AUT Journal of Electrical Engineering
10.22060/EEJ.2026.24224.5664

# A Centralized Machine Learning Intrusion Detection System Against Distributed Denial-of-Service Attacks in Wireless Sensor Networks

Mina Malekzadeh*[1], Alireza Hosseini[2]

[1]Associate Professor, Electrical and Computer Engineering Faculty, Hakim Sabzevari University, Sabzevar, Iran
[2]Electrical and Computer Engineering Faculty, Hakim Sabzevari University, Sabzevar, Iran
m.malekzadeh@hsu.ac.ir



**Abstract:**

Wireless sensor networks (WSNs) are vulnerable to distributed denial-of-service (DDoS) attacks, which can severely degrade overall performance and compromise system availability and reliability. To effectively protect against such attacks, this work introduces a centralized intrusion detection system (IDS) framework utilizing machine learning (ML) techniques. The IDS integrates six different ML models to accurately classify malicious traffic and distinguish it from legitimate network traffic. However, developing and validating a robust ML-based defense solution requires a comprehensive understanding of the attack's behavior and impact. Therefore, we initially simulate a baseline WSN architecture and conduct different DDoS attacks, focusing specifically on two critical architectural layers: Cluster Heads and the Base Station. To identify vulnerabilities introduced by DDoS traffic saturation and resource exhaustion, the severity of the attacks is further quantified through network-level metrics. This empirical analysis provides four labeled datasets necessary to train the ML models in the IDS framework across multiple operational phases, including the baseline phase before the attacks, the active attack phase during DDoS attacks, and the recovery phase after the attacks. Experimental results demonstrate that the IDS achieves high detection performance and significantly reduces the adverse effects of the attacks. Furthermore, based on the findings, the IDS facilitates rapid network recovery, restoring performance to levels close to normal operations.

**Keywords:** Dataset Generation, IDS, WSNs, Machine Learning, DDOS attacks

10.22060/EEJ.2026.24224.5664

## 1. Introduction

Wireless Sensor Networks (WSNs) are characterized by their scalability, energy efficiency, and autonomous operation and are designed to operate in diverse and resource-constrained environments. WSNs are instrumental in enabling real-time data acquisition and transmission across a wide array of application domains, including environmental monitoring, precision agriculture, healthcare diagnostics, smart city infrastructure, military surveillance, and industrial automation. Wireless sensor networks comprise a large number of small, distributed sensor nodes that collaborate to collect and transmit data. These nodes are typically low-power, resource-constrained devices designed to monitor specific environmental or physical parameters such as temperature, humidity, motion, vibration, or pressure. To achieve this, they are deployed in dense configurations across a given area and communicate wirelessly to deliver the collected data [1].

Due to the limited computational power, memory, and energy reserves of the sensor nodes, WSNs employ a hierarchical and hybrid communication architecture, where sensors are grouped into clusters. Each cluster is coordinated by a Cluster Head (CH), which is a node with higher energy reserves or computational capacity. The CH performs local data aggregation, filtering redundant or irrelevant information to reduce communication overhead. It then forwards the processed data to a central Base Station (BS), which serves as the network's interface to external systems. The BS is responsible for centralized data processing, long-range communication, and integration with cloud platforms or decision-support systems. This tiered architecture is distributed at the lower level, where sensor nodes interact with cluster heads, and centralized at the upper level, where cluster heads forward data to the base station. By combining distributed local processing with centralized global control, this layered architecture enables WSNs to reduce communication overhead, minimize energy consumption, extend network lifetime, and lower latency in data delivery. However, it also introduces critical vulnerabilities, particularly at the CHs

and BS levels, which act as communication and processing hubs. Because Cluster Heads and the Base Station handle large volumes of traffic and perform essential coordination roles, they become prime targets for attackers seeking to disrupt network operations. One of the most critical threats in this context is the Distributed Denial-of-Service (DDoS) attack [2], in which attackers flood the network with excessive traffic to overwhelm key nodes and exhaust their resources. In such attacks, sensor nodes may be manipulated to generate excessive data, Cluster Heads may become bottlenecks, and the Base Station may be rendered inaccessible. The consequence is a breakdown in communication, degradation of data integrity, and potential failure of the entire monitoring system.

Addressing these vulnerabilities is a critical step toward enhancing the reliability and overall performance of WSNs, especially in sensitive applications where data integrity and network stability are highly important. Traditional security algorithms tend to be computationally intensive and often unsuitable for resource-constrained environments. This highlights the need for security solutions that are not only robust but also resource-efficient, in alignment with the limited energy, memory, and processing capabilities of WSNs [3]. In response to these challenges, this work proposes a centralized Intrusion Detection System (IDS) that leverages a diverse set of machine learning (ML) models to detect and mitigate DDoS attacks in WSNs. The primary contributions of this work are as follows:

- Baseline WSN implementation for comparative analysis: WSN architecture is simulated in MATLAB to generate a baseline dataset, serving as a consistent reference point for meaningful comparative evaluation of both intrusion impacts and detection strategies.
- Dual-Layer DDoS modeling for hierarchical vulnerability analysis: Unlike conventional approaches that model attacks in a generic manner, this work explicitly targets both Cluster Heads and the Base Station within the WSN hierarchy. A dedicated attack module is developed to simulate multiple types of DDoS attacks at these critical layers. This dual-layer

perspective determines how vulnerabilities propagate through the hierarchy, providing a more realistic and comprehensive analysis of hierarchical vulnerabilities.

- Quantitative impact assessment: The dual-layer DDoS model is employed to quantify performance degradation in WSNs under attack conditions, capture the cascading effects on network-level performance, and generate attack datasets to be compared with baseline results to evaluate both the severity of the attacks and the effectiveness of the proposed IDS.
- Centralized ML-Based IDS: A centralized IDS is developed, integrating six ML models to classify network traffic and detect malicious activity with minimal computational overhead.
- IDS Phase-Based evaluation: The IDS models are evaluated across three operational phases: baseline phase before the attacks, the active attack phase during DDoS attacks, and the recovery phase after the attacks. This phase-based evaluation enables a dynamic and realistic assessment of model performance and resilience, facilitating the identification of the most effective model for practical deployment in WSN environments.

The remainder of this work is organized as follows. Section 2 reviews the relevant works on security approaches against DDoS attacks in WSNs. Section 3 describes the design of the WSN, DDoS attacks, and the proposed IDS model. Section 4 presents the results. Section 5 concludes the work.

## 2. Related Works

Due to the critical importance of securing WSNs against DDoS attacks, extensive research has been devoted to this area. Many studies have explored machine learning and other intelligent approaches to enhance detection and prevention mechanisms. Authors in [4] introduce a lightweight intrusion detection approach for WSNs using four ML classifiers, including RF, KNN, SGD, and XGBoost. They are evaluated on the WSN-DS dataset, and the results show that XGBoost achieves better performance compared to the other classifiers. The work is primarily focused on optimizing detection efficiency within a static dataset, without modeling dynamic attack progression or hierarchical vulnerabilities at Cluster

Heads and the Base Station. Its evaluation emphasizes classifier metrics but does not incorporate network-level indicators such as packet reception rate, end-to-end delay, or node lifetime. Moreover, the scope remains limited to four classifiers, leaving other potential models unexplored and offering little insight into network recovery.

In [5], a combination of DT, RL, KNN, XGBoost, and LightGBM classifiers with a Multilayer Perceptron (MLP) is applied to the WSN-DS dataset for intrusion detection. While the reported results highlight improvements through data balancing and feature scaling, the reliance on a static dataset prevents the system from adapting to dynamic attack behaviors. Moreover, hierarchical vulnerabilities at cluster heads and the base station are not modeled, and the evaluation remains confined to accuracy metrics rather than broader measures of network-level performance.

