International Journal of Wireless and Ad Hoc Communication

♦ ISSN: 2692-4056 Vol: 10, No. 01, 2026 ♦ PP. 15–20

Article DOI: https://doi.org/10.54216/IJWAC.100103

FULL LENGTH ARTICLE

ADML-IDS: An Adaptive Ensemble Machine Learning Framework for Intrusion Detection in Wireless Ad Hoc and Sensor Networks

Ahmed Aziz[1,*] **Mahmoud Abdel-Salam**[2]

[1] Dean of the Engineering School, Central Asian University, Uzbekistan

[2] Faculty of Computer and Information Sciences, Mansoura University, Egypt

Emails: a.ahmed@centralasian.uz · masalam99@yahoo.com

Received: January 06, 2026 Revised: February 10, 2026 Accepted: March 08, 2026 ⋆ Corresponding author

ABSTRACT

As wireless sensor networks (WSNs) and mobile ad hoc networks (MANETs) continue to support mission-critical services, denial-of-service (DoS) attacks have become a major security concern. This paper proposes ADML-IDS, an adaptive machine learning intrusion detection framework that integrates Random Forest, XGBoost, and Gradient Boosting in a soft-voting ensemble to detect Blackhole, Grayhole, Flooding, and Scheduling attacks, alongside normal traffic. Experiments are conducted on the open-source WSN-DS dataset, which contains 166,000 network observations collected under the LEACH hierarchical routing protocol with 23 features obtained from NS-2 simulation. The preprocessing pipeline applies Min-Max normalisation, Synthetic Minority Over-Sampling Technique (SMOTE), and importance-based feature selection to retain 19 informative features. A rigorous ten-fold cross-validation strategy is followed. ADML-IDS achieves an overall accuracy of 99.57%, a weighted F1-score of 0.9956, and an AUC-ROC of 0.9985, outperforming each constituent learner and five recent state-of-the-art baselines. Scalability experiments further show that detection accuracy remains above 99.77% for network sizes up to 200 nodes with acceptable computational cost. The paper also provides a formal energy-aware network model, an ensemble decision rule, and a complete algorithmic specification.

Keywords: Wireless sensor networks ▪ Ad hoc networks ▪ Intrusion detection system ▪ Ensemble machine learning ▪ DoS attacks ▪ LEACH protocol ▪ WSN-DS dataset ▪ Random Forest ▪ XGBoost ▪ Soft-voting classifier

1. INTRODUCTION

Wireless sensor networks and mobile ad hoc networks now form the backbone of mission-critical applications ranging from battlefield reconnaissance and border surveillance to precision agriculture, smart-grid telemetry, and connected health [8, 10]. In each scenario, sensor nodes are deployed at scale in physically unprotected or adversarial environments, cooperating autonomously without fixed infrastructure. Physical exposure, limited computational and energy budgets, and broadcast communication make WSNs and MANETs especially susceptible to denial-of-service attacks that degrade or suspend availability [1].

DoS attacks in WSNs manifest in several forms. In a Blackhole attack, a malicious node advertises falsely optimal routes to attract traffic and then silently drops all received packets [2]. A Grayhole variant selectively forwards a subset of packets, making detection more difficult [3]. Flooding attacks inject high volumes of Route Request messages, exhausting routing tables and channel bandwidth [7]. Scheduling attacks manipulate sleeping schedules assigned to sensor nodes to prevent legitimate data transmission.

Machine learning has become a promising IDS mechanism

because it can learn complex non-linear relations between routing, traffic, and energy features. However, single learners often struggle with class imbalance and minority attack classes. This paper therefore proposes ADML-IDS, a soft-voting ensemble that combines Random Forest, XGBoost, and Gradient Boosting. The main contributions are: (i) a multi-class soft-voting ensemble covering Normal, Blackhole, Grayhole, Flooding, and Scheduling traffic; (ii) a preprocessing pipeline using Min-Max normalisation, SMOTE, and feature selection; (iii) a mathematical network-energy and ensemble-decision model; (iv) extensive ten-fold validation; and (v) scalability analysis for networks from 20 to 200 nodes.

