8] and the use of these papers to optimize detection accuracy through feature selection are essential in dealing with this issue. We are given a wireless communication system, and that still features should be designed in terms of the system's properties.

Among other issues, one can list the model performance comparison and the need to choose an algorithm out of many for the application. These intrusion detection models must be evaluated, considering the particularities of wireless networks and their ability to cope with noise and dynamic environments [9]. Effective evaluation ensures that the schemes can defend against having critical knowledge and messages controlled by an adversary. As a result, we need to develop complex and realistic models for evaluation, taking the nature of wireless networks into account [2], [10].

Conversely, IDS in delivery for wireless networks has an added challenge because its success depends on three factors: scalability, flexibility, and efficiency. Wireless traffic is station-type and involves high-speed as well as high-volume data flows that require fast and precise responses to threats. Increased confrontation levels, such as underperformance bottlenecks, network interference, and the appearance of new forms of attacks, pose a complexity in the development of IDS solutions that would contain flexibility and robustness. Supervised learning techniques are found to have a significant role in the accomplishment of extensive security and accuracy linked to intrusion detection [11], [12].

The main objective of this research is to develop and evaluate a supervised machine learning-based IDS framework that is capable of effectively detecting and classifying attacks in wireless sensor networks using an inter-dataset evaluation approach. This framework specifically integrates MLP, SVM, and LR algorithms to assess detection performance and generalization capabilities.

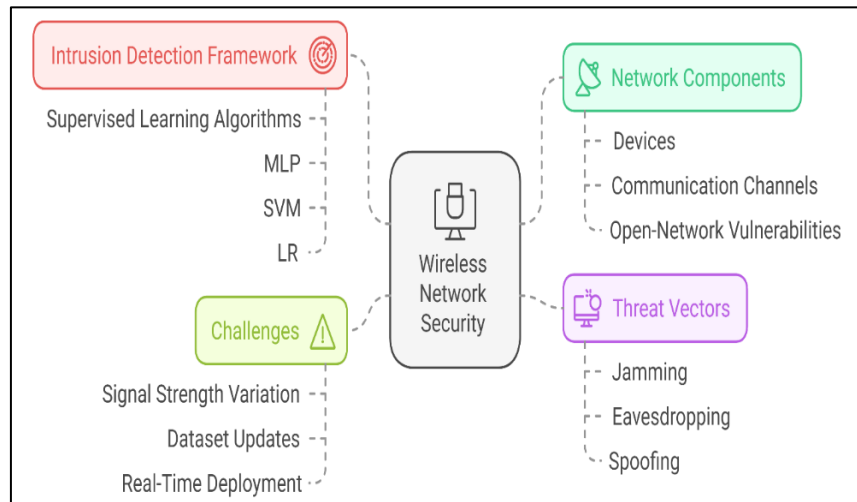


Figure 1. Overview of wireless sensor network vulnerabilities and intrusion detection framework

The novelty of this study lies in the application of a dual cross-dataset strategy that tests algorithm robustness across heterogeneous datasets (KDD-Cup99 and NSL-KDD). Unlike previous works that rely solely on in-dataset validation, our approach evaluates how well models trained on one dataset perform on another, thus reflecting real-world deployment challenges. Enterprises include slow changes in signal strength, large data outputs, and unpredictability of attacks that require solutions tailored to the wireless environment. The diagram in Fig.1 shows the relationship between these elements, presenting a conceptual framework of wireless network security.

2. RELATED WORKS

Wireless sensor networks (WSN) have been widely studied because of their great dependence on wireless communication and because new threats are emerging and attacks are more complex [13]. This section provides the literature with a summary of accomplishments and methods that

have been carried out using supervised learning algorithms, followed by feature selection and real-world datasets for IDS in wireless networks [14].

Several non-fragile publications deliberated over the use of heuristic learning approaches to optimize IDS functioning. For example, [15], an IDS based on Support Vector Machines (SVM) was suggested for the classification of flow traffic into benign and malicious. Therefore, their approach was very accurate in identifying the attacks and was able to minimize false alarms, especially in situations where the networks may encounter different types of attacks. Likewise, [16] looked at the application of MLP for anomaly detection in WSNs, where it was suggested that this type of model offers more dependable capacities for outlining decision boundaries while offering desirable detection rates. But at the same time, their work pointed out that the main obstacle is choosing the right compromise between the number of calculations required and the effectiveness of detecting intrusions.

Feature selection has also been another important research area discussed in IDS research. In [17], to provide an effective weighting of features inherent to wireless technology, a new concept is introduced that focuses on signal strength, number of lost packets, and channel usage. Their results showed that the extension of these domain-specific features enhanced the efficiency of the intrusion detection and implemented rejection of extra baggage or unrelated data, determining low computational complexity. Moreover, at [18], future research also proved the efficiency of dimensionality reduction methods like PCA for making the IDS model scalable in a high-dimensional wireless context.

