IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 24 July 2024, accepted 7 August 2024, date of publication 12 August 2024, date of current version 26 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3442529

RESEARCH ARTICLE

Hybrid Intrusion Detection System for RPL IoT Networks Using Machine Learning and Deep Learning

USAMA SHAHID[1], MUHAMMAD ZUNNURAIN HUSSAIN[2], MUHAMMAD ZULKIFL HASAN[3], ALI HAIDER[4], JIBRAN ALI[5], AND JAWAD ALTAF[6]

[1]School of Business, Computing and Social Sciences, University of Gloucestershire, GL50 2RH Cheltenham, U.K.
[2]Department of Computer Science, Bahria University Lahore Campus, Lahore 54600, Pakistan
[3]Faculty of Information Technology, University of Central Punjab, Lahore 54000, Pakistan
[4]Senior Cyber Security Consultant, Dell SecureWorks, Providence, RI 02903, USA
[5]Resident Engineer at Premier Systems, Karachi 74000, Pakistan
[6]National College of Ireland (NCI), Dublin 1, D01 K6W2 Ireland

Corresponding author: Muhammad Zunnurain Hussain (zunnurain.bulc@bahria.edu.pk)

ABSTRACT The Internet of Things (IoT) is transforming everyday objects. However, its devices' limited memory, processing power, and network capabilities make them susceptible to security breaches. The Routing Protocol for Low-Power and Lossy Networks (RPL) is a promising IoT protocol but faces significant security challenges. Existing research often focuses on individual attacks, utilizing various mitigation strategies, including machine learning and deep learning for detection. This paper proposes an Intrusion Detection System (IDS) using the ROUT-4-2023 dataset, which encompasses Black Hole, Flooding, DODAG Version Number, and Decreased Rank attacks. The study utilizes statistical information graphs to investigate network traffic features encompassing all four attacks. Additionally, it experiments with various machine learning models and deep learning architectures for comparative analysis, focusing on confusion matrix outcomes and computational efficiency. Results indicate that the Random Forest classifier achieves 99% accuracy, while Transformers reach 97% F1-Score with a training time of only 16.8 minutes over five epochs.

INDEX TERMS Intrusion detection system, data science, machine learning, deep learning, security, RPL, routing protocols, IoT, black hole attack, decreased rank attack, DODAG VNA, flooding attack.

I. INTRODUCTION

The advent of the Internet of Things (IoT) has facilitated the integration of diverse, innovative applications across numerous sectors, including industry, healthcare, and agriculture, marking a paradigm shift in technology [1]. The security of connected devices is paramount in the swiftly evolving IoT landscape. The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) stands out as a crucial routing protocol tailor-made to meet the unique requirements of IoT networks [2]. However, as IoT systems' deployment expands, so does the spectrum of threats targeting these networks, necessitating robust defensive measures [3].

Researchers utilize datasets comprising attack scenarios to meet the critical demand for protection solutions. One such pivotal resource is the ROUT-4-2023 dataset, which encompasses data on four distinct routing attacks targeting the RPL protocol: Blackhole, Flooding, DODAG Version Number, and Decreased Rank Attacks [4]. Originating from simulations conducted in the Cooja network simulator, this dataset provides a comprehensive basis for developing and evaluating Intrusion Detection Systems (IDS) tailored to RPL-based IoT networks.

Efforts to enhance IoT security have been undertaken using machine learning and deep learning [5], [6], [7]. However, the current IDS cannot mark and counter new threat patterns featured in the ROUT-4-2023 attacks. The dataset appears promising for researchers seeking to develop advanced IDS

The associate editor coordinating the review of this manuscript and approving it for publication was Hang Shen.

by applying mitigation strategies, algorithms, machine learning and deep learning techniques.

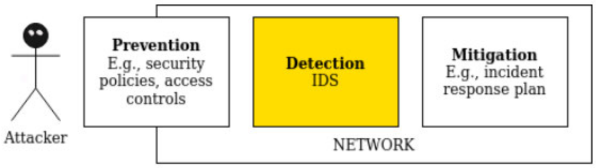

Attacker
Prevention
E.g., security policies, access controls
Detection
IDS
Mitigation
E.g., incident response plan
NETWORK

FIGURE 1. Network defense [4].

Incorporating a variety of attack scenarios into a single dataset like ROUT-4-2023 offers multiple advantages for the security of IoT networks. It facilitates exploring inter-attack relationships, devising comprehensive defensive strategies, and simplifies analytical procedures for enhanced efficiency. Furthermore, it enables in-depth evaluation of vulnerabilities and defensive mechanisms. Fundamentally, this approach augments understanding of the intricacies within RPL-based IoT networks, potentially leading to more robust security protocols.

This study presents an exploratory data analysis of the ROUT-4-2023 dataset, outlining its characteristics, organization, and significance in advancing IoT security research using statistical information visualization. Furthermore, the study extends to implementing various machine learning models and deep learning architectures on an integrated dataset encompassing all four types of attacks. This approach aims to develop an IDS and perform a comparative analysis of these models.

The paper is organized as follows: Section II reviews the literature on the four RPL-based attack types under consideration. Section III discusses the analytical approach adopted within this study. Section IV presents the results, while Section V discusses these findings. Finally, Section VI concludes the paper.

II. LITERATURE REVIEW

A. BLACK HOLE ATTACK

A Black Hole attack occurs when a network's malicious node discards all packets meant to be forwarded to the sink node. This attack comprises two primary stages. First, the malicious node attracts its neighbours to select it as the parent by advertising a falsified low rank. This action compromises the network topology by disrupting optimal path selection, creating a suboptimal topology. In the second stage, the malicious node drops all packets from other nodes.

IoT networks are notably compromised by the Black Hole attack, which disrupts standard packet routing, leading to packet loss, network congestion, and interruption of service. Due to adaptability and scalability constraints, extant IDS often struggle with identifying and neutralizing Black Hole attacks.

Figure 2(a) illustrates a standard operational state within an IoT network where 15 nodes have successfully formed a Directed Acyclic Graph (DODAG), functioning as intended. Conversely, Figure 2(b) presents a scenario where the network is under the duress of a Black Hole attack [8]. In this instance, the node with identifier 9 disrupted the RPL routing protocol, positioning itself as a preferential parent, thus misleading neighbouring nodes to route their data through it. This act effectively creates a void where packets are absorbed by the malicious node, leading to data loss within the network.

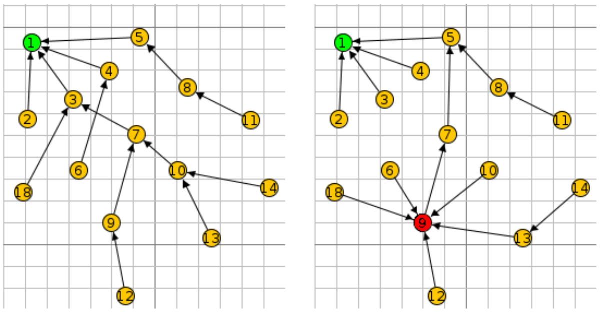


FIGURE 2. Black hole attack (a) Normal behaviour (b) Active behaviour [4].

Measures such as secure routing protocols, trust-based frameworks, and hierarchical models are implemented to mitigate the impact of these attacks. Nonetheless, these solutions frequently require enhancement to navigate the limitations of IoT devices and the fundamental challenges involved.

One of the research studies employed NS2 and Simulink simulations to develop a Black Hole defence algorithm, demonstrating that implementing such a mitigation strategy can markedly enhance network performance. The results show a Packet Delivery Ratio (PDR) of 98.21%, which closely approximates the performance of unaffected networks [9]. However, the study does not consider the potential impact of differing network topologies and traffic patterns on the algorithm's effectiveness, which may constrain its practical applicability.

Conversely, Adam's work focused on developing novel attack variants inspired by the Black Hole attack and evaluating these variants on an IDS trained on conventional Black Hole attacks. Data for these simulations were gathered using the Cooja simulator and subsequently processed to train a Random Forest Classifier. The findings suggest that machine learning can effectively identify such attacks [8]. Nevertheless, the absence of real-world validation raises questions about the practical applicability of these findings.

Another study proposed a deep learning-based framework for detecting routing attacks in unsecured RPL networks. This framework analyses and processes network traffic, extracts features, and defines target-based intrusion thresholds, leading to the detection of routing attacks. Extensive simulation results validate the model's efficiency, demonstrating reliable detection accuracy of up to 98.70% [10]. Although the proposed model demonstrates promising results, its practical deployment in dynamic network environments with varying traffic patterns remains to be validated.

B. FLOODING VERSION NUMBER ATTACK

Flooding Version Number Attacks (VNAs) exploit vulnerabilities within the RPL version numbering system by overwhelming the network with artificially incremented version numbers. This tactic exhausts network resources and significantly degrades performance.

A study examines the negative impact of VNAs on crucial network parameters, including control overhead, energy consumption, latency, and Packet Delivery Ratio (PDR), through simulations [11]. The results indicate an 182% increase in energy consumption, underscoring the urgent necessity for robust security measures to mitigate VNAs and safeguard RPL-based IoT networks against these threats.