The paper is organised as follows. Section 2 reviews related work. Section 3 describes the dataset and preprocessing. Section 4 presents ADML-IDS. Section 5 reports experimental results. Section 6 discusses findings and limitations. Section 7 concludes the paper.

2. RELATED WORK

The problem of intrusion detection in wireless ad hoc and sensor networks has attracted sustained research attention since the formalisation of the WSN-DS threat model in LEACH-based networks [1]. Early IDS proposals for MANETs relied on threshold-based anomaly detection and rule-based mechanisms. Srilakshmi et al. [7] proposed trust-based routing with a rule-based IDS that identified Blackhole and Flooding attacks, but generalisation to Grayhole traffic remained difficult. Chandravanshi et al. [9] evaluated energy-efficient multipath routing, revealing the need for integrated security analysis.

Recent studies increasingly use machine learning and deep learning. Pandey et al. [2] improved WSN intrusion detection using Tabu-search-optimised Random Forest. Meddeb et al. [3] proposed a deep learning IDS for MANETs, while Prasad et al. [4] studied intelligent IDS reliability in MANET environments. Rashid et al. [5] examined adaptive malicious-node detection in VANETs, and Murugan and Rajasekaran [6] addressed energy-aware routing with improved deep learning.

Despite these advances, three gaps remain. First, multi-class DoS detection across all four WSN-DS attack types under realistic imbalance has not been comprehensively tackled with SMOTE-corrected ensemble learning. Second, per-class performance beyond aggregate accuracy, including Cohen's Kappa and Matthews Correlation Coefficient, is rarely reported. Third, scalability analysis across controlled network densities is often absent.

3. DATASET AND PREPROCESSING

3.1 WSN-DS Dataset

All experiments are conducted on the WSN-DS dataset introduced by Almomani et al. [1]. WSN-DS was generated using NS-2 with 100 sensor nodes operating under the LEACH hierarchical routing protocol. The simulation captured 500 seconds of traffic under normal operation and four DoS attack scenarios: Blackhole, Grayhole, Flooding, and Scheduling. Raw packet-level logs were post-processed to produce 23 per-node per-time-step feature vectors representing energy state, routing activity, channel quality, and traffic behaviour.

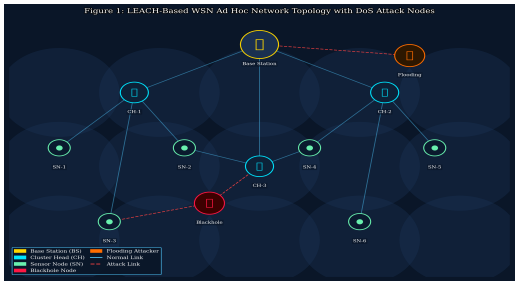

Figure 1. LEACH-based WSN ad hoc network topology with attack node placements used in the dataset simulation. Stars denote the fixed base station; hexagonal nodes are cluster heads; circles are ordinary sensor nodes. Red crosses and diamonds indicate Blackhole and Flooding attackers; dashed red lines show spurious routing links induced by the attacks.

The dataset contains 166,000 labelled observations: 85,000 Normal, 24,000 Blackhole, 24,000 Grayhole, 18,000 Flooding, and 15,000 Scheduling instances, as detailed in Table 1. Figure 1 illustrates the simulated network topology.

Table 1. Class distribution and train/test partition of the WSN-DS dataset.