Availability of the dataset and annotation are important factors that are closely related to IDS development. As proposed in [19], the paper showed the challenges associated with data labeling to incorporate realistic traffic data, especially in emerging attacks. Their study suggested synthetic network traffic generation for the modeling of different kinds of intrusions. They similarly [20] pointed out the need for frequent updating of datasets due to dynamic and ever-changing attackers' behaviors, knowledge of which was important as outdated data reduced the accuracy of machine learning-based systems.

Some of the recent articles highlighted the capacity of employing supervised machine learning algorithms in real-time IDS for WSNs. At [17], the authors examined the application of LR together with SVM and MLP to distinguish between DDoS and botnet attacks. According to their findings, while the LR model offered a sufficient accuracy rate, the SVM model outperformed in precision, while they observed better recall rates using the MLP model. These results justify the adoption of composite frameworks where various algorithms are integrated and deployed to solve various security issues in wireless systems.

However, existing IDS approaches still face difficulties in real-time implementation and flexibility when facing dynamic conditions of a network [21]. In [22], it identified bottlenecks provoked by high-volume traffic in WSNs and developed architectures to manage intensive data rates. Further, [13] discussed the possibility of utilizing the lighter versions of learners in order to avoid challenges resulting from performance restrictions and still provide highly accurate detection.

On the basis of the literature review, it can be concluded that the role of machine learning approaches, especially ones based on supervised learning, has yet to be fully utilized in improving the results of intrusion detection in WSNs. It is for this reason that problems like dataset quality, feature selection, and real-time usability remain some of the constraints with such systems. This current study extends such efforts by incorporating SVM into a sophisticated IDS model, overcoming these limitations, and contributing to the ongoing debate over wireless network security. Table 1 summarizes and analyzes the related works on IDS in WSNs based on supervised machine-learning techniques. These include the selection of the specific algorithm to be used, the type and size of the data set used, the features chosen, and most importantly, the evaluation measures and conclusions drawn from the study.

Table 1. Comparative analysis of supervised machine learning-based intrusion detection systems in wireless sensor networks

Ref.	Algorithm(s)	Dataset	Features	Performance Metrics	Key Findings
[10]	SVM	NSL-KDD	Packet size, protocol type	Precision, Recall, F1-Score	Demonstrated high precision with reduced false positives; limited scalability in high-dimensional datasets.
[16]	MLP	UNSW-NB15	Signal strength, traffic volume	Accuracy, Detection Rate	Effective in modeling complex decision boundaries, computational overhead remains a challenge.
[17]	Feature Selection + SVM	Real-world network traffic logs	Signal strength, channel usage	Feature Importance, Accuracy	Improved efficiency by selecting domain-specific features unique to wireless networks; reduced data dimensionality.
[23]	PCA + SVM	CIC-IDS2017	Reduced feature set	Precision, Accuracy	Demonstrated scalability in handling high-dimensional datasets; reduced model complexity without compromising detection accuracy.
[10]	Synthetic Dataset Creation	Custom synthetic datasets	Packet type, timing information	False Positive Rate, Recall	Proposed a method to generate synthetic datasets that cover diverse attack types, addressing real-world dataset limitations.
[11]	SVM, MLP, Logistic Regression	NSL-KDD, CIC-IDS2018	Signal strength, latency	Precision, Recall, F1-Score	SVM provided higher precision; MLP offered better recall for identifying true positives, highlighting the value of hybrid algorithm frameworks.
[13], [22]	Lightweight SVM	IoT-23	Lightweight traffic features	Latency, Accuracy, and Scalability	Developed lightweight models to balance resource constraints and detection performance in real-time environments.

Hence, although several studies have explored the use of supervised machine learning in IDS for WSNs, key limitations persist, particularly in terms of model generalizability across datasets, feature selection specific to wireless environments, and real-time deployment under high-volume traffic. Moreover, most studies validate models using only single-dataset evaluations, limiting their applicability to real-world scenarios. This research addresses these gaps by introducing a dual cross-dataset evaluation strategy, integrating MLP, SVM, and LR, and applying wireless-specific features to enhance detection performance and scalability across heterogeneous WSN conditions.

