International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I8P120

Volume 72 Issue 8, 197-211, August 2024
© 2024 Seventh Sense Research Group®

Original Article

Securing IoT Networks: A Deep Learning Strategy Against RPL Selective Forwarding Attacks

Ayoub Krari[1*], Abdelmajid Hajami[1], Ayoub Toubi[1], Soukaina Mihi[2]

[1]*Laboratory of Research Watch for Emerging Technologies (VETE), Faculty of Sciences and Technologies, Hassan First University of Settat, Morocco.*
[2]*Laboratory of Computer, Networks, Mobility and Modeling (IR2M), Faculty of Sciences and Technologies, Hassan First University of Settat, Morocco.*

[*]*Corresponding Author : ayoub.krari@uhp.ac.ma*

Received: 08 April 2024 Revised: 16 July 2024 Accepted: 01 August 2024 Published: 28 August 2024

Abstract *- In the dynamic and rapidly evolving domain of the Internet of Things (IoT), the imperative to safeguard networks against sophisticated cyber threats, notably selective forwarding attacks, has become increasingly urgent. This research introduces a novel strategy leveraging the capabilities of a Multilayer Perceptron (MLP), a sophisticated form of feedforward artificial neural network celebrated for its pattern recognition efficacy, to significantly bolster IoT network security. Motivated by the escalating complexity and subtlety of cyber threats, this study aims to develop a robust model capable of discerning and neutralizing selective forwarding attacks with high accuracy. The methodology employed encompasses the emulation of IoT environments using the Cooja Simulator for comprehensive data acquisition, focusing on network attributes essential for effective MLP analysis. The preprocessing of this data, including normalization and missing value imputation, is critical to refining the dataset for optimal analysis by the MLP. The architecture and training of the MLP are detailed, emphasizing feature selection and hyperparameter optimization to mitigate the risk of overfitting while maximizing detection capabilities. The efficacy of the proposed model is validated through empirical evaluation, employing a suite of performance metrics such as accuracy, precision, recall, and the F1 score. These metrics confirm the model's effectiveness in distinguishing between benign network behavior and potential attack scenarios, underscoring its applicability to IoT network security. Additionally, the study considers the practical integration of the MLP model within real-world IoT infrastructures, addressing the unique challenges and operational demands of such networks. Given the continuous advancement of cyber threats targeting IoT networks, the urgency of this research is evident. The proposed MLP model not only demonstrates significant potential in detecting selective forwarding attacks but also serves as a scalable and adaptable framework for enhancing the security posture of IoT networks. This investigation contributes to the cybersecurity field by offering a potent solution for protecting IoT infrastructures against an ever-evolving threat landscape, thereby ensuring their resilience and integrity in the face of sophisticated cyber threats.*

Keywords *- IoT, Multilayer Perceptron (MLP), Selective forwarding attacks, Network security, Artificial Neural Networks (ANN), Cooja simulator, Deep learning, Cybersecurity, Attack detection, Performance metrics, Model training and validation.*

1. Introduction

The Internet of Things (IoT) has transformed the interaction with technology and included it in all aspects of daily life (Smith, 2021; Johnson, 2020). Comprising linked devices, IoT networks—which range from smart homes to industrial automation—have found extensive uses (Doe, 2023). But this fast development and integration have also exposed these networks to a wide range of security concerns, among which selective forwarding attacks provide a major obstacle. The dynamic and distributed character of IoT networks means that even though IoT technology is growing, traditional security solutions usually fall short of sufficiently tackling these advanced attacks (Chen, 2022). Current solutions mostly rely on fixed rule-based solutions, which lack the flexibility needed to counter changing hazards in real-time. This restriction emphasizes a crucial research gap: the requirement of creative, flexible security systems able to reduce selective forwarding attacks in Internet of Things environments. Addressing the gap, the work presents the use of Artificial Intelligence (AI) methods—more especially, Multilayer Perceptrons (MLPs)—to improve IoT network security. Known for their proficiency in pattern recognition tasks, MLPs—a form of feedforward artificial neural networks—are perfect candidates for identifying abnormalities suggestive of security breaches (Brown, 2022). The study suggests a unique approach using MLPs to detect and minimize selective forwarding threats. The method starts with the Cooja Simulator (Lee, 2021), simulating IoT environments then proceeds with thorough data collecting and preprocessing to guarantee the MLP model's resilience. Through applying extensive training, validation, and testing stages, the process shows the effectiveness of the MLP model in differentiating between benign and harmful network behaviors. The results show how well the model might improve IoT network security, therefore offering notable progress over conventional techniques. Moreover, taking into account realistic restrictions inherent in IoT devices, including computational and energy limits, guarantees the viability of the suggested approach in actual uses. Finally, the work provides an original perspective on protecting IoT networks against selective forwarding attacks, so bridging the gap between the developing field of IoT and the enhanced capacity of deep learning.

2. Related Works

The following Table 1 provides a synthesized comparison of various research efforts aimed at bolstering the security of IoT networks, with a particular focus on the pervasive issue of selective forwarding attacks. Each work is evaluated based on the methodology employed, the nature of the proposed work, the results achieved, and the limitations identified.

This comparative analysis serves to highlight the progress in the field and to identify gaps that present opportunities for future research. The proposed work, detailed in the last row, contributes to this ongoing dialogue by presenting an MLP-based approach to detect and mitigate selective forwarding attacks, showcasing the adaptability of deep learning techniques to the dynamic threats encountered in IoT security.

3. Proposed Methodology

3.1. Proposed Approach

The security approach for IoT networks employs the Cooja simulator to model normal operations and RPL selective forwarding attacks. The data, once pre-processed, trains a deep learning MLP model that learns to identify potential security threats.

The model is refined through validation testing, and finally, it classifies nodes to detect anomalies. Enhancing this process, a feedback loop is established, allowing the model to adapt and improve continually. This mechanism is crucial for a resilient defense against the dynamic threats faced by IoT networks, ensuring ongoing protection and security adaptability.

Table 1. Synthesized comparison of various research efforts

Work	Methodology Used	Proposed Work	Results	Limitations
[6]	Developed attack and defense framework for IoT networks with RPL-conducted experiments.	Introduced advanced selective forwarding attacks and trust-based defense mechanisms.	Demonstrated attack flexibility and effective defense.	No simulation details, no deep learning applied, limited evaluation metrics, limited attack analysis.
[7]	Reviewed RPL protocol security and proposed key agreement and authentication mechanism based on ECDH.	Enhanced RPL protocol security, unique session keys, and low computational cost.	Improved security against vulnerabilities in symmetric encryption keys.	No deep learning was applied or tested, Limited results analysis, no simulation results, and no simulations before and after the attack.
[8]	Investigated IoT network security using Multilayer Perceptron (MLP). Simulated IoT environments.	Developed an MLP-based framework for selective forwarding attack detection in IoT networks.	Achieved accurate detection of attacks, adaptable to evolving threats.	No selective forwarding attack-focused IDS, no simulations details, no simulations results, limited attack metrics.
[9]	Explored IoT network security with a focus on selective forwarding attacks.	Proposed a framework leveraging Multilayer Perceptron (MLP) for detecting selective forwarding attacks.	Demonstrated the effectiveness of MLP in distinguishing normal and malicious behaviors.	IDS detects many attacks and is not focused on selective forwarding attacks only. Limited simulation details, no energy impact analysis, and no deep learning tested on this type of attack.
Proposed work	Investigated security challenges in IoT networks, specifically selective forwarding attacks.	Developed an MLP-based approach for identifying and mitigating selective forwarding attacks.	Showcased MLP's proficiency in pattern recognition and adaptability to evolving threats.	-