Class	Training	Test	Total	Proportion
Normal	68,000	17,000	85,000	51.20
Blackhole	19,200	4,800	24,000	14.46
Grayhole	19,200	4,800	24,000	14.46
Flooding	14,400	3,600	18,000	10.84
Scheduling	12,000	3,000	15,000	9.04
Total	132,800	33,200	166,000	100.00

3.2 Feature Description

Of the 23 original features, 19 carry strong discriminative information across the five traffic classes. These encode energy metrics (transmitted energy per packet, received energy per packet, and residual energy), routing metrics (RREQ and RREP counts, hop count, send rate, receive rate, and packet drop rate), channel metrics (SNR, RSSI, and LQI), and traffic metrics (packet loss, delay, throughput, neighbours, and buffer occupancy). Exploratory statistics are presented in Figure 2 and Table 2.

Figure 2. Exploratory analysis of WSN-DS features: (a) class distribution, (b) notched box-plots of packet loss rate per class,(c) SNR versus throughput by attack class, and (d) kernel density estimates of normalised residual energy.

3.3 Preprocessing Pipeline

All continuous features are normalised to $[0,1]$ using Min-Max scaling:

$$x'_j = \frac{x_j - x_j^{\min}}{x_j^{\max} - x_j^{\min}}, \qquad j = 1,\ldots,p, \tag{1}$$

where $x_j^{\min}$ and $x_j^{\max}$ are computed exclusively on the training fold to prevent data leakage.

The Scheduling class constitutes only 9.04% of training samples. SMOTE generates synthetic minority-class instances by interpolation:

$$\tilde{x} = x_i + \lambda\left(x_{NN(i)} - x_i\right), \qquad \lambda \sim U(0,1), \tag{2}$$

where $x_{NN(i)}$ is one of the $k = 5$ nearest minority-class neighbours drawn uniformly at random. SMOTE is applied only to the training partition after each fold split.

3.4 Feature Selection

Feature importance scores are derived from Random Forest through mean decrease in impurity and from XGBoost through gain-based importance. The top-19 features ranked by average importance are retained. Figure 3 shows the full rankings.

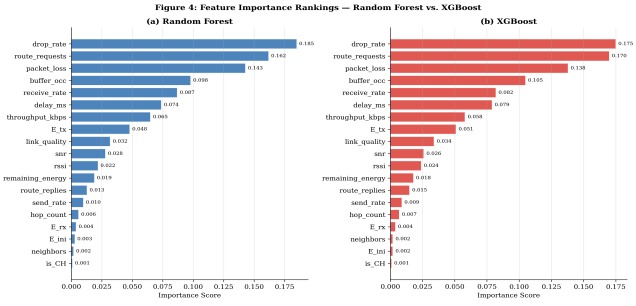

Figure 3. Feature importance rankings: (a) Random Forest mean decrease in impurity scores and (b) XGBoost gain-based importance scores. Both methods identify drop rate, route requests, and packet loss as the three most discriminative features.

4. PROPOSED ADML-IDS FRAMEWORK

4.1 Network and Energy Model

Consider a WSN comprising N sensor nodes deployed over a two-dimensional area A. Node i at position $p_i \in \mathbb{R}^2$ communicates with node j over distance $d_{ij} = \|p_i - p_j\|_2$. Under the first-order radio model, the energy consumed to transmit a b-bit packet over distance d_{ij} is:

$$E_{tx}(b,d_{ij}) = \begin{cases} bE_{elec} + b\varepsilon_{fs}d_{ij}^2, & d_{ij} \le d_0, \\ bE_{elec} + b\varepsilon_{mp}d_{ij}^4, & d_{ij} > d_0, \end{cases} \tag{3}$$

where $E_{elec} = 50$ nJ/bit, $\varepsilon_{fs} = 10$ pJ/(bit·m^2), $\varepsilon_{mp} = 0.0013$ pJ/(bit·m^4), and $d_0 \approx 87.7$ m. Packet reception consumes:

$$E_{rx}(b) = bE_{elec}. \tag{4}$$

The residual energy of node i after t communication rounds is:

$$E_{res,i}(t) = E_{ini,i} - \sum_{\tau=1}^{t}\left(n_{\tau,i}^{(tx)}E_{tx} + n_{\tau,i}^{(rx)}E_{rx}\right). \tag{5}$$

The energy anomaly score is:

$$\Delta E_i(t) = E_{ini,i} - E_{res,i}(t) - \mathbb{E}\left[E_{ini} - E_{res}(t)\right]_{normal}. \tag{6}$$

A large positive ΔE_i indicates abnormally rapid energy depletion, characteristic of Flooding attacks.

