APPLICATIONS OF
MODELLING AND SIMULATION
http://arqiipubl.com/ams eISSN 2600-8084 VOL 10, 2026, 64-77

Development of a Hybrid DL-ML IDS for Blackhole Attack Detection in Heterogeneous IoT-EHT Networks

Mina Malekzadeh* and Alireza Naseri

Electrical and Computer Engineering Faculty, Hakim Sabzevari University, Sabzevar, Iran

*Corresponding author: m.malekzadeh@hsu.ac.ir

Submitted 21 October 2025; Revised 01 January 2026; 19 January 2026; Available online 28 January 2026.

Abstract: The heterogeneous nature of data transmission within the Internet of Things (IoT) demands efficient communication. The IEEE 802.11be standard, known as extremely high throughput (EHT), introduces advanced capabilities that can meet these demands. However, extending IoT into the EHT domain inevitably transfers existing vulnerabilities, exposing IoT–EHT networks to threats that can compromise functionality. A major threat is the blackhole attack, in which a malicious node advertises the best routing path, attracts legitimate traffic, and discards it. To detect this threat within IoT–EHT networks, we propose DML-IDS, a hybrid intrusion detection system framework that leverages different machine learning and deep learning models. We further introduce a dataset generation method that reflects diverse IoT conditions, capturing both normal and under-attack performance across three key features: proximity, sensor density, and payload size. These datasets are used to train the framework and to assess the attack severity. The framework is implemented to determine both network-level and detection-level results. Simulation outcomes reveal that sensor density and payload size are more reliable indicators of blackhole attack behavior than proximity, underscoring the importance of aligning detection architectures with feature dynamics. Moreover, the findings demonstrate consistently high reliability of ML and DL models, with ML outperforming DL across the features.

Keywords: Blackhole attacks; Deep learning; Intrusion detection system; IoT networks; Machine learning.

1. INTRODUCTION

The Internet of Things (IoT) networks connect various devices to facilitate seamless data transfer. The networks consist of different types of sensors that collect data from their surrounding environments and transmit it to their base stations (BS). The BS serves as a central device that communicates with processing units, which analyze the data and make decisions based on this analysis. Depending on the scale of the IoT networks, the processing units can be simple local servers for smaller networks or cloud data centers for larger IoT networks. The diversity of data collected by different types of sensors requires high efficiency in IoT networks, which primarily depends on their integration of advanced connectivity methods, such as wired, wireless, or cellular options. This integration facilitates the interconnection of diverse applications and allows them to operate effectively across different environments. With this wide range of interconnected devices, IoT networks can collect and analyze vast amounts of data, leading to increased efficiency and convenience. Among these connectivity methods is the IEEE 802.11be standard, also known as extremely high throughput (EHT) Wi-Fi 7. While traditional IoT deployments often rely on low-power standards such as IEEE 802.15.4 or LoRaWAN, these technologies struggle to meet the demands of next-generation applications such as smart healthcare monitoring, autonomous vehicular communication, industrial IoT, and immersive Augmented and Virtual Reality (AR/VR) IoT services, which all require high bandwidth and reliability. On the other hand, Wi-Fi 7 introduces advanced capabilities, including multiband operation, flexible frequency utilization, and enhanced bandwidth techniques to deliver higher throughput and lower latency [1]. These advancements position Wi-Fi 7 as a particularly suitable foundation for emerging IoT-EHT environments, where real-time responsiveness and resilience are critical [2].

However, despite these advantages, the integration of IoT with EHT also introduces new security challenges that can compromise network integrity and reliability. One critical threat is the blackhole attack, in which a malicious node advertises the optimal routing path to attract legitimate packets and then discards them, thereby disrupting communication and degrading overall system performance [3]. These attacks not only lead to the loss of network data but also disrupt communication by targeting the reliability of IoT applications and causing system failures. In order to address these attacks, traditional security solutions, such as trust-based intrusion detection systems (IDS) and cryptographic methods, have been widely employed in IoT networks to monitor traffic and identify suspicious activity. However, their effectiveness can be limited by insufficient adaptability to evolving attack patterns or high computational overhead. In contrast, learning-based approaches utilizing deep

learning (DL) or machine learning (ML) algorithms can offer greater efficiency in analyzing traffic behavior, detecting anomalies, and effectively identifying blackhole attacks. Accordingly, this work proposes DML-IDS, a hybrid intrusion detection framework for heterogeneous IoT–EHT networks that integrates deep and machine learning algorithms to detect blackhole attacks. By adaptively learning from network behavior, the framework enhances detection accuracy, enabling early identification of malicious activity. The key contributions include:

- We propose DML-IDS, a hybrid intrusion detection framework by leveraging different deep learning and machine learning models to address blackhole attacks in heterogeneous IoT–EHT networks.
- We design and simulate a four-tier IoT-EHT network, which serves as the foundation for subsequent diverse dataset generation and provides a realistic basis for practical deployment conditions.
- We introduce a diverse dataset generation approach that captures both normal and under-attack network performance across three critical IoT experimental features, including proximity, sensor density, and payload size, as indicators of attack behavior. This ensures the framework is trained on comprehensive datasets that reflect practical deployment variability and enhance its ability to generalize across different real-world operational conditions.
- We conduct a two-level evaluation method, encompassing feature-wise and detection-wise analysis, to (i) assess IoT–EHT network vulnerability and resistance to blackhole attacks, include severity level analysis, (ii) measure the efficiency of attack behavior indicators, and (iii) validate the effectiveness of the proposed DML-IDS framework and provide comparative insights into its detection capabilities.

The remainder of this work is organized as follows. Section 2 reviews the relevant literature on security approaches against blackhole attacks. Section 3 describes the design implementation of the IoT-EHT, blackhole attacks, and the proposed DML-IDS framework. Section 4 presents the results. Section 5 concludes the work

2. RELATED WORKS

Existing studies on blackhole attack detection can broadly be classified into three categories: trust-based approaches, cryptography and routing-based approaches, and AI-based approaches, each reflecting a distinct strategy against malicious behavior. A range of studies has examined trust-based approaches, which aim to establish and maintain trust among nodes by monitoring their behavior. The authors in [4] discuss that the two types of popular attacks on IoT networks are external and internal attacks. They state that while various solutions exist for external IoT attacks (e.g., IDS and cryptography), defenses against internal attacks remain limited and therefore propose a trust management system (TMS) for internal attacks by employing Principal Component Analysis (PCA). A comparison between machine learning (decision tree, random forest, XGBOOST, AdaBOOST), and long short-term memory (LSTM) and Bidirectional LSTM (BiLSTM) approaches is also presented, which shows Bi-LSTM outperforms both traditional and machine learning methods, achieving MSE of 0.005, RMSE of 0.070, MAE of 0.256, and R2 of 0.95. NS3 is used in [5] to detect Blackhole attacks in Mobile Ad Hoc Networks (MANETs) using the K-Nearest Neighbor (KNN) algorithm for clustering and fuzzy inference for selecting the cluster head. The number of nodes is varied with a beta distribution, and Josang mental logic used to calculate the trust of each node. The results show that the method improves the performance compared to recent blackhole detection methods, such as a combination of Artificial Neural Network (ANN) and Support Vector Machine (SVM). The Low Power Lossy Networks (RPL) networks are investigated in [6]. They propose a delta-threshold-based trust model called the Optimized Reporting Module (ORM), which utilizes a forgetting curve to mitigate black hole attacks in Green IoT systems. The number of intruders varies to determine the detection efficiency of the model. The results obtained from the simulation of the proposed scheme demonstrate that it achieves a higher detection rate and lower false positive alarms compared to the existing scheme. Authors in [7] consider a trust-based security solution as a feasible approach for IoT networks due to its simple integration and resource-constrained nature of smart devices. They propose a security, mobility, and trust-based model (SMTrust) for securing RPL-based IoT routing against blackhole attacks, considering the static as well as mobile nodes. The simulation results show that SMTrust performs better than the existing trust-based methods for securing RPL in terms of topology stability is 46%, reduction in packet loss rate is 45%, and 35% increase in throughput, with 2.3% increase in average power consumption.