The WSN-DS dataset is also used in [6] to train homogeneous and heterogeneous ensemble models for intrusion detection in WSNs. The heterogeneous ensemble integrates Adaptive Random Forest (ARF) with Hoeffding Adaptive Tree (HAT), whereas the homogeneous ensemble employs multiple HAT classifiers. Despite this methodological variety, the study is limited by its dependence on static data and the absence of simulated attack scenarios. Although vulnerabilities at different layers are acknowledged, the analysis does not provide a comprehensive view of attack propagation, while the energy consumption of sensor nodes is also left unexamined.

Public datasets, such as NSDL and UNSW, are used in [7] with Cisco Packet Tracer to evaluate intrusion detection using KNN, DT, and ANN enhanced by a PSO-based feature selection. The optimization demonstrates that PSO + ANN yields superior classification accuracy compared to other combinations. However, the study's emphasis on feature selection overshadows critical aspects such as hierarchical vulnerabilities in WSNs. Its evaluation framework is restricted to accuracy, overlooking resilience indicators like sensor lifetime. Moreover, the scope is narrow by considering only three algorithms while excluding other widely adopted models.

A lightweight intrusion detection scheme for WSNs is proposed to compare DT with RF, XGBoost, and KNN classifiers by using Gini-based feature selection to detect DoS attacks [8]. The DT classifier achieves 99.5% accuracy with reduced processing time, underscoring its efficiency. However, the focus is limited to DoS scenarios, leaving DDoS attacks and hierarchical vulnerabilities unaddressed. The evaluation highlights accuracy and runtime but neglects network-level performance metrics. Moreover, the reliance on the public WSN-DS dataset restricts adaptability to evolving attack behaviors.

The study in [9] benchmarks a wide range of algorithms, including KNN, LR, SVM, GBoost, DT, NB, alongside LSTM and MLP deep learning models, all trained on the WSN-DS dataset. GBoost emerges as the top performer in terms of detection accuracy and execution speed. Nevertheless, the analysis remains algorithm-centric, without examining how attacks propagate through hierarchical layers such as cluster heads or the base station. Dynamic traffic variations and staged attack scenarios are absent, and the trade-off between detection precision and network sustainability is not explored. Network-level indicators are excluded, and the scope is confined to DoS attacks, which are less demanding than DDoS in WSN environments.

The Orange toolbox is used in [10] to evaluate Adaboost, RF, and CN2 Rule Inducer classifiers on the WSN-DS dataset from Kaggle. Results show better performance with Adaboost reaching 100%. However, the study is primarily a benchmarking exercise on static data, offering little insight into dynamic or evolving attack behaviors. Hierarchical vulnerabilities at cluster heads and the base station are not investigated, and resilience indicators such as packet reception rate, end-to-end delay, or node mortality are not present. The scope is restricted to three classifiers, and the emphasis on accuracy overlooks how detection strategies affect overall network performance.

The NSL-KDD dataset is employed in [11] to train traditional classifiers such as KNN, SVM, LDA, DT, and RF, alongside deep learning methods including MLP, LSTM, and BiLSTM. BiLSTM emerges as the most effective, achieving the highest accuracy among all tested models. However, the study remains focused on classification outcomes, overlooking hierarchical vulnerabilities in WSNs and failing to

incorporate network performance metrics. Dynamic traffic behaviors and attack phases are not simulated, and the energy demands of deep learning models on sensor nodes are left unexamined, raising concerns about real-world applicability.

The authors in [12] employ advanced neural designs, notably a Soft Swish–Linear Scaling Adam CNN (SS-LSACNN) combined with a Two's Complement Shift Reverse (TCSLR) operation for data recovery. Sensor nodes are clustered using a Chebyshev Distance-based K-Means algorithm, and performance exceeds 95% across detection metrics. Despite these promising results, the approach does not investigate vulnerabilities at cluster heads or the base station. Its scope leaves out key network-level indicators such as node lifetime. Moreover, reliance on CC-SMOTE and computationally heavy neural operations may hinder deployment in resource-constrained WSNs.

In [13], machine learning is applied to classify DDoS attacks within Software Defined Networking (SDN) environments. Eight algorithms are tested, ranging from NB and LR to DT, RF, XGBoost, and CatBoost, with tree-based models achieving near-perfect accuracy while others lag behind. It is tailored to SDN contexts and does not apply to hierarchical vulnerabilities in WSNs. Evaluation is limited to classifier accuracy, with no consideration of network-level resilience. Furthermore, the effect of the models on the resource consumption level is not reconciled, while static datasets restrict adaptability to evolving attack scenarios.

DOSAD-WSN-PCCNN, a lightweight detection framework for DoS attacks in WSNs, is introduced in [14]. The approach is built on a progressive cyclical convolutional neural network (PCCNN) and integrates several optimization techniques: advanced preprocessing with a variational Bayesian–based extreme correntropy cubature Kalman filter (VBECKF), feature selection using a variable velocity strategy particle swarm optimization algorithm (VSPSOA), and parameter tuning via the Tyrannosaurus optimization algorithm (TOA). Evaluation on the WSN-DS dataset demonstrates strong performance, achieving up to 99.5% accuracy and surpassing basic methods by more than 25% across key metrics. However, the framework does not extend to DDoS attacks or consider hierarchical vulnerabilities at

cluster heads and the base station. Its evaluation is confined to static datasets, leaving dynamic adaptability unexplored. While the design shows potential for real-time use, the reliance on several complex optimization algorithms may introduce overhead that undermines feasibility in highly resource-constrained environments.

The authors in [15] introduce a hybrid machine learning model for intrusion detection in WSN and IoT environments. The approach combines KMeans-SMOTE (KMS) for class balancing and PCA for dimensionality reduction, along with DT, RF, and XGBoost classifiers. The hybrid (KMS + PCA + RF) model achieves outstanding results, with 99.94% accuracy and f1-score on the WSN-DS dataset and 99.97% accuracy and f1-score on the TON-IoT dataset. Despite these impressive results, the study does not explore hierarchical vulnerabilities in WSNs, nor does it evaluate resilience indicators like node lifetime. While the model demonstrates scalability and robustness, the computational cost of PCA and ensemble classifiers may pose challenges in resource-constrained deployments. Moreover, the reliance on static datasets limits insight into dynamic attack evolution and adaptive responses in real-world scenarios.

Collectively, these studies highlight the need for efficient DDoS detection solutions to strengthen network resilience. Despite considerable progress, several challenges remain unresolved, and addressing them constitutes the central objective of this work. A primary limitation is that many existing approaches depend on computationally intensive models that are not suitable for resource-constrained sensor nodes, while the impact of detection algorithms on network lifetime and energy consumption is often disregarded, limiting their practical deployment. Moreover, reliance on static public datasets without functional WSN implementations or simulated DDoS scenarios further undermines generalizability to real-world traffic. Evaluation scope also remains narrow, focusing primarily on detection accuracy while overlooking key network-level parameters such as delay, throughput, and sensor lifetime. Finally, most studies emphasize attacks on cluster heads, leaving equally critical threats to base station unexplored.

## 3. System Model

10.22060/EEJ.2026.24224.5664

The challenges inherent to WSNs highlight the need for approaches that are not only accurate in detecting DDoS attacks but also lightweight, energy-aware, and adaptable to the resource-constrained nature of WSNs in real-world deployments. This section outlines the design and implementation of the proposed ML-based IDS, developed to identify and mitigate malicious DDoS traffic while preserving network efficiency.

### 3-1- WSN simulation

Initially, we simulate a baseline WSN architecture in MATLAB serving as a consistent reference point for meaningful comparative evaluation of both intrusion impacts and detection strategies. The simulated WSN is depicted in Fig. 1, which provides a visual representation of the network design used in our experiments.