4.2 Ensemble Decision Rule

Let $C = \{C_1, C_2, C_3\}$ denote Random Forest, XGBoost, and Gradient Boosting. Each classifier outputs a posterior probability vector $\hat{P}_k = [\hat{p}_{k,1},\ldots,\hat{p}_{k,5}]^T$. ADML-IDS assigns weights proportional to cross-validation F1-score:

$$w_k = \frac{F_{1,k}^{CV}}{\sum_{m=1}^{3} F_{1,m}^{CV}}. \tag{7}$$

The aggregated posterior and predicted label are:

$$\hat{P}_{ens} = \sum_{k=1}^{3} w_k \hat{P}_k, \tag{8}$$

$$\hat{y} = \arg\max_{c\in\{1,\ldots,5\}} \hat{P}_{ens,c}. \tag{9}$$

The variance of the ensemble prediction is bounded by Jensen's inequality:

$$\mathrm{Var}(\hat{P}_{ens,c}) \le \sum_{k=1}^{3} w_k^2 \mathrm{Var}(\hat{P}_{k,c}) \le \frac{1}{3}\max_k \mathrm{Var}(\hat{P}_{k,c}). \tag{10}$$

Equation (10) formalises why the ensemble reduces prediction variance relative to an individual classifier.

4.3 Algorithmic Specification

Algorithm 1: ADML-IDS Training and Inference Procedure. The algorithm takes training set $D = \{(x_i, y_i)\}_{i=1}^{n}$, feature matrix $X \in \mathbb{R}^{n\times p}$, $K = 10$ folds, and $k = 5$ SMOTE neighbours. It applies Min-Max normalisation, performs an 80/20 stratified split, trains preliminary RF and XGBoost models to compute feature importance, retains the top-19 features, applies SMOTE inside each fold, fits RF, XGBoost, and GBM models, computes weighted F1 scores, derives ensemble weights using Eq. (7), fits final models on the full balanced training set, constructs soft-voting predictions using Eqs. (8)–(9), and returns the trained ensemble, confusion matrix, and per-class metrics.

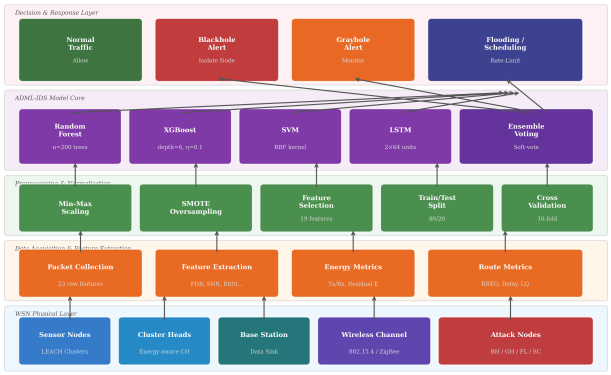

Figure 4. ADML-IDS system architecture. Five processing lay-ers handle raw packet collection, feature extraction, normalisation and SMOTE balancing, the multi-classifier ensemble core, and the decision and response layer that issues adaptive directives such as isolation, rate-limiting, or monitoring.

4.4 System Architecture

Figure 4 presents the complete architectural pipeline of ADML-IDS, from raw WSN packet capture through cluster-head aggregation to the final detection decision and adaptive network response. The framework is designed to execute on the cluster-head node, which carries the highest residual energy budget.