In contrast to trust-based mechanisms, cryptographic and routing-based approaches focus on safeguarding data and ensuring resilient network paths. In [8], the authors consider blackhole attacks as a critical security threat to Vehicular Ad Hoc Networks (VANET) that deteriorates the network efficiency. They present a cryptographic-based approach integrated into the Ad Hoc Distance Vector (AODV) protocol by route request (RREQ) and route reply (RREP) packets to identify and eliminate the attack. The results show that the approach is efficient in terms of various performance metrics, such as a higher Packet Delivery Ratio (PDR) of 95%, higher throughput of 87%, higher blackhole attack detection ratio of 98%, lower end-to-end delay of 75%, a lower collision rate of 71%, and a lower normalized routing load of 89% compared to the existing approaches. Similarly, in [9], the authors address blackhole attacks as one of the most challenging security issues in VANETs and Autonomous and Connected Vehicles (ACVs). The proposed defense mechanism relies on node counts and routing algorithms. The simulation results show more satisfactory results in terms of PDR, end-to-end delay, packet loss rate, routing overhead, and throughput against existing solutions. The vulnerabilities of Named Data Networking (NDN), including content poisoning and blackhole attacks, are examined in [10]. A two-component method is provided to mitigate these attacks. The first component is a proactive reputation updating algorithm to update the reputation of forwarding candidates based on whether they must be detoured upon packet failures. The second component is a reputation-based probabilistic forwarding strategy that selects the next-hop router for interest packets probabilistically based on the reputations of forwarding candidates. The simulation shows that the model can effectively identify and isolate attackers. In [11], a distributed timer-based mechanism is proposed to perform malicious blackhole node detection in the Ripple Routing Protocol (RPL) networks with IPv6 over Low-

Power Wireless Personal Area Networks (6LoWPAN). This mechanism is implemented using the Cooja simulator on the Contiki-NG operating system, and the results show that it can detect blackholes with high accuracy, resulting in a decrease in packet loss, with the true positive rate reaching up to 100%. The authors of [12] also focus on RPL-based networks and present an approach to protect them against blackhole attacks by route optimization for adaptive detection. The approach utilizes multiple parent nodes and a parent evaluation system to enhance route reliability against blackhole attacks. They stated that the approach does not address sinkhole attacks because they cause low damage and are often used along blackhole attacks, and can be detected when blackhole attacks are detected. Simulation results show that the approach provides better protection against blackhole attacks with much lower overheads for small RPL networks.

The research in [13] initially examines the consequences of the blackhole attack on IoT networks and then explores the potential of an authentication algorithm to identify blackhole nodes. This technique aims to track and prohibit malicious nodes from affecting the network, assuring its security against unauthorized access. NS2 and Simulink are used to implement the model and obtain network throughput and PDR. The results show improvements in throughput, close to those of an unaffected network, with PDR measured at 98.21%. In [14], blackhole attacks in the IoT healthcare sector are investigated through the design of an optimal shortest path strategy. The proposed secure framework detects and prevents blackhole attacks using a baiting process, while packet security is reinforced with an Elliptic Curve Cryptography (ECC)-based hashing function. To determine the optimal route, a hybrid algorithm is introduced by integrating the Deer Hunting Optimization Algorithm (DHOA) with the DragonFly Algorithm (DA), termed Dragonfly-based DHOA (D-DHOA). The model is evaluated under varying numbers of nodes and rounds, with performance measured in terms of delay and packet loss ratio. Results demonstrate that the convergence of the proposed approach improves by 50% compared to DHOA and by 66.6% compared to the Whale Optimization Algorithm (WOA).

Building on these traditional defenses, AI-based approaches have introduced adaptive and intelligent mechanisms for detecting and mitigating attacks. The blackhole attacks in MANETs are discussed in [15]. A hybrid approach is presented, which includes anomaly detection to establish a baseline of normal behavior using data mining techniques, including K-means and decision trees, and cryptographic verification via Public Key Infrastructure (PKI) and digital signatures for suspicious nodes. The results show that compared to existing solutions like the dynamic source routing (DSR) protocol and Watchdog, this hybrid method provides more reliable and resilient network performance, dynamically adapting to evolving threats. Additionally, [16] investigates blackhole attacks in MANETs, where MATLAB is used to develop a mitigation system based on an ANN combined with the swarm-based Artificial Bee Colony (ABC) optimization technique. The approach focuses on anomaly detection by defining node thresholds and identifying deviations caused by blackhole attacks. Simulation results compare the performance of AODV with and without ABC in terms of PDR, throughput, and delay. The findings indicate that AODV with ABC & ANN achieves improvements of 0.63%, 13.02%, and 18.39% in PDR, throughput, and delay, respectively, compared to existing solutions. Authors in [17] discuss the threats associated with blackhole attacks in IoT networks. To mitigate these attacks, they propose a method leveraging the K-Means algorithm, called K-Means Clustering-Based Trust (KmeansT), to enhance IoT network security. Simulation results are obtained by varying the number of blackhole nodes and comparing performance with RPL and trust-based RPL. The findings demonstrate that KmeansT achieves superior protection against blackhole attacks, as reflected in improved end-to-end delay, packet delivery ratio, and detection accuracy.

In [18], an intrusion detection framework is proposed to mitigate blackhole attacks in healthcare wireless sensor networks. The framework primarily employs Proportional Overlapping Score-Based Minkowski K-Means Clustering (POS-MKC) for data minimization and categorization. To evaluate its effectiveness, the framework is implemented using NS2 with varying numbers of nodes and compared against Secure Route Discovery in AODV (SRD-AODV) and Adaptive Sink Aware (ASA). Simulation results demonstrate that the proposed framework achieves superior performance by reducing delay and computational complexity while improving packet delivery ratio and attack detection accuracy. In [19], blackhole attacks are described as severe threats to medical sensor networks. To address this issue, the authors propose Simulated Annealing Blackhole Attack Detection (SABD), which is based on the Enhanced Gravitational Search Algorithm (EGSA) to detect and isolate malicious nodes in WSNs. EGSA-SABD is evaluated using the NS2 Simulator with varying node counts, and its performance is measured in terms of blackhole attack detection probability and energy consumption. The results show that EGSA-SABD improves detection probability by 13% and reduces energy consumption by 21% compared to existing approaches. In [20], the authors consider blackhole attacks targeting wireless sensor networks. They introduce Anomaly Detection with the SVM (ADSVM) method to prevent attacks before they affect IoT performance. The model is implemented in Contiki-NG with the Cooja simulator, considering both static and mobile IoT networks by varying the number of nodes. Simulation results demonstrate that ADSVM achieves an accuracy of 84.37% under eightfold cross-validation, highlighting its effectiveness in forecasting and preventing blackhole attacks.

Although prior studies propose diverse detection approaches, several gaps remain that need to be addressed. Many rely exclusively on publicly available datasets, which restricts applicability to dynamic or evolving network conditions and fail to capture realistic traffic variations or attack scenarios. Feature-level analysis is also remains limited. While node count is often considered, other essential features, such as payload size and proximity, which can influence the performance, are overlooked. This narrow focus limits the robustness of findings and leaves important dimensions of detection reliability unexplored. Furthermore, no prior work has addressed blackhole attacks in IoT environments integrated with Wi-Fi7 (EHT) networks as an emerging heterogeneous technology. Existing methods also lack comparative analysis of different learning algorithms, which is crucial for evaluating their effectiveness and identifying strengths and weaknesses in detecting blackhole attacks. To address these gaps, this work introduces a simulation-based environment that enables feature-aware network modeling, diverse dataset generation, integration of Wi-Fi7 with IoT networks, multi-condition attack scenarios, and comparative performance evaluation, thereby enhancing the resilience and adaptability of blackhole attack detection in IoT–EHT networks.

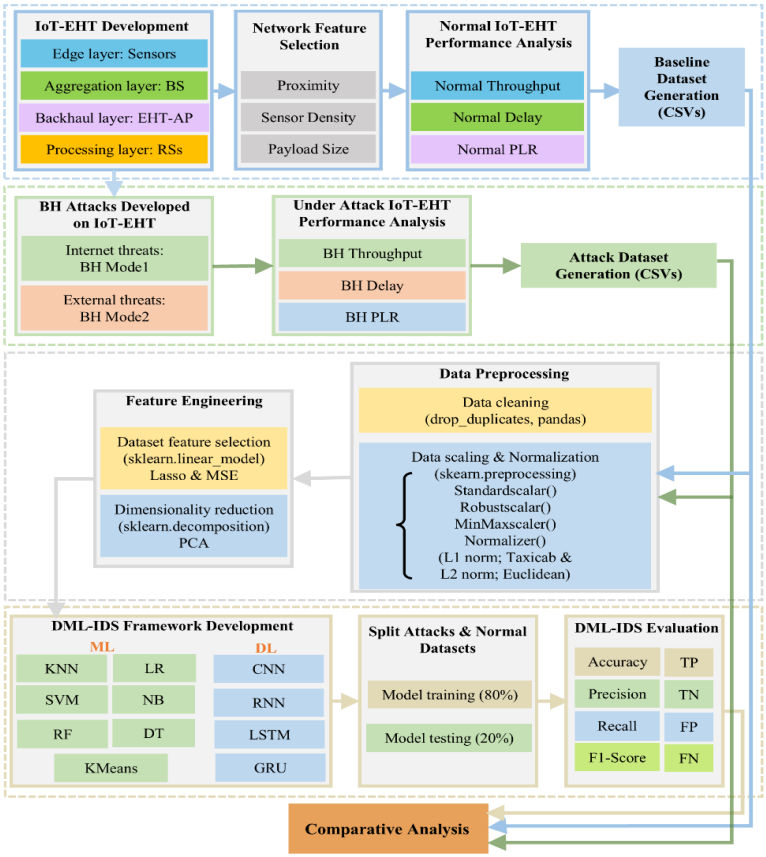

Figure 1. Proposed DML-IDS framework.

3. PROPOSED APPROACH

The proposed framework, illustrated in Figure 1, is implemented in the NS-3 (version 3.43) network simulator [21] to support blackhole attack detection in heterogeneous IoT–EHT networks.