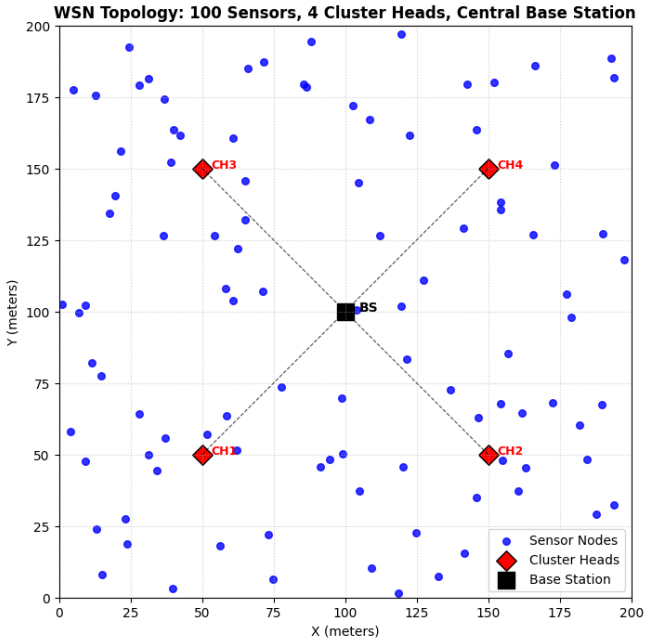



Fig. 1. System model

MATLAB is used to simulate a WSN network, where sensors are deployed throughout an operational area of 200 × 200 square meters. This size is chosen to provide a comprehensive area for deploying sensor nodes, allowing for a realistic representation of a WSN in a moderately sized environment. The primary network configurations are structured with respect to several critical parameters. For the number

of sensor nodes, a total of 100 sensor nodes were randomly deployed throughout the simulation area. This random distribution is intended to create a diverse network topology, representing real-world scenarios where sensor nodes are positioned in various locations to perform their functions effectively. Furthermore, the initial energy of each sensor node is initialized with an energy capacity of 0.5 joules. This value reflects a typical energy reserve for low-power devices used in WSNs, emphasizing the importance of energy-efficient communication during data transmission and reception activities.

Moreover, the base station, which serves as the central hub for data collection and communication with the sensor nodes, is positioned at the center of the environment (coordinates: 100, 100). This central placement is significant as it aims to minimize the distance that data must travel from the sensors to the base station, thereby reducing latency and energy consumption during communication processes.

There are five cluster heads located at central points within their respective clusters of sensor nodes. Each cluster head is responsible for gathering fixed-size data from the sensors within its cluster and aggregating it to reduce redundancy before sending it to the base station. This head cluster configuration ensures efficient communication in the WSN network. In evaluating IDS security against DDoS attacks, a fixed packet size is employed to ensure consistency in traffic volume and maintain controlled experimental conditions. This uniformity enables a clearer assessment of mitigation effectiveness by eliminating variability introduced by heterogeneous packet sizes. Accordingly, a packet size of 4000 B is selected in the simulation environment for both regular and malicious traffic, providing a balanced and realistic representation of network load.

### 3-2- Datasets generation

The simulated WSN is subsequently employed to generate four distinct datasets, each corresponding to specific rounds and purposes. These datasets align with three operational phases of the network, including the baseline phase before the attacks, the active attack phase during DDoS attacks, and the recovery phase after the attacks. This phase-based evaluation facilitates a comprehensive assessment of intrusion impacts and the effectiveness of detection mechanisms.

#### 3-2-1- Baseline phase; Rounds 1 to 20

In this phase, WSN operates under normal conditions to establish baseline performance using key network-level metrics, including the number of dead nodes, end-to-end transmission delay, and packet reception rate. The resulting baseline dataset (*df_before*) captures the network's behavior in the absence of attacker activity, serving as a critical reference point for evaluating the impact of subsequent DDoS attacks.

#### 3-2-2- Active attack phase; Rounds 21 to 40

In this phase, an attack module is further developed in the simulated WSN, comprising ten attacker nodes configured to transmit malicious packets during the designated rounds. These nodes implement two types of DDoS attacks: one targeting the base station (BS) and the other targeting the cluster heads (CH). The rationale for selecting two different types of targets lies in their distinct hierarchical roles within the WSN, which may lead to varying impact levels when subjected to DDoS attacks. Cluster heads play a critical role in managing local sensors and performing data aggregation within their respective clusters. Thus, attacks directed at CHs can have localized effects, potentially disrupting data collection and processing in specific regions of the WSN. In contrast, the base station serves as the primary communication hub, aggregating data from all cluster heads and coordinating network-wide communication. Thus, disrupting the BS through DDoS attacks can have global effects, potentially leading to complete network failure. This distinction between localized disruptions at the CH level and global outages at the BS level underscores the importance of evaluating both targets when assessing overall WSN vulnerability. The two resulting attack datasets (*df_attack_BS* and *df_attack_CH*) capture the network's behavior under these distinct adversarial conditions and provide critical references for evaluating vulnerability and resilience.

#### 3-2-3- Recovery phase; Rounds 41 to 60

In this phase, the performance of the WSN is evaluated after the termination of the attacks, and the recovery dataset (*df_recovery*) is generated. Analyzing post-attack performance is important to determine

10.22060/EEJ.2026.24224.5664

the extent of the damage caused by the attacks and to assess the network's ability to regain stability. Fig. 2 illustrates the WSN architecture with the presence of ten attacker nodes, along with a description of several related parameters in Table 1.

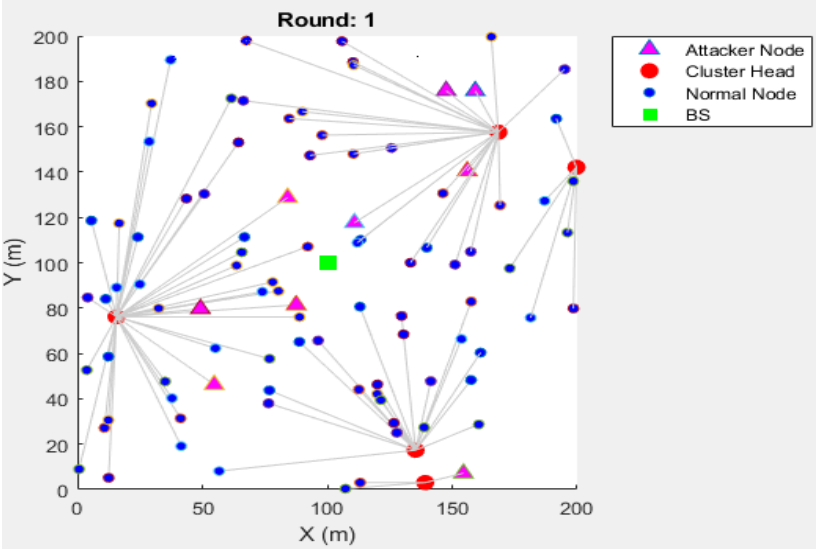



Fig. 2. DDoS attack module in WSN architecture

Table 1. Parameter description

| Parameter | Value |
|---|---|
| No. Sensors | *100* |
| No. Attackers | *10* |
| No. Rounds | *1-20: No attack*<br>*21-40: Under DDoS attacks*<br>*41-60: After attacks* |
| No. Clusters | *5* |
| No. Base stations | *1* |
| WSN area | *200 × 200 $m^2$* |

### 3-2-4- Data extraction

To enable effective training of IDS for DDoS detection, the four distinct generated datasets (*df_before*, *df_attack_BS*, *df_attack_CH*, *df_recovery*), collected across three distinct operational phases (before, during, and after the attacks), are consolidated into a single labeled dataset (*df_dataset*). Labels are assigned to the data of each phase to distinguish normal and malicious traffic patterns. Traffic from

rounds 1 to 20 (pre-attack phase) and rounds 41 to 60 (recovery phase) is labeled as normal, representing legitimate communication patterns under no attack conditions. In contrast, traffic from rounds 21 to 40 (attack phase), during which the network is actively targeted by different DDoS attacks, is labeled as malicious. The labeling scheme is summarized as follows:

- Before attack (rounds 1–20), label as Normal (*Nor_before*).
- During attack (rounds 21–40), label as Malicious (*Mal_BS, Mal_CH*).
- After attack (rounds 41–60), label as Normal (*Nor_after*).