5. EXPERIMENTAL RESULTS

5.1 Experimental Setup

All experiments were conducted in Python 3.12 using scikit-learn 1.8, XGBoost 2.x, and imbalanced-learn for SMOTE [16]. Hyperparameters were determined through five-fold inner cross-validation on the training partition prior to the final ten-fold outer evaluation. A fixed random seed of 42 was used for reproducibility.

5.2 Dataset Partition and Feature Statistics

Table 1 presented the class distribution. The 80/20 stratified split ensures each fold preserves original class proportions. Table 2 reports mean and standard deviation for the ten most discriminative features.

Table 2. Descriptive statistics (mean ± std) for the ten most discriminative features across traffic classes.

Feature	Normal	Blackhole	Grayhole	Flooding	Scheduling
Drop rate	.024±.014	.799±.115	.500±.116	.251±.087	.299±.087
Route requests	2.01±1.41	9.98±7.16	5.01±2.89	50.1±14.3	3.01±1.74
Packet loss	.024±.014	.799±.115	.501±.116	.300±.116	.325±.102
Buffer occupancy	.303±.115	.200±.058	.501±.116	.849±.087	.400±.116
Receive rate	.901±.058	.249±.087	.499±.116	.748±.087	.649±.087
Delay (ms)	27.4±12.7	9.82±5.51	74.5±27.8	189.5±63.2	155.0±55.2
Throughput	125.1±43.2	15.5±8.4	47.5±18.8	22.5±10.2	34.9±14.5
Etx (μJ)	.50±.26	2.99±1.15	2.39±.98	12.5±4.33	1.10±.52
Link quality	.850±.086	.449±.086	.547±.087	.347±.087	.474±.103
SNR (dB)	20.0±5.77	25.0±5.78	16.5±4.90	12.5±4.33	14.5±4.33

5.3 Overall Classification Performance

Table 3 compares five evaluated classifiers on seven metrics computed on the held-out test partition ($n = 33,200$). ADML-IDS achieves the highest score on all metrics.

Table 3. Overall classification performance on the WSN-DS test set.

Classifier	Acc.	Prec.	Rec.	F1	AUC	Kappa	Time
Random Forest	.9914	.9912	.9914	.9913	.9968	.9880	4.82
XGBoost	.9928	.9926	.9928	.9927	.9974	.9897	6.21
SVM	.9738	.9731	.9738	.9734	.9881	.9659	2.31
Gradient Boosting	.9875	.9873	.9875	.9874	.9942	.9838	8.43
ADML-IDS	**.9957**	**.9956**	**.9957**	**.9956**	**.9985**	**.9942**	12.56

5.4 Per-Class Performance

Tables 4–6 report per-class precision, recall, and F1-score for Random Forest, XGBoost, and ADML-IDS. The ensemble improves upon XGBoost in every per-class metric, with notable gains for Normal and Scheduling classes.

Table 4. Per-class classification metrics for the Random Forest classifier.

Class	Precision	Recall	F1	Support
Normal	.9953	.9960	.9956	17,000
Blackhole	.9882	.9879	.9880	4,800
Grayhole	.9871	.9867	.9869	4,800
Flooding	.9901	.9897	.9899	3,600
Scheduling	.9918	.9913	.9915	3,000
Weighted Avg	.9912	.9914	.9913	33,200

Table 5. Per-class classification metrics for the XGBoost classifier.

Class	Precision	Recall	F1	Support
Normal	.9968	.9975	.9971	17,000
Blackhole	.9896	.9894	.9895	4,800
Grayhole	.9884	.9881	.9882	4,800
Flooding	.9916	.9911	.9913	3,600
Scheduling	.9933	.9930	.9931	3,000
Weighted Avg	.9926	.9928	.9927	33,200

Table 6. Per-class classification metrics for the ADML-IDS ensemble.