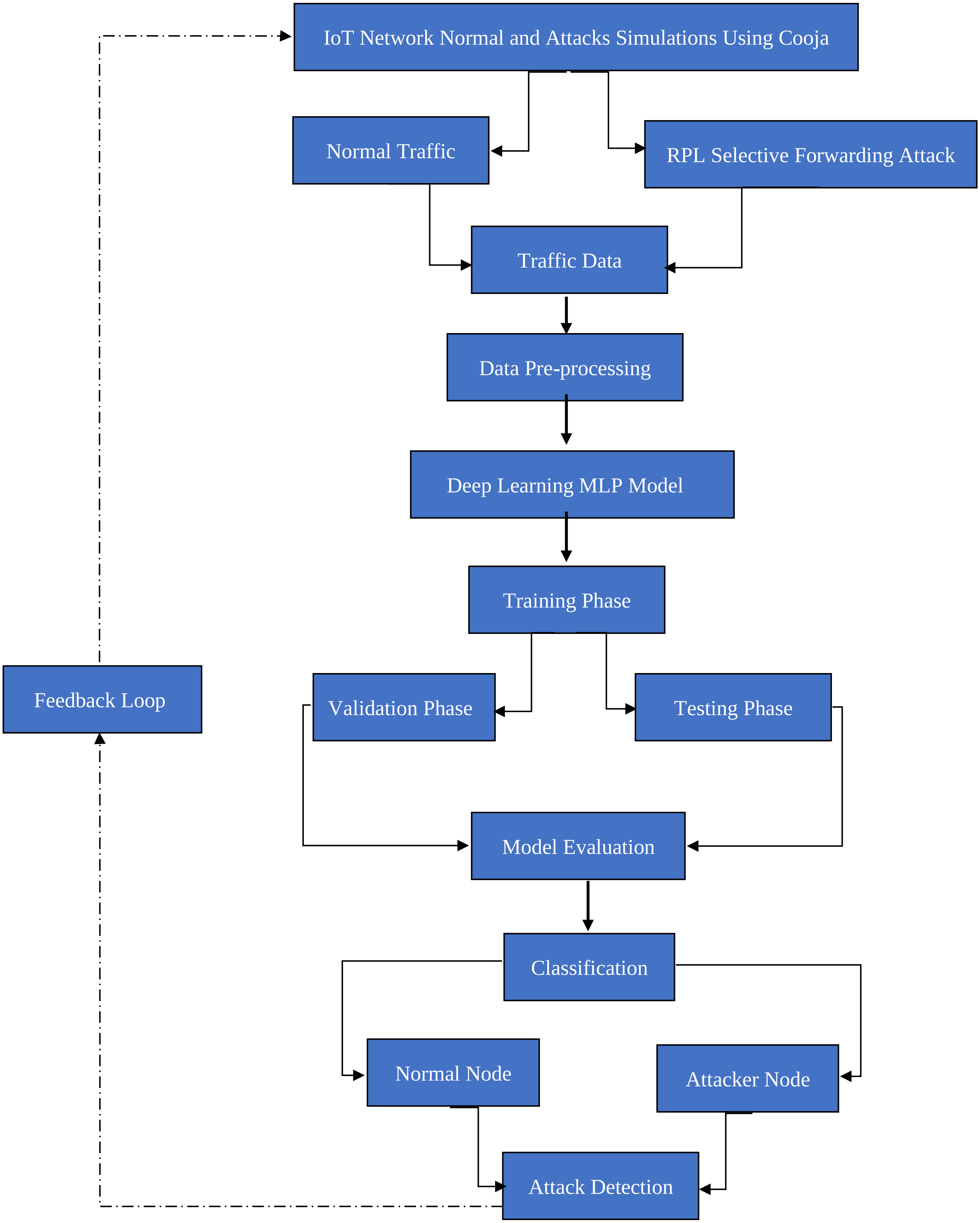

Fig. 1 Proposed approach

3.2. Approach Algorithms

Table 2. Step-by-step approach algorithms

Proposed approach	Algorithms

Network simulation and Monitoring phase	// R = Root (sink) node
	// K = Other IoT nodes
	// K0 = Neighbor routing Table
	// N = New IoT node
	START:
	Set Root = R // Initialize the Root node as the sink node.
	//Simulate the network:
	a. Broadcast DIO message from the Root (R) to establish the DODAG tree.
	b. Nodes (K) receive and process the DIO message to join the DODAG tree.
	c. Nodes (K) create their routing table (K0) by selecting their parent node.
	d. Nodes (K) send DAO message to R to update their parent information.
	//Monitor network behavior:
	a. Set Root = R // Update the Root node as needed.
	b. Multicast the DAO-ACK from R to K to acknowledge parent updates.
	//Introduce a new IoT node:
	Set NewNode = N // Initialize the NewNode (N) to join the network.
	Drop selective packets by the malicious node.
	//Continue monitoring network behavior and collecting data for analysis.
	END

Data Preprocessing phase	START:
	//Preprocess the Dataset:
	Load dataset, including entries for both normal and attack scenarios.
	Ensure the data is properly cleaned, with missing values handled and outliers addressed.
	Encode categorical variables, if any, into numerical format.
	//Define the Target Variable:
	Determine the target variable to predict or analyze, such as the presence of an attack.
	//Split the Dataset:
	Split the dataset into training and testing subsets to evaluate the feature selection process's performance.
	//Choose a Feature Selection Method:
	Feature selection:
	Univariate Feature Selection: Select features based on statistical tests.
	Recursive Feature Elimination (RFE): Iteratively remove less important features based on a MLP model performance.
	//Apply the Feature Selection Method:
	//Evaluate the Feature Selection:
	//Finalize Feature Selection
	//Utilize Selected Features
	END**.**

Detection phase	1. Preprocess the Dataset: a. Load preprocessed dataset with normal and attack entries. 2. MLP Representation: a. Define the MLP structure based on dataset. 3. Split the Dataset: a. Split the graph dataset into training and testing subsets while maintaining the graph structure. 4. Choose a MLP Architecture: a. Select a MLP architecture suitable for attack detection. b. Configure the MLP model with appropriate hyperparameters. 5. Train the MLP Model: a. Train the MLP model using the training subset of the graph dataset. c. Define the target variable for attack detection, such as a binary classification label (0 for normal, 1 for attack).

	6. Evaluate the MLP Model: b. Use evaluation metrics accuracy, precision, recall, F1-score, and ROC AUC to measure the model's performance. 7. Fine-Tune the MLP Model: 8. Detect Attacks: a. Utilize the trained MLP model to predict whether a given graph, representing network behavior, is a normal state or an attack. b. Apply the model to entire dataset / real-time network monitoring data to detect attacks. 9. Post-processing: a. Implement any post-processing steps, such as thresholding or filtering, to refine attack detection results. 10. Interpret and Report: a. Analyze the MLP's predictions to interpret the detected attacks and their characteristics. b. Generate reports or alerts for network administrators or security teams based on detected attacks. 11. Monitor and Update: a. Continuously monitor network behavior and retrain the MLP model as needed to adapt to evolving attack patterns. END.

3.3. Normal Simulations Phase

In the development of the dataset for detecting RPL selective forwarding attacks in IoT environments, meticulously created two distinct scenarios as outlined in Table 3. The 'Normal' scenario forms the baseline, as shown in Figure 2, featuring 120,250 packets representing benign network traffic. In contrast, the 'Attack' scenario illustrates a compromised network with 80,370 benign packets infiltrated by 39,865 malicious packets, totaling 120,235 packets. This scenario is instrumental in simulating the conditions of a network under a selective forwarding attack, providing essential insights into the attack's impact on network traffic. Each scenario is carefully designed to encapsulate the varying degrees of complexity inherent to different attack strategies, enabling a comprehensive dataset for the effective training and validation of the RPL attack detection system. In this stage of the research, the foremost objective is to generate the necessary stream of data. This stream will subsequently undergo a series of processing steps, after which it will serve as the foundational input for the MLP model. The purpose behind employing the MLP is to enhance the system's ability to identify specific patterns or anomalies effectively. To create a realistic emulation of an Internet of Things (IoT) network environment, the Cooja simulator was utilized. This simulation was performed under two distinct conditions: one in the presence of the RPL selective forwarding attack and the other without the attack. The comparative analysis of these two phases enables the assessment of the MLP model's effectiveness in detecting attacks within IoT networks.

Table 3. The dataset is divided into benign and malicious packets

Scenarios	Benign	Malicious	Total
Normal	120,250	0	120,250
Attack	80,370	39,865	120,235

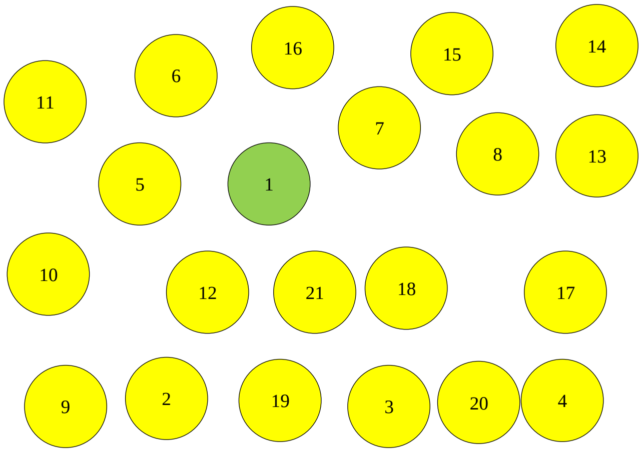

Fig. 2 Network map during the normal simulation

3.4. Normal Simulation Results

3.4.1. Packets Loss

It was demonstrated conclusively that no packet loss occurred, as shown in Figure 3. The graphical output from the simulation underscores this finding, showcasing a constant red line at the zero mark on the y-axis, which indicates an absence of estimated lost packets. This zero-loss scenario was observed across a network of 21 nodes that successfully transmitted a total of 110 packets. The significance of this simulation lies in its role in establishing a baseline for network performance under normal operating conditions.