3.1 Simulating the IoT-EHT Network

We design and develop a four-tier IoT-EHT network topology. The key components in this hierarchical setup include:

- Edge layer: IoT sensor nodes are deployed to support low-rate wireless personal area networks (LR-WPANs) and IPv6 over low-power wireless personal area networks with header compression (6LoWPAN-HC) protocol stacks. The HC employs RFC 6282 to compress the long IPv6 headers and make them suitable for use in IoT networks. Sensors in this layer gather environmental data and transmit it to the next layer for further processing.
- Aggregation layer: a central base station (BS) serves as the hub to which the sensors are directly connected. The BS is designed with a dual-interface configuration to serve two primary functions:
  - Sensor communication: the first interface supports LR-WPAN and 6LoWPAN-HC protocols, establishing a local link between the BS and the sensors to receive the collected data.
  - External communication: the second interface utilizes 802.11be protocols for communication with an EHT-based Access Point (EHT-AP).
- Backhaul layer: the EHT-AP resides in this layer to serve as a connection point to the outside of the IoT network. Therefore, it is equipped with an EHT interface for communication with the BS and a Gigabit Ethernet interface for data transmission to the Remote Server (RS).
- Processing layer: in this layer, data received by the RS undergoes further processing to measure and evaluate the performance of the IoT-EHT network under various conditions. This processing is essential for ensuring optimal functionality and security of the network.

This structural topology enhances efficiency during data collection and ensures fast, reliable data transmission through dual interfaces. It also enables high-speed uploads to servers, providing timely access to critical information while improving the overall speed and reliability of communication. An example of the four-tier structure with 6 sensors is visualized in Figure 2.

3.2 Dataset Generation

After simulating the IoT-EHT network, we use it as the foundation for generating diverse datasets to ensure that DML-IDS is trained on comprehensive data that captures the variability of its practical deployments and enhances its ability to generalize across different real-world operational conditions. These conditions are represented at the feature-level by varying three experimental features, including the proximity of the BS to the sensors, the density of the sensors, and the payload size of the

data collected by the sensors in IoT-EHT networks, while also considering both normal (no attack) and attack conditions as follows.

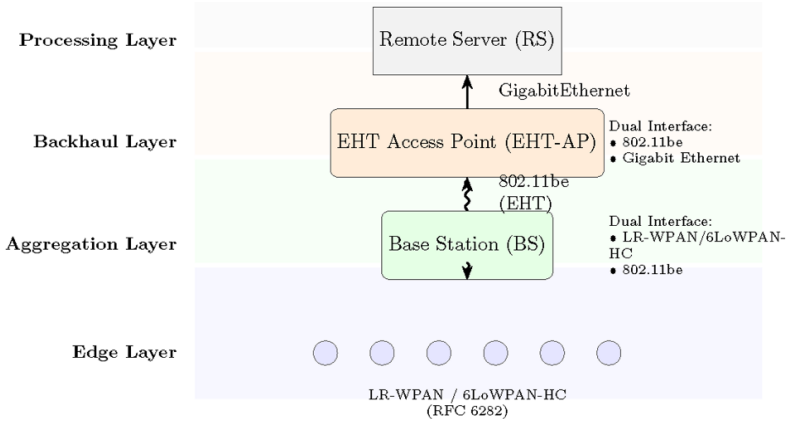

Figure 2. Four-tier IoT-EHT structure.

The proximity of the BS to the sensors can affect transmission efficiency. Longer distances can lead to increased signal degradation and higher transmission delays, potentially affecting network throughput. Accordingly, various distance scenarios are evaluated to identify vulnerabilities that attackers may exploit to disrupt communication, particularly in networks where sensors are located far from the BS. Moreover, the density of sensors deployed in the IoT networks can influence communication dynamics and data acquisition efficiency. Higher sensor density can enhance data collection capabilities, enabling more detailed environmental monitoring. However, it may also lead to increased bandwidth competition and create additional opportunities for attackers. The effects of varying sensor density on network performance with and without blackhole attacks are evaluated. This analysis helps identify optimal sensor configurations without compromising network efficiency. Additionally, the size of data packets transmitted across the IoT-EHT networks can impact both performance and security. IoT sensors generate diverse data types, resulting in varying payload sizes depending on the environment. Smaller packets may reduce transmission time and improve responsiveness, but can also increase overhead and the rate of packet fragmentation. On the other hand, larger packets can decrease the frequency of transmissions, potentially enhancing efficiency. Therefore, the impact of different payload sizes on network performance is investigated both in the presence and absence of blackhole attacks. Collectively, this feature-level analysis approach aims to optimize data transmission and meet the diverse requirements of IoT applications.

Once the experimental features are selected, it is essential to establish their sequence values in accordance with the characteristics of IoT networks in order to determine the optimal thresholds and also use them as attack behavior indicators. For each experimental feature, sequence values are established according to IoT network characteristics, with thresholds calculated as:

$$\begin{gathered} a_n = a_{initial} + (n-1)d_{difference} \\ a_n = [x_i, x_{i+1}, \cdots\cdots, x_T] = i \in [1, 2, \cdots\cdots, T] \end{gathered} \tag{1}$$

where a_n is the n-th item in the sequence, $a_{initial}$ is the first item, $d_{difference}$ is the common difference between the items, T is the threshold, and n is the round number of runs. The resulting sequences and configurations are summarized in Table 1.

After selecting the values of the three experimental features, the next step is dataset generation. To evaluate the contribution of the experimental features, we vary them one at a time. This results in three sets of separate datasets that are independently used to train and test the models. This approach allows us to obtain distinct performance metrics for each feature across all models, and the resulting feature-level comparison reveals how models perform under different conditions while identifying which features contribute most to blackhole attack detection. Dataset generation proceeds in two stages: baseline datasets and attack datasets. Initially, extensive experiments are conducted to determine a deep analysis of normal IoT-EHT network behavior. We characterize this normal behavior in the absence of blackhole attacks to obtain essential baseline results that reflect normal network performance. These normal performance results are then used to create baseline datasets for subsequent analysis and comparison with attack datasets. Because we capture the results by Wireshark [22] in PCAP format, we further convert them to CSV datasets with CICFlowMeter [23] and Argus [24] tools.

Following this baseline assessment, the attacks are conducted over the IoT-EHT network. A dual-mode attack module is implemented to conduct two different types of attacks for comparative analysis purposes:

- Mode1 (Internal Blackhole Threats): this mode represents the conventional blackhole attack, in which malicious nodes are placed within the IoT-EHT network. These malicious nodes advertise optimal routes, intercept incoming packets from legitimate nodes, and then drop them, thereby disrupting normal communication.
- Mode2 (Outsider Disruption Threats): this mode represents an extended disruption attack model to evaluate how external adversaries can conduct blackhole-like attacks without formally joining the network [24, 25]. External adversaries intercept incoming packets from legitimate nodes and drop them to disrupt normal data transmission,

thereby producing effects comparable to blackhole behavior. When combined with Mode1, this dual-mode attack module enables a comprehensive analysis of the network resilience against both insider and outsider threats.

The performance of the IoT-EHT network under these attack modes is measured to generate attack datasets in CSV format. When merged with baseline datasets, these serve three purposes: assessing the vulnerability of IoT networks to blackhole attacks by comparing the attack and baseline data, enabling severity analysis through comparison of internal and external attack impacts to determine which type poses a greater threat, and training the proposed DML-IDS framework to distinguish between benign and malicious activities in the IoT-EHT network.

The datasets consist of two categories of features. The first category includes raw traffic-level features (e.g., *src_ip, dst_ip, src_port, dst_port, protocol, timestamp, flow_duration, num_forward_packets, num_backward_packets, bytes_forward, bytes_backward, hop_count*), which represent the fundamental characteristics of IoT/EHT traffic, thus remain constant across experiments. The second category comprises experimental features (proximity, sensor density, and payload size), which are varied individually in each experiment to analyze their influence on attack impact and detection. Each dataset is labeled according to the attack condition ($label \in \{mode1, mode2, normal\}$). The simulation environment is designed to allow flexible selection of simulation time, attack duration, and baseline duration based on the desired number of samples, thereby enabling customized sample-space generation. The evaluation in this work is presented using 10,000 samples per dataset. Table 2 provides the hardware specifications and tools used to run the simulation experiment and generate datasets.

Table 1. IoT-EHT simulation parameters.

Parameter	Values
Base station proximity	{10,30,50,…,130} m
Payload size	{20,30,40,…,100} B
Sensors density	{5,10,15,…,30}
IPHC (Rfc6282)	true
EHT Frequency	BAND_5 GHz
channelWidth	80 MHz
EhtMcs	7
ChannelNum	11
RxSensitivity	-110 dBm
TxPower	5 dBm
Networking Technologies	LR-WPAN, 6LoWPAN, 802.11be EHT, IPv6
TxPowerSpectralDensity	(5, 11)

Table 2. Hardware specifications and tools.