There are four types of attacks that exploit the RPL design to launch assaults from outside an IoT network: DIS flooding, Hello flooding, Clone ID, and DODAG Inconsistency attacks [12], [13], [14]. However, a study suggests that all these four attacks directly or indirectly use the DIS flooding attack, which is notably common and impactful when executed from outside targeted IoT networks [15].

It undermines network nodes by frequently sending DIS (DODAG Information Solicitation) messages, which increases control packet overhead, depletes energy resources, and disrupts routing processes. This attack jeopardizes the stability and performance of the network, irrespective of whether the DIS messages are transmitted via unicast or multicast.

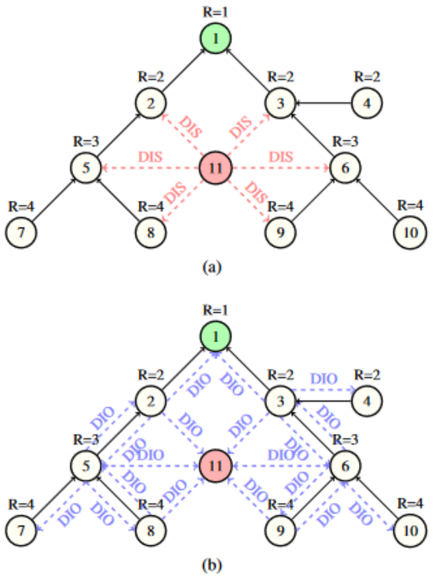


FIGURE 3. DIS flood attack [8].

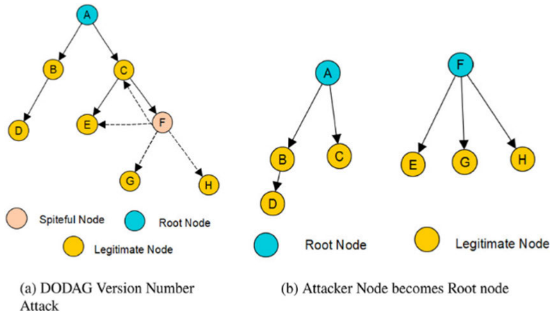
Figure 3 exemplifies the impact of a DIS flood attack on an RPL network. In Figure 3(a), the assailant, node 11, propagates multicast DIS messages within its vicinity. In Figure 3(b), the attack escalates network overhead and power consumption; targeted nodes, including nodes 2, 3, 5, 6, 8, and 9, receive the DIS messages, causing them to reset their trickle timers and propagate multicast DIO (DODAG Information Object) messages.

Although several mitigation approaches are documented [16], [17], [18], most assessments utilize either grid or random topology. Nevertheless, one study examines how network topology influences the efficacy of RPL attacks, specifically considering hop distance and the number of attackers in DIS flooding scenarios to facilitate the development of effective attack mitigation strategies [15]. However, this study neglects to consider the potential influence of dynamic network conditions and real-time adaptive responses on the effectiveness of these mitigation strategies.

C. DOGAG VERSION NUMBER ATTACK

A DODAG version number attack exploits fraudulent version numbers to trigger unnecessary rebuilds in RPL's loop-free topology maintenance. Despite RPL's efficiency and adaptability, it is vulnerable to security breaches due to its lack of robust security features [19]. This undermines network integrity by increasing overhead, depleting energy resources, causing channel availability issues, and inducing routing loops.

A study analyses the DODAG versioning mechanism within the RPL protocol, focusing on the impact of potential attacks on network overhead, delivery ratio, end-to-end latency, rank inconsistencies, and loop formation. The study highlights the vulnerabilities of the DODAG versioning system and the threats posed by its malicious exploitation, emphasizing the lack of stringent security and key management in RPL frameworks [20]. Notably, this research also asserts the risks that may prevail should the mentioned vulnerabilities be exploited by adversarial actors.



(a) DODAG Version Number Attack

(b) Attacker Node becomes Root node

FIGURE 4. (a) DODAG VNA (b) Attacker node becomes root node [10].

Figure 4 delineates the repercussions of a DODAG Version Number Attack (VNA) on a network comprising eight nodes. In Figure 4 (a), the network dynamics pre-attack is depicted, with one malicious node (F), the DODAG root (A), and other legitimate nodes. Initially, node F integrates into the DODAG legitimately before manifesting as a malicious entity. It then alters the version number within the DIO messages (indicated by dotted arrows) and disseminates them to adjacent nodes (C, E, H, and G). While node C rejects this falsified message, nodes E, H, and G accept it, leading to a revision in their version numbers and, consequently, the formation of a new DODAG, as illustrated in Figure 4 (b). In this altered structure, node F assumes the position of the root node, thereby illustrating the profound impact of the DODAG Version Number Attack [10].

1) DODAG INCONSISTENCY ATTACK

Similar to the study of RPL security environments, the wireless sensor networks (WSNs) community has examined security measures extensively. Researchers have explored trust mechanisms to enhance the security of WSNs and suggest extending these methods to RPL networks [21], [22]. However, this approach may prove ineffective if malicious nodes execute DODAG inconsistency attacks, as they can easily remain undetected due to their transmission of unaltered control messages.

A proposed framework by researchers categorizes a wide range of attacks according to the confidentiality, integrity, and availability (CIA) model and incorporates general countermeasures to address each attack [23]. Conversely, another study introduces a mitigation strategy that enables nodes to adapt to DODAG inconsistency dynamic attacks [24]. Nevertheless, this adaptive approach necessitates optimal hyper-parameter configurations for effectiveness.

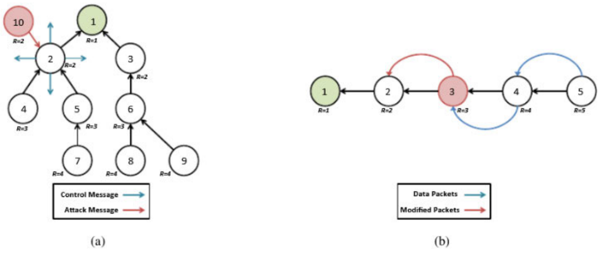


FIGURE 5. (a) DODAG inconsistency attack scenarios [11].

Figure 5 portrays scenarios of a DODAG inconsistency attack. In Figure 5(a), the malicious node ten dispatches packets with the 'R' flag to node 2. As a result, when node 3, acting as the attacker, receives packets from its descendants, it modifies them by adding the 'R' flag before forwarding. Nodes that receive packets with the 'R' flag discard them, which triggers a reset of the trickle timer that governs control message transmission, leading to an increase in network overhead.

D. DECREASE RANK ATTACK

The Decreased Rank Attack targets the RPL's rank mechanism, altering nodes' understanding of their position within the network hierarchy. It can be combined with other methods to damage the network further. For instance, selective forwarding or Blackhole attacks become more effective when the attacker positions itself strategically to receive all traffic from neighbouring nodes [25], [26].

A study comprehensively analyses the RPL protocol's vulnerability to Decreased Rank attacks, utilizing the Random Direction Mobility Model (RDM) for mobile scenarios within the Cooja simulator [27]. It considers both static and mobile network contexts. The findings reveal the disruptive impact of this attack on the routing hierarchy, leading to decreased packet delivery ratio (PDR) and throughput and increased Average End-to-End Delay (AE2ED), expected transmission count (ETX), and Average Power Consumption (APC). This underscores the evolving security requirements of IoT networks and the necessity for developing measures to ensure security and mitigate the risks associated with RPL-based IoT networks.

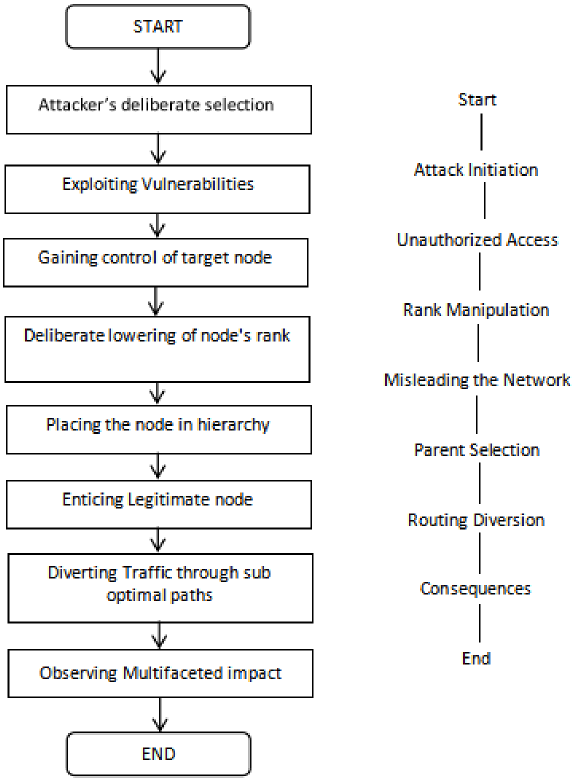

START
Attacker's deliberate selection
Exploiting Vulnerabilities
Gaining control of target node
Deliberate lowering of node's rank
Placing the node in hierarchy
Enticing Legitimate node
Diverting Traffic through sub optimal paths
Observing Multifaceted impact
END
Start
Attack Initiation
Unauthorized Access
Rank Manipulation
Misleading the Network
Parent Selection
Routing Diversion
Consequences
End

FIGURE 6. Decrease rank attack flowchart [12].