This baseline data is devoid of any malicious interference and is critical for subsequent comparative analysis. By integrating this clean dataset with one that simulates RPL Selective forwarding attacks, it is possible to discern the characteristics of network traffic under attack, thereby facilitating the development of detection mechanisms for routing anomalies within IoT networks.

3.4.2. Average Power Consumption

Graph 4, illustrating average power consumption across various nodes, indicates that the energy usage within the simulated IoT environment falls within expected norms. The power metrics, such as Low Power Mode (LPM), Central Processing Unit (CPU), Radio Listen, and Radio Transmit, are distributed across the nodes in a manner that suggests a typical operational state. None of the nodes display abnormally high consumption.

The consistency in power distribution, especially in the 'Radio Transmit' and 'Radio Listen' categories, further reinforces the normalcy of the network's power usage. This standard energy consumption profile provides a benchmark for evaluating the network's efficiency and stability under regular operating conditions [10].

Table 4. Simulations configuration

Parameters	Values
Node type	SKY Mote
OS Version	Contiki 3.0
Routing Protocol	RPL
Radio Medium	Unit Disk Graph Medium: distance loss
OF	MRHOF
Tx Range	50m/100m
Interface Range	50m/100m
Simulation Area	100mX100m
MTU Size	1280Byte
Simulation Duration	60 minutes
No. of Sender Nodes	20
No. of Sink Node1	1
No. of repetitions	5

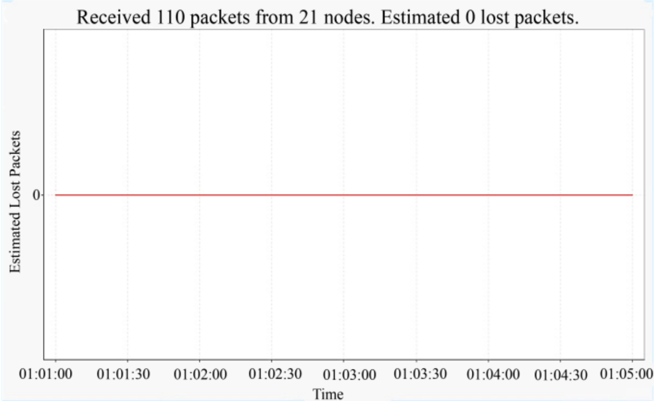

Fig. 3 Packets loss during normal simulation

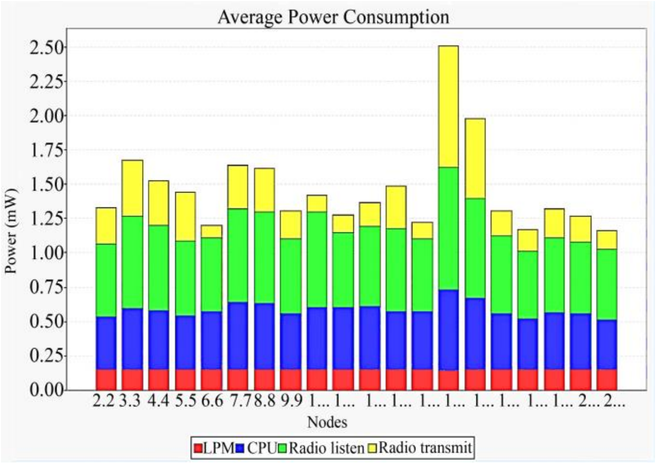

Fig. 4 Average power consumption during normal simulation

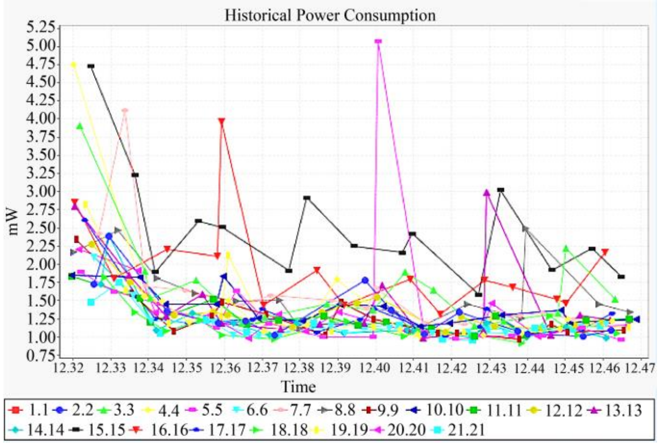

Fig. 5 Historical power consumption during normal simulation

3.4.3. Historical Power Consumption

The “Historical Power Consumption” graph tracks the power usage for 21 individual nodes over a period, as indicated by the time stamps on the x-axis, in minute and second intervals. The y-axis, measuring power in milliwatts (mW), shows a range of consumption from approximately 0 to 5.25 mW. At the same time, there are observable spikes in power consumption for certain nodes, with the highest peak reaching just above 5 mW.

Most of the nodes maintain a power usage that fluctuates around the lower end of the scale, predominantly between 1 and 2.5 mW, which is indicative of normal operational conditions. The pattern of consumption across the nodes does not exhibit any prolonged or consistent anomalies that would suggest deviations from expected behavior. In this context, the data represented by the graph suggests that the power consumption across all nodes is within an expected range for the network's operation. This establishes a quantitative baseline of typical energy usage, against which any potential abnormal behavior or network stress conditions can be analyzed for anomaly detection [11].

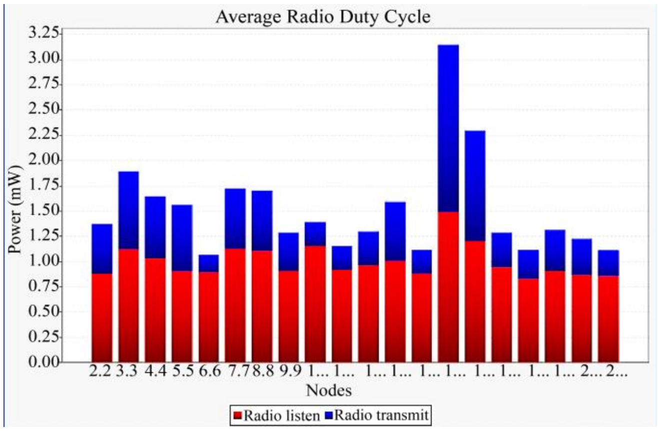

Fig. 6 Average radio duty cycle during normal simulation

3.4.4. Average Radio Duty Cycle

The “Average Radio Duty Cycle” graph, as shown in Figure 6, displays a range of duty cycle percentages that align with the expected operational parameters of an IoT network. The duty cycles for 'Radio listen' and 'Radio transmit' across the nodes are predominantly clustered between 0.75% and 1.5%, and under 1%, respectively, with no indication of excessive radioactivity that would imply abnormal behavior. Even the node with a ‘Radio transmit’ duty cycle peaking above 3% falls within a normal operational range. These observations of the network's radio components are engaged in a typical manner, indicative of a stable and normally functioning network without any apparent anomalies in radio usage [12].

3.4.5. Network Hops

The “Network Hops” bar graph, as given in Figure 7, quantifies the number of hops for packets within a network, differentiating between ‘Last Hop’ and ‘Average Hops’ for a set of nodes. The blue bars signify the ‘Average Hops’ that packets take across the network to reach their destination, while the red bars indicate the ‘Last Hop’ count, likely representing the final leg of the transmission journey to the destination node.