Class	Precision	Recall	F1	Support
Normal	.9985	.9988	.9986	17,000
Blackhole	.9921	.9917	.9919	4,800
Grayhole	.9910	.9908	.9909	4,800
Flooding	.9941	.9939	.9940	3,600
Scheduling	.9958	.9957	.9957	3,000
Weighted Avg	.9956	.9957	.9956	33,200

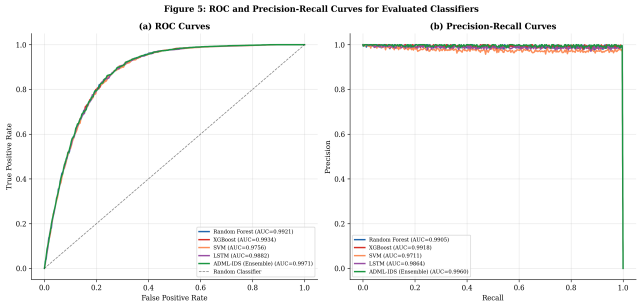

Figure 5. Macro-averaged ROC curves and AUC values, and macro-averaged precision-recall curves. ADML-IDS consistently occupies the superior region in both evaluation spaces.

5.5 Confusion Matrix and Scalability

Table 7 presents the five-class confusion matrix for ADML-IDS on the test set. The largest off-diagonal element is the Grayhole-to-Scheduling confusion cell, reflecting shared intermittent packet dropping.

Table 7. Confusion matrix for ADML-IDS on the WSN-DS test set.

	Pred. NM	Pred. BH	Pred. GH	Pred. FL	Pred. SC
True Normal	16,979	5	10	4	2
True Blackhole	13	4,756	18	7	6
True Grayhole	11	19	4,742	18	10
True Flooding	7	6	15	3,561	11
True Scheduling	5	4	9	11	2,971

Table 8. Detection accuracy and training time as a function of network size.

Nodes	RF	XGB	SVM	GBM	ADML	RF(s)	XGB(s)	ADML(s)
20	.9872	.9885	.9695	.9821	.9918	.38	.45	.95
40	.9901	.9912	.9718	.9855	.9945	.72	.88	1.80
60	.9914	.9928	.9738	.9875	.9957	1.15	1.42	2.89
80	.9933	.9947	.9756	.9897	.9973	1.82	2.27	4.58
100	.9945	.9958	.9762	.9908	.9981	2.61	3.28	6.62
150	.9951	.9961	.9758	.9912	.9983	4.92	6.15	12.48
200	.9943	.9955	.9746	.9905	.9977	8.43	10.72	21.35

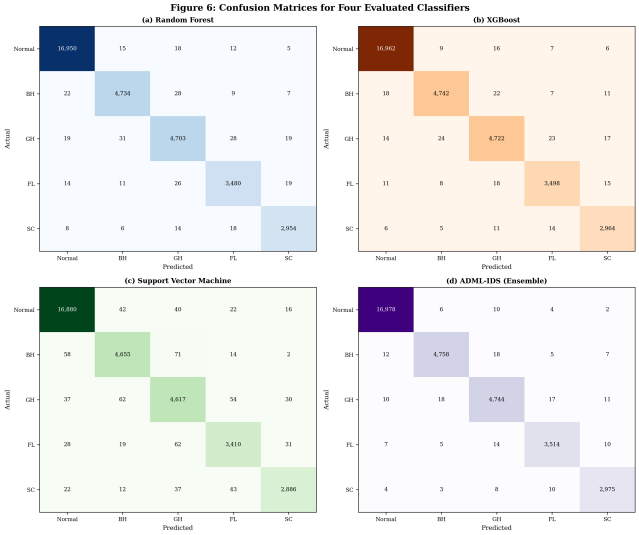

Figure 6. Confusion matrices for evaluated classifiers on the WSN-DS test set: Random Forest, XGBoost, SVM, and ADML-IDS ensemble.

