International Journal on
“Technical and Physical Problems of Engineering”
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

June 2024 | Issue 59 | Volume 16 | Number 2 | Pages 175-184

NEURAL NETWORK-BASED DETECTION MECHANISM AGAINST RPL DIS FLOODING ATTACKS IN IOT NETWORKS

A. Krari [1] A. Hajami [1] E. Jarmouni [2] K. Errakha [3]

1. Laboratory of Research Watch for Emerging Technologies (VETE), Faculty of Sciences and Technology, Hassan I University, Settat, Morocco, ayoub.krari@uhp.ac.ma, abdelmajid.hajami@uhp.ac.ma
2. Laboratory of Radiation-Matter and Instrumentation (RMI), Faculty of Sciences and Technology, Hassan I University, Settat, Morocco, e.jarmouni@uhp.ac.ma
3. Laboratory of Computer, Networks, Mobility and Modeling (IR2M), Faculty of Sciences and Technology, Hassan I University, Settat, Morocco, kaoutar.errakha@uhp.ac.ma

Abstract- This paper introduces a cutting-edge security mechanism specifically developed for Internet of Things (IoT) networks, aiming to counteract RPL Protocol Destination Information Solicitation (DIS) flooding attacks. Motivated by the urgent need to enhance IoT security against such sophisticated cyber threats, the research focuses on leveraging Artificial Neural Networks (ANNs) for creating a robust detection system. The objective is to efficiently differentiate between normal network behavior and malicious flooding attempts, thereby safeguarding IoT networks. The methodology adopted involves a comparative analysis of three different machine and deep learning algorithms. These algorithms are meticulously tested and evaluated to determine their effectiveness in the context of detecting DIS flooding attacks. This comparative approach not only provides a comprehensive understanding of each algorithm's performance but also identifies the most efficient technique for real-world application. Results from extensive simulations demonstrate the system's capability to accurately identify RPL Protocol DIS flooding attacks with high accuracy and minimal false positives. The performance of each tested algorithm is thoroughly compared, highlighting their respective strengths and limitations in the context of IoT security. The urgency of this research is underscored by the rapid expansion of IoT networks and the corresponding escalation in security challenges. The significance of the work lies in its contribution to IoT security, offering a novel solution to a specific yet critical issue. Moreover, this research lays the groundwork for future advancements in IoT security, emphasizing the need for intelligent and adaptive security mechanisms in our increasingly connected world. The paper concludes by emphasizing the proactive and intelligent security layer provided by the proposed mechanism, enhancing the overall resilience of IoT networks against these specific types of attacks.

Keywords: Artificial Neural Networks, DIS Flooding Attacks, Internet of Things, RPL Protocol, Security.

1. INTRODUCTION

The Internet of Things (IoT) has experienced rapid growth as it connects an ever-expanding array of devices, generating vast amounts of data. The global IoT network now links billions of devices [1], with that number projected to reach 26 billion by 2030 [2]. Each object within this network possesses a unique ID and communicates with other smart devices [2]. However, this massive proliferation of connected devices presents significant challenges, particularly concerning the security of smart devices and the overall IoT network. Another pressing issue faced by the IoT security research community involves addressing the limitations of power devices, which are often battery-based [3].

The resource-constrained nature of smart devices in the Internet of Things makes traditional security mechanisms like cryptography and authentication unsuitable for addressing IoT security challenges [4]. To overcome the security issues, an Intrusion Detection System has been proposed as an energy-efficient and accurate security mechanism to detect routing attacks. IDS not only strives to maintain robust security but also does so in an energy-efficient manner, thereby addressing a key concern that arises due to the limited power resources of IoT devices. By employing advanced techniques in anomaly detection and behavior analysis, IDS aims to ensure a level of security that is commensurate with the dynamic and ever-evolving threat landscape that accompanies the expansion of the IoT.