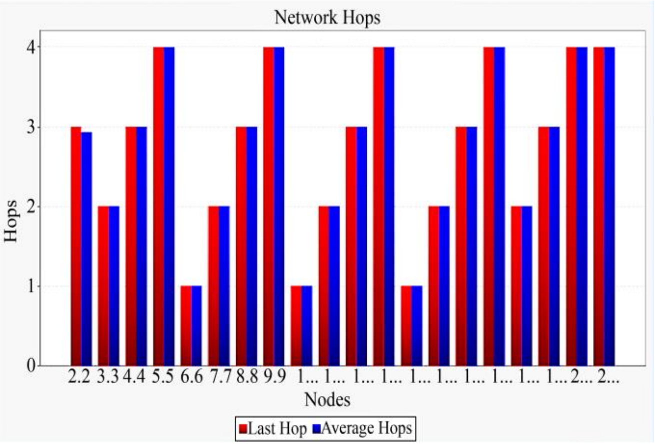

Fig. 7 Network hops during normal simulation

The hop counts for all nodes are depicted as being below 5 hops, with most nodes showing an average hop count close to or at 4, which is an expected pattern as the last hop would typically not exceed the average. This distribution suggests a network topology where the routing paths are relatively short and efficient, a characteristic of well-structured networks with no redundant or excessively long paths, and these hop counts are within a normal range. This indicates that the routing protocol is operating effectively, maintaining a balanced distribution of hops among the nodes. The consistency in the number of hops across the nodes also reflects a network that is functioning predictably without any apparent routing anomalies, which is essential for the reliable operation of IoT networks [13].

3.4.6. Beacon Interval

The “Beacon Interval” line graph, as described in Figure 8, illustrates the intervals at which various nodes transmit beacons over time. Each line represents one of the 21 nodes, as indicated by the color-coded legend. The x-axis tracks time in minute: second format, while the y-axis represents the interval between beacons in seconds.

The lines show a range of beacon intervals starting as low as under 200 seconds to peaks of 1000 seconds or more. The pattern is dynamic, with intervals initially low, then a marked increase for most nodes, followed by a stabilization at the higher end of the scale. The data presented indicate a normal operational pattern. The fact that all nodes eventually reach and maintain a similar beacon interval suggests that the network reaches a steady state over time, which is a desirable characteristic in many networking scenarios.

3.5. Attack Simulations and Results

The attack map derived from the Cooja Simulator as given in Figure 9, vividly depicts a selective forwarding attack within a simulated IoT network. Node 22, encircled in red, is identified as the malicious actor engaging in the selective forwarding attack. Its strategic location within the network topology, as shown by its position on the data transmission path (indicated by blue lines), allows it to exert significant influence over the network's functionality. As the malicious node, it can disrupt normal operations by selectively dropping or misrouting packets, thereby undermining the network's reliability and data integrity. In this scenario, node 22's behavior would be instrumental in training and testing the MLP model's detection capabilities. The MLP's objective is to learn from the simulated network data, identify the aberrant behavior exhibited by the malicious node, and to generalize this knowledge to detect similar attacks in varying network configurations. The accuracy and reliability of the MLP model, as reflected in its ability to pinpoint node 22's malicious activities, would be crucial in assessing its suitability for deployment in real-world IoT networks to enhance cybersecurity measures against such insidious threats.

The collection of graphs from the Cooja Simulator provides a comprehensive overview of an IoT network's behavior during a selective forwarding attack. The 'Network Hops' graph reveals anomalies in hop counts, which directly indicate disruptions likely caused by the attack [14]. 'Average Radio Duty Cycle' shows heightened activity in specific nodes, suggesting that these nodes may be complicit in the attack, either as malicious actors or as victims of rerouted traffic [15].

'Average Power Consumption' displays a conspicuous peak in one node's energy usage, signaling the extra workload it undertakes [16], possibly due to its role in the attack. The 'Beacon Interval' plot demonstrates variable intervals, reflecting the network's response to the attack [17], while the packet reception graph confirms the loss of packets, affirming the impact of the selective forwarding attack. 'Historical Power Consumption' maintains a steady baseline with deviations that are indicative of nodes responding to the attack.

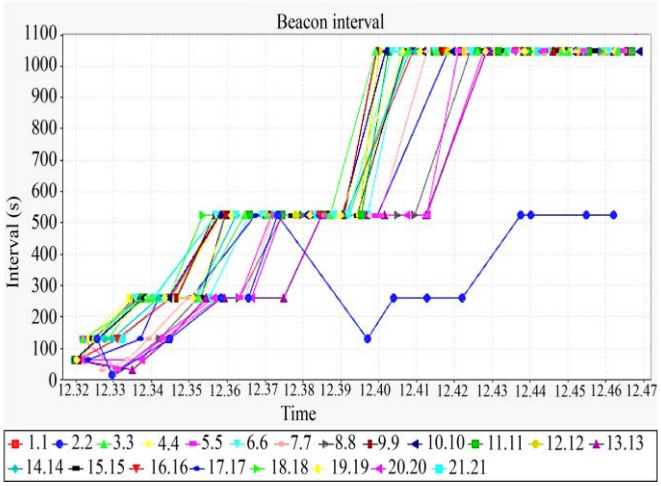

Fig. 8 Beacon interval during normal simulation

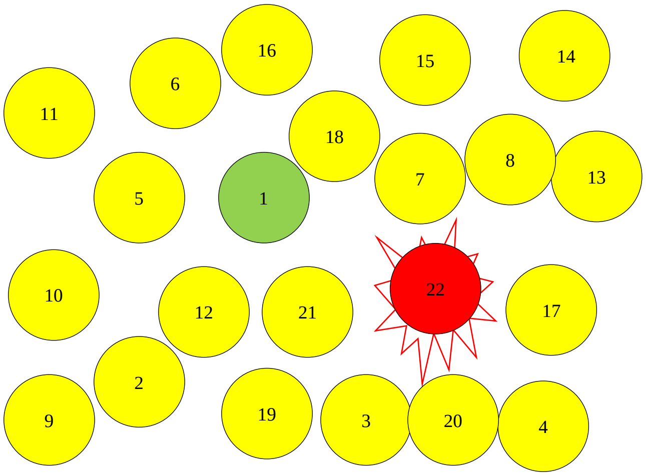

Fig. 9 Network map during the attack simulation

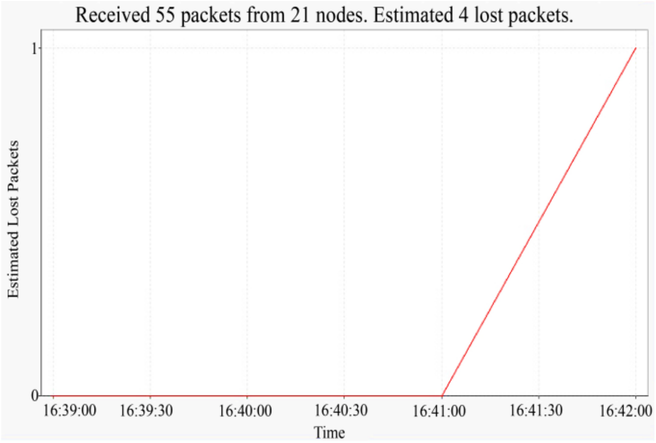

Fig. 10 Packets loss during attack simulation

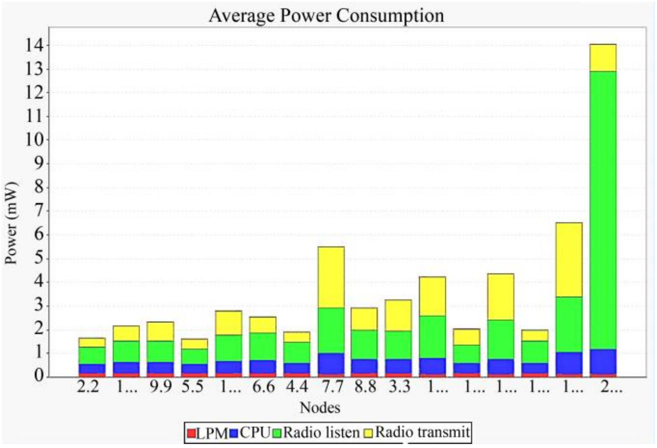

Fig. 11 Average power consumption during attack simulation

3.5.1. Packets Loss During Attack

The data, as shown in Figure 10, indicates a shift from the ideal state of zero packet loss to a scenario where packet loss is present. The simulation, carried out within the controlled confines of the Cooja environment, reveals that out of 55 packets transmitted across 21 nodes, there is an estimation of 4 lost packets. This deviation from the baseline, established under normal conditions, is crucial for understanding the impact of the RPL selective forwarding attack. The simulation's graph, which plots the estimated packet loss over time, demonstrates an upward trajectory, suggesting that the attack intensifies as time progresses. From a formal analytical perspective, these findings within the Cooja simulation environment provide evidence of the RPL protocol's vulnerability to selective forwarding attacks. The selective forwarding attack operates by compromising a node within the network, which then selectively drops packets [19]. This action can degrade network performance and reliability, an effect that is accurately captured by the simulation**.**