Parameter	Description
CPU	13th Generation Intel i5 processor
RAM	16 GB DDR4
Storage	1 TB PCIe Gen4 NVMe
NIC	Intel Wi-Fi7
Graphic	Integrated Intel Iris Xᵉ Graphics
CICFlowmeter openjdk-8-jd	v.4.0
Wireshark	v.4.4.1-0-g575b2bf4746e
Argus	v.5.0.0
PyCahrm	v.2024

3.3 Dataset Preprocessing

The obtained datasets require preprocessing to ensure data quality and consistency for effective analysis. We perform data cleaning using the *drop_duplicates()* method in pandas to eliminate duplicate entries and reduce redundancy across the datasets. Additionally, we apply data scaling and normalization techniques to standardize the features and improve the performance of the subsequent analyses. Specifically, we compare several methods from the *sklearn.preprocessing* library, including *MinMaxScaler()*, which scales features to a specified range, *Normalizer()* with both *l1* (Taxicab distance) and *l2* (Euclidean) norms, *StandardScaler()*, which standardizes features by removing the mean and scaling to unit variance, and *RobustScaler()*, which scales features using statistics that are robust to outliers. On the other hand, the effectiveness of blackhole attacks in IoT networks, as well as the protection offered by the corresponding security solutions, depends on several key features. To capture this complexity, we conduct extensive experiments under a variety of network conditions, parameters, and features while generating baseline and attack datasets. As a result, the obtained datasets exist in high-dimensional spaces with a wide range of features, some of which may introduce redundancy into the proposed framework. It is essential to select subsets of the most relevant features from these datasets before feeding them into the DML-IDS framework. To achieve this, we apply feature selection and dimensionality reduction techniques to the preprocessed datasets. We first use Lasso regression from *sklearn.linear_model* module, which identifies and selects features that directly impact the performance of IoT-EHT networks by evaluating feature importance based on Mean Squared Error (MSE). We utilize Principal Component Analysis (PCA) from *sklearn.decomposition* module to further reduce the dimensionality of raw traffic-level features (e.g., IPs, ports, packet counts) by transforming correlated variables into a smaller set of principal components.

3.4 Proposed DML-IDS

The proposed framework consists of different learning models, including Logistic Regression (LR), K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Naive Bayes (NB), Random Forest (RF), Decision Tree (DT), K-means clustering (K-means), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), and Gated Recurrent Unit (GRU). The models are chosen based on their unique and complementary abilities in capturing different aspects of IoT-EHT traffic behavior and detecting anomalies associated with blackhole attacks. LR simplicity makes it effective for binary classification tasks such as distinguishing normal traffic from blackhole attack traffic, though its reliance on linear relationships can limit its ability to capture more complex attack patterns. KNN can be suited for detecting localized anomalies, but its computational cost can increase with dataset size, while it is sensitive to irrelevant features that can affect real-time attack detection in IoT-EHT networks. SVM is efficient in high-dimensional spaces and can model complex decision

boundaries, which is advantageous for differentiating attack traffic, but it requires careful kernel selection and may struggle with scalability when applied to large datasets. NB is fast and lightweight, making it attractive for resource-constrained IoT devices, but its assumption of feature independence can affect IoT-EHT traffic, where features such as packet counts and payload sizes are correlated. RF provides robustness against noise and overfitting and determines which traffic features are most indicative of blackhole attacks, though it can be computationally heavy. DT is simple and fast to train, but it can be prone to overfitting. KMeans is useful when labeled data is limited, however, its sensitivity to initialization and assumptions may not align with the irregular nature of blackhole traffic. Deep learning models extend the framework's ability to capture more complex dependencies. CNN excels at learning spatial feature hierarchies to identify structured traffic patterns, but is requires large datasets and can be less effective at modeling sequential dependencies. RNN can capture temporal dependencies in sequential traffic, which is valuable for detecting attacks that evolve over time, though they can suffer from limited long-term memory. LSTM overcomes this limitation by modeling long-term dependencies more effectively, making it more suitable for detecting persistent attack behaviors, but it can be computationally intensive and slower to train. GRU provides a more efficient alternative to LSTM, offering comparable performance with reduced computational cost, though it may underperform when modeling highly complex or long-term traffic dependencies.

After selecting the models, all the preprocessed CSV datasets are divided into training (80%) and testing (20%) subsets. This split is widely adopted because it balances sufficient data for training with a meaningful portion for unbiased evaluation, helping reduce overfitting. Subsequently, the models are trained on the datasets to distinguish legitimate traffic from suspicious activities caused by blackhole attacks. Their performance depends on hyperparameters, which are optimized using the Grid Search (GS) technique. GS systematically tests combinations to identify the best configuration, ensuring the models achieve high accuracy and generalize effectively to unseen data. Descriptions of the hyperparameters used by the ML and DL models are provided in Tables 3 and 4, respectively.

Finally, the performance evaluation is conducted across two levels of metrics: network-level and detection-level. At the network level, results are obtained to evaluate IoT-EHT network performance under baseline operation (no blackhole attack), compare the impacts of the two attack modes (mode 1 and mode 2) to determine which is more severe, and analyze feature-wise behavior under both normal and attack conditions to assess how each feature influences performance. The evaluation is conducted using metrics, including throughput (rate of successful packet delivery from sensors to the RS), delay (average time taken for a packet to travel from the sensors to the RS), and the packet loss rate (PLR; proportion of packets that fail to reach the RS compared to the total packets transmitted by the sensors). At the detection level, the effectiveness of individual models within the DML-IDS framework is evaluated, highlighting the capability of each model to identify malicious blackhole activities in IoT-EHT networks. These results are measured through a confusion matrix in terms of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN), alongside accuracy, precision, recall, and F1-score.

Table 3. ML training hyperparameters.

Model	Key parameters	Tested values (grid search)
RF	n_estimators	100, 200, 300, 500
	max_depth	10, 20, 30, None
SVM	kernel	linear, rbf, poly
	C	0.1, 1, 10, 100
	gamma	scale, auto, 0.1, 0.01
KNN	n_neighbors	3, 5, 7, 10
	metric	Euclidean, Manhattan, Minkowski
	weights	uniform, distance
DT	max_depth	5, 10, 20, None
	min_samples_split	2, 5, 10, 20
LR	max_iter	100, 200, 500, 1000
	C	0.1, 1, 10
	solver	liblinear, saga, lbfgs
NB	var_smoothing	1e-9, 1e-8, 1e-7, 1e-10
K-Means	init	'k-means++'
	max_iter	300
	n_init	10

Table 4. DL training hyperparameters.

Model	Layer	Details
CNN	Input Layer	Shape = (X_train_dense.shape[1], 1)
	Conv1D Layer	64 filters, kernel size = 3, activation = 'relu'
	MaxPooling1D Layer	Pool size = 2
	Flatten Layer	Flatten the output of the previous layer
	Dense Layer	64 units, activation = 'relu'
	Dense Layer	1 unit, activation = 'sigmoid'
RNN	Input Layer	Shape = (X_train_dense.shape[1], 1)
	SimpleRNN Layer	64 units, activation = 'relu'
	Dense Layer	1 unit, activation = 'sigmoid'
LSTM	Input Layer	Shape = (X_train_dense.shape[1], 1)
	LSTM Layer	64 units, activation = 'relu'
	Dense Layer	1 unit, activation = 'sigmoid'
GRU	Input Layer	Shape = (X_train_dense.shape[1], 1)
	GRU Layer	64 units, activation = 'relu'
	Dense Layer	1 unit, activation = 'sigmoid'

4. SIMULATION RESULTS

This section presents two sets of findings: first, network-level results, and second, detection-level results. Together, these provide a comprehensive evaluation of attack impacts, severity, and resilience, feature-wise behavior, and the models' ability to distinguish between benign and malicious activities in IoT–EHT networks.

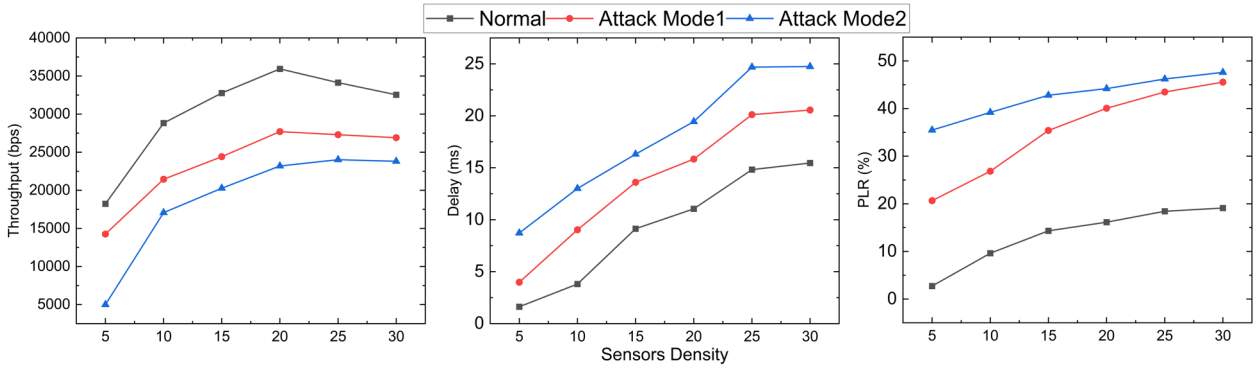

Figure 3. Severity distribution of BH attacks under varying sensor density conditions.