This labeling strategy ensures that the IDS learns both pre-attack and post-attack normal behavior and can distinguish it from malicious traffic. The consolidated dataset includes diverse features, including packet types, timestamps, source and destination IP addresses, types of targets (BS, CH), normal packets, attack packets, and all DDoS attack activities. To prepare the dataset for IDS training, preprocessing steps are applied, including data cleaning, handling of missing values, and feature normalization and scaling. Python libraries such as Pandas and scikit-learn are employed to facilitate this process. The resulting dataset is then used as input to each model within the IDS framework.

### 3-3-IDS framework development

Python is used to develop and implement the IDS framework, which integrates multiple machine learning models to monitor WSN traffic and detect malicious activities.

#### 3-3-1- Model selection

To mitigate DDoS attacks in WSNs, six ML models, including Random Forest (RF), Support Vector Machine (SVM), Logistic Regression (LR), K-Nearest Neighbors (KNN), Naive Bayes (NB), and K-Means, are integrated into the IDS and evaluated for their effectiveness in traffic classification and anomaly detection. These models are selected for their complementary strengths, enabling the framework to address both the computational constraints and the DDoS vulnerabilities inherent to WSNs. RF

10.22060/EEJ.2026.24224.5664

demonstrates robustness against noisy data and efficiently handles high-dimensional feature spaces, which are common in network traffic analysis. SVM provides strong boundary discrimination, enabling reliable differentiation between attack patterns and normal behavior even when feature distributions overlap. LR offers a lightweight design that may align with the resource limitations of sensor nodes. KNN is effective in capturing local traffic anomalies, which is critical when DDoS attacks originate from compromised nodes within the network. NB, with its probabilistic simplicity, enables fast and efficient classification, making it suitable for real-time detection. Finally, K-Means serves as an unsupervised benchmark to explore natural traffic groupings without relying on labeled data, thereby addressing scenarios where attack signatures are unknown or evolving. However, because our consolidated dataset contains labeled instances, and K-Means is inherently unsupervised, using it on a labeled dataset requires careful justification. Thus, to apply K-Means in an unsupervised manner to evaluate its ability to discover inherent structure in the data, we don't use labels during training (we only use features), and they are withheld from our dataset during clustering, to be used solely for performance validation. This approach allows us to assess how effectively K-Means can distinguish malicious from benign traffic without prior knowledge, while also enabling a direct comparison between its clustering performance and the supervised models integrated into the IDS. The pseudocode for preparing the labeled dataset for K-Means clustering within the IDS framework is presented as follows.

| Pseudocode: K-Means clustering on our labeled dataset |
| --- |
| 1: Load consolidated dataset.<br><br>2: Separate the data into:<br>- X → all feature columns (exclude the 'Label' column).<br>- y → the 'Label' column (true labels for evaluation only).<br><br>3: Initialize the K-Means clustering model:<br>- Set number of clusters to 2 (binary classification: attack vs. normal).<br>- Set random seed for reproducibility.<br><br>4: Fit the K-Means model using the feature data X.<br><br>5: Retrieve the predicted cluster labels from the fitted model. |

6: Evaluate clustering performance:
- Compute accuracy between predicted labels and true labels (y).
- Compute F1-score between predicted labels and true labels.
- Generate the confusion matrix comparing predicted vs. true labels.

7: Display the evaluation results:
- Print accuracy.
- Print F1-score.
- Print confusion matrix.

### 3-3-2- Model training and evaluation

Each model in the IDS framework is trained to analyze incoming data packets in the WSN and distinguish between normal and malicious traffic. The consolidated dataset (*df_dataset*) is split into 80% for training and 20% for testing, ensuring balanced evaluation. After training the IDS, it is essential to determine its effectiveness and evaluate its impact on WSN stability under DDoS attack conditions. The effectiveness of the IDS is defined by its ability to accurately identify malicious packets, mitigate DDoS attacks with high precision, and maintain network reliability and performance in the presence of these security threats. To achieve this, evaluation is conducted across two levels of metrics: network-level and detection-level. At the network level, the number of dead nodes, the packet reception rate (PRR), and the end-to-end delay are measured to determine how well the IDS preserves operational integrity under attacks. At the detection level, the analysis focuses on true positives (TP), true negatives (TN), false positives (FP), false negatives (FN), accuracy, and F1-score. Together, these metrics provide a comparative view of the IDS's performance, reflecting both its ability to sustain network reliability and its precision in detecting and mitigating malicious traffic.

## 4. Results and Discussion

In this section, we first present the results of implementing the WSN under normal operating conditions to observe its standard behavior in the absence of attacks, thereby establishing the baseline data for subsequent analysis. Next, we report the results of conducting DDoS attacks on both the base station (BS)

and the cluster heads (CH), highlighting the severity and impact of these attacks through direct comparison with the baseline outcomes. Finally, we present the results of deploying the proposed IDS and evaluate its success rate in mitigating these attacks, demonstrating its effectiveness in preserving WSN performance and stability under adversarial conditions.

### 4-1- Attacks on BS

The base station serves as the central hub that gathers data from all sensors in the WSN to send to external networks for further processing and analysis. We conduct DDoS attacks directly on the base station to measure the corresponding effects on the communication status.

#### 4-1-1- Number of dead nodes

The sensor nodes rely on battery power. This makes them particularly vulnerable to attacks that increase their energy consumption and potentially cause node failure. To evaluate this vulnerability, DDoS attacks are conducted to assess their impact on draining the energy resources of the sensor nodes. The results in terms of the number of dead sensors (non-functional) are illustrated in Fig. 3.

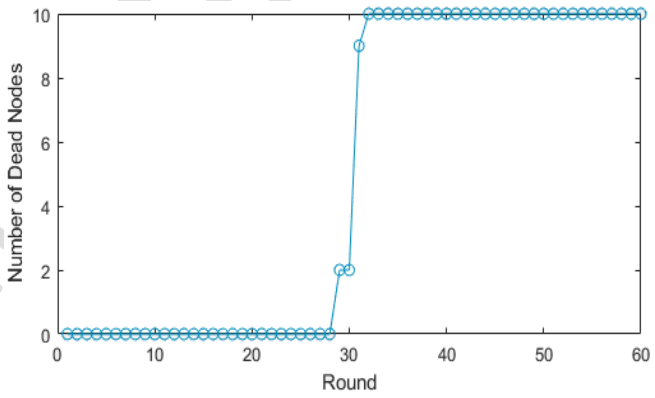



Fig. 3. Number of dead sensors

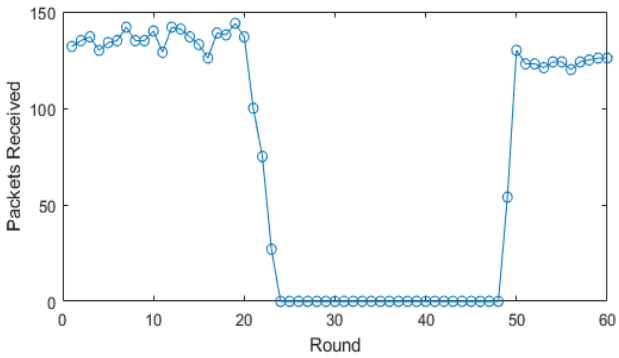
The results show the number of dead sensor nodes in the WSN over 60 rounds, divided into three phases based on the presence of the DDoS attacks. In Rounds 1 to 20, where there is no attack, WSN operates

10.22060/EEJ.2026.24224.5664

normally, and all the sensor nodes are functional. The number of dead nodes remains consistently at 0. This indicates that no sensors have failed during this period. However, in rounds 21 to 40, when the WSN is under DDoS attacks, due to resource saturation, there is a sudden spike in the number of dead nodes, reaching a maximum of 10 by round 30. This significant increase suggests that the DDoS attacks have a severe impact on the WSN's performance. The attacks overwhelm the nodes, and the excessive communication and processing demands deplete their energy faster, resulting in total failure to communicate. The network's resilience is compromised, and the attack significantly degrades performance. After the attacks finish, the network does not recover to its initial state immediately. The presence of 10 dead nodes indicates a lasting impact from the DDoS attack, suggesting that some nodes are still compromised and disabled. The network’s inability to recover quickly after the attacks also highlights the importance of the attacks and the strong need for implementing robust security solutions to protect against such attacks.