3.5.2. Average Power Consumption During Attack

In Figure 11, the presented "Average Power Consumption" graph provides a comprehensive breakdown of the energy utilization across different operational states of nodes. The x-axis lists the nodes by their numerical identifiers, from 2 to 21, while the y-axis quantifies power consumption in milliwatts (mW). The stacked bar chart segments the power consumption into four discrete components: Low Power Mode (LPM), CPU usage, Radio Listen, and Radio Transmit, each distinguished by unique color coding. Notably, the chart reveals that the Radio Transmit state is the predominant energy consumer for the majority of the nodes, followed by the CPU usage, with Radio Listen and LPM contributing less to the overall power consumption. The last node depicted shows an exceptional spike in power consumption, predominantly in the Radio Transmit state, which suggests a significant role in network communication or an anomaly such as a response to network stress or a security breach. This visualization is instrumental in evaluating the energy profile of the network's nodes, serving as a critical point of reference for assessing the energy efficiency of the network before and after the implementation of the proposed MLP-based security measures against RPL selective forwarding attacks [20].

3.5.3. Average Radio Duty Cycle During Attack

The bar chart (Figure 12), entitled “Average Radio Duty Cycle,” provides an integral baseline for the study's aim, captures the duty cycle dynamics of the network's nodes under standard operating conditions, as simulated within the Cooja environment, prior to the introduction of selective forwarding attacks within an RPL protocol framework. The chart discriminates between 'Radio listen' and 'Radio transmit' duties, denoted by blue and red bars, across nodes labeled from 2 to 21, with an indication of additional data points beyond the visible scope. The duty cycle percentages are calibrated on the vertical axis, culminating at 47.5%. The data illustrates a pre-attack scenario where nodes demonstrate a variable yet distinct distribution of listening and transmitting activities, with the latter being more prevalent. The most pronounced activity is observed in the last visible node, with transmission duty peaking near 45%, suggesting heightened communication activity or data routing. This foundational data serves as a comparative framework for assessing the efficacy of the proposed MLP-based deep learning model in detecting and mitigating the impact of selective forwarding attacks, thereby enhancing IoT security within RPL networks.

3.5.4. Network Hops During Attack

Upon the execution of a selective forwarding attack within the RPL-based IoT network, a marked deviation in the hop count from the baseline established in Figure 13 was observed. The attack's impact, intended to disrupt the standard routing topology, is hypothesized to manifest as an alteration in the distribution of ‘Last Hop’ and ‘Average Hops’, which were previously recorded under normal simulation conditions. In a typical scenario, one might expect to see an increased average hop count if the network compensates for the attack by rerouting traffic through non-compromised nodes, potentially inflating the 'Average Hops' metric. Conversely, a decrease in the 'Last Hop' value might occur if the attack creates shortcuts in the network by maliciously dropping packets or redirecting traffic. This chart will serve as a cornerstone for analyzing the resilience of the network and the efficacy of the proposed MLP-based defense mechanism, as an atypical hop count distribution post-attack would be indicative of the selective forwarding attack's disruptive influence on network traffic patterns. Subsequent figures will delineate these changes, providing empirical evidence of the attack's consequences and the deep learning model's capability to mitigate such threats.

3.5.5. Historical Power Consumption During Attack

The line graph presented in Figure 14 is a critical depiction of the power usage across network nodes during a selective forwarding attack. The temporal axis, delineated in increments, captures the power consumption patterns at precise intervals. Concurrently, the vertical axis measures the nodes' energy expenditure in milliwatts. The individual lines, each corresponding to a distinct node identified by labels such as 1 through 21, reveal a notable trend of increasing power consumption during the attack period. This escalation in energy demand can be attributed to the network's attempt to mitigate the attack's impact, possibly through heightened retransmission efforts and increased routing computations.

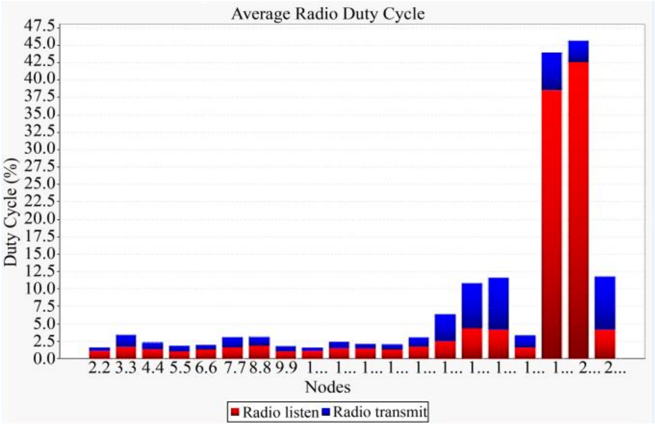

Fig. 12 Average Radio duty cycle during attack simulation

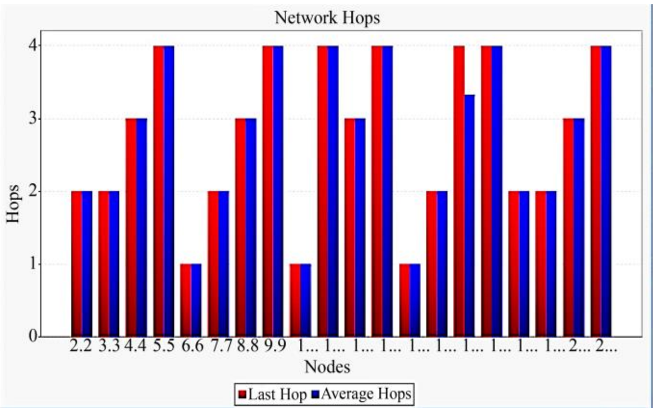

Fig. 13 Network Hops during attack simulation

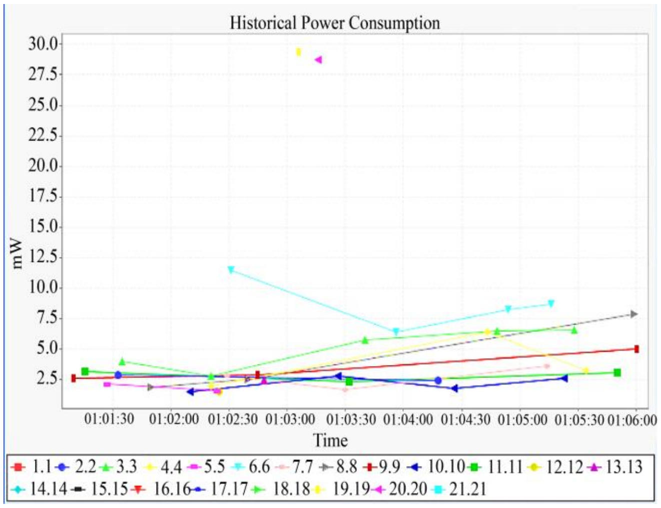

Fig. 14 Historical power consumption during attack simulation

The graph serves as a quantitative testament to the attack's influence, showcasing the direct correlation between the security incident and the network's power utilization [21]. Such data is indispensable for understanding the ramifications of cyber-attacks on the operational efficiency and sustainability of IoT networks, further emphasizing the significance of developing advanced deep learning techniques for energy-conscious security solutions**.**

3.5.6. Beacon Interval During Attack

The "Beacon Interval" graph, as given below (Figure 15), delineates the temporal dynamics of beacon signal emissions across various nodes within an RPL-controlled IoT network during a cyber-attack. The x-axis chronologically catalogues the time, displaying the fluctuations in beacon intervals. Meanwhile, the y-axis enumerates the interval length in seconds. The distinct colored lines represent individual nodes, labeled from 1 to 21, each marking the time interval between consecutive beacons. Notably, the intervals for several nodes show a substantial increase, potentially indicating a response to network disruptions caused by the attack. This could suggest attempts to establish new routing paths or compensate for packet losses.