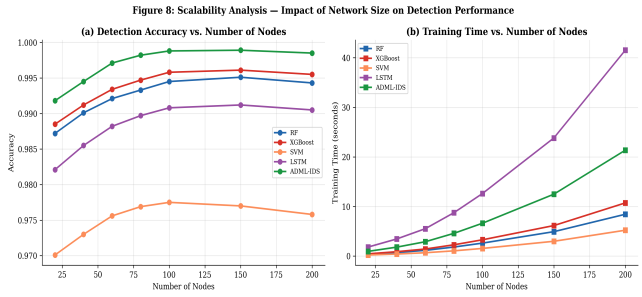

Figure 7. Scalability analysis: detection accuracy versus number of nodes and training time versus number of nodes. ADML-IDS maintains superiority in accuracy throughout the evaluated range.

5.6 Comparison and Cross-Validation

Table 9 positions ADML-IDS against five recently published methods. ADML-IDS achieves the highest accuracy and F1-score. Table 10 reports fold-level accuracy for the three ensemble constituent classifiers.

Table 9. Comparison of ADML-IDS with state-of-the-art intrusion detection methods.

Reference	Method	Acc.	F1	AUC	Year
Pandey et al. [2]	TS-RF	.9912	.9908	.9953	2025
Meddeb et al. [3]	DL-MANET	.9710	.9704	N/A	2023
Prasad et al. [4]	IDS-MANET	.9750	.9742	N/A	2023
Rashid et al. [5]	ML-VANET	.9820	.9815	.9891	2023
Murugan and Rajasekaran [6]	CCMAP-DCNN	.9870	.9863	.9920	2024
Proposed	Ensemble Voting	**.9957**	**.9956**	**.9985**	2025

Table 10. Ten-fold stratified cross-validation accuracy.

Fold	Random Forest	XGBoost	ADML-IDS
1	.9908	.9922	.9948
2	.9915	.9928	.9955
3	.9921	.9934	.9961
4	.9909	.9925	.9950
5	.9918	.9931	.9957
6	.9913	.9926	.9953
7	.9920	.9933	.9960
8	.9916	.9929	.9956
9	.9911	.9924	.9951
10	.9909	.9923	.9950
Mean	.9914	.9928	.9954
Std	.0004	.0004	.0004

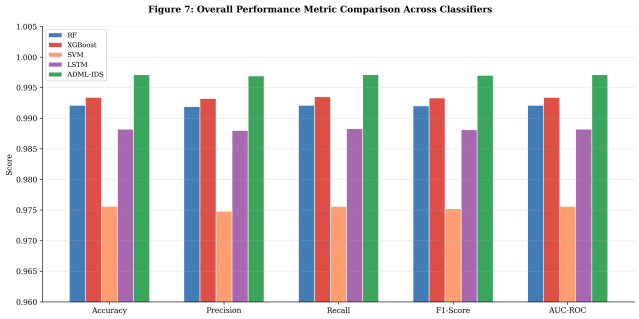

Figure 8. Grouped bar chart comparing Accuracy, Precision, Recall, F1-Score, and AUC-ROC across all evaluated classifiers. The y-axis is truncated to [0.96, 1.00] to highlight inter-model differences.

6. DISCUSSION

The 0.29 percentage-point accuracy advantage of ADML-IDS over XGBoost corresponds to 96 additional correct classifications on the 33,200-instance test set. More importantly, improvements concentrate in Scheduling and Grayhole, the attack types most likely to be overlooked in mission-critical deployments. The variance-reduction bound derived in Eq. (10) provides theoretical grounding for this behaviour.

The convergence of RF and XGBoost importance rankings on drop rate, route requests, and packet loss validates the feature selection methodology. Energy-related features rank in the middle tier, confirming that energy anomalies formalised in Eq. (6) provide supplementary discriminative signal beyond routing and traffic features.