Figure 6 depicts the sequence of events in a Decreased Rank attack on an RPL-based network. Such an attack typically follows a pattern starting with the attacker's deliberate selection and exploitation of vulnerabilities to gain unauthorized access to the network. The attacker then manipulates the network by deceptively lowering a node's rank, misleading the network's routing processes, and ultimately diverting traffic, which could result in suboptimal routing paths and a multifaceted impact on network performance and integrity.

A further study critiques the current security features in RPL, including optional cryptography modes, deeming them inadequate due to resource constraints and their potential to impact performance negatively. It further develops a Secure Objective Function (Sec-OF) to address Decreased Rank Attacks, aiming to enhance the stability of RPL-based IoT networks [28]. The proposed approach employs a secure objective function that dynamically adjusts rank values to strengthen the resilience of RPL-based IoT networks against malicious manipulations. Thus, this proactive defence significantly contributes to IoT network protection, necessitating further investigation.

III. METHODOLOGY

The paper adhered to data science practices, starting with data collection and pre-processing. This was followed by exploring the dataset to identify and understand patterns within its features. This approach facilitated effective modelling using machine learning and deep learning to identify and compare the most influential computational methods. The research was conducted using the Python programming language due to the availability of open-source tools. The system used was the MacBook Air M2, equipped with 8GB of RAM.

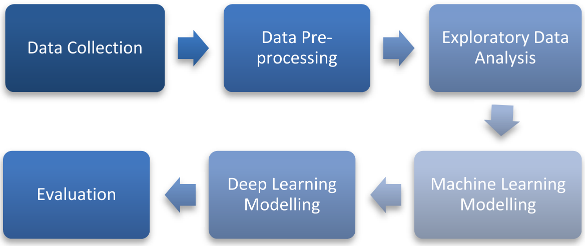


FIGURE 7. **Methodology diagram.**

A. DATA COLLECTION

The study employed the Rout-4-2023 dataset, developed by Murat and Mehmet, for analyzing RPL-based routing attacks on IoT systems [4]. This dataset was published under the IEEE Data Port. It simulates four distinct routing attacks on IoT devices using Cooja, which are provided below:

1) Blackhole Attack
2) DODAG Version Number Attack
3) Flooding Attack
4) Decreased Rank Attack

The dataset was chosen due to its balance and representativeness of real-world attack scenarios, enabling models to identify and predict various types of attacks accurately. It comprised ".csv" files detailing four different routing attacks.

B. DATA PRE-PROCESSING

The four datasets were integrated to create a single model for predicting various types of attacks. The dataset comprises numerical features with differing value ranges, potentially presenting challenges for model interpretation and understanding feature-attack-type relationships. All features were scaled using StandardScaler from sklearn to address this, ensuring uniform value ranges. The string values representing attack types were also converted to numerical values using *LabelEncoder* from *sklearn*.

The dataset was then divided into training and testing sets in a stratified manner, with twenty per cent allocated to testing. This allocation aimed to preserve the class distribution in both sets, which is crucial in classification tasks to ensure the development of reliable and generalizable models.

C. EXPLORATORY DATA ANALYSIS

The exploratory analysis utilized various visualizations with the help of open-source tools in Python to summarise and disseminate the primary characteristics of integrated dataset features from different attack types. The libraries employed for visualizations were *Seaborn* and *Matplotlib* because of their significant GitHub stars, community support, and consistent programming interface for various visualization analyses. The following text discusses the visualizations being conducted.

1) DATA DISTRIBUTION ANALYSIS

A count plot was employed to compare the frequencies of various attack records with standard records.

2) FEATURE FREQUENCY ANALYSIS

The research employed histograms to examine the frequency distribution of all dataset features, aiming to identify patterns or potential skewness.

3) OUTLIER AND QUARTILE ANALYSIS

A box plot, also known as a whisker plot, was utilized to depict the distribution, outliers, and variability of all features within the dataset.

4) CORRELATIONAL ANALYSIS

Correlation analysis was employed to uncover relationships between features, ensuring significant feature selection for modelling and understanding network characteristics and dependencies between features.

5) PACKET LENGTH ANALYSIS

The research hypothesized that packet length might vary with different types of attacks. Consequently, a violin plot was employed to examine the distribution of packet lengths during attack scenarios compared to non-attack scenarios.

6) NETWORK TRAFFIC DATA ANALYSIS CONCERNING ATTACK SCENARIOS

Given the dataset's large size, a stratified sample of five thousand data points, encompassing all attack types, was utilized to create the pair plot. Selected features were included to aid in discerning trends and patterns among multiple variables, thereby enhancing research comprehension. Feature selection was based on correlation analysis.

7) SCATTER ANALYSIS OF TWO SELECTED FEATURES

A scatter plot was employed on selected features based on correlation analysis and various hypotheses to disseminate trends and patterns across different attack types.

D. MACHINE LEARNING MODELLING

Predicting attack types falls under supervised learning, specifically classification. Numerous classification algorithms exist, each possessing distinct advantages and disadvantages. Selecting an appropriate algorithm relies on computational efficiency, interpretability, and the dataset's characteristics. This research predominantly employs the Decision Tree (DT) [29], Random Forests (RF) [30], Stochastic Gradient Descent (SGD) [31], and Gaussian Naïve Bayes (GNB) [32]. These algorithms were selected for their computational efficiency with large datasets and diverse mathematical learning approaches. This variety aids in identifying the most effective algorithm for the dataset under consideration.

This research performed machine learning modelling through the *Sklearn* library, chosen for its consistent interface across various algorithms. Its popularity is evidenced by over 58,000 GitHub stars and 778,000 users, as reported by GitHub, alongside substantial community support.

E. DEEP LEARNING MODELLING

The architecture of a neural network, which delineates its structure and the types of layers it comprises, profoundly influences its performance and appropriateness for tasks. Selecting an appropriate neural network architecture depends on several factors, including computational efficiency, resource consumption, and architecture's adaptability. This research utilizes four distinct architectures: Feed-Forward Neural Network (FFNN) [33], Convolutional Neural Network (CNN) [34], Long Short-Term Memory Networks (LSTM) [35], and Transformers [36]. The rationale for selecting diverse neural network architectures was to determine the dataset's most influential and optimal design.

This research performed deep learning modelling through the *Tensorflow* and *Keras* libraries, chosen for robust functionality and widespread use in a community. The neural networks were configured for training by specifying the *Adam* optimizer, *sparse_categorical_crossentropy* as the loss function, and tracking *accuracy* as a performance metric. This configuration was selected to manage multi-class classification tasks efficiently. The configuration of each neural network in this research is illustrated below.

1) FEED-FORWARD NEURAL NETWORK

Figure 7 illustrates an FFNN incorporating dropout layers to mitigate overfitting and enhance generalization in a multi-class classification task.

2) CONVOLUTIONAL NEURAL NETWORK

Figure 8 illustrates a CNN designed to extract features from sequential data and classify them into multiple categories. This is achieved through convolutional, pooling, and dense layers.

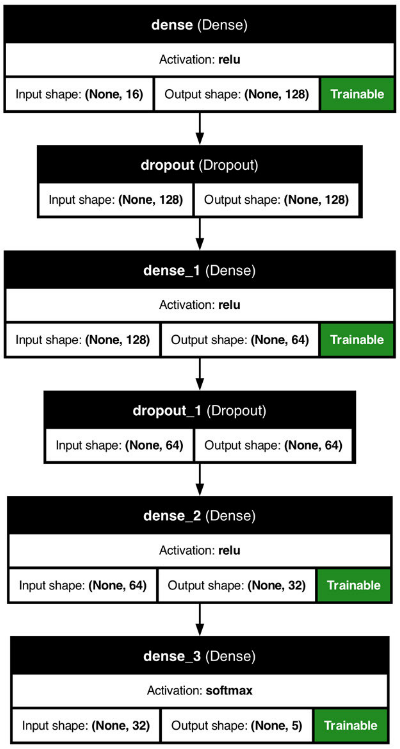


FIGURE 8. Feed-forward neural network architecture.

3) LONG SHORT-TERM NETWORK

Figure 9 depicts an LSTM model designed to capture sequential data's temporal dependencies and classify them into multiple categories. It leverages LSTM units, dropout for regularization, and dense layers for classification.