3. METHODOLOGY

3.1 The Proposed Framework

The proposed framework brings forward an inter-dataset evaluation strategy whose main purpose is to link and operate datasets in a complementary manner, minimizing individual weaknesses while leveraging mutual strengths. Based on this structure, a relational matrix is established between two datasets to enable a comprehensive evaluation of machine learning-based intrusion detection models across diverse scenarios. This approach avoids reliance on static, single-dataset validation and simulates more realistic, heterogeneous WSN environments. The main workflow of the proposed approach is illustrated in Fig. 2, including the preprocessing and feature selection of the dataset, training and testing the model. It comprehensively consists of in-dataset and cross-dataset evaluations where models are trained and tested on the KDD-Cup99 and NSL-KDD datasets. The figure above illustrates a feedback loop for model optimization and shows that a

cross-dataset training results in a stronger generalization ability and model robustness against diverse data distributions.

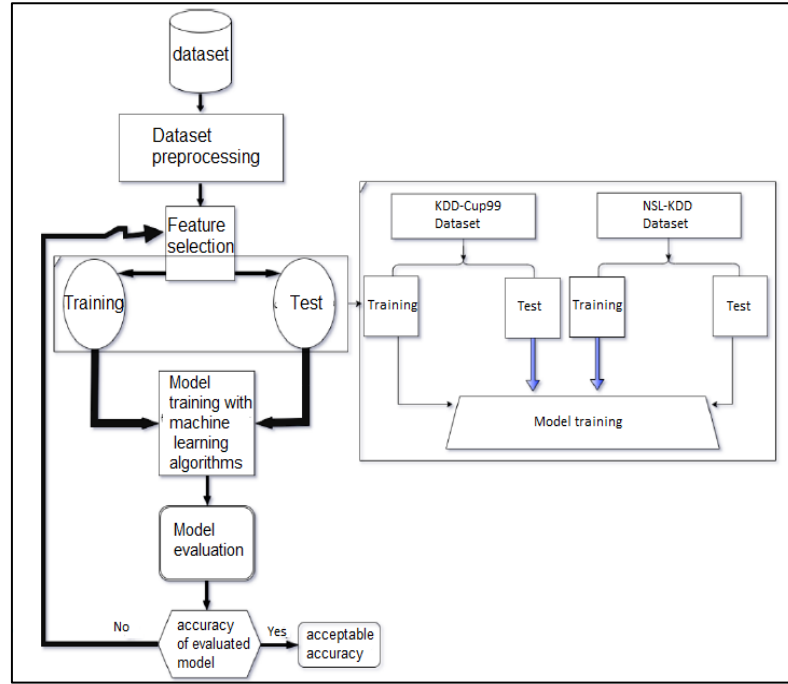


Figure 2. Steps of the proposed methodology

First. Interconnected Datasets: It interconnects the datasets where one could be a subset of the other, enabling interoperability in training and testing. This procedure improves model generalization as it evaluates the performance in different dataset contexts.

Second. A Workflow for Evaluation: Several steps are involved in the plan of action for evaluating nursing collaboratives:

- a) Preprocessing: Noise is removed, noise removed, features are scaled, and the dimension is reduced to make the model more efficient.
- b) Splitting the Dataset: The Data is divided into Training and Test sections.
- c) Model training: To determine the optimal performance, models are trained on the training data.

Evaluation metrics used shown in (1), (2), and (3):

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad \dots (1)$$

$$Precision = \frac{TP}{TP+FP} \quad \dots (2)$$

$$Recall = \frac{TP}{TP+FN} \quad \dots (3)$$

Where TP, TN, FP, and FN are true positives, true negatives, false positives, and false negatives, respectively.

Third. Cross-Dataset Protocol: One of the most important aspects of this work is the double cross-dataset evaluation procedure used instead of the classical single-dataset evaluation.

- a) Train on Dataset A → Test on Dataset B
- b) Train on Dataset B → Test on Dataset A

This iterative process contributes to increased confidence in the adaptability of models and minimizes the likelihood of overfitting or overreliance on a single data set.

Fourth. Cross-Dataset Strategy Dual Implementation: Achieving model robustness and generalization, we enforce both directions for dataset pairing. This double-stage approach improves the robustness of training (calibration) as well as the amount of overfit that can occur, while also offering some perception into the consistency of detection across datasets.

3.2 Multilayer Perceptron (MLP)

The framework comprises a class of ANN called MultiLayer Perceptron (MLP). MLP has several layers (input, hidden, and output), and neurons are completely connected between layers. It is good at learning complicated, non-linear mappings between data. Then, the forward progress of the MLP is presented as in (4):

$$a^{(l)} = \sigma(W^{(l)}a^{(l-1)} + b^{(l)}) \quad \dots (4)$$

Where:

- $a^{(l)}$ = Activations of layer l.
- $W^{(l)}$ = Weight matrix for layer l
- $b^{(l)}$ = Bias vector for layer l.
- σ = Activation function (e.g., ReLU, Sigmoid).