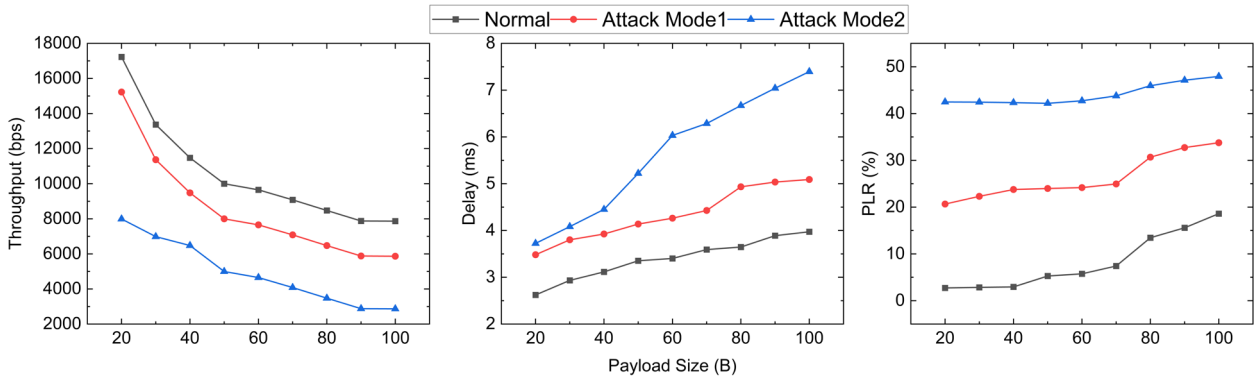

Figure 4. BH attack effects influenced by payload size.

4.1 Sensor Density

While increasing sensor density in IoT-EHT networks can improve data collection, it may also expand the potential BH attack surface. Dense deployments lead to more complex routing paths, which can be exploited by malicious nodes to intercept and drop larger amounts of traffic. To assess how sensor density influences IoT-EHT network vulnerability and operational stability, we measure the performance under varying density conditions, both in normal operation and during a BH attack. Figure 3 presents the severity of blackhole attacks as influenced by the sensor density feature, offering insight into how node concentration shapes the dynamics of intrusion impact.

The results highlight not only the severe vulnerability of IoT-EHT networks to blackhole attacks, but also that increasing sensor density amplifies the severity of these attacks, further degrading network performance. The baseline results (without attacks) indicate that the IoT network exhibits an initial increase in throughput as additional sensors are joined to the network and transmit data. Under normal conditions, adding sensors improves throughput up to a saturation point. After reaching a peak of around 15-20 sensors, it starts to decline due to network congestion and increased contention for bandwidth. When attacks occur, they significantly reduce throughput at all sensor density levels, with attack mode2 causing a higher level of degradation. This is because, unlike internal attackers (mode1), which can be constrained by trust thresholds, external attackers operate outside the trust boundaries. This makes them harder to detect and isolate, allowing them to access and drop a larger portion of network traffic on a larger scale, while mode1 is limited in this scope. Their strategic positioning near high-traffic zones further amplifies their impact on network performance. Additionally, routing disruptions during attacks create inefficient paths, which, along with higher traffic volume, further increase delays in all attack modes. The second mode causes even greater delays because attackers can corrupt a larger volume of traffic. The PLR results indicate that the BH attacks severely affect network reliability. In both modes of attack, the attackers attempt to redirect traffic to themselves and drop packets, which results in an increased PLR. At a lower sensor density, the performance differences between normal and attack modes are smaller, but as the density increases, the differences increase significantly. Attack mode2 can reach nearly 50% PLR, meaning half of the packets are being lost. A PLR exceeding 50% can lead to severe service disruption, particularly in real-time IoT applications.

4.2 Data Payload Size

The diversity of data collected by different sensors in IoT-EHT networks enables the transmission of multiple data types, ranging from lightweight environmental readings to complex medical or multimedia data, which further reflects the functional heterogeneity of IoT systems. As each type of data requires a distinct payload size, IoT configurations may respond differently to these variations, which can result in routing complexity and security exposure. Thus, analyzing how payload size shapes network vulnerability and the severity of BH attacks is critical for designing robust mitigation strategies that remain effective across diverse data loads. Figure 4 illustrates the relation among payload size, IoT-EHT network performance, and the severity of BH attacks.

The baseline behavior of the network shows that throughput decreases as payload size increases. Larger packets carry more data, resulting in fewer packets being transmitted per second and thus lowering the overall data rate. Moreover, the loss

of larger packets leads to more retransmissions, which further reduces the network efficiency. These conclude that transmitting smaller packets in IoT networks contributes to effective throughput. However, the BH attack results indicate severe throughput degradation even for smaller packets, particularly with attack mode2. Without attacks, the normal IoT network experiences the lowest delay, starting at approximately 3ms for small packets and increasing to around 4ms for larger packets. When attacks begin, the initial impact on delay is not significant in either attack mode. However, as the payloads become larger, the difference in delay increases. In BH mode1, the delay ultimately reaches 5ms, compared to 7ms when the second mode of attack targets the network. Packet transmission time increases linearly with size as more data in a single packet leads to longer queuing and processing times. Since attack mode2 affects more packets, the increasing number of retransmissions results in higher latency. This highly affects the overall performance of IoT networks because a high delay causes the subsequent processing commands to arrive too late, making real-time control impossible. With regard to the reliability of the IoT network, before the attack, the network has the lowest PLR, staying mostly below 5% for small packets but rising near 15% for larger packets. However, the BH attacks severely impact the reliability of the IoT networks by raising the PLR to 35% and 50% in the first and second modes of attacks, respectively. When a blackhole attack drops a large packet, more data is lost at once. This means that larger packets are more exposed to BH attacks, thus their transmission should be avoided in blackhole-prone networks.

4.3 BS Proximity

While the proximity of the BS can influence the communication efficiency of the sensors, it is equally important to investigate whether this spatial arrangement affects the behavior and impact of blackhole attacks. Understanding how malicious nodes leverage their position, whether near or far from the BS, can uncover critical vulnerabilities in routing dynamics. To explore this dimension, the IoT-EHT network is implemented under varying proximity conditions to evaluate performance during normal operations and under blackhole attacks. Figure 5 illustrates the variation in blackhole attack severity as the proximity changes.

While these results also highlight the severe vulnerability of IoT networks to blackhole attacks, the proximity feature proves less effective in influencing performance compared to sensor density and payload size features. In normal conditions, when no BH attack is targeting the network, the performance remains relatively stable and drops slightly as the proximity increases, with a sharp drop after 110 m. This decline is expected due to the natural degradation of signal strength over longer distances. However, when the BH attack starts over the IoT-EHT network, a significant performance degradation is observed regardless of the mode of the attack. In mode2, throughput decreases significantly, with a steady decline that becomes more severe with distance. This suggests that an attacker outside the IoT network is effectively disrupting the flow of data, and by blocking transmission, it causes substantial reductions in the overall network capacity. In mode1, throughput decreases at a slower rate compared to mode2, but it remains consistently lower than normal network. This indicates that the internal threats impact throughput, though their effect is less severe than external threats. Delay is a critical factor, especially for time-sensitive IoT applications. In mode1, the delay is consistently higher than in normal conditions. While the difference is small at short distances, it becomes significant as distance increases, exceeding 4 ms after 90 m. In contrast, the IoT network experiences the highest delay during mode2, remaining close to 6ms and rising sharply after 90 m. This suggests that external blackhole threats disrupt communication more severely. In the context of the PLR results, a gradual increase is observed at greater distances, but the rates consistently remain low (below 5%) regardless of the distance when there is no attack. This indicates that the communication between devices in the network operates with minimal loss in normal conditions when no attacks are present. The worst impact is observed in mode2. A sharp increase of over 40% is observed from the beginning, indicating that the attacker within the IoT network causes significant packet loss even at close distances. The attacker disrupts network traffic by interfering with routing paths and redirecting packets. While packet loss in mode1 is lower than in mode2, it still exceeds normal conditions, remaining around 20%. This suggests that local attackers, with limited control over communication, cause fewer lost packets compared to external attackers.

After presenting network-level results on the impacts of blackhole attacks through feature-aware analysis of proximity, sensor density, and payload size, the following sections report detection-level performance of the DML-IDS framework, demonstrating its capacity to enhance the security and resilience of heterogeneous IoT–EHT networks against such attacks.