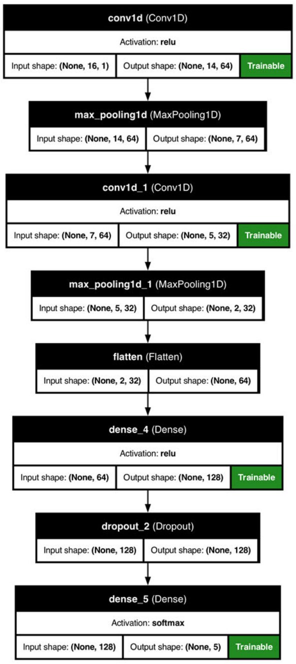

conv1d (Conv1D)
Activation: relu
Input shape: (None, 16, 1)
Output shape: (None, 14, 64)
Trainable
max_pooling1d (MaxPooling1D)
Input shape: (None, 14, 64)
Output shape: (None, 7, 64)
conv1d_1 (Conv1D)
Activation: relu
Input shape: (None, 7, 64)
Output shape: (None, 5, 32)
Trainable
max_pooling1d_1 (MaxPooling1D)
Input shape: (None, 5, 32)
Output shape: (None, 2, 32)
flatten (Flatten)
Input shape: (None, 2, 32)
Output shape: (None, 64)
dense_4 (Dense)
Activation: relu
Input shape: (None, 64)
Output shape: (None, 128)
Trainable
dropout_2 (Dropout)
Input shape: (None, 128)
Output shape: (None, 128)
dense_5 (Dense)
Activation: softmax
Input shape: (None, 128)
Output shape: (None, 5)
Trainable

FIGURE 9. Convolutional neural network architecture.

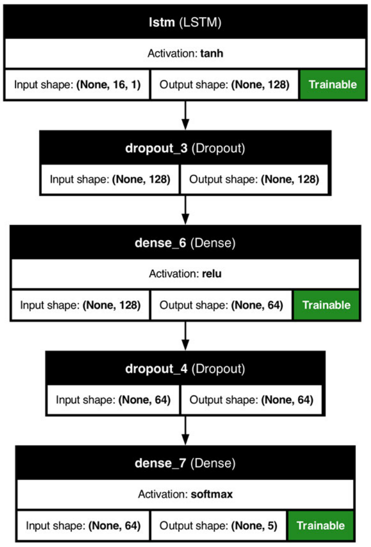


FIGURE 10. Short-term neural network architecture.

4) TRANSFORMERS

Figure 10 depicts a Transformer model employing a Multi-Head Attention mechanism with two heads and two key dimensions. This is followed by normalization, dropout, and dense layers for classifying sequential data.

F. EVALUATION

A confusion matrix was used to assess classification models. As discussed below, several significant performance metrics were derived from the confusion matrix to evaluate classification models' effectiveness.

1) ACCURACY

Accuracy was used to determine the ratio of correctly predicted instances to the total number of instances. Higher accuracy signifies a model that generates more correct predictions overall.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

2) PRECISION

Precision was used to determine the ratio of correctly predicted positive instances to total predicted positives. A higher precision indicates that the model correctly identifies positive instances while making fewer prediction errors.

$$\text{Precision} = \frac{TP}{TP + FP}$$

3) RECALL

Recall was used to determine the ratio of correctly predicted positive instances to all instances within the positive class. A higher recall indicates that the model effectively identifies most actual positive instances, although it may occasionally classify negatives as positives.

$$\text{Recall} = \frac{TP}{TP + FN}$$

TABLE 1. Routing attack dataset sizes.

Dataset Name	No. of rows
Black Hole Attack	404134
DODAG Version Number Attack	468060
Flooding Attack	398782
Decreased Rank Attack	368999

TABLE 2. Features of the rout-4-2023 dataset.

Name	Description
TIME	Simulation time
SOURCE	Source Node IP
DESTINATION	Destination Node IP
LENGTH	Packet Length
INFO	Packet Information
TR	Transmission Rate (per 1000_ms)
RR	Reception Rate (per 1000 ms)
TAT	Transmission Average Time
RAT	Reception Average Time
TPC	Transmitted Packet Count (per second)
RPC	Received Packet Count (per second)
TTT	Total Transmission Time
TRT	Total Reception Time
DAO	DAO Packet Count
DIS	DIS Packet Count
DIO	DIO Packet Count
CATEGORY	Attack Type or Normal
LABEL	Normal/Malicious Label

4) F1-SCORE

F1-Score was used to determine the harmonic mean of precision and recall, balancing these two metrics. A higher F1-Score indicates that the model effectively balances precision and recall, resulting in accurate and comprehensive predictions.

$$F1 - \text{score} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

IV. RESULTS

The analytical methodology results are presented below and discussed in Section V.

A. DATA COLLECTION RESULTS

The dataset contained no empty or duplicate values; all features were numerical.

TABLE 3. Machine learning comparison metric.

Classifier	Accuracy	Attack	Precision	Recall	F1 Score	Support
RF	0.99	Blackhole	1	1	1	26856
		Dodag	1	1	1	34049
		Flooding	1	1	1	27115
		Normal	1	1	1	211997
		Rank	1	1	1	27978
DT	0.99	Blackhole	1	1	1	26856
		Dodag	1	1	1	34049
		Flooding	1	1	1	27115
		Normal	1	1	1	211997
		Rank	1	1	1	27978
SGD	0.75	Blackhole	0.43	0.04	0.07	26856
		Dodag	0.63	0.72	0.67	34049
		Flooding	0.85	0.97	0.91	27115
		Normal	0.76	0.91	0.83	211997
		Rank	0.52	0	0	27978
GNB	0.52	Blackhole	0.26	0.17	0.2	26856
		Dodag	0.36	1	0.53	34049
		Flooding	0.68	1	0.81	27115
		Normal	0.76	0.45	0.56	211997
		Rank	0.19	0.36	0.25	27978

B. EDA RESULTS

This section presents the results of the exploratory data analysis for steps undertaken as outlined in Section III.

1) DATA DISTRIBUTION ANALYSIS

Fig. 12.

2) FEATURE FREQUENCY ANALYSIS

Fig. 13.

3) OUTLIER AND QUARTILE ANALYSIS

Figs. 14–17.

4) RELATIONSHIP ANALYSIS

Fig. 18.

5) PACKET LENGTH ANALYSIS

Fig. 19.

6) NETWORK TRAFFIC DATA ANALYSIS CONCERNING ATTACK SCENARIOS

Fig. 20 and 21.

7) SCATTER ANALYSIS OF TWO SELECTED FEATURES

Fig. 22–25.

C. MACHINE LEARNING RESULTS

Fig. 26 and table 3.

TABLE 4. Deep learning models training time.

Model	Epochs	Avg. Time Per Epoch (Sec)	Total Time (Mins)
FFNN	50	15.78	14.93
CNN	50	86.74	63.68
LSTM	25	223.8	93.25
Transformers	5	197.8	16.48

TABLE 5. Deep learning comparison metric.

Classifier	Accuracy	Category	Precision	Recall	F1 Score	Support
FFNN	0.87	Blackhole	0.68	0.21	0.32	26856
		Dodag	0.99	0.96	0.97	34049
		Flooding	1	0.99	0.99	27115
		Normal	0.84	0.99	0.91	211997
		Rank	0.99	0.39	0.56	27978
CNN	0.92	Blackhole	0.72	0.54	0.62	26856
		Dodag	0.99	0.99	0.99	34049
		Flooding	1	1	1	27115
		Normal	0.91	0.97	0.94	211997
		Rank	0.94	0.69	0.8	27978
LSTM	0.98	Blackhole	0.92	0.89	0.9	26856
		Dodag	1	1	1	34049
		Flooding	1	1	1	27115
		Normal	0.98	0.98	0.98	211997
		Rank	0.95	0.94	0.94	27978
Transformer	0.98	Blackhole	0.94	0.9	0.92	26856
		Dodag	1	1	1	34049
		Flooding	1	1	1	27115
		Normal	0.98	0.99	0.99	211997
		Rank	0.94	0.96	0.95	27978

D. DEEP LEARNING RESULTS

Tables 4 and 5 and Fig. 27.

V. DISCUSSION

A. ANALYSIS OF DATASET AND FEATURE VARIABILITY

Table 2 indicates minor differences in dataset sizes for each attack, while Table 3 outlines the features and their interpretations. Despite these variations, Figure 12 demonstrates that when integrated, regular records are nearly four times more frequent than attack records, which remain relatively consistent in number. This imbalance suggests a typical real-world scenario where benign traffic dominates, yet the presence of attacks, though less frequent, poses significant security risks. This distribution underscores the importance of focusing on anomaly detection systems that can accurately identify infrequent but potentially harmful activities in IoT networks.