#### 4-1-2- Packet reception rate

The packet reception rate (PRR) is an important metric for evaluating the impact of DDoS attacks on WSN performance. By analyzing PRR, the severity of the attacks, their influence on overall network functionality, and the network’s ability to withstand such threats can be assessed. Accordingly, PRR is measured to indicate how effectively the attack on the base station saturates network resources. The corresponding results are presented in Fig. 4.



10.22060/EEJ.2026.24224.5664

Fig. 4. Legitimate packet reception rate

The results before starting the attacks indicate the normal, stable network performance with an average PRR of 140. However, when the attacks start, the performance is immediately affected. The PRR initially drops while fluctuating between 100 and 25, indicating the beginning of the DDoS attack. As the attacks progressed, the PRR drops to zero and remains there even for some duration after the attacks. This sharp decline in performance shows that the base station's resources are fully occupied by the malicious packets, and the WSN is unable to handle legitimate sensor data. After the attack, the PRR gradually recovers, increasing from zero back up to 140. This suggests that the WSN is not able to immediately restore normal operations and requires time to recover from the effects of the attacks and return to stable performance.

### 4-1-3- E2E delay

DDoS attacks generate network congestion through the injection of malicious packets, resulting in longer transmission times for data packets moving from the legitimate source to the destination. Such delays can have a significant impact on real-time applications that depend on timely data transmission. To identify vulnerabilities in WSNs under adverse conditions of DDoS attacks, we measure the end-to-end delay (s), illustrated in Fig. 5.

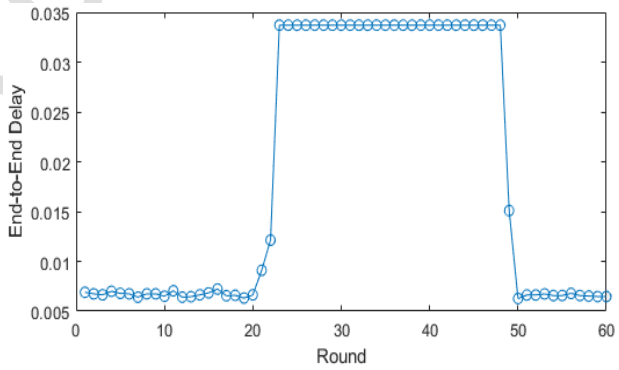



Fig. 5. End-to-end delay of legitimate traffic

10.22060/EEJ.2026.24224.5664

The delay of data delivery is around 0.007s, indicating a low and stable network performance without any DDoS attack. When the attack starts, the delay spikes significantly, reaching a peak of around 0.034s, causing a significant increase in the delay during the attack period. After the attack ends, the delay begins to decrease but still remains elevated compared to the pre-attack phase. The resource saturation effect is so high that even when the attack ends in round 20, the delay still remains high until around round 32. After that, the base station resources are finally released and returned to normal. The delay gradually decreases, returning to the normal range of around 0.007s.

### 4-2- Attacks on CHs

Cluster heads are responsible for collecting data from sensor nodes within their cluster and transmitting it to the base station. Given their crucial role in energy efficiency and traffic management, they are particularly vulnerable to being overwhelmed by malicious packets. We conduct DDoS attacks on cluster heads to assess their effects on the WSNs' overall performance.

#### 4-2-1- Number of dead nodes

The DDoS attacks are conducted against the cluster heads to evaluate their impact on the energy depletion of the sensor nodes. The outcomes, measured by the number of dead sensors, are depicted in Fig. 6.

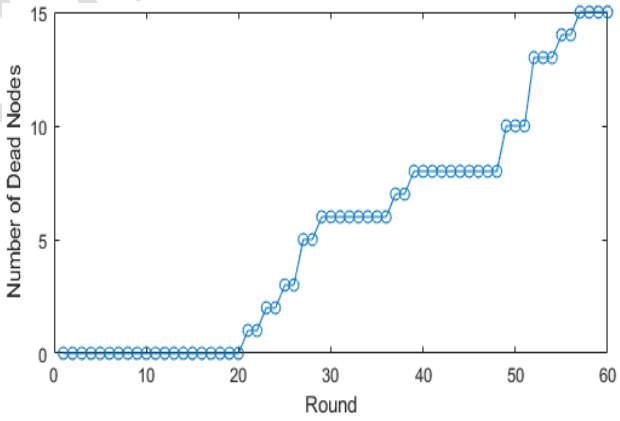



Fig. 6. Number of dead sensors

10.22060/EEJ.2026.24224.5664

The number of dead sensors remains at zero throughout the pre-attack period. This suggests a stable and fully functional WSN. All the cluster heads effectively manage data aggregation and communication with no interruptions. Thereby, all the sensor nodes remain operational, suggesting normal power consumption and network efficiency. In contrast, when the attacks start, there is a noticeable increase in the number of dead sensors, rising from 0 to around 10. The increase in the number is not linear but occurs in steps, which means some nodes fail immediately due to high energy exhaustion, while others survive longer but eventually fail. The reason is related to the varying distances of the sensors from cluster heads. The results also show that when the attacks stop, the number of dead nodes continues to rise compared to the pre-attack phase. The reason for continued node failure is that the sensors that survived the attack may have low remaining energy, causing delayed failures. Moreover, the loss of cluster heads forces some sensors to work harder to retransmit data, increasing their energy consumption. These results further indicate that the attacks on CHs are more effective compared to BS.

#### 4-2-2- Packet reception rate

The cluster heads are targeted by DDoS attacks to evaluate their resilience and capacity for maintaining packet delivery under malicious traffic conditions. This further provides a basis for comparison with the effects observed when targeting the base station. The packet reception outcomes are illustrated in Fig. 7.

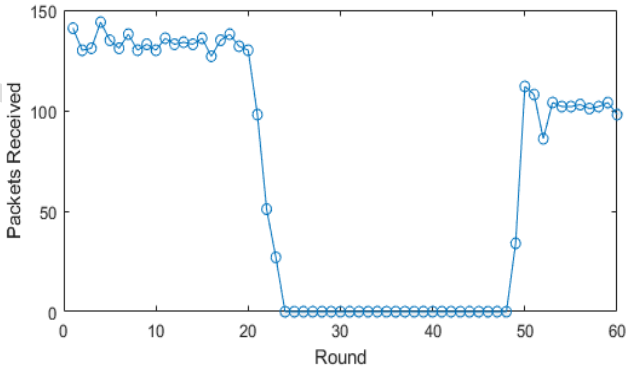



Fig. 7. Legitimate packet reception rate

10.22060/EEJ.2026.24224.5664

The WSN consistently receives up to 150 packets per round, and the cluster heads efficiently manage data aggregation and forwarding to ensure optimal network operation. As soon as the attack begins, packet reception decreases significantly so that it reaches zero around round 25. This sharp decline suggests that the malicious traffic generated by the DDoS attacks has overwhelmed the cluster heads, and they fail under excessive conditions, leading to severe disruptions in collecting and forwarding data. The communication failure continues even after the attacks until round 48 after which a gradual recovery is observed. As the cluster heads are recovering, the WSN's steady operation is resumed around the 50th round. The PRR returns to 100, which is steady but still lower than before the attacks. The reason is that the WSN is still in a recovery phase, and the nodes and cluster heads that were dead after the disruptions caused by the attacks are reinitialized, and communication is restored. Similar to the BS attacks, the number of normal packets received at the CHs dropped to zero. However, the reduction in received packets occurred more rapidly, reflecting its higher complexity.

### 4-2-3- E2E delay

To evaluate the effects of malicious DDoS traffic on the timing of data transmission and assess the WSNs' capacity to handle traffic during these attacks, we perform DDoS attacks on cluster heads and measure the latency of data delivery(s). The results of this analysis are depicted in Fig. 8.