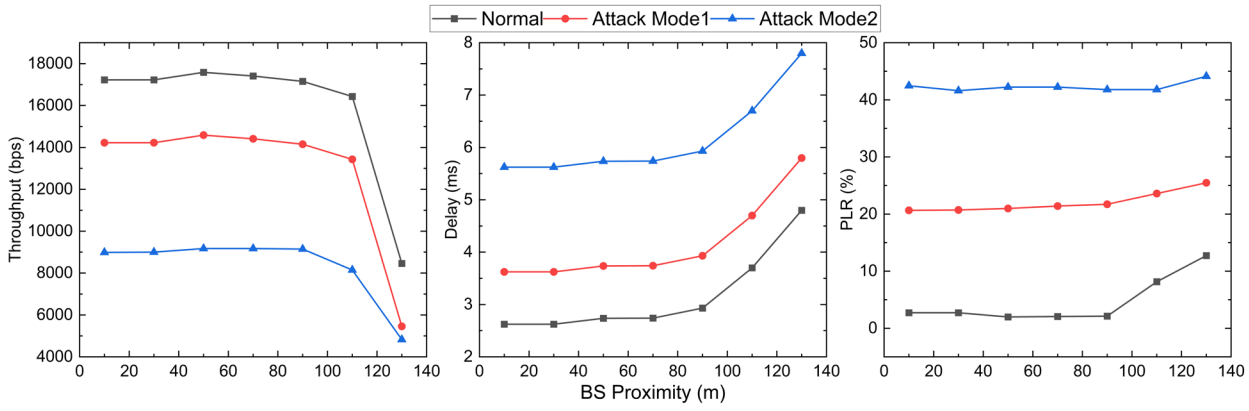

Figure 5. BH attack effects influenced by the proximity feature.

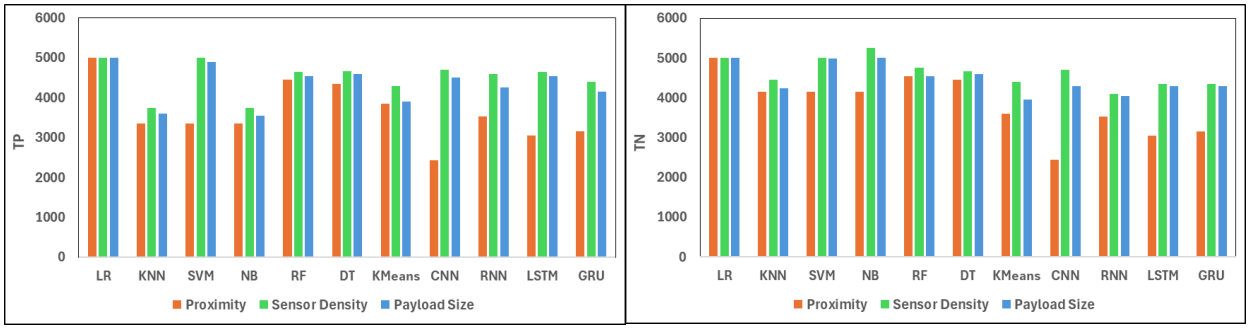

Figure 6. Comparative success rates of DML-IDS to detect BH attacks.

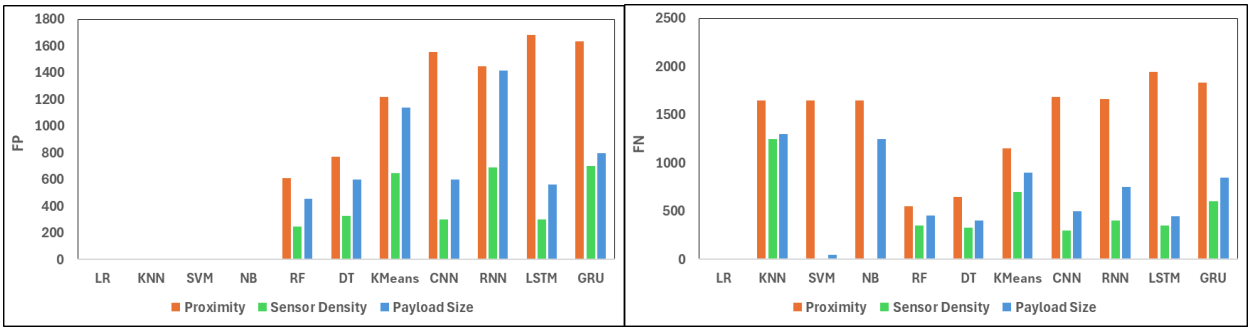

Figure 7. DML-IDS failure rate in detecting BH attacks.

4.4 True Detection (TP and TN) of BH Attacks

True positive (TP) indicates the rate at which the DML-IDS correctly identifies the attacks by flagging the compromised traffic patterns. In IoT-EHT networks, high TP values indicate strong sensitivity to threats, which is especially critical in dynamic environments where early detection prevents data loss and network disruption. In contrast, a true negative (TN) indicates the model's capacity to avoid false alarms by correctly classifying benign network activity as non-malicious. A high TN rate contributes to trust in the system's decisions and minimizes overhead, which are essential for maintaining operational stability and avoiding unnecessary interventions. The comparative results for TP and TN for each learning model are illustrated in Figure 6.

The comparative analysis of TP and TN results across multiple ML and DL models within the DML-IDS framework highlights performance variations shaped by the features. For sensor density, ML models show clear separation. LR achieves perfect TP and TN because density provides complete separability. SVM follows closely, as margin-based classification aligns well with density patterns. RF and DT are also reliable, exploiting density splits to capture attack behavior. KMeans achieves moderate balance, while NB and KNN sit lower, with weaker TP but higher TN due to their conservative detection style. In DL models, CNN performs strongly to capture structured density signals. RNN, LSTM, and GRU also remain stable with solid TP and TN, but slightly lower than CNN, showing that sequential modeling adds value. ML models also lead with regard to payload size. LR reaches perfect TP and TN, confirming that payload volume is a strong indicator of blackhole activity for this model. SVM follows closely because the payload size fits its classification boundaries well. RF and DT remain highly effective, producing balanced TP and TN. NB and KNN are moderate, leaning toward higher TN but lower TP, while KMeans struggles most, unable to separate payload distinctions clearly. In DL models, CNN performs well, benefiting from structured input that convolution can exploit. LSTM and GRU deliver solid results, slightly ahead of RNN, reflecting sequential modeling of traffic flow and packet size variations. For proximity, ML models show more variation. LR remains perfect, followed by RF and DT with strong but slightly reduced TP and TN compared to other features. SVM is moderate, as proximity does not align well with its margin-based boundaries. KNN, NB, and KMeans together are at lower levels, favoring TN over TP and missing more attacks. In DL models, RNN, GRU, and LSTM drop further, showing that sequential modeling cannot fully compensate for distance-based signals. CNN performs lower, underperforming in TP, confirming proximity is its main limitation compared to other features.

4.5 False Detection (FP and FN) of BH Attacks

False positives (FP) reflect failures that happened due to erroneously flagging legitimate activity as malicious BH, resulting in the blocking of legitimate nodes or traffic. These misclassifications in resource-constrained IoT-EHT networks can degrade performance, as each false alert consumes valuable bandwidth and energy. In contrast, false negatives (FN) are actual blackhole attacks that the model fails to detect, allowing malicious behavior to persist unnoticed. These are among the most critical errors, as they compromise data integrity and disrupt network operation. In IoT-EHT networks, high FN rates can lead to cascading failures, especially in dense sensor deployments. The rate of FP and FN failures for different feature dimensions and learning models is depicted in Figure 7.

The FP and FN outcomes reveal detection challenges across different features. For sensor density, LR, SVM, and NB achieve perfect detection with no FP or FN, reflecting complete separability. RF and DT remain more reliable, producing

relatively fewer FP and FN since tree-based splits capture density well. KNN also avoids false positives but suffers from high FN, missing attacks due to its reliance on local neighbors. KMeans generates higher FP and FN, highlighting the limits of clustering in attack-specific density. Within DL models, CNN performs strongly with relatively low FP and FN, while LSTM is close behind, showing stable outcomes. RNN records higher FP but moderate FN, and GRU struggles most, with both FP and FN elevated. For the payload size feature, ML approaches again lead. LR achieves best detection with no FP or FN, while SVM is nearly perfect, with zero FP and very low FN. RF and DT follow with balanced FP and FN, reflecting robustness but also sensitivity to payload variations. NB and KNN achieve zero false positives but miss many attacks, producing high FN because of restrictive assumptions. KMeans struggles like before, with both FP and FN elevated, confirming unsupervised clustering is less suited to payload distinctions. Among DL models, CNN performs strongly with manageable FP and FN, while LSTM and GRU deliver solid results, slightly ahead of RNN, which captures sequential traffic patterns. For the proximity feature, ML models show more variations. LR remains high with no FP or FN, but SVM, NB, and KNN, while avoiding false positives, have higher FN as proximity does not provide strong separation. RF and DT come next, showing moderate FP and FN, reflecting their ability to handle proximity splits but with reduced stability compared to density or payload size features. KMeans produces substantial FP and FN, confirming clustering also struggles with proximity. Within deep learning models, RNN, GRU, and CNN show high FP and FN, demonstrating that sequential and convolutional approaches cannot fully handle distance-based effects. LSTM performs worst with the highest FP and FN, confirming proximity is its main limitation.

4.6 Accuracy of BH Attacks Detection

Accuracy is the proportion of both legitimate and BH attack activities that are correctly classified by the model. It offers a general measure of the model's overall consistency across all classification tasks, including variations in proximity, sensor density, and payload size. Figure 8 illustrates the accuracy scores achieved for each model-feature combination.