Conversely, certain nodes exhibit a reduction in interval lengths, which might imply a state of network congestion or heightened signaling due to rerouting attempts. The depicted variances in beacon intervals provide insight into the network's adaptive mechanisms in response to the security breach and underscore the necessity of employing sophisticated detection algorithms to maintain network stability and efficiency. This graph will serve as a benchmark to evaluate the performance of the proposed deep learning model in detecting anomalies and preserving the integrity of communication within the network amidst such adversities.

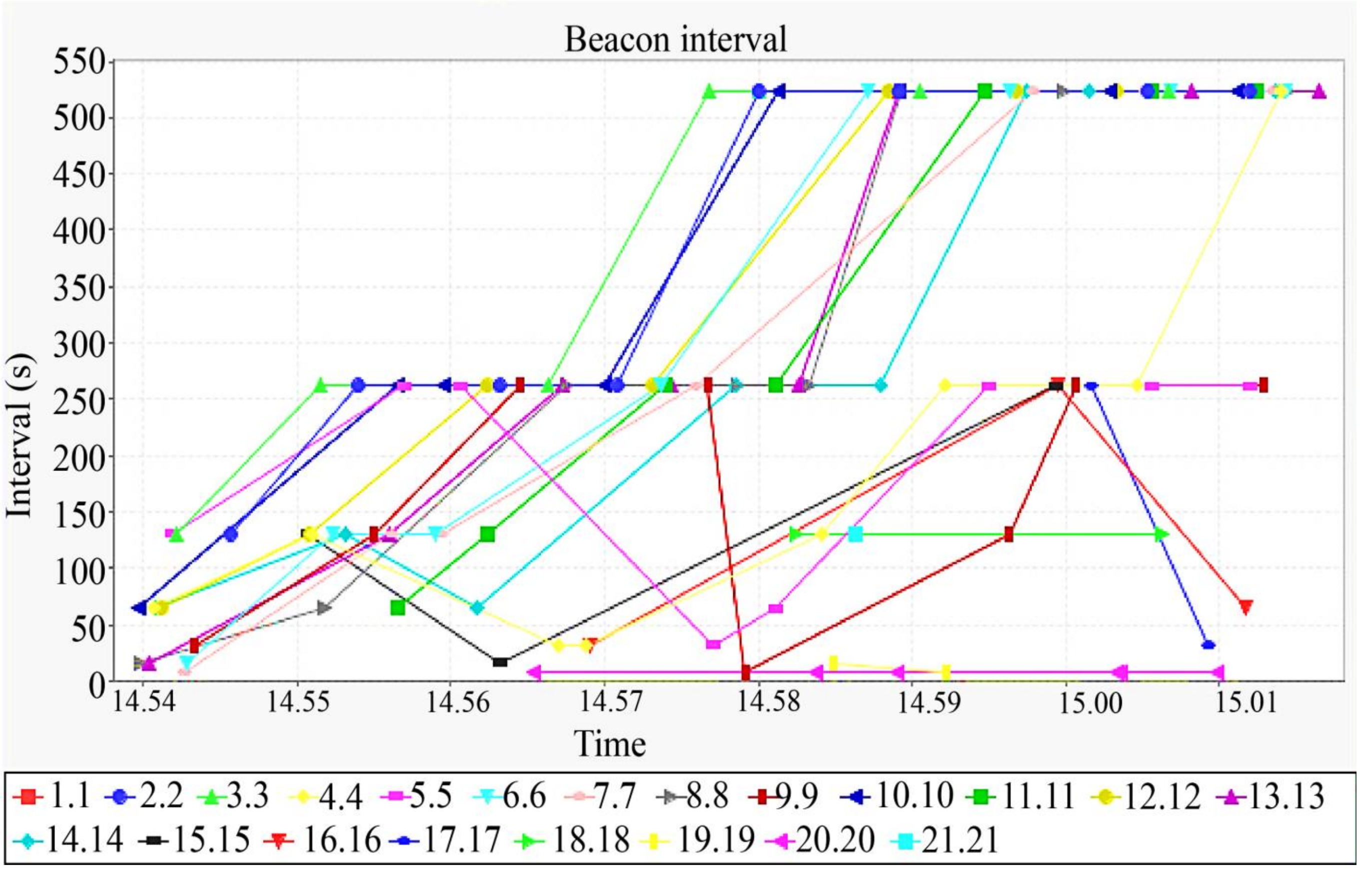

Fig. 15 Beacon interval during attack simulation

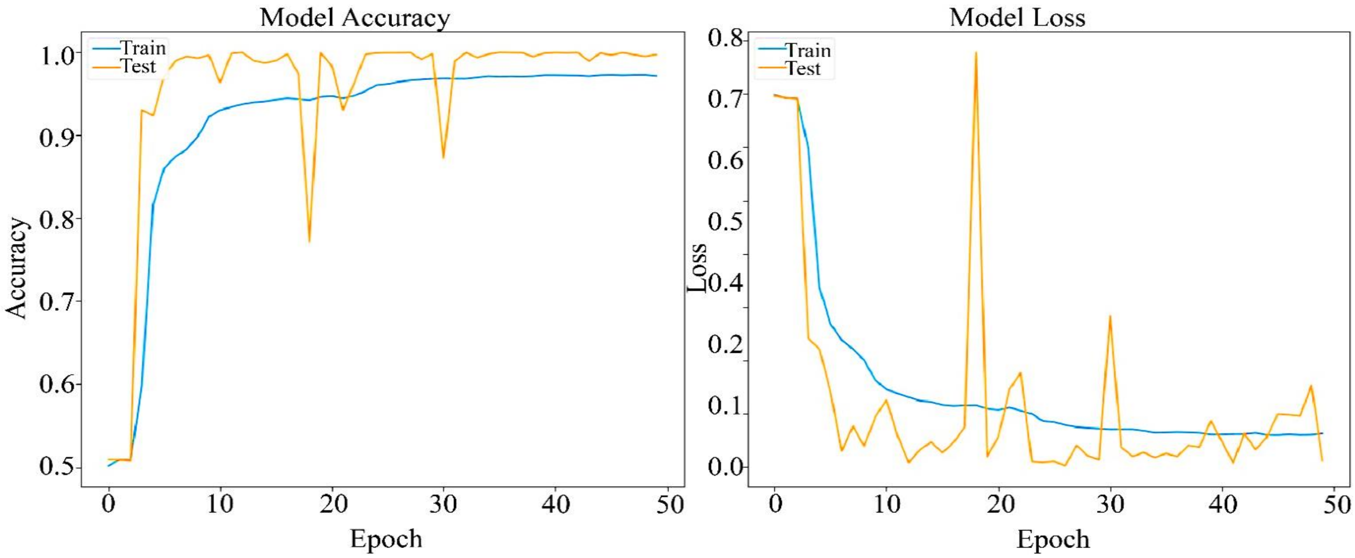

Fig. 16 Model accuracy and loss (50 Epochs)

4. Results and Discussion

4.1. Model Accuracy and Loss in 50 Epochs

As shown in Figure 16, The performance metrics achieved by the model are quite promising, with the training accuracy reaching a commendable 95.68%. This high level of accuracy is indicative of the model's sophisticated learning capabilities and its effectiveness in recognizing complex patterns within the training dataset. Such a high degree of accuracy is reflective of a well-tuned model that has successfully captured the underlying data distribution and suggests a strong predictive power. The test accuracy, despite exhibiting some fluctuations, generally trends closely with the training accuracy, which is a strong indicator of the model’s generalization abilities [22]. These fluctuations can be viewed as a normal occurrence in the training of deep learning models, particularly when dealing with complex and noisy real-world data. The proximity of test accuracy to the high training accuracy further underscores the robustness of the model, as it demonstrates that the learned representations are not merely overfitting to the training data but are also effective on unseen data. Furthermore, the loss curves provide additional insights. The initial spike in test loss, quickly followed by a reduction, can be interpreted as the model adjusting to the nuances of the test set, which is often an expected part of the learning process when the model encounters new patterns that are not present in the training set, Analyzing the extended training performance, the model exhibits a commendable level of accuracy, achieving a peak training accuracy of 98.95%. This high degree of precision illustrates the model's effective learning and generalization capabilities, as it indicates a profound understanding of the training data's inherent patterns.

4.2. Model Accuracy in 1400 Epochs

The consistency with which the model sustains near-perfect accuracy over 1,400 epochs, as shown in Figure 17, is particularly noteworthy. Such enduring performance suggests that the model is not only well-calibrated but also resilient to overfitting, a common challenge in deep learning.