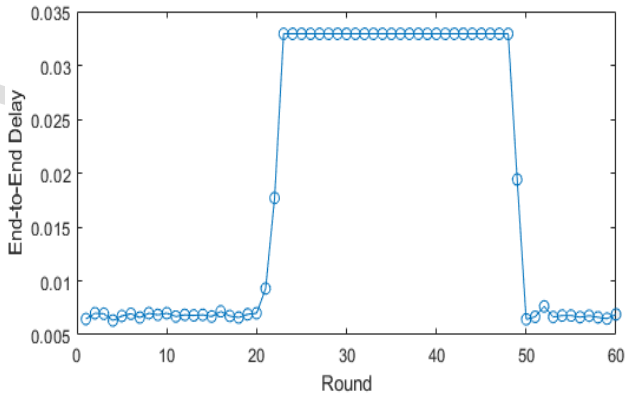



Fig. 8. End-to-end delay of legitimate traffic

Stable low delay values, around 0.007s, indicate efficient communication between nodes and cluster heads when there is no active attack on the WSN. When the attacks begin, a sharp increase in end-to-end delay is observed, and it quickly rises to around 0.035s. The overwhelmed cluster heads struggle to process excessive incoming traffic. Queues are building up at cluster heads, and legitimate packets get delayed due to high volumes of malicious traffic. Moreover, some packets are lost due to congestion and failed communication paths, and they have to be retransmitted. The retransmission delays contribute to the overall delay, which is another reason that the delay remains high for a while even after the attack. It takes several rounds for the delay to return to lower values, suggesting that the recovery from the attack is not instantaneous. Some nodes and cluster heads are still dealing with effects such as energy depletion, processing bottlenecks, and rebuilding of network paths for route reconvergence. The delay begins to decrease slowly around round 49, indicating that the network returns to the original performance. Comparing the delay values shows that the attack effects are significantly higher on CHs compared to BS. The recovery time to return to normal delay levels after the attack ends is also longer than when targeting the BS.

### 4-3-IDS performance

The above results highlight that DDoS attacks significantly degrade the performance of WSN networks. Now, we implement the proposed IDS within the network throughout the rounds to determine its effectiveness level in detecting malicious DDoS activities and preventing these attacks within WSN networks. The assessment focuses on the IDS's response and overall capabilities when the attacks target cluster heads and the base station.

#### 4-3-1- Malicious packet detection rate

The effectiveness of the IDS in detecting and blocking malicious attack packets targeting the cluster heads and the base station is illustrated in Fig. 9.

10.22060/EEJ.2026.24224.5664

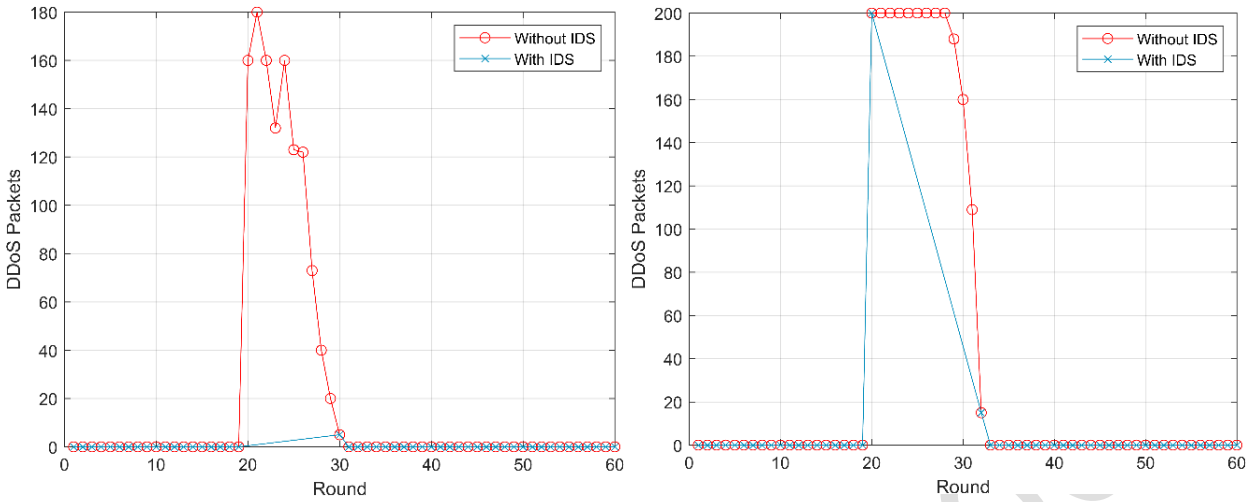



Fig. 9. IDS performance during DDoS attacks on CHs (left) and on BS (right)

In the pre-attack phase, WSN experiences no packet filtering, as no malicious traffic is present. When the attacks start, the unprotected WSN is immediately overwhelmed by the malicious packets. In the absence of IDS, the WSN is highly vulnerable to DDoS attacks, which leads to a significant performance degradation. In contrast, a protected WSN leverages the IDS to proactively identify and block malicious packets before they reach the nodes. This frees up crucial WSN resources, maintaining performance and minimizing disruption. Furthermore, when the IDS is enabled, initially, a sharp increase in malicious packet reception is observed in the protected WSN. However, after that, the IDS successfully blocks the attack packets, and the number of malicious packets received in the WSN consistently remains zero throughout the attack. The reason for this initial increase is that the IDS requires time to analyze traffic patterns and learn to recognize the attack. During this time, the IDS might not yet have recognized the incoming packets as malicious, leading to a temporary spike after which it quickly adapts, effectively blocking subsequent malicious packets.

#### 4-3-2- True detection rate

True positives (TP) are instances where malicious traffic is correctly flagged as an attack. A high TP rate means most DDoS attempts are stopped before harming network performance, while a low TP rate leaves

10.22060/EEJ.2026.24224.5664

the WSN exposed to resource exhaustion and disruption. True negatives (TN) denote benign traffic correctly recognized as normal. High TN values preserve legitimate sensor communication and trust, whereas low TN values cause misclassification, blocking normal nodes, and reducing efficiency. The IDS evaluation of true detection performance against DDoS attacks at both Cluster Heads and the Base Station is presented in Fig. 10.

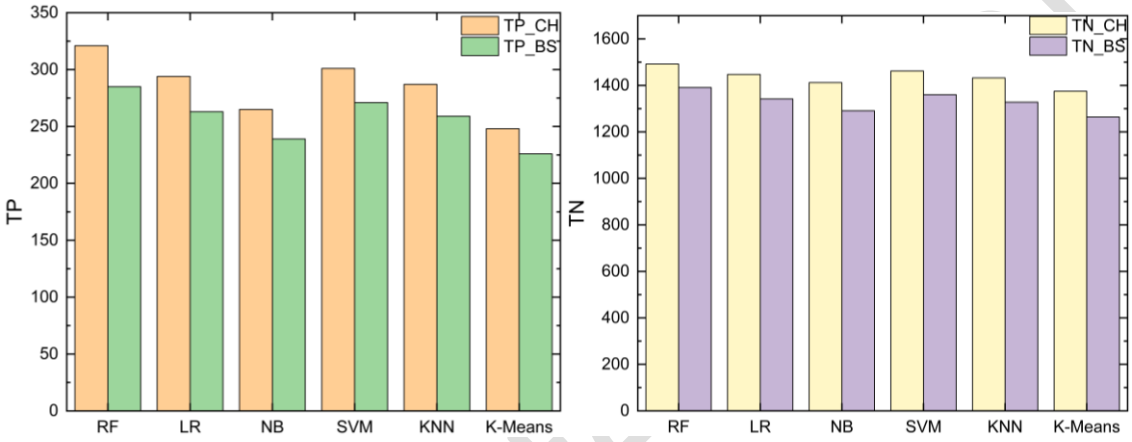



Fig. 10. True detection rate

Across both TP and TN, a clear performance distinction is observed between Cluster Heads and Base Station results. RF consistently achieves the highest values (321 TPs at CHs and 285 TPs at the BS; 1492 TNs at CHs and 1391 TNs at the BS), with its ensemble learning enabling robust generalization across both distributed (CHs) and centralized (BS) layers. The smaller decline at the BS confirms RF's scalability under heterogeneous traffic. SVM high results (301/271 TPs; 1462/1360 TNs) also show that it can effectively separate attack and benign traffic at CHs, though its margin-based approach weakens with aggregated noise at the BS. LR results (294/263 TPs; 1447/1342 TNs) also show that it performs reliably in structured, linearly separable CH regions but loses accuracy when nonlinear overlaps increase at the BS. KNN shows moderate results (287/259 TPs; 1432/1328 TNs) due to its reliance on local comparisons, making it vulnerable to feature ambiguity in centralized traffic. NB underperforms (265/239 TPs; 1412/1291 TNs) due to independence assumptions that fail to capture correlated attack or benign