For sensor density, the strongest accuracy comes from LR and SVM, both reaching high scores because density provides clear separation that fits linear and margin-based boundaries. RF and DT also perform at a high level, as tree-based splits capture density patterns effectively. KMeans achieves moderate accuracy compared to NB and KNN, which remain lower, limited by independence assumptions and sensitivity to local neighbors. In deep learning models, CNN shows strong accuracy, able to exploit structured density signals, while LSTM, RNN, and GRU also deliver solid but slightly lower results, reflecting the limits of sequential modeling compared to classical approaches. For payload size, LR again reaches perfect accuracy, and SVM is nearly flawless, confirming that payload size is a strong indicator of blackhole activity. RF and DT remain highly dependable, while NB and KNN achieve moderate accuracy. KMeans records the lowest accuracy among ML methods, showing clustering struggles with payload distinctions. In DL models, CNN performs strongly, benefiting from structured input that convolution can exploit. LSTM and GRU provide solid accuracy, slightly ahead of RNN, which captures sequential traffic flow but less effectively. For proximity, LR maintains perfect accuracy, and RF and DT follow with strong but slightly reduced accuracy compared to other features. KNN, SVM, NB, and KMeans perform at moderate levels, showing proximity is less discriminative and leads to missed detections. In DL models, RNN, GRU, and LSTM drop further, indicating that sequential modeling cannot fully compensate for weak distance-based data. CNN performs lower with accuracy falling below 0.5, confirming previous results as proximity is its limitation compared to density and payload size features.

4.7 Precision of BH Attacks Detection

In blackhole attack detection, accuracy serves as a useful baseline for comparing models, but it can be misleading in imbalanced datasets. In IoT-EHT networks, where attack instances may be relatively rare, accuracy must be interpreted alongside more discriminative metrics. Therefore, we evaluate precision to determine how many of the instances flagged as blackhole attacks are truly malicious. Precision becomes especially critical when features such as payload size, proximity, or sensor density fluctuate, as these variations can introduce classification noise. High precision ensures that alerts are both meaningful and actionable, conserving system resources and maintaining trust in its alerts. The precision performance for each model is depicted in Figure 9.

For sensor density, the top performers are LR, KNN, SVM, and NB, all reaching perfect precision since density provides clear separability that eliminates detection errors. RF and DT follow closely, with very high precision values, showing that tree-based models partition density effectively but still allow a few misclassifications. KMeans is lower, reflecting the limitations of clustering in capturing density-based attack patterns. Among the DL models, CNN and LSTM achieve similarly strong results, both benefiting from structured density data. GRU and RNN, by contrast, deliver lower performance, remaining functional but less effective. For payload size, LR, KNN, SVM, and NB all reach perfect accuracy, showing that payload size is a highly discriminative feature. RF and DT also achieve strong accuracy, benefiting from their ability to split payload ranges effectively. KMeans falls behind, struggling to distinguish payload variations. In deep learning models, LSTM and CNN perform at a similarly high level, with LSTM slightly ahead, both leveraging structured input to maintain strong precision. GRU and RNN deliver lower performance, capturing sequential traffic patterns but with greater variability and less stability. For proximity, LR, KNN, SVM, and NB again achieve perfect precision, demonstrating their robustness even when the feature offers weaker separation. RF and DT follow with respectable scores, showing that tree-based methods can extract meaningful patterns from proximity data. KMeans performs less effectively, as clustering struggles to interpret spatial relationships. In the DL category, GRU and RNN exhibit lower precision, indicating that sequential modeling does not fully compensate for the limitations of proximity. CNN and LSTM perform similarly, but with reduced effectiveness compared to other features, confirming that proximity remains a challenging input for deep learning architectures.

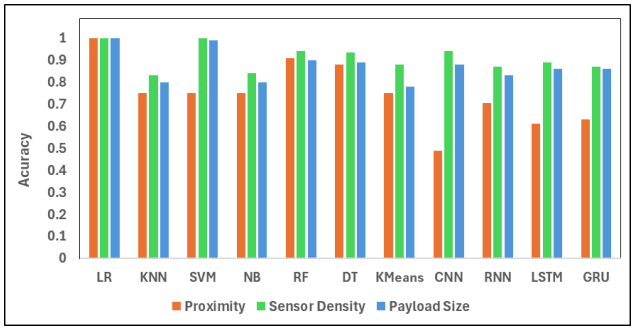

Figure 8. Accuracy levels achieved by each model in DML-IDS for the detection of BH attacks.

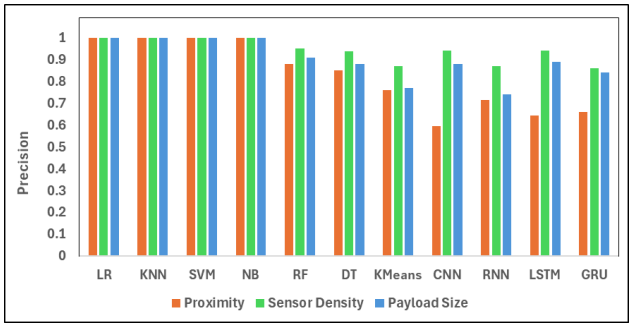

Figure 9. DML-IDS precision to detect BH attacks.

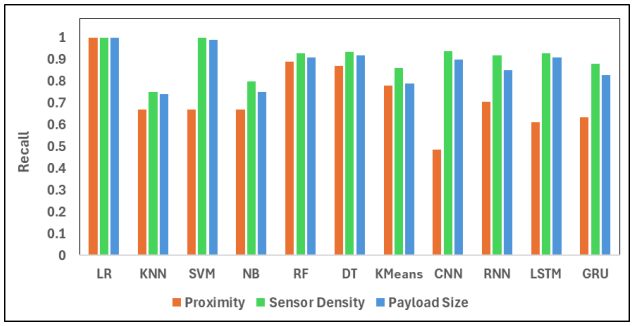

Figure 10. DML-IDS recall for detection of BH attacks.

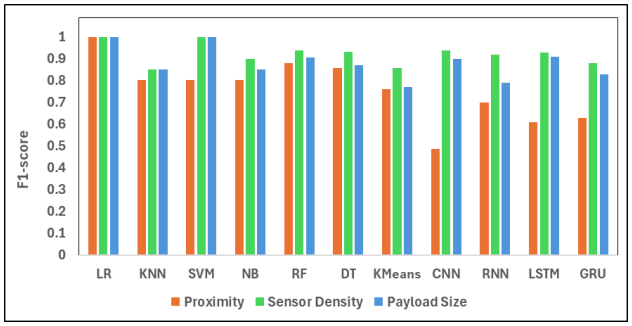

Figure 11. DML-IDS F1-score for detection of BH attacks.

4.8 Recall of BH Attacks Detection

Recall emphasizes completeness by measuring the model's ability to detect actual BH attacks among all the attack instances. In IoT-EHT networks, high recall is critical for proactive defense, particularly under frequent or evolving threats, to ensure that the model does not overlook the BH attacks. We measure recall to assess each model's sensitivity to harmful patterns across varying conditions of proximity, sensor density, and payload size features. Figure 10 illustrates the recall performance of each model.

For sensor density, recall is strongest overall because this feature separates normal and malicious traffic clearly. Among ML models, LR and SVM achieve perfect recall, capturing all attack instances without omission. RF and DT follow closely, demonstrating strong recall through effective partitioning of density patterns. KMeans performs moderately, limited by its unsupervised nature. NB and KNN fall behind, with lower recall due to rigid assumptions and sensitivity to local structure. In deep learning models, CNN and LSTM show similarly strong recall, both benefiting from the structured nature of dense inputs. RNN and GRU, however, deliver lower performance, with more missed detections and less consistency. For payload size, recall remains high for several ML models. LR reaches perfect recall, and SVM nearly competes, confirming that payload size is also a reliable indicator of attack behavior. DT and RF maintain strong recall, NB and KNN show reduced recall due to conservative classification, and KMeans performs the weakest as before. Among DL models, LSTM and CNN perform at a similarly high level, with LSTM slightly ahead, both leveraging structured input to detect attacks reliably. GRU and RNN are more variable, with lower performance and greater difficulty capturing sequential patterns. For proximity, recall varies widely. LR remains perfect, while RF and DT also achieve solid recall, extracting useful patterns despite weaker separation. KMeans performs moderately, detecting some attacks but missing others. SVM, NB, and KNN group together at lower recall levels, struggling to identify threats due to the limited informativeness of the proximity feature. In DL models, RNN shows the highest recall, ahead of GRU and LSTM, though all three face challenges with distance-based signals. CNN records the lowest recall, confirming proximity is its most limiting feature.

4.9 F1-score of BH Attacks Detection

The F1-score is especially valuable when false positives and false negatives carry significant consequences. Unlike accuracy, which may obscure performance in imbalanced datasets, the F1-score offers a more balanced evaluation of detection reliability. In IoT-EHT networks, where both detection performance and resource efficiency are critical, this metric helps identify models that perform reliably under real-world constraints. Figure 11 presents the variation in F1-scores across the learning models and feature conditions.