Indeed, due to its capability of recognizing non-linear relationships and its expandability, MLP is suitable for intrusion detection problems. Fig. 3 shows the structure of an MLP network employed in this work. It includes the input layer, which takes feature vectors in the dataset, one or more hidden layers learning non-linear patterns, and an output layer that does the classification. Every node (neuron) in a layer is connected to every node in the next layer. This structure enables the MLP to learn complex decision boundaries, and hence, it is suitable for detecting obscure and distributed intrusion patterns in WSN data. We choose the MLP because it is powerful for modeling nonlinear relationships with high-dimensional intrusion detection.

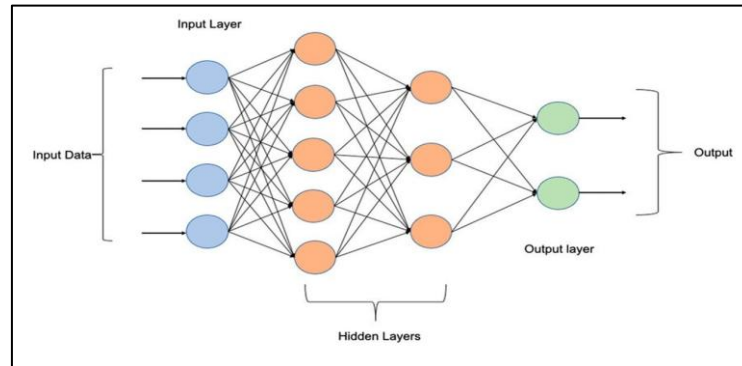


Figure 3. Structure of a typical MLP network

3.3 Support Vector Machine (SVM)

The second most significant algorithm in the framework is SVM. The SVM algorithm is implemented in a way that it finds the best boundary that discriminates the data points into two areas, regions. For two-class classification, equation (5) is the mathematical expression of the decision boundary:

$$f(x) = w^T x + b \quad \dots (5)$$

Where:

- w : Weight vector defining the hyperplane's orientation.
- x : Input vector.
- b : Bias term determining the hyperplane's position.

SVM, which separates hyper-planes in high-dimensional space and kernel functions that implicitly transform non-linear problems, is another reason why it can be used for intrusion detection. It was chosen due to its well-known accuracy and generalization capabilities even when the class boundaries are clearly separable.

3.4 Logistic Regression (LR)

We choose Logistic Regression (LR), which is a staple model for binary classification, as it has low computationally complexity and it can work effectively in a real-time binary classification

scenario, which is required in low-resource wireless settings. Calculates the probabilities using (6) as follows:

$$P(y = 1 | x) = \frac{1}{1 + e^{-z}} \quad \dots (6)$$

Where $z = w^T x + b$, LR provides a straightforward yet effective approach for intrusion detection tasks, particularly in resource-constrained environments.

3.5 Data Analysis and Data Collection

The dataset component plays a critical role in training and evaluating IDS performance. Two well-known datasets were utilized: The KDD-Cup99 dataset, which forms one of the foundational benchmarks in intrusion detection research, comprises 42 features and categorizes data into five distinct classes: one representing normal traffic and four representing various types of network attacks. While it provides a comprehensive overview of network traffic behaviors, it has been widely criticized for its high redundancy and imbalanced distribution of records, which can lead to biased model training. To address these limitations, the NSL-KDD dataset was introduced as a refined and enhanced version. NSL-KDD eliminates duplicate records, balances the dataset more effectively, and offers improved representativeness, making it more suitable for fair training and evaluation of machine learning-based intrusion detection systems. Table 2 presents classes in the dataset.

Table 2. Classes in the dataset

Class	Description
DoS	Denial of Service attacks target system availability.
R2L	Remote-to-local attacks aim to gain unauthorized access via techniques like password guessing.
U2R	User-to-root attacks escalate user privileges to the root/admin level.
Probing	Reconnaissance attacks are used to identify vulnerabilities through scanning tools like Nmap.

3.6 Hyperparameter Tuning and Model Configuration

To ensure optimal performance, each machine learning model was subjected to a hyperparameter tuning process using grid search with cross-validation. For the **MLP**, key parameters such as the number of hidden layers, neurons per layer, learning rate, and activation functions (ReLU, Sigmoid) were varied. The final model utilized two hidden layers with 8 and 6 neurons, respectively, a learning rate of 0.01, and ReLU activation, which yielded the best convergence. For SVM, tuning focused on the choice of kernel (linear, polynomial, RBF), regularization parameter **C**, and kernel coefficient γ (gamma). The best performance was achieved using the RBF kernel, with **C = 10** and $\gamma = 0.1$, providing a balanced trade-off between bias and variance. However, the cross-dataset results indicated sensitivity to data distribution, suggesting that more adaptive kernel selection or domain adaptation techniques may be needed for improved generalization.