Figure 13 illustrates varied distributions of dataset features, highlighting consistent data collection over time and identifying distinct transmission, reception, and attack-specific

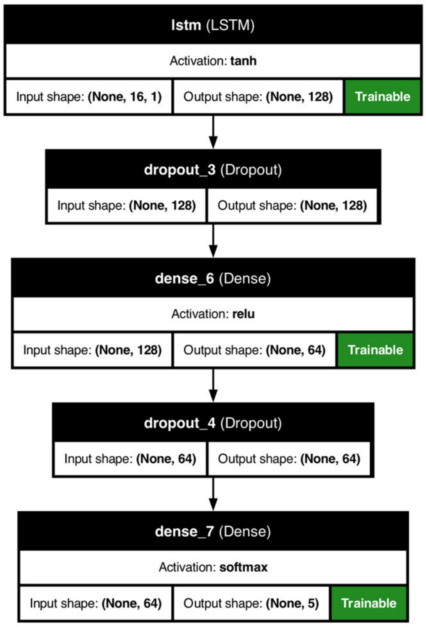


FIGURE 11. Transformers architecture.

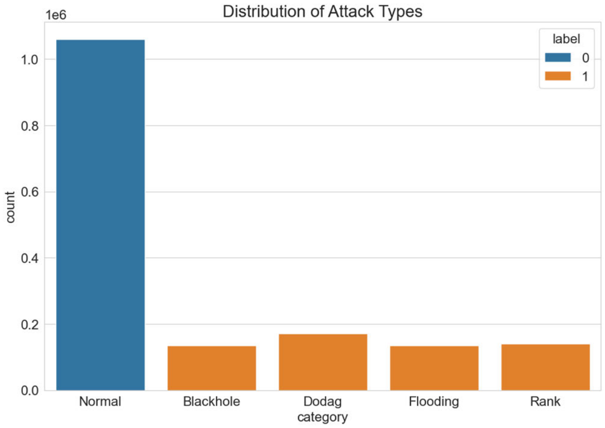


FIGURE 12. Distribution of network records by attack type.

characteristics. These insights emphasize the necessity for targeted security measures based on statistical information, reinforcing the need for continuous monitoring and feature-based anomaly detection to enhance the robustness of IoT network security.

B. FEATURE ANALYSIS AND ANOMALY DETECTION

The boxplots in Figures 14-17 reveal key features' variability and central tendency. 'Time' exhibits numerous outliers, indicating sporadic data spikes, while 'source' and 'destination' distributions suggest concentrated communication activities among specific nodes. Transmission and reception rate features show relatively consistent interquartile ranges but include some outliers, pointing to occasional anomalies in network traffic. Attack-specific features such as 'dis' also present outliers, reflecting irregularities associated with attack instances. These observations are crucial for developing robust intrusion detection systems by focusing on anomaly detection and variability analysis to enhance IoT network security.

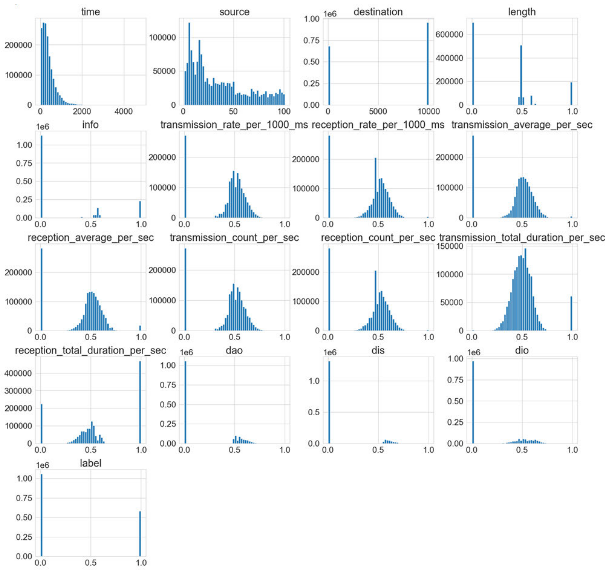


FIGURE 13. Frequency distribution of network features.

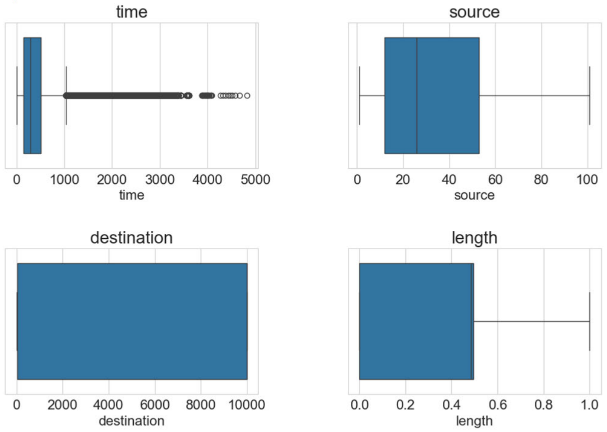


FIGURE 14. (A) Illustration of outliers and quartiles in network features.

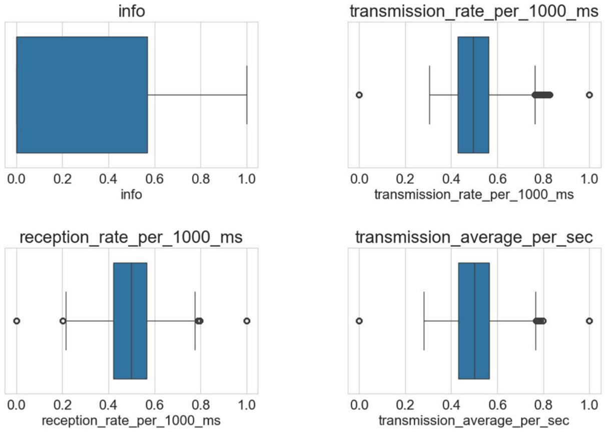


FIGURE 15. (B) Illustration of outliers and quartiles in network features.

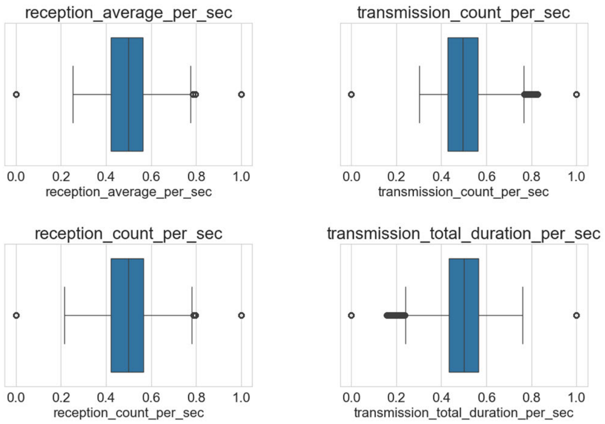


FIGURE 16. (C) Illustration of outliers and quartiles in network features.

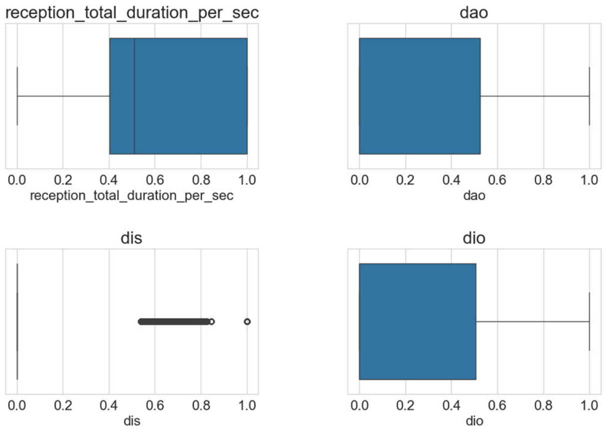


FIGURE 17. (D) Illustration of outliers and quartiles in network features.

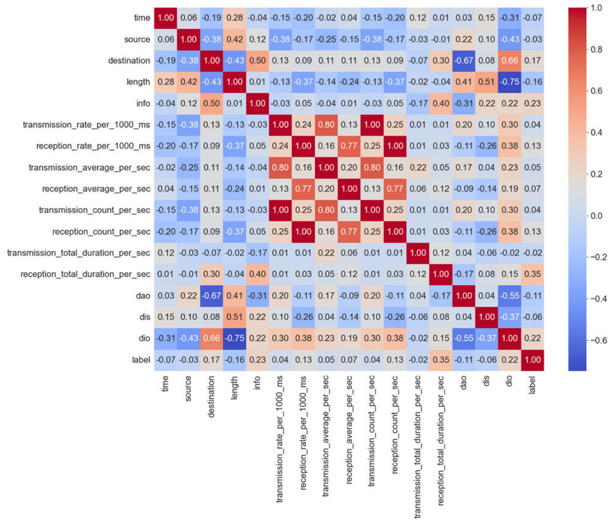


FIGURE 18. Relationship depiction between network features.

C. CORRELATION AND FEATURE INTERRELATIONSHIPS

The correlation matrix in Figure 18 highlights relationships between various features. Notable positive correlations, such as 'transmission_rate_per_1000_ms' with 'transmission_average_per_sec' and 'transmission_count_per_sec', indicate that higher transmission rates correlate with increased transmission averages and counts. Similarly, 'reception_rate_per_1000_ms' strongly correlates with 'reception_average_per_sec' and 'reception_count_per_sec'. Leveraging these relationships can improve the monitoring of correlated features for detecting abnormal traffic patterns and potential intrusions, thereby aiding in developing more efficient and targeted intrusion detection algorithms.