For sensor density, the highest F1-scores are achieved by LR and SVM, both reaching perfect values due to the feature's strong ability to separate benign and malicious traffic. RF and DT follow closely, showing that tree-based methods can effectively capture density-based patterns with minimal error. NB performs well, while KMeans lands in the middle range, limited by its unsupervised nature. KNN records the lowest F1-score, hindered by its dependence on local neighbor comparisons. In deep learning, CNN and LSTM deliver similarly high performance, both benefiting from the structured nature of dense inputs. RNN slightly outperforms GRU, which remains functional but with lower scores. For payload size, LR and SVM once again reach perfect F1-scores, confirming that this feature is also highly effective for distinguishing attack behavior.

RF and DT maintain strong performance, successfully dividing payload ranges to detect threats. NB and KNN show similar moderate results, reflecting cautious detection strategies that reduce overall balance, while KMeans performs weakest as before. Among DL models, LSTM and CNN achieve comparable high scores, with LSTM slightly ahead, both leveraging structured input to maintain reliable detection. GRU and RNN are less consistent, with lower F1-scores due to variability in capturing sequential traffic patterns. When evaluated on proximity, LR maintains a perfect F1-score, while RF and DT also deliver strong results, showing that tree-based algorithms can uncover useful spatial patterns. SVM, NB, and KNN fall into a mid-range performance, able to detect attacks but missing enough to lower their overall balance. KMeans performs lowest among the ML models due to the complexity of interpreting distance-based inputs. Among deep learning models, RNN leads with the highest F1-score, slightly outperforming GRU and LSTM, though they struggle to extract reliable patterns from proximity data. CNN shows lower performance, with F1-scores dropping below 0.5, confirming that proximity is its least effective feature.

5. CONCLUSION

This work investigates the vulnerabilities introduced by blackhole attacks in IoT-EHT networks and presents a hybrid intrusion detection framework (DML-IDS) built upon a diverse set of deep learning and machine learning models. The corresponding datasets are generated across three key IoT experimental features, including proximity, sensor density, and payload size, to reflect varied IoT conditions under both normal and attack scenarios. Feature-wise analysis of the results confirms that detection outcomes are strongly influenced by characteristics of the experimental features. The results show that sensor density and payload size yield better detection performance compared to BS proximity. This is because density and payload size directly amplify the observable effects of blackhole attacks, producing clearer anomalies for classification. Variations in node density directly affect the volume and diversity of traffic patterns. Blackhole attacks in dense networks cause more pronounced anomalies, such as sudden packet drops, which are easier for ML and DL models to learn. Similarly, larger payloads amplify the observable consequences of packet drops. When blackhole nodes discard large packets, the impact on throughput and packet delivery ratio is more severe, producing stronger patterns to classify. In contrast, proximity primarily influences routing paths and topology rather than the attack signature. Models trained on proximity alone tend to show weaker separation between benign and malicious behavior, leading to reduced contributions to detection outcomes. Model-wise analysis also reflects these dynamics and further reveals distinct strengths across individual models of the DML-IDS framework. Machine learning models such as LR, RF, DT, and SVM consistently demonstrate reliable performance due to their effective partitioning of feature patterns. In contrast, deep learning models, though also reliable, depend more heavily on feature representation, which causes their performance to fluctuate across different features. Overall, these findings underscore the importance of aligning model architecture with feature dynamics and suggest that hybrid approaches can enhance resilience and adaptability for real-time intrusion detection in heterogeneous IoT-EHT environments.

ACKNOWLEDGEMENT AND FUNDING

The authors receive no financial support for the research, authorship, and publication of this article.

DECLARATION OF CONFLICTING INTERESTS

The authors declare no potential conflicts of interest with respect to the research and publication of this article.

REFERENCES

[1] N. Dawar, K. N. Nguyen, A. Sehgal, Y. Zhu, B. L. Ng and J. Choi, Enhancing wi fi 7: Traffic flow intelligence and multi link operation for optimal efficiency, *IEEE Access*, 13, 2025, 63298-63309.

[2] V. Frascolla, D. Cavalcanti and R. Shah, Wi-Fi evolution: The path towards wi-fi 7 and its impact on IIoT, *IEEE Journal of Mobile Multimedia*, 19(1), 2023, 1-14.

[3] R. K. Dhanaraj, L. Krishnasamy, O. Geman and D. R. Izdrui, Black hole and sink hole attack detection in wireless body area networks, *Computers, Materials and Continua*, 68(2), 2021, 1949-1965.

[4] H. Tyagi, R. Kumar and S. K. Pandey, Trust evaluation and prediction framework using time-series analysis and deep learning approach during blackhole attack in internet of things (IoT), *Arabian Journal for Science and Engineering*, 50, 2025, 19597-19614.

[5] G. Farahani, Black hole attack detection using k-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks, *Security and Communication Networks*, 2021, 8814141.

[6] M. A. Khan, R. N. B. Rais, O. Khalid and S. Ahmad, Trust-based optimized reporting for detection and prevention of black hole attacks in low-power and lossy green IoT networks, *Sensors*, 24, 2024, 2-22.

[7] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. Humayun, A. O. Ibrahim and A. Abdelmaboud, A trust-based model for secure routing against RPL attacks in internet of things, *Sensors*, 22(18), 2022, 1-20.

[8] R. K. Dhanaraj, S. K. H. Islam and V. Rajasekar, A cryptographic paradigm to detect and mitigate blackhole attack in VANET environments, *Wireless Networks*, 28, 2022, 3128–3142.

[9] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan and A. Aldegheishem, Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles, *IEEE Access*, 8, 2020, 199618-199628.

[10] N. Yang, K. Chen and M. Wang, SmartDetour: Defending blackhole and content poisoning attacks in IoT NDN networks, *IEEE Internet of Things Journal*, 8(15), 2021, 12119-12136.

[11] D. K. Sharma, S. K. Dhurandher, S. Kumaram, K. D. Gupta and P. K. Sharma, Mitigation of black hole attacks in 6LoWPAN RPL-based wireless sensor network for cyber physical systems, *Computer Communications*, 189, 2022, 182-192.
[12] K. Sanders and S. S. Yau, An effective approach to protecting low-power and lossy IoT networks against blackhole attacks, *IEEE International Conferences on Internet of Things (iThings), GreenCom, CPSCom, SmartData and Congress*, Melbourne, Australia, 2021, 65-72.
[13] I. A. Reshi, S. Sholla and Z. A. Najar, Safeguarding IoT networks: Mitigating black hole attacks with an innovative defense algorithm, *Journal of Engineering Research*, 12, 2024, 133-139.
[14] T. A. S. Srinivas and S. S. Manivannan, Black hole and selective forwarding attack detection and prevention in IoT in health care sector: Hybrid meta-heuristic-based shortest path routing, *Journal of Ambient Intelligence and Smart Environments*, 13, 2021, 133-156.
[15] M. Yazdanypoo, S. Cirillo and G. Solimando, Developing a hybrid detection approach to mitigating black hole and gray hole attacks in mobile ad hoc networks, *Applied Sciences*, 14(17), 2024, 1-13.
[16] P. R. Kavita, S. Verma and G. N. Nguyen, Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network, *IEEE Access*, 8, 2020, 121755-121764.
[17] M. Shameer and L. Gnanaprasanambikai, K-means clustering-based trust (KmeansT) evaluation mechanism for detecting blackhole attacks in IoT environment, *International Journal of Computing and Digital Systems*, 16, 2024, 1-13.
[18] J. L. Webber, A. Arafa, A. Mehbodniya, S. Karupusamy, B. Shah, A. K. Dahiya and P. Kanani, An efficient intrusion detection framework for mitigating blackhole and sinkhole attacks in healthcare wireless sensor networks, *Computers and Electrical Engineering*, 111, 2023, 1-12.
[19] R. K. Dhanaraj, R. H. Jhaveri, L. Krishnasamy, G. Srivastava and P. K. R. Maddikunta, Black-hole attack mitigation in medical sensor networks using the enhanced gravitational search algorithm, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 29, 2021, 297-315.
[20] N. Panda and M. Supriya, Blackhole attack prediction in wireless sensor networks using support vector machine, *Advances in Signal Processing, Embedded Systems and IoT*, 992, 2023, 321-331.
[21] The ns-3 Network Simulator. Available: https://www.nsnam.org. (Accessed: Dec. 23, 2025).
[22] Wireshark, Available: https://www.wireshark.org. (Accessed: Dec. 23, 2025).
[23] CICFlowMeter, Available: https://github.com/ahlashkari/CICFlowMeter. (Accessed: Dec. 23, 2025).
[24] Argus, Available: https://openargus.org/using-argus. (Accessed: Dec. 23, 2025).
[25] G. Sharma, J. Grover and A. Verma, Performance evaluation of mobile RPL-based IoT networks under version number attack, *Computer Communications*, 197, 2023, 12-22.
[26] K. J. Dong, A comprehensive analysis of routing vulnerabilities and defense strategies in IoT networks, *Cryptography and Security*, 2024, 1-12.