Logistic Regression was tuned using regularization strength **C** and solver selection. The model performed best with **C = 1.0** and the 'liblinear' solver for binary classification tasks. All models were implemented within the Scikit-learn package with the additional use of 5-fold cross-validation for tuning to avoid fitting to the validation set.

4. RESULTS

We show the results of experiments with the application of the proposed type of categorization, here with emphasis on checking the performance gain achieved by using the supervised output of machine learning tools. Selection about the accuracy, recall, precision, and F1-score of the results is conducted in different conditions (i.e., inter-dataset, cross-dataset test).

4.1. Multilayer Perceptron (MLP) Results

Table 3 shows the outcomes of the MLP algorithm experimented with different DSM pair combinations. The table consists of recall, precision, F1-score, and accuracy under in-dataset and Cross-dataset. The results in Table 3 show that, in the in-dataset/cross-dataset based evaluations,

the MLP algorithm also performs stably well. Its stability and high recall in all cases, particularly the perfect recall of 1.000 when trained in KDD-Cup99 and tested in NSLKDD, indicate its better ability to detect all positive intrusion examples. This means that MLP can be well applied in dynamic WSNs where it is important to generalize between different data distributions.

Table 3. Performance metrics for MLP algorithm

Algorithm	Dataset	Recall	Precision	F1	Accuracy
MLP	KDD-Cup99, KDD-Cup99	0.997	0.997	0.997	0.998
MLP	NSL-KDD, NSL-KDD	0.998	0.987	0.990	0.981
MLP	KDD-Cup99, NSL-KDD	1.000	0.991	0.990	0.991
MLP	NSL-KDD, KDD-Cup99	0.999	0.994	0.997	0.994

4.2. Support Vector Machine (SVM) Results

Table 4 shows the Metrics of the SVM algorithm under the same proportions in the dataset tables. The table also shows that the algorithm can do both within-dataset and between-dataset assessments, which aids the evaluation of the overall generality and stability of the algorithm.

Table 4. Performance metrics for SVM algorithm

Algorithm	Dataset	Recall	Precision	F1	Accuracy
SVM	KDD-Cup99, KDD-Cup99	1.000	0.995	0.998	0.995
SVM	NSL-KDD, NSL-KDD	1.000	0.984	0.992	0.983
SVM	KDD-Cup99, NSL-KDD	1.000	0.993	0.992	0.990
SVM	NSL-KDD, KDD-Cup99	0.522	0.994	0.658	0.457

While SVM demonstrates strong performance in in-dataset settings, its recall drops significantly to 0.522 in the cross-dataset case where training was done on NSL-KDD and testing on KDD-Cup99. The overall accuracy also declines to 0.457, indicating a sharp decrease in the model's ability to detect positive cases when applied to a differently distributed dataset. This performance drop is likely due to the mismatch in feature distributions, data representations, and underlying statistical patterns between the datasets. KDD-Cup99 is more redundant and imbalanced, whereas NSL-KDD is cleaner and balanced, making cross-generalization for SVM more difficult.

Despite this, SVM maintains a high precision (0.994), meaning that when it does predict a positive case, it is almost always correct, suggesting its usefulness in high-security contexts where false positives must be minimized.

4.3. Logistic Regression (LR) Results

In more detail, the performance of the Logistic Regression (LR) algorithm is shown in Table 5 below. To determine its applicability in intrusion detection tasks, this algorithm is tested on the same dataset configurations.

Table 5. Performance Metrics for Logistic Regression Algorithm

Algorithm	Dataset	Recall	Precision	F1	Accuracy
LR	KDD-Cup99, KDD-Cup99	0.997	0.996	0.954	0.997
LR	NSL-KDD, NSL-KDD	0.977	0.974	0.857	0.983
LR	KDD-Cup99, NSL-KDD	0.714	0.759	0.814	0.974
LR	NSL-KDD, KDD-Cup99	0.001	0.001	0.822	0.918

Logistic Regression performs well in in-dataset configurations with high accuracy and reasonable precision. However, in the cross-dataset test where the model is trained on NSL-KDD and evaluated on KDD-Cup99, recall and precision drop drastically to 0.001, which indicates the model's inability to detect intrusions in unfamiliar data environments correctly. This supports the interpretation that LR, though useful as a lightweight baseline model, is not suitable for adaptive intrusion detection where datasets differ in structure and distribution.

4.4. Summary and Practical Implications

Among the three algorithms, MLP stands out for its high stability and strong generalization capability across datasets. It demonstrates impressive recall and accuracy in intra-dataset and inter-dataset scenarios and is an appropriate algorithm for real-time detection of dynamic and uncategorized wireless networks. The high precision of SVM would suggest that it is indeed useful in cases where false alarms need to be minimized, such as critical infrastructure protection. Nevertheless, its decrease in recall in some cases indicates not good robustness without further fine-tuning or feature alignment. Although Logistic Regression is simple and fast, it is not stable between datasets, which demonstrates its poor extension for practical WSN applications.