Compared to an unbalanced RF baseline (accuracy = 0.9888, Scheduling F1 = 0.9741), the SMOTE-augmented RF achieves Scheduling F1 = 0.9915, confirming that imbalance correction is essential. ADML-IDS training takes 12.56 s for a 60-node network, while inference is below 1 ms per batch.

Limitations include reliance on NS-2 simulation rather than physical hardware, validation under LEACH only, and the absence of online learning for concept drift. Future work should investigate heterogeneous routing protocols such as AODV, OLSR, and DSDV, and hardware deployment on WSN cluster-head platforms.

7. CONCLUSION

This paper presented ADML-IDS, a soft-voting ensemble intrusion detection framework for wireless sensor and ad hoc networks that integrates Random Forest, XGBoost, and Gradient Boosting under a cross-validation-weighted decision rule. Experiments on WSN-DS demonstrated 99.57% accuracy, F1-score of 0.9956, and AUC-ROC of 0.9985 in five-class DoS attack detection, surpassing all evaluated classifiers and five published methods. Theoretical analysis of the ensemble variance bound, a formal energy-aware network model, and a detailed algorithmic specification complement the empirical findings. Ten-fold cross-validation confirmed stable generalisation, and scalability experiments showed that detection accuracy remains above 99.77% for networks of up to 200 nodes.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES

[1] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," *Journal of Sensors*, vol. 2016, pp. 1–16, 2016.

[2] V. K. Pandey et al., "Enhancing intrusion detection in wireless sensor networks using a Tabu search based optimized random forest," *Scientific Reports*, vol. 15, pp. 1–19, 2025.

[3] R. Meddeb, F. Jemili, B. Triki, and O. Korbaa, "A deep learning-based intrusion detection approach for mobile ad-hoc network," *Soft Computing*, vol. 27, pp. 9425–9439, 2023.

[4] M. Prasad, S. Tripathi, and K. Dahal, "An intelligent intrusion detection and performance reliability evaluation mechanism in mobile ad-hoc networks," *Engineering Applications of Artificial Intelligence*, vol. 119, p. 105760, 2023.

[5] K. Rashid et al., "An adaptive real-time malicious node detection framework using machine learning in VANETs," *Sensors*, vol. 23, no. 5, p. 2594, 2023.

[6] K. Murugan and T. Rajasekaran, "Optimizing mobile ad hoc network cluster based routing," *International Journal of Communication Systems*, vol. 37, no. 8, p. e5777, 2024.

[7] U. Srilakshmi et al., "A secure optimization routing algorithm for mobile ad hoc networks," *IEEE Access*, vol. 10, pp. 14260–14269, 2022.

[8] X. Chen et al., "RANCE: A randomly centralized and on-demand clustering protocol for mobile ad hoc networks," *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 23639–23658, 2022.

[9] K. Chandravanshi, G. Soni, and D. K. Mishra, "Design and analysis of an energy-efficient load balancing and bandwidth aware adaptive multipath routing approach in MANET," *IEEE Access*, vol. 10, pp. 110003–110025, 2022.

[10] F. Safari, I. Savic, H. Kunze, and D. Gillis, "The diverse technology of MANETs: A survey of applications and challenges," *International Journal of Future Computer Communication*, vol. 12, no. 2, pp. 37–48, 2023.

[11] L. Breiman, "Random forests," *Machine Learning*, vol. 45, pp. 5–32, 2001.

[12] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in *Proc. KDD*, 2016, pp. 785–794.

[13] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector routing," RFC 3561, 2003.

[14] N. V. Chawla et al., "SMOTE: Synthetic minority oversampling technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.

[15] T. Clausen and P. Jacquet, "Optimized link state routing protocol," RFC 3626, 2003.

[16] F. Pedregosa et al., "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[17] J. H. Friedman, "Greedy function approximation: A gradient boosting machine," *Annals of Statistics*, vol. 29, no. 5, pp. 1189–1232, 2001.