10.22060/EEJ.2026.24224.5664

behaviors, with sharper declines at the BS. K-Means, as an unsupervised model, records the lowest values (248/226 TPs; 1375/1264 TNs), which denote its lower reliability among other tested models to distinguish traffic without labeled guidance, and its drop at the BS highlights lower adaptability to complex traffic. All the results show that all models experience performance decline at the BS, reflecting increased heterogeneity, traffic aggregation, and noise. The BS receives traffic from multiple CHs, leading to larger volumes and greater diversity of data. This aggregation introduces feature overlap between benign and malicious traffic, making separation and classification between malicious and benign flows more difficult. Moreover, centralized traffic often contains redundant packets, retransmissions, and mixed flows, which increase noise. Models that rely on clean separation struggle more under these conditions, reducing TP and TN values.

### 4-3-3- False detection rate

A false positive (FP) is when normal traffic is wrongly flagged as malicious. High FP rates waste energy and resources, disrupt legitimate communication, and reduce trust, while low FP rates minimize false alarms and support smooth operation. False negatives (FN) occur when attacks are misclassified as normal traffic. High FN rates are critical, as they let adversarial flows bypass detection and exhaust WSN resources, whereas low FN rates reflect strong resilience against undetected attacks. IDS evaluation of false detection in terms of FP and FN is shown in Fig. 11.

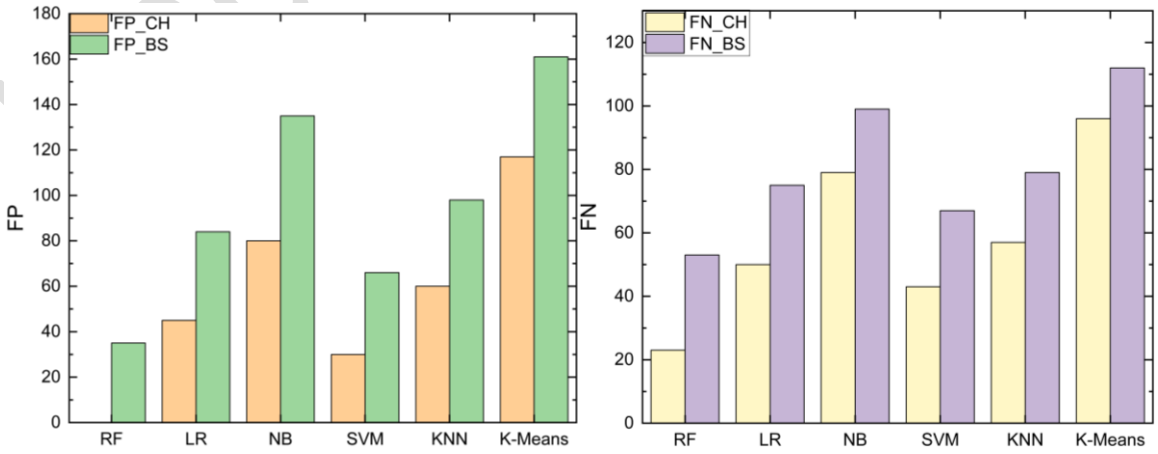


Fig. 11. False detection rate

In terms of misclassifying normal traffic, all models demonstrate practical value, though their performance varies in degree. RF achieves the lowest FP (0 at CHs and 35 at the BS) and FN (23 at CHs and 53 at the BS) values, reflecting its ensemble learning capacity to generalize across diverse traffic while maintaining robust discrimination between benign and malicious flows. A minimal increase at the BS highlights its resilience under centralized complexity. SVM follows (30/66 FPs; 43/67 FNs), performing well overall but showing greater susceptibility to misclassification when traffic becomes noisy and overlapping at the BS. LR (45/84 FPs; 50/75 FNs) offers moderate reliability, effective in structured environments but weaker when benign and attack features overlap. KNN (60/98 FPs; 57/79 FNs) is more vulnerable to local noise and feature ambiguity, as its proximity-based classification struggles with aggregated flows. NB (80/135 FPs; 79/99 FNs) underperforms due to independence assumptions that limit its ability to capture correlations in benign traffic. K-Means records the highest error rates (117/161 FPs; 96/112 FNs), underscoring its limited ability to separate normal traffic without labeled guidance. Across all models, FP and FN values rise at the BS due to traffic aggregation, heterogeneity, and noise. RF and SVM stand out as high performers with strong resilience, LR and KNN form the medium group with moderate reliability but greater sensitivity to overlap and noise, while NB and K-Means perform lowest, reflecting limited suitability.

#### 4-3-4- Detection accuracy

Accuracy reflects overall classification performance. In WSNs, high accuracy ensures reliable distinction between malicious and legitimate packets, supporting both security and efficiency. Low accuracy indicates frequent misclassifications, which undermine network resilience. The accuracy results are presented in Fig. 12.

10.22060/EEJ.2026.24224.5664

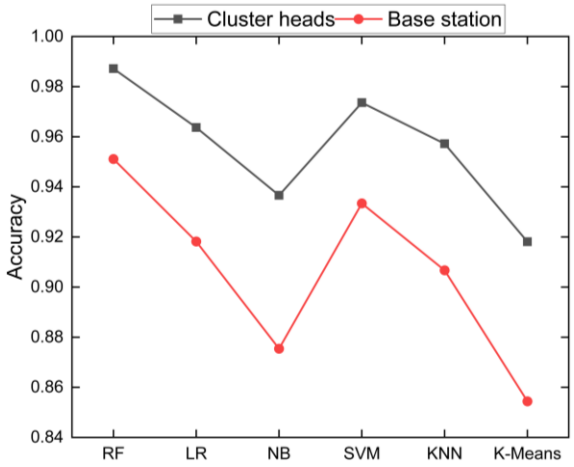



Fig. 12. Detection Accuracy

The models all demonstrate meaningful detection capability, but their accuracy results reveal different levels of performance across CH and BS layers in WSNs. At CHs, traffic is more localized and easier to classify, while at the BS, aggregated traffic introduces heterogeneity and noise, reducing accuracy across all models. RF achieves the highest accuracy (0.9872 at CHs and 0.9511 at BS), underscoring its ensemble-based design to generalize across heterogeneous attack traffic and maintain resilience even under the increased complexity of centralized traffic. SVM ranks second (0.9736/0.9334), benefiting from its margin-based classification framework that effectively separates attack and benign flows. However, its performance declines slightly at the Base Station, where feature overlap and noise reduce its margin advantage. LR (0.9637/0.9182) and KNN (0.9572/0.9067) provide moderate reliability. LR performs well in linearly separable environments, making it effective at Cluster Heads, but its adaptability weakens in nonlinear, aggregated traffic. KNN, by contrast, relies on local instance comparisons, which makes it sensitive to scaling and noise. This sensitivity becomes more pronounced at the Base Station, where traffic heterogeneity leads to higher misclassification rates. NB and K-Means remain useful but show limitations when traffic complexity increases. NB achieves 0.9366/0.8754, constrained by its assumption of feature independence that prevents effective modeling of correlated traffic behavior. K-Means

performs lower (0.9181/0.8544), highlighting its lower ability to reliably distinguish attack and benign traffic without labeled guidance.