These findings demonstrate the significance of dataset quality, distribution adaptation, and test setting for IDS research and development. These results also suggest that hybrid or ensemble methods exploiting the strengths of MLP (high recall) and SVM (high precision) would offer a more balanced and robust solution to real-world WSN security problems.

5. DISCUSSION

The proposed experiment results validate the importance of using supervised machine learning algorithms such as MLP, SVM, and LR to perform intrusion detection in WSNs. In this section, we discuss their implications, compare them with existing results, and point out possible practical usages. The introduced approach was compared with two recent approaches on intrusion detection. For example, in [24], the authors used SVM and Decision Tree algorithms, and in [16], MLP and Random Forest with the KDD-Cup99 dataset were studied. A comparative study was carried out with the help of performance measures, accuracy, precision, recall, and F1-score under the cross-dataset evaluation situation.

Table 6 shows a comparison of the accuracy, precision, recall, and F1-score of MLP, SVM, and LR-based approaches of this work to other works. The comparison shows that the proposed approach obtains good results on both settings: in-dataset and cross-dataset.

Table 6: Comparative Performance Analysis

Algorithm	Dataset	Metric	Our Study	Ref. [15]	Ref. [16]
MLP	KDD-Cup99, NSL-KDD	Accuracy	0.991	-	0.965
MLP	KDD-Cup99, NSL-KDD	Precision	0.991	-	0.960
MLP	KDD-Cup99, NSL-KDD	Recall	1.000	-	0.962
MLP	KDD-Cup99, NSL-KDD	F1-Score	0.990	-	0.961
SVM	NSL-KDD, KDD-Cup99	Accuracy	0.457	0.621	-
SVM	NSL-KDD, KDD-Cup99	Precision	0.994	0.690	-
SVM	NSL-KDD, KDD-Cup99	Recall	0.522	0.551	-
SVM	NSL-KDD, KDD-Cup99	F1-Score	0.658	0.612	-
LR	NSL-KDD, KDD-Cup99	Accuracy	0.918	-	0.855
LR	NSL-KDD, KDD-Cup99	Precision	0.001	-	0.850
LR	NSL-KDD, KDD-Cup99	Recall	0.001	-	0.858
LR	NSL-KDD, KDD-Cup99	F1-Score	0.822	-	0.856

From this analysis, it can be inferred that the MLP classifier used in this article is better than the ones proposed by [13], particularly for the cross-database experiment. The model always detected all positive samples with high precision and recall, and thus it's suitable for detecting intrusion at large-scale(heterogeneous) data. But there were some possible limitations. SVM's recall and accuracy were considerably reduced on multi-dataset tests to the point that, specifically from NSL-KDD to KDD-Cup99, the impact was substantial, indicating that it is sensitive to bias in distribution and feature difference across datasets. This may indicate that differences might inhibit the generalization ability of SVM in data quality, noise, and feature scaling.

To alleviate this issue, a domain adaptation method or transfer learning could be applied in future work to align the feature spaces across datasets. Furthermore, kernel function optimization and robust feature selection schemes (e.g., Recursive Feature Elimination or PCA) might increase

SVM's cross-domain performance. Another restriction comes from the generalization capacity of Logistic Regression on datasets. Despite high in-dataset performances on LR, recall and precision were not preserved across distributions. This reiterates the requirement of regularization, better hyperparameter optimization, and thematically considering the ensemble in order to increase the reliability of the latter.

In conclusion, we have demonstrated the potential for supervised learning for WSN-IDS and identified the potential for improvement in its generalization, scalability, and real-time deployment. The findings further support the significance of complementary dataset evaluations to expose the limitations of algorithms, which may not be apparent in single-dataset testing.

6. CONCLUSION

This work introduced a solution aiming to enhance the performance of intrusion detection systems (IDS) in wireless sensor networks (WSNs) based on Supervised Machine Learning (SML) techniques, including Multilayer Perceptron (MLP), Support Vector Machine (SVM), and Logistic Regression (LR). We proposed a novel approach, which consisted of an inter-dataset evaluation model and a dual cross-dataset strategy for robust performance evaluation across different test conditions. The experimental results demonstrated that MLP achieved better recall, precision, F1-score and overall accuracy compared to other models, for both in-dataset and cross-dataset evaluations. SVM showed very high precision, but underperformed in recall across datasets with different distributions, highlighting its sensitivity to domain shifts. LR was used as a relatively computationally efficient baseline with a good performance on in-dataset setups but with low capacity to generalise to unseen data, especially on cross-evaluation scenarios. The proposed model was also successful at reducing overfitting and model bias by implementing feature selection procedures, multiple rounds of evaluation, and making a clear division between training and test domains.