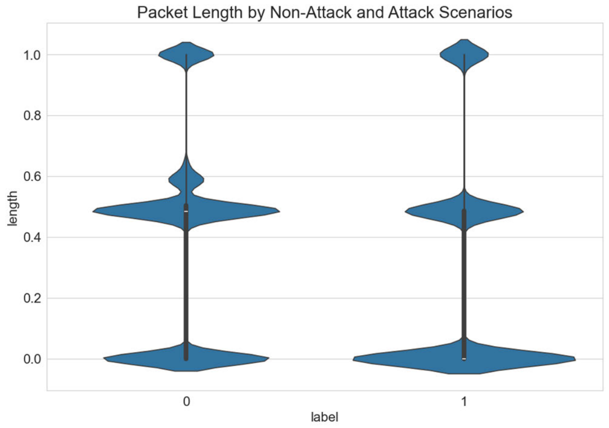


FIGURE 19. Comparative illustration of packet lengths in attack and non-attack scenarios.

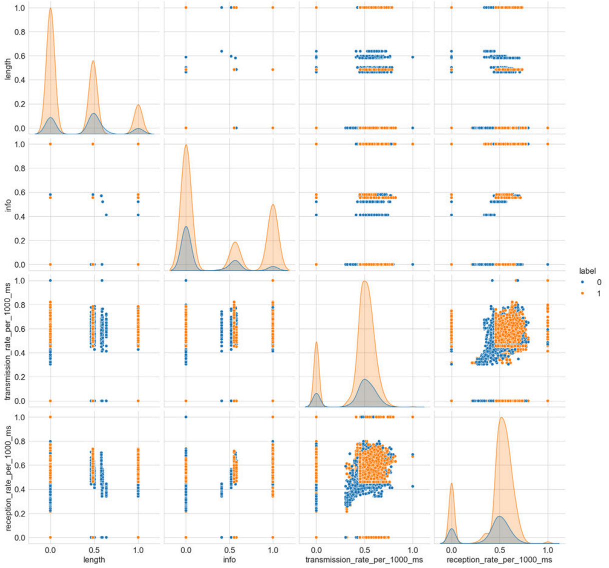


FIGURE 20. (A) Pair plot analysis of network traffic data.

D. PACKET LENGTH ANALYSIS AND ATTACK SCENARIOS

The violin plot in Figure 19 depicts the distribution of packet lengths in non-attack (label 0) and attack (label 1) scenarios. Both distributions display a similar spread with notable concentrations around specific lengths. However, attack scenarios exhibit a slightly broader range, suggesting variability

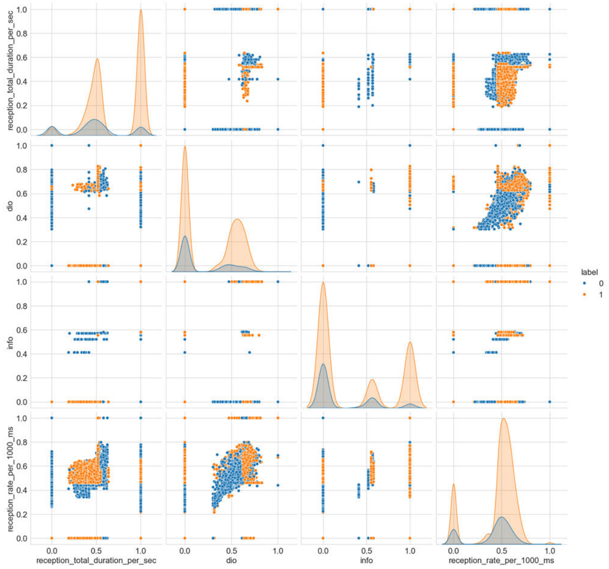


FIGURE 21. (B) Pair plot analysis of network traffic data.

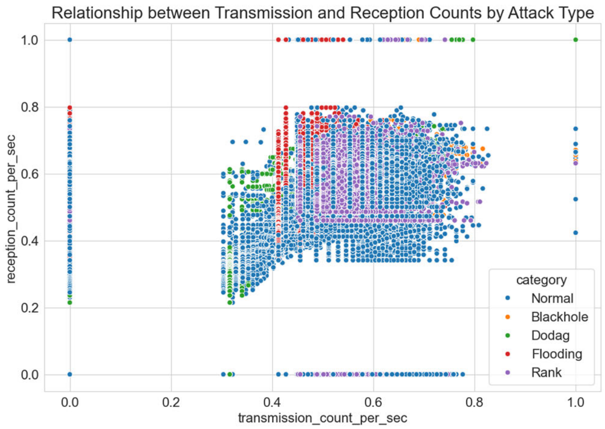


FIGURE 22. Relationship between transmission and reception counts by attack type.

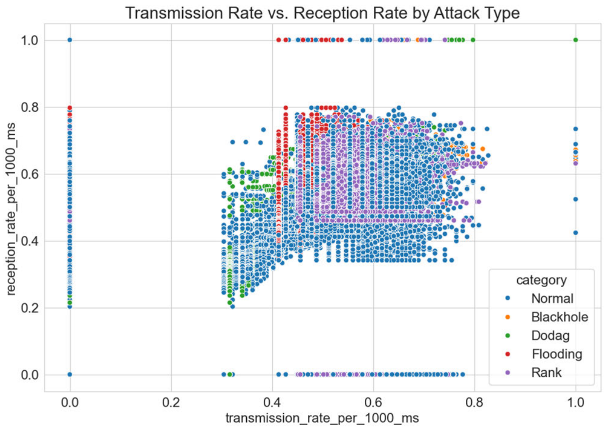


FIGURE 23. Transmission rate vs. reception rate by attack type.

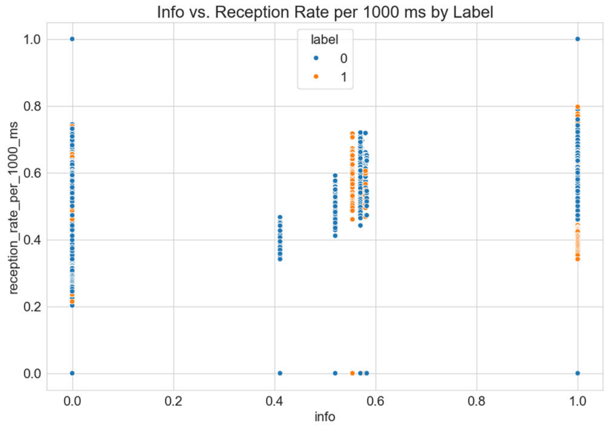


FIGURE 24. Info vs reception rate per 1000ms by label.

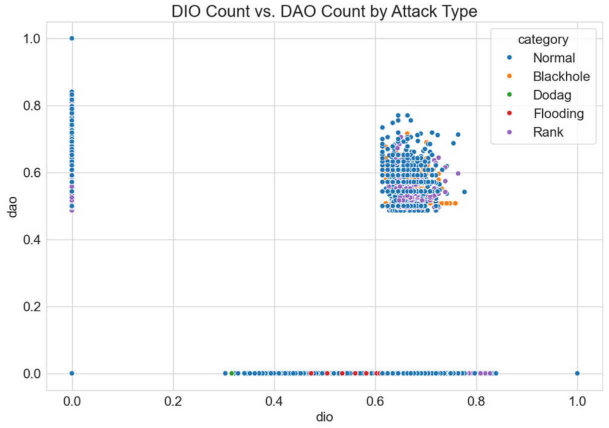


FIGURE 25. DIO count vs DAO count by attack type.

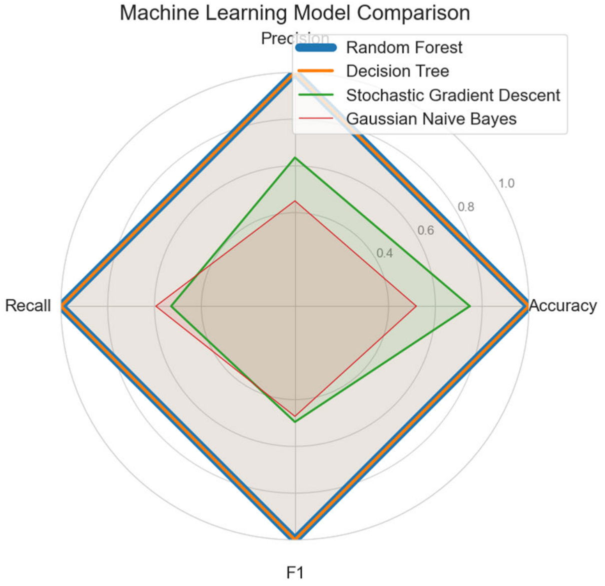


FIGURE 26. Illustration of machine learning model results across various metrics.

in packet lengths during attacks. This insight implies that packet length could be a distinguishing feature in identifying attack patterns, which could be integrated into anomaly detection models for enhanced IoT network security.