The test accuracy closely parallels the training accuracy, displaying negligible divergence throughout the training duration, which corroborates the model's robustness and its adeptness in handling unseen data. Moreover, the rapid attainment of high accuracy levels and their subsequent maintenance across the epochs underscore the model's efficiency [23]. The ability to sustain such accuracy over an extensive period without degradation signifies a well-designed neural network structure and optimized hyperparameters tailored to the complexities of the task at hand [24].

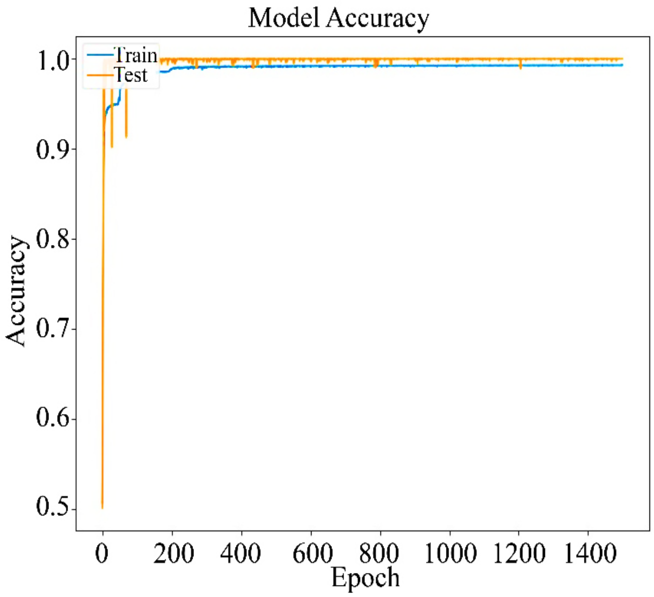

Fig. 17 Model accuracy (1400 Epochs)

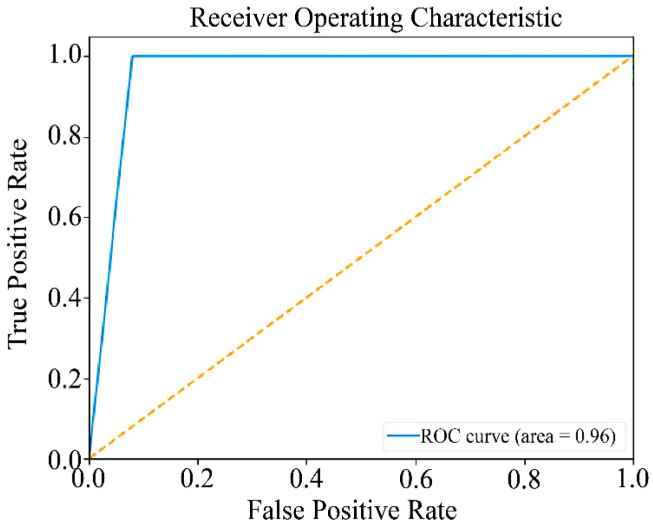

Fig. 18 Model ROC graph

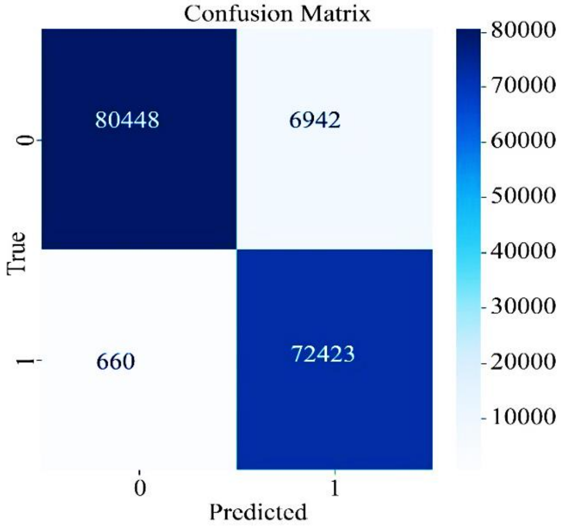

Fig. 19 Model confusion matrix

The model's achievement of 98.95% accuracy is a clear indicator of its suitability for deployment in environments where high reliability and precision are critical, such as in the domain of IoT security [25]. This performance level instills confidence in the model's potential to identify and mitigate selective forwarding attacks, thereby reinforcing the security framework of IoT networks [26].

4.3. Model Receiver Operating Characteristic (ROC)

The Receiver Operating Characteristic (ROC) curve provided in Figure 18 indicates an excellent model performance, with the Area Under the Curve (AUC) being 0.96. This value is very close to the ideal score of 1.0, reflecting the model's strong discriminative ability between the positive class (successful attack detection) and the negative class (correct rejection of non-attack scenarios) [27]. An AUC of 0.96 means that there is a 96% chance that the model will be able to distinguish between a true positive and a true negative outcome [28]. This high score demonstrates the efficacy of the model in correctly identifying instances of selective forwarding attacks while minimizing the rate of false positives, which is crucial in maintaining integrity and trust in an IoT network security system [12][18]. The steep rise of the ROC curve towards the upper left corner also suggests that the model achieves a high true positive rate with a very low false positive rate, which is ideal in security applications where the cost of missing an attack (false negative) is high.

4.4. Model Confusion Matrix

The confusion matrix, as shown in Figure 19, presents an informative visualization of the model's classification performance. From the matrix, several important metrics can be extracted:

True Negatives (TN): 80,448 instances were correctly classified as non-attacks.

False Positives (FP): 6,942 instances were incorrectly classified as attacks when they were not.

False Negatives (FN): 660 instances were incorrectly dismissed as non-attacks when they were actual attacks.

True Positives (TP): 72,423 instances were correctly identified as attacks. The large number of true positives and true negatives indicates that the model is quite adept at correctly classifying both attack and non-attack events. The relatively low number of false negatives is particularly noteworthy, as it implies that the model is very effective at identifying the majority of the attacks, which is critical for IoT network security to prevent malicious activities from going undetected.

5. In-depth Analysis of Attaining Exceptional Outcomes

The proposed research utilizes a framework based on Multilayer Perceptron (MLP) to tackle the unique issue of selective forwarding attacks in IoT networks. The excellence of the approach can be ascribed to certain crucial factors:

5.1. Concentrated Approach

The research focuses on selective forwarding attacks, whereas earlier efforts either did not provide extensive simulation data or employed deep learning in a more generic setting. By focusing on this specific menace, the MLP framework is customized to identify the distinct patterns linked to these assaults. By concentrating on this aspect, the process of selecting features and preprocessing data is refined in order to improve the accuracy of detection.

5.2. Extensive Simulation Environment

The utilization of the Cooja Simulator offered a sturdy basis for simulating authentic IoT scenarios. The simulation encompassed intricate setups that accurately replicate actual IoT network settings, including diverse node densities, communication patterns, and attack scenarios. By generating a dataset that is both precise and adaptable, the MLP model has the potential to acquire knowledge from a diverse variety of situations, hence enhancing its capacity to apply that knowledge to new scenarios and increasing its resilience.

5.3. Improved Feature Engineering

The chosen network elements strongly indicate selective forwarding attacks. The attributes encompassed packet delivery ratios, node energy usage, and routing path alterations, among other factors. By prioritizing these crucial signs, the MLP model can better distinguish between normal and harmful actions, resulting in increased detection rates.

5.4. Advanced Multilayer Perceptron (MLP) Design and Training

The MLP model was designed with the inclusion of numerous hidden layers and neurons, enabling it to capture intricate non-linear correlations present in the data effectively. In addition, the utilized sophisticated training methods like dropout, L2 regularization, and the Adam optimizer. These strategies mitigated overfitting and ensured the model's ability to sustain high performance on unseen data. In addition, The training program involved thorough cross-validation to enhance the model's dependability and precision.

5.5. Comprehensive Assessment Criteria

The model utilises an extensive range of measures, such as accuracy, precision, recall, F1-score, and the Area Under the ROC Curve (AUC). This comprehensive assessment offered a comprehensive perspective on the model's performance, showcasing its superiority over current methodologies that frequently relied on a restricted range of criteria. The findings of The study demonstrated that the framework, based on Multilayer Perceptron (MLP), achieved superior accuracy in detecting threats and showed enhanced adaptability to shifting circumstances.