Additionally, the study raised the importance of cross-dataset evaluation as a more pragmatic baseline for IDS performance compared with traditional in-dataset validation. Although having various strong points, the study also has a few drawbacks, e.g., the difficulty of generalizing SVM within different data backgrounds, the sensitiveness of the model to the data unbalance, and finally, the scant real-time response. Dealing with these limitations is crucial for practical applications, e.g., resource-constrained or high-speed WSN deployments. It will be in the interest of future work to build ensemble and hybrid systems, which capitalize on the advantages of several models, such as complementing MLPs' good recall and CI DTOs with SVM's hyper precision.

Furthermore, incorporating adaptive models that can learn in real time and self-automatically update themselves to current threats will increase system robustness. Extensions of such a framework to other, more representative datasets and applicability to real WSN deployments will also support validation of its practical relevance. In summary, our work represents an important contribution to the current discussions on intelligent security by presenting a scalable, efficient, and generic method for IDS in WSN. Insights obtained in this research provide an important base for the development of future secure directed wireless communication systems for the dynamic situation of the cyber-attack.

CONFLICT OF INTEREST

The authors declare that there is *no conflict of interest* regarding the publication of this paper.

REFERENCES

- [1] M. A. Talukder, S. Sharmin, M. A. Uddin, M. M. Islam, and S. Aryal, "MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs," *Int J Inf Secur*, vol. 23, no. 3, pp. 2139–2158, Jun. 2024, doi: 10.1007/S10207-024-00833-Z/TABLES/9.
- [2] T. Kim, L. F. Vecchietti, K. Choi, S. Lee, and D. Har, "Machine Learning for Advanced Wireless Sensor Networks: A Review," *IEEE Sens J*, vol. 21, no. 11, pp. 12379–12397, Jun. 2021, doi: 10.1109/JSEN.2020.3035846.

- [3] Z. S. Jassim and M. M. Kassir, "Enhancing Malware Detection Through Machine Learning Techniques," *InfoTech Spectrum: Iraqi Journal of Data Science*, vol. 1, no. 1, pp. 1–15, Jun. 2024, doi: 10.51173/IJDS.V1I1.4.
- [4] M. Ahmad, Q. Riaz, M. Zeeshan, H. Tahir, S. A. Haider, and M. S. Khan, "Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set," *EURASIP J Wirel Commun Netw*, vol. 2021, no. 1, pp. 1–23, Dec. 2021, doi: 10.1186/S13638-021-01893-8/FIGURES/9.
- [5] D. E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, "Cybersecurity Issues in Wireless Sensor Networks: Current Challenges and Solutions," *Wirel Pers Commun*, vol. 117, no. 1, pp. 177–213, Mar. 2021, doi: 10.1007/S11277-020-07213-5/METRICS.
- [6] H. Jalo and M. Heydarian, "A Hybrid Technique Based on RF-PCA and ANN for Detecting DDoS Attacks IoT," *InfoTech Spectrum: Iraqi Journal of Data Science*, vol. 1, no. 1, pp. 28–41, Jun. 2024, doi: 10.51173/IJDS.V1I1.9.
- [7] M. Iorio, F. Risso, and C. Casetti, "When latency matters," *ACM SIGCOMM Computer Communication Review*, vol. 51, no. 4, pp. 2–14, Dec. 2021, doi: 10.1145/3503954.3503956.
- [8] Y. Kayode Saheed, A. Idris Abiodun, S. Misra, M. Kristiansen Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting internet of things network attacks," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 9395–9409, Dec. 2022, doi: 10.1016/J.AEJ.2022.02.063.
- [9] S. Li, X. Lin, W. Xu, and J. Li, "AI-Generated Content-Based Edge Learning for Fast and Efficient Few-Shot Defect Detection in IIoT," *IEEE Trans Serv Comput*, 2024, doi: 10.1109/TSC.2024.3433529.
- [10] B. Al-Fuhaidi, Z. Farae, F. Al-Fahaidy, G. Nagi, A. Ghallab, and A. Alameri, "Anomaly-Based Intrusion Detection System in Wireless Sensor Networks Using Machine Learning Algorithms," *Applied Computational Intelligence and Soft Computing*, vol. 2024, no. 1, p. 2625922, Jan. 2024, doi: 10.1155/2024/2625922.
- [11] R. Kavitha, C. K. Gautam, and P. K. Vera, "Performance Comparison of Routing Protocols for Mobile Wireless Mesh Networks," *2024 International Conference on Optimization Computing and Wireless Communication, ICOCWC 2024*, 2024, doi: 10.1109/ICOCWC60930.2024.10470657.
- [12] A. S. Abdalla and V. Marojevic, "Security Threats and Cellular Network Procedures for Unmanned Aircraft Systems: Challenges and Opportunities," *IEEE Communications Standards Magazine*, vol. 6, no. 4, pp. 104–111, Dec. 2022, doi: 10.1109/MCOMSTD.0003.2100108.
- [13] M. Zakariah, S. A. AlQahtani, A. M. Alawwad, and A. A. Alotaibi, "Intrusion Detection System with Customized Machine Learning Techniques for NSL-KDD Dataset," *Computers, Materials and Continua*, vol. 77, no. 3, p. 4025, Dec. 2023, doi: 10.32604/CMC.2023.043752.
- [14] K. Ramana, A. Revathi, A. Gayathri, R. H. Jhaveri, C. V. L. Narayana, and B. N. Kumar, "WOGRU-IDS — An intelligent intrusion detection system for IoT assisted Wireless Sensor Networks," *Comput Commun*, vol. 196, pp. 195–206, Dec. 2022, doi: 10.1016/J.COMCOM.2022.10.001.
- [15] M. Revanesh, S. S. Gundal, J. R. Arunkumar, P. J. Josephson, S. Suhasini, and T. K. Devi, "Artificial neural networks-based improved Levenberg–Marquardt neural network for energy efficiency and anomaly detection in WSN," *Wireless Networks*, vol. 30, no. 6, pp. 5613–5628, Aug. 2024, doi: 10.1007/S11276-023-03297-6/METRICS.
- [16] R. A. A. Saleh, L. Al-Awami, M. Ghaleb, and A. A. Abudaqa, "Lightweight Intrusion Detection for IoT Systems Using Artificial Neural Networks," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 568 LNICST, pp. 45–59, 2025, doi: 10.1007/978-3-031-64954-7_3.
- [17] Z. A. Abbood, D. Ç. Atilla, and C. Aydin, "Enhancement of the performance of MANET using machine learning approach based on SDNs," *Optik (Stuttg)*, vol. 272, p. 170268, Feb. 2023, doi: 10.1016/J.IJLEO.2022.170268.
- [18] H. Xu, Y. Lu, and Q. Guo, "Application of Improved Butterfly Optimization Algorithm Combined with Black Widow Optimization in Feature Selection of Network Intrusion Detection," *Electronics* 2022, Vol. 11, Page 3531, vol. 11, no. 21, p. 3531, Oct. 2022, doi: 10.3390/ELECTRONICS11213531.