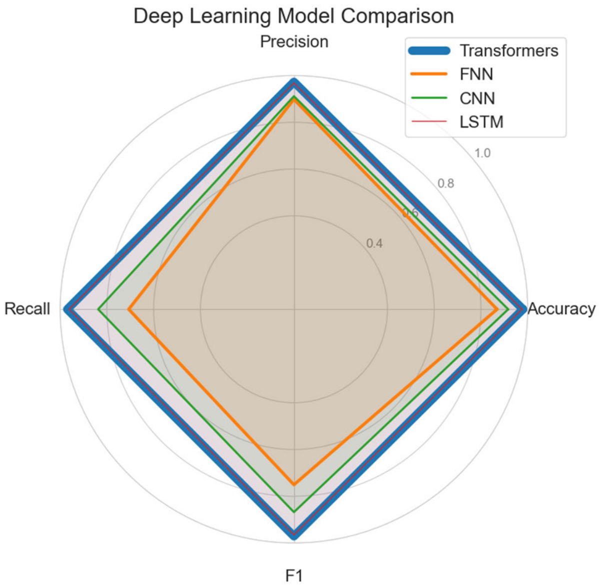


FIGURE 27. Illustration of deep learning model results across various metrics.

E. CLUSTERING AND FEATURE PRIORITIZATION

The pair plots in Figures 20-21 illustrate relationships between multiple features in the dataset, differentiating between attack (label 1) and non-attack (label 0) scenarios. They reveal distinct clustering patterns in features such as 'transmission_rate_per_1000_ms', 'reception_rate_per_1000_ms', and 'info', which are significantly impacted during attacks. These insights suggest that prioritizing these features can enhance the accuracy of anomaly detection models and real-time monitoring systems in IoT networks.

Figures 22-25 further demonstrate distinct clustering patterns between standard and various attack types using scatter plots. Specifically, 'transmission_count_per_sec' and 'reception_count_per_sec' (Figure 22) and 'transmission_rate_per_1000_ms' and 'reception_rate_per_1000_ms' (Figure 23) show clear differentiation between regular traffic and attack scenarios. The 'info' vs 'reception_rate_per_1000_ms' plot (Figure 24) reveals the separation between standard and attack labels, while the 'DIO' vs 'DAO' counts (Figure 25) effectively distinguish between different attack types. These patterns can inform the development of precise anomaly detection models by focusing on these key features for enhanced security in IoT networks.

F. MACHINE LEARNING MODEL PERFORMANCE

Figure 26 and Table 4 highlight the performance comparison of various machine-learning models for intrusion detection. The radar chart indicates that Random Forest (RF) and Decision Tree (DT) models achieve near-perfect precision, recall, accuracy, and F1 scores across all attack types, as Table 4 confirms. In contrast, Stochastic Gradient Descent (SGD) and Gaussian Naive Bayes (GNB) exhibit significantly lower performance. These findings suggest that ensemble methods like RF and DT should be prioritized for developing effective and reliable intrusion detection systems in IoT networks.

G. DEEP LEARNING MODEL EFFICIENCY

Figure 27 and Table 5 compare the performance and training times of various deep-learning models for intrusion detection. The radar chart indicates that Transformers and LSTM models achieve the highest performance across all metrics. Table 5 shows that Transformers are the most time-efficient, achieving high performance with significantly shorter training times. Table 5 confirms that Transformers and LSTM provide superior accuracy and F1 scores across all attack types. These insights suggest that Transformers are highly effective and efficient for developing advanced IDS in IoT networks compared to LSTM, CNN, and FFNN.

H. COMPARATIVE ANALYSIS OF ML AND DL MODELS

Both approaches exhibit strong capabilities in comparing machine learning and deep learning models for intrusion detection within IoT networks. Random Forest and Decision Tree models achieve near-perfect scores across all metrics. However, deep learning models, particularly Transformers and LSTM, offer superior performance, especially in managing complex and varied attack types. Transformers also excel in training efficiency. While traditional machine learning models provide robust and reliable results, deep learning models, particularly Transformers, present a compelling accuracy and computational efficiency advantage. This advantage makes them highly suitable for advanced IoT network security applications.

I. IMPLICATIONS AND FUTURE DIRECTIONS

This study underscores the need for continued research and development in intrusion detection for IoT networks, mainly focusing on integrating deep learning models due to their superior performance and efficiency. Future work should explore the deployment of these models in real-world IoT environments, considering the dynamic and diverse nature of IoT traffic. Additionally, incorporating real-time data and adaptive learning mechanisms can further enhance the robustness and reliability of these intrusion detection systems.

VI. CONCLUSION

In conclusion, the ROUT-4 dataset is essential for addressing security challenges posed by RPL attacks within IoT environments. It aids in creating and evaluating IDS by integrating data from simulations of four distinct RPL-specific assaults: Flooding, Black Hole, DODAG Version Number, and Decreased Rank attacks.

This study conducts exploratory data analysis to comprehensively understand attack characteristics and network vulnerabilities, employing statistical information graphs. Results suggest that meticulous examination of attack patterns and network traffic can enable IDS developers to refine detection algorithms, reducing computational processing and improving the accuracy of distinguishing malicious actions and legitimate network behaviour.

The study utilizes various machine learning models and deep learning architectures with the ROUT-4-2023 dataset, facilitating a transition from theoretical knowledge to practical defensive applications. Machine learning ensembling methods like random forests exhibit superior performance. Despite being relatively new and less studied, transformers show high effectiveness and efficiency in developing advanced IDS in IoT networks.

By offering a comprehensive framework for assessing, comprehending, and mitigating threats faced by RPL-based IoT networks, the study significantly advances research in IoT security. This research lays the groundwork for developing more robust defences and IDS, ultimately enhancing the security and resilience of IoT ecosystems.

REFERENCES

[1] I. S. Alsukayti and M. Alreshoodi, "RPL-based IoT networks under simple and complex routing security attacks: An experimental study," *Appl. Sci.*, vol. 13, no. 8, p. 4878, Apr. 2023, doi: 10.3390/app13084878.

[2] (2013). *Routing Attacks and Countermeasures in the RPL-Based Internet of Things-Linus Wallgren, Shahid Raza, Thiemo Voigt*. Accessed: Jun. 14, 2024. [Online]. Available: https://journals.sagepub.com/doi/10.1155/2013/794326

[3] R. Kumar, A. Malik, and V. Ranga, "Security concerns over IoT routing using emerging technologies: A review," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 7, Jul. 2023, Art. no. e4798, doi: 10.1002/ett.4798.

[4] M. EMEC. (2023). *ROUT-4-2023: RPL Based Routing Attack Dataset for IoT*. Accessed: Jun. 14, 2024. [Online]. Available: https://ieee-dataport.org/documents/rout-4-2023-rpl-based-routing-attack-dataset-iot

[5] Y. Al Sawafi, A. Touzene, and R. Hedjam, "Hybrid deep learning-based intrusion detection system for RPL IoT networks," *J. Sensor Actuator Netw.*, vol. 12, no. 2, p. 21, Mar. 2023, doi: 10.3390/jsan12020021.

[6] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: A deep learning–based intrusion detection framework for securing IoT," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, Mar. 2022, Art. no. e3803, doi: 10.1002/ett.3803.

[7] R. Bokka and D. T. Sadasivam, "Machine learning techniques to detect routing attacks in Rpl based Internet of Things," *Int. J. Electr. Eng. Technol.*, vol. 12, pp. 346–356, Jul. 2021.

[8] A. Pettersson. *Implementing and Evaluating Variations of the Blackhole Attack on RPL*. Accessed: Jun. 14, 2024. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1696160/FULLTEXT01.pdf

[9] I. A. Reshi, S. Sholla, and Z. A. Najar, "Safeguarding IoT networks: Mitigating black hole attacks with an innovative defense algorithm," *J. Eng. Res.*, vol. 12, no. 1, pp. 133–139, Mar. 2024, doi: 10.1016/j.jer.2024.01.014.

[10] W. Choukri, H. Lamaazi, and N. Benamar, "A novel deep learning-based framework for blackhole attack detection in unsecured RPL networks," in *Proc. Int. Conf. Innov. Intell. Informat., Comput., Technol. (3ICT)*, Nov. 2022, pp. 457–462, doi: 10.1109/3ICT56508.2022.9990664.

[11] M. Rouissat, M. Belkheir, and H. S. A. Belkhira, "A potential flooding version number attack against RPL based IoT networks," *J. Electr. Eng.*, vol. 73, no. 4, pp. 267–275, Aug. 2022, doi: 10.2478/jee-2022-0035.

[12] A. Verma and V. Ranga, "Security of RPL based 6LoWPAN networks in the Internet of Things: A review," *IEEE Sensors J.*, vol. 20, no. 11, pp. 5666–5690, Jun. 2020, doi: 10.1109/JSEN.2020.2973677.

[13] S. M. Muzammal, R. K. Murugesan, and N. Z. Jhanjhi, "A comprehensive review on secure routing in Internet of Things: Mitigation methods and trust-based approaches," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4186–4210, Mar. 2021, doi: 10.1109/JIOT.2020.3031162.