### 4-3-5- F1-score

F1-score is a key measure of detection effectiveness, with higher values reflecting a stronger balance in identifying attacks while minimizing misclassification of benign traffic. In WSNs, a high F1-score indicates reliable intrusion detection under complex conditions, whereas a low F1-score denotes reduced suitability for maintaining security and efficiency. The F1-score results at both CHs and BS levels are presented in Fig. 13.

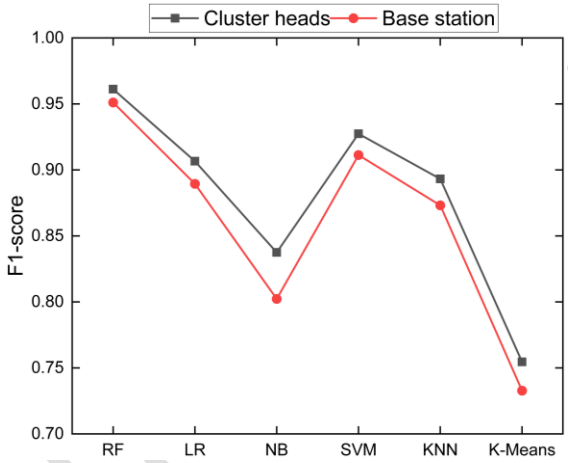



Fig. 13. F1-score

The detection quality of IDS models under DDoS attacks reveals that RF achieves the highest F1-scores (0.9612 at CHs and 0.9511 at BS). These results underscore RF's ability to combine multiple decision paths through its ensemble design, ensuring stable performance even when traffic patterns become irregular at the Base Station. By leveraging this architecture, RF consistently identifies attack signatures while minimizing the misclassification of benign traffic, making it reliable across both distributed and centralized WSN layers. SVM follows (0.9274 at CHs and 0.9113 at BS), maintaining strong separation due to its margin-based design, although its performance declines slightly in Base Station, where

overlapping features reduce clarity. LR results (0.9066 at CHs and 0.8895 at BS) show it is performing reliably in structured environments but losing adaptability when traffic distributions become nonlinear or ambiguous at the Base Station. KNN achieves lower scores (0.8932 at CHs and 0.8732 at BS), but its dependence on neighborhood similarity makes it vulnerable to distortions from uneven traffic density and localized noise, particularly at the Base Station. NB is further limited (0.8375 at CHs and 0.8023 at BS) by its independence assumption, lowering its ability to capture correlated traffic behavior. K-Means produces the lowest scores (0.7546 at CHs and 0.7328 at BS), reflecting its slower ability in distinguishing malicious flows without labeled guidance. Collectively, while the models show different levels of effectiveness to block the DDoS packets, F1-scores decline at the BS across all models due to traffic aggregation and variability during the attacks.

## 5. Conclusion

This work addressed the vulnerability of WSNs to DDoS attacks by designing a centralized IDS framework that integrates six ML models (RF, SVM, LR, KNN, NB, and K-Means). A baseline WSN and a dual-layer attack model targeting both Cluster Heads and the Base Station were simulated to capture hierarchical vulnerabilities and cascading traffic effects. Network-level metrics such as packet delivery ratio, end-to-end delay, and sensor lifetime were measured across baseline, attack, and recovery phases, producing four labeled datasets for IDS training and validation. The results indicate that DDoS attacks significantly degrade WSN performance, with a more pronounced impact on CHs. Disruption at the CH level rapidly propagates through the network, amplifying adverse effects compared to attacks targeting the BS.

To detect and mitigate these attacks, the IDS was implemented, demonstrating high detection performance across all phases and effectively reducing the impact of the attacks. The RF and SVM models exhibited superior detection capabilities, while LR and KNN maintained reliable but less robust performance. Conversely, NB and K-Means showed lower effectiveness under DDoS conditions.

Notably, all models experienced a performance decline at the BS level. At CHs, traffic is localized and easier to classify, while at the BS, overlapping flows complicate detection and lower accuracy. These findings highlight the value of a multi-model IDS approach, where complementary strengths of individual algorithms can be leveraged to enhance overall resilience. For future work, reinforcement learning models could be explored to further strengthen the IDS, enabling adaptive defense strategies that can dynamically respond to evolving DDoS attack patterns in WSNs.

## References

[1] Y.Y. Ghadi, T. Mazhar, T. Al Shloul, T. Shahzad, U.A. Salaria, A. Ahmed, H. Hamam, Machine learning solutions for the security of wireless sensor networks: A review, IEEE Access, 12 (2024) 12699-12719.

[2] R. Bukhowah, A. Aljughaiman, M.H. Rahman, Detection of dos attacks for IoT in information-centric networks using machine learning: Opportunities, challenges, and future research directions, Electronics, 13(6) (2024) 1031.

[3] T. Khan, K. Singh, M. Shariq, K. Ahmad, K. Savita, A. Ahmadian, S. Salahshour, M. Conti, An efficient trust-based decision-making approach for WSNs: Machine learning oriented approach, Computer Communications, 209 (2023) 217-229.

[4] M. Loughmari, A. El Affar, A lightweight machine learning approach for denial-of-service attacks detection in wireless sensor networks, International Journal of Electrical and Computer Engineering (IJECE), 15(2) (2025) 2089-2097.

[5] M.A. Talukder, S. Sharmin, M.A. Uddin, M.M. Islam, S. Aryal, MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs, International Journal of Information Security, 23(3) (2024) 2139-2158.

[6] H. Tabbaa, S. Ifzarne, I. Hafidi, An online ensemble learning model for detecting attacks in wireless sensor networks, arXiv preprint arXiv:2204.13814, (2022).

[7] V. Sivagaminathan, M. Sharma, S.K. Henge, Intrusion detection systems for wireless sensor networks using computational intelligence techniques, Cybersecurity, 6(1) (2023) 27.

[8] M.A. Elsadig, Detection of denial-of-service attack in wireless sensor networks: A lightweight machine learning approach, IEEE Access, 11 (2023) 83537-83552.

[9] R. Wazirali, R. Ahmad, Machine Learning Approaches to Detect DoS and Their Effect on WSNs Lifetime, Computers, Materials & Continua, 70(3) (2022).

[10] A.M. Arabiat, Y.G. Eljaafreh, Intrusion Detection in Wireless Sensor Networks Using ML Based Classification of Denial of Service (DoS) Attacks, Journal of Communications, 20(4) (2025) 501-514.

[11] M. Esmaeili, S.H. Goki, B.H.K. Masjidi, M. Sameh, H. Gharagozlou, A.S. Mohammed, ML-DDoSnet: IoT intrusion detection based on denial-of-service attacks using machine learning methods and NSL-KDD, Wireless Communications and Mobile Computing, 2022(1) (2022) 8481452.

[12] V.K. Singh, D. Sivashankar, K. Kundan, S. Kumari, An Efficient Intrusion Detection and Prevention System for DDOS Attack in WSN Using SS-LSACNN and TCSLR, Journal of Cyber Security and Mobility, 13(1) (2024) 135-159.

[13] O. Ussatova, A. Zhumabekova, Y. Begimbayeva, E.T. Matson, N. Ussatov, Comprehensive DDoS Attack Classification Using Machine Learning Algorithms, Computers, Materials & Continua, 73(1) (2022).

[14] E. Sivanantham, N.K. Priyadarsini, M. Thankaraj, T.V. Lakshmi, Effective Denial-of-Service Attack (DoS) Detection Using Progressive Cyclical Convolutional Neural Network (CNN) in Wireless Sensor Networks, International Journal of Communication Systems, 38(14) (2025) e70217.

[15] M.A. Talukder, M. Khalid, N. Sultana, A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction, Sci. Rep., 15(1) (2025) 4617.