- [19] A. Guillen-Perez, A. M. Montoya, J. C. Sanchez-Aarnoutse, and M. D. Cano, "A Comparative Performance Evaluation of Routing Protocols for Flying Ad-Hoc Networks in Real Conditions," *Applied Sciences* 2021, Vol. 11, Page 4363, vol. 11, no. 10, p. 4363, May 2021, doi: 10.3390/APP11104363.
- [20] H. Tabbaa, S. Ifzarne, and I. Hafidi, "An Online Ensemble Learning Model for Detecting Attacks in Wireless Sensor Networks," *Computing and Informatics*, vol. 42, no. 4, pp. 1013–1036, Apr. 2022, doi: 10.31577/cai_2023_4_1013.
- [21] M. Pawlicki, A. Pawlicka, R. Kozik, and M. Choraś, "The survey on the dual nature of xAI challenges in intrusion detection and their potential for AI innovation," *Artificial Intelligence Review* 2024 57:12, vol. 57, no. 12, pp. 1–32, Oct. 2024, doi: 10.1007/S10462-024-10972-3.
- [22] L. Alsulaiman and S. Al-Ahmadi, "Performance Evaluation of Machine Learning Techniques for DoS Detection in Wireless Sensor Network," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 13, no. 2, Apr. 2021, doi: 10.5121/ijnsa.2021.13202.
- [23] A. Mojtahedi, F. Sorouri, A. N. Souha, A. Molazadeh, and S. S. Mehr, "Feature Selection-based Intrusion Detection System Using Genetic Whale Optimization Algorithm and Sample-based Classification," vol. 3, no. 2, p. 2021, Jan. 2022, doi: <https://doi.org/10.48550/arXiv.2201.00584>.
- [24] F. A. H. J. AL-Bermani, "Application of Neural Networks for Predicting the Exchange Rate of the Iraqi Dinar Against the US Dollar and Comparison with the Box-Jenkins Method for Time Series 2015-2022," *Iraqi Statisticians journal*, vol. 2, no. 1, pp. 09–28, Jan. 2025, doi: 10.62933/EGNTS624.