[14] Anthea Mayzaud, Remi Badonnel, and Isabelle Chrisment, "A taxonomy of attacks in RPL-based Internet of Things," *Int. J. Netw. Secur.*, vol. 18, no. 3, pp. 1–26, May 2016.

[15] J. Zhao, X. Liu, M. Baddeley, and I. Haque, "Analyzing the impact of topology on flooding attacks in low-power IoT networks," Dalhousie Univ., Jun. 2024, p. 4. [Online]. Available: https://dcsi.cs.dal.ca/wp-content/uploads/2021/07/24.pdf

[16] A. O. Bang, U. P. Rao, P. Kaliyar, and M. Conti, "Assessment of routing attacks and mitigation techniques with RPL control messages: A survey," *ACM Comput. Surveys*, vol. 55, no. 2, pp. 1–36, Jan. 2022, doi: 10.1145/3494524.

[17] A. Verma and V. Ranga, "Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 2, Feb. 2020, Art. no. e3802, doi: 10.1002/ett.3802.

[18] C. D. Morales-Molina, A. Hernandez-Suarez, G. Sanchez-Perez, L. K. Toscano-Medina, H. Perez-Meana, J. Olivares-Mercado, J. Portillo-Portillo, V. Sanchez, and L. J. Garcia-Villalba, "A dense neural network approach for detecting clone ID attacks on the RPL protocol of the IoT," *Sensors*, vol. 21, no. 9, p. 3173, May 2021, doi: 10.3390/s21093173.

[19] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, *A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)*, document RFC 7416, 2015.

[20] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "A study of RPL DODAG version attacks," in *Monitoring and Securing Virtualized Networks and Services*. Berlin, Germany: Springer, 2014, pp. 92–104.

[21] H. C. Leligou, P. Trakadas, S. Maniatis, P. Karkazis, and T. Zahariadis, "Combining trust with location information for routing in wireless sensor networks," in *Wireless Communications and Mobile Computing*. Hoboken, NJ, USA: Wiley, 1002, doi: 10.1002/wcm.1038.

[22] P. Karkazis, P. Trakadas, Th. Zahariadis, A. Hatziefremidis, and H. C. Leligou, "RPL modeling in J-Sim platform," in *Proc. 9th Int. Conf. Networked Sens. (INSS)*, Jun. 2012, pp. 1–2, doi: 10.1109/INSS.2012.6240559.

[23] T. Tsao, R. Alexander, M. Dohler, V. Daza, and A. Lozano. (2012). *A Security Framework for Routing Over Low Power and Lossy Networks*. Accessed: Jun. 14, 2024. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-roll-security-framework

[24] A. Sehgal, A. Mayzaud, R. Badonnel, I. Chrisment, and J. Schönwälder, "Addressing DODAG inconsistency attacks in RPL networks," in *Proc. Global Inf. Infrastruct. Netw. Symp. (GIIS)*, Sep. 2014, pp. 1–8, doi: 10.1109/GIIS.2014.6934253.

[25] A. O. Bang and U. P. Rao, "EMBOF-RPL: Improved RPL for early detection and isolation of rank attack in RPL-based Internet of Things," *Peer-to-Peer Netw. Appl.*, vol. 15, no. 1, pp. 642–665, Jan. 2022, doi: 10.1007/s12083-021-01275-3.

[26] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3685–3692, Oct. 2013, doi: 10.1109/JSEN.2013.2266399.

[27] A. Hkiri, "RPL-based IoT networks under decreased rank attack: Performance analysis in static and mobile environments," *Comput., Mater. Continua*, vol. 78, no. 1, pp. 227–247, 2024, doi: 10.32604/cmc.2023.047087.

[28] B. Ghaleb, A. Al-Dubai, A. Hussain, J. Ahmad, I. Romdhani, and Z. Jaroucheh, "Resolving the decreased rank attack in RPL's IoT networks," 2023, *arXiv:2305.10025*.

[29] L. Breiman, J. H. Friedman, R. A. Olshen, and C. J. Stone, *Introduction to Tree Classification*. Boca Raton, FL, USA: CRC Press, 1984.

[30] L. Breiman, "Random Forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, Oct. 2001, doi: 10.1023/a:1010933404324.

[31] H. Robbins and S. Monro, "A stochastic approximation method," *Ann. Math. Statist.*, vol. 22, no. 3, pp. 400–407, Sep. 1951, doi: 10.1214/aoms/1177729586.

[32] L. Devroye, L. Gyrfi, and G. Lugosi, "Parametric classification," in *A Probabilistic Theory of Pattern Recognition*. Cham, Switzerland: Springer, 1996, pp. 263–278.

[33] G. Bebis and M. Georgiopoulos, "Feed-forward neural networks," *IEEE Potentials*, vol. 13, no. 4, pp. 27–31, Oct. 1994, doi: 10.1109/45.329294.

[34] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proc. IEEE*, vol. 86, no. 11, pp. 2278–2324, Nov. 1998, doi: 10.1109/5.726791.

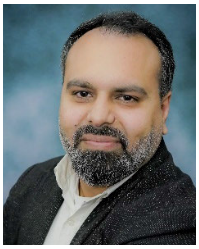
[35] D. E. Rumelhart and J. L. McClelland, "Learning internal representations by error propagation," in *Parallel Distributed Processing: Explorations in the Microstructure of Cognition: Foundations*. Cambridge, MA, USA: MIT Press, 1987, pp. 318–362.

[36] A. Vaswani, "Attention is all you need," 2023, *arXiv:1706.03762*.

USAMA SHAHID received the B.Sc. degree (Summa Cum Laude and Hons.) in computer science from Bahria University, Pakistan, in 2021, and the M.Sc. degree in data science from the University of Gloucestershire, U.K., in 2024. Currently, he holds the position of a Lecturer in AI and data science with the University of Gloucestershire, where his duties encompass teaching and research. He is a U.K. Global Talent in digital technology sector. He has contributed to the industry by developing research-driven digital products based on machine learning and large language models. During the B.Sc. degree, he received the Gold Medal Award.

MUHAMMAD ZUNNURAIN HUSSAIN received the B.S. degree in telecommunication engineering from the University of Management and Technology (UMT), Lahore, Pakistan, in 2011, and the M.Sc. degree in research in the field of computer networking from the University of Bedfordshire, U.K., in 2014. He is currently pursuing the Ph.D. degree in computer networks with the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM). He is serving with the Department of Computer Science, Bahria University Lahore Campus. He is an Academician with a couple of years teaching and administrative experience at public and private universities in Pakistan. He is the only Asian with more than 2000 international certifications.

MUHAMMAD ZULKIFL HASAN received the B.S. degree in telecommunication engineering from the University of Management and Technology (UMT), Lahore, Pakistan, in 2011, and the M.Sc. degree in research in the field of computer networking from the University of Bedfordshire, U.K., in 2014. He is currently pursuing the Ph.D. degree in computer networks with the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM). He is serving with the Faculty of Information Technology, University of Central Punjab, Lahore. He is an Academician with a couple of years teaching and administrative experience at public and private universities in Pakistan.



ALI HAIDER received the B.S. degree in information technology from the University of the Punjab, Collage of Information Technology, Lahore, Pakistan, in 2007. He is currently with Dell SecureWorks, USA, as a Sr. Cybersecurity Consultant. He has earned several international credentials in networking and cyber security, such as SANS, Cisco Expert (CCIE), CISSP, CISM, and CRISC. With more than 15 years of global experience, he is a multi-award-winning professional recognized as a Judge, Mentor, and esteemed Consultant in the fields of technology and cybersecurity. His extensive career has spanned across diverse regions including the Middle East, U.K., Europe, AUS, and USA, where he has consistently assumed leadership roles within prominent global technology and consulting firms.

JIBRAN ALI received the Bachelor of Science degree in information technology from Bahria University, in 2021. He is an accomplished professional currently serving as a Resident Engineer with Premier Systems, Pakistan. He operates in a hybrid work setting in Pakistan, where he has been making significant contributions. Prior to this role, he was associated with Multinet Pakistan, KK Networks, Lahore, Punjab, Pakistan. He was promoted from a Senior Network Engineer to the Deputy Manager of networks with KK Networks. He actively engaged in programming and was involved in telecommunications and networking societies. His educational and professional journey is highlighted by his ability to leverage platforms like LinkedIn to advance his career.

JAWAD ALTAF received the bachelor's degree in computer science engineering from Comsats Institute of Information Technology in Lahore, Pakistan. Currently, he is pursuing the master's degree in cybersecurity from the National College of Ireland, Dublin, along with working as a Teaching Assistant with the School of Computing. He has taught academics as a Lecturer in computer science with the Superior Group of Colleges, and Concordia Group of Colleges, Lahore. He is a member of Saudi Engineering Council with industry experience of eight years in the field of network security, system administration, and ITSM. He holds multiple certifications in various technologies, including CISCO, FORTINET, SOPHOS, KASPERSKY, MICROSOFT, ALI BABA, and HUAWEI.