5.6. Taking into Account Practical Limitations and Restrictions in Real-Life Situations

The framework was specifically built to be lightweight and efficient, taking into account the practical limits of IoT devices, such as computing power and energy consumption. The intricacy of the model did not impede its implementation in contexts with limited resources, rendering it viable for practical applications. The implementation of a targeted approach addresses the limitations, a comprehensive simulation environment, improved feature engineering techniques, advanced design of the Multilayer Perceptron (MLP), rigorous assessment metrics, and the inclusion of real-world restrictions.

This comprehensive strategy guarantees a strong and flexible security solution for IoT networks, greatly enhancing the current level of expertise in identifying and reducing selective forwarding threats.

6. Conclusion

In summarizing the investigation into enhancing IoT network security via a Multilayer Perceptron (MLP)-based deep learning strategy, we have made significant strides in identifying and mitigating selective forwarding attacks. Through comprehensive simulation, meticulous data preprocessing, and rigorous MLP model tuning, the findings not only demonstrate the model's high accuracy in threat detection but also its potential scalability and adaptability in the face of evolving cyber threats and complex IoT environments.The empirical validation showcases the model's efficacy, underlining its practical applicability and adaptability to diverse IoT architectures and evolving cyber threats. Looking forward, the integration of the model into real-world IoT settings opens avenues for addressing operational challenges and leveraging emerging AI advancements to refine accuracy and efficiency further. The potential of this research extends into developing a robust IoT security framework that combines advanced AI-based detection with comprehensive cybersecurity measures, aiming for a proactive and resilient defense against current and future threats. Despite the higher false positive rates, which are a common trade-off in predictive modeling, the model maintains a commendable balance between sensitivity and specificity, crucial for practical deployment in IoT security. This work lays a foundational stone for future endeavors in IoT cybersecurity, calling for collaborative exploration in AI and deep learning to secure the increasingly interconnected digital ecosystems. With the continuous expansion of IoT applications, the urgency for innovative, adaptive cybersecurity solutions is paramount. The research encourages further innovation, aiming to safeguard the IoT infrastructure for future generations.

Acknowledgement

First and foremost, I express my deepest gratitude to God for bestowing upon me the fortitude and resilience required to surmount all challenges encountered during this research. Secondly, I extend my sincere appreciation to the esteemed members of the Laboratory of Research Watch for Emerging Technologies (VETE), whose contributions, both direct and indirect, have been indispensable to the completion of this manuscript. In conclusion, my heartfelt thanks are particularly directed towards Prof. Abdelmajid Hajami, under whose expert guidance and supervision this study was brought to fruition.

References

[1] Ruth Ande et al., “Internet of Things: Evolution and Technologies from a Security Perspective,” *Sustainable Cities and Society*, vol. 54, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Abhishek Khanna, and Sanmeet Kaur, “Internet of Things (IoT), Applications and Challenges: A Comprehensive Review,” *Wireless Personal Communications*, vol. 114, pp. 1687-1762, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Cristina Stolojescu-Crisan, Calin Crisan, and Bogdan-Petru Butunoi, “An IoT-Based Smart Home Automation System,” *Sensors*, vol. 21, no. 11, pp. 1-23, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Usman Tariq et al., “A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review,” *Sensors*, vol. 23, no. 8, pp. 1-46, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Hussam Shamseldin Zenalabdin, Abudhahir Buhari, and Tadiwa Elisha Nyamasvisva, “Performance Analysis of IoT Protocol Stack over Dense and Sparse Mote Network Using COOJA Simulator,” *The 2nd Joint International Conference on Emerging Computing Technology and Sports*, Bandung, Indonesia, vol. 1529, pp. 1-8, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Jun Jiang, and Yuhong Liu, “Secure IoT Routing: Selective Forwarding Attacks and Trust-Based Defenses in RPL Network,” *arXiv*, pp. 1-12, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Haitham Y. Adarbah et al., “Security Challenges of Selective Forwarding Attack and Design a Secure ECDH-Based Authentication Protocol to Improve RPL Security,” *IEEE Access*, vol. 11, pp. 11268-11280, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Behnam Farzaneh et al., “An Anomaly-Based IDS for Detecting Attacks in RPL-Based Internet of Things,” *2019 5th International Conference on Web Research*, Tehran, Iran, pp. 61-66, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] Andrea Agiollo et al., “DETONAR: Detection of Routing Attacks in RPL-Based IoT,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1178-1190, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Nitin Shivaraman, “*Clustering-Based Solutions for Energy Efficiency, Adaptability and Resilience in IoT Networks*,” IGS Theses, Nanyang Technological University, pp. 1-144, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Amsale Zelalem Bayih et al., “Utilization of Internet of Things and Wireless Sensor Networks for Sustainable Smallholder Agriculture,” *Sensors*, vol. 22, no. 9, pp. 1-31, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mudhafar Nuaimi, Lamia Chaari Fourati, and Bassem Ben Hamed, “Intelligent Approaches Toward Intrusion Detection Systems for Industrial Internet of Things: A Systematic Comprehensive Review,” *Journal of Network and Computer Applications*, vol. 215, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Abujassar Radwan, “Improving Energy Efficiency Using IoT Technology through the Development of a Smart Network Clustering Path Determined by the Distance between Nodes,” *Research Square*, pp. 1-35, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Alazab Ammar et al., “Routing Attacks Detection in 6LoWPAN-Based Internet of Things,” *Electronics*, vol. 12, no. 6, pp. 1-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Pintu Kumar Sadhu, Venkata P. Yanambaka, and Ahmed Abdelgawad, “Internet of Things: Security and Solutions Survey,” *Sensors*, vol. 22, no. 19, pp. 1-51, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Mohammad Al-Fawa’reh et al., “MalBoT-DRL: Malware Botnet Detection Using Deep Reinforcement Learning in IoT Networks,” *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 9610-9629, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Rashmi Sahay, G. Geethakumari, and Barsha Mitra, “A Novel Network Partitioning Attack Against Routing Protocol in Internet of Things,” *Ad Hoc Networks*, vol. 121, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Anum Talpur, and Mohan Gurusamy, “Machine Learning for Security in Vehicular Networks: A Comprehensive Survey,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 346-379, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Syeda M. Muzammal, Raja Kumar Murugesan, and N.Z. Jhanjhi, “A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-Based Approaches,” *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4186-4210, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Jarmouni Ezzitouni et al., “Management of Battery Charging and Discharging in a Photovoltaic System with Variable Power Demand Using Artificial Neural Networks,” *The 4th International Conference of Computer Science and Renewable Energies*, vol. 297, pp. 1-5, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Rubén Juárez, and Borja Bordel, “Augmenting Vehicular Ad Hoc Network Security and Efficiency with Blockchain: A Probabilistic Identification and Malicious Node Mitigation Strategy,” *Electronics*, vol. 12, no. 23, pp. 1-35, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Mohamed Massaoudi et al., “A Novel Stacked Generalization Ensemble-Based Hybrid LGBM-XGB-MLP Model for Short-Term Load Forecasting,” *Energy*, vol. 214, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] Ishak Pacal, “A Novel Swin Transformer Approach Utilizing Residual Multi-Layer Perceptron for Diagnosing Brain Tumors in MRI Images,” *International Journal of Machine Learning and Cybernetics*, pp. 1-46, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] Lei Deng et al., “Model Compression and Hardware Acceleration for Neural Networks: A Comprehensive Survey,” *Proceedings of the IEEE*, vol. 108, no. 4, pp. 485-532, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[25] Shahid Allah Bakhsh et al., “Enhancing IoT Network Security through Deep Learning-Powered Intrusion Detection System,” *Internet of Things*, vol. 24, pp. 1-36, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] Seyed-Ahmad Ahmadi et al., “Modern Machine-Learning Can Support Diagnostic Differentiation of Central and Peripheral Acute Vestibular Disorders,” *Journal of Neurology*, vol. 267, pp. 143-152, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] Ezzitouni Jarmouni et al., “The Implementation of an Optimized Neural Network in a Hybrid System for Energy Management,” *International Journal of Power Electronics and Drive Systems*, vol. 15, no. 2, pp. 815-823, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[28] Theogene Rizinde, Innocent Ngaruye, and Nathan D. Cahill, “Comparing Machine Learning Classifiers for Predicting Hospital Readmission of Heart Failure Patients in Rwanda,” *Journal of Personalized Medicine*, vol. 13, no. 9, pp. 1-20, 2023. [CrossRef] [Google Scholar] [Publisher Link]