The explosive growth of the Internet of Things has engendered a labyrinthine network of interconnected devices, replete with the potential for immense data generation and exchange. While this interconnectedness heralds a new era of technological advancement, it also ushers in a host of challenges, particularly in the realm of security and energy efficiency. The proposed utilization of Intrusion Detection Systems tailored for the unique characteristics of IoT devices holds promise as an astute measure to grapple with these challenges, thereby fostering a safer and more sustainable IoT landscape.

Registered: 230924 Article Info: 1795 Accepted: 240524
Reserved: 240118 Available: 240630

The Routing Protocol for Low-Power and Lossy Networks is responsible for IoT network routing [5], forming DODAGs trees to connect IoT devices [5]. Due to the limitations in memory, communication, processing, and power consumption of IoT objects, 6LoWPAN protocols are essential [5]. However, RPL is susceptible to various attacks, including the threatening Direct DIS Flooding attack, which aims to drain power and energy from smart devices, rendering IoT services unavailable [6]. This paper focuses on the DIS Flooding attack, discussing, explaining, and simulating it with different scenarios. Additionally, a machine learning-based IDS model is proposed to prevent and detect this simulated attack. The IDS system offers a trust-based secure solution, strengthening the security of the RPL protocol.

This paper makes a significant contribution to IoT security by presenting a unique machine and deep learning-based Intrusion Detection System (IDS), specifically designed to address RPL Protocol DIS Flooding attacks. Its distinctive approach lies in the comparative analysis of three varied machine and deep learning algorithms, a method not extensively explored in existing research. This analysis not only bolsters security measures but also attentively considers the energy constraints of IoT devices, a vital aspect often overlooked in other studies. The practical application of these algorithms is further validated through rigorous real-world simulations, distinguishing this research in its field. By integrating a trust-based security mechanism, the paper advances the IDS framework, adding a novel layer of protection. This comprehensive approach positions the paper as a pivotal contribution to both the advancement of IoT security and the efficient management of IoT device energy resources.

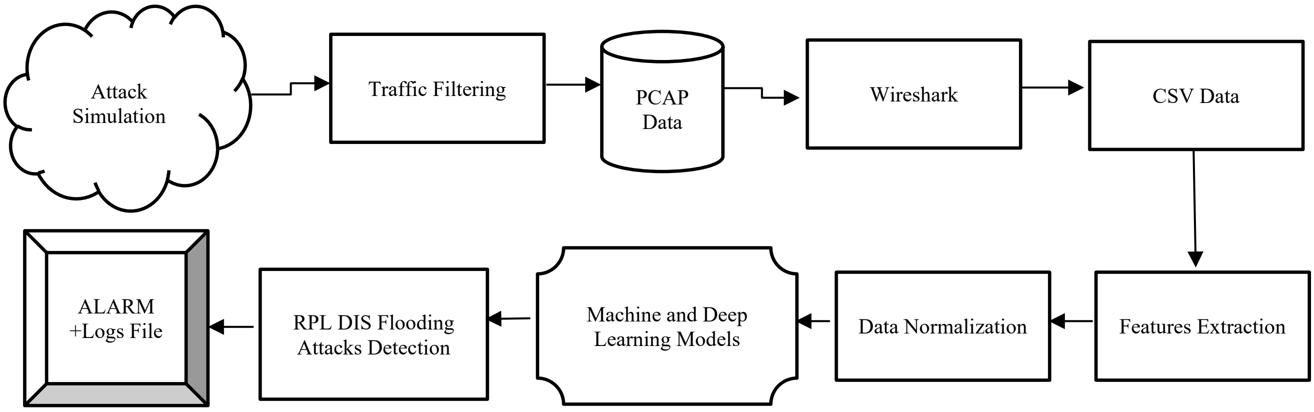
2. PROPOSED SOLUTION

2.1. Solution Description

In our study, we conducted simulations of the DIS attack to obtain malicious data and then simulated the expected behavior of nodes to obtain benign data for our proposed model. The PCAP analyzer in the Cooja open-source simulator was employed to transform the data into a PCAP file [7], which was subsequently converted into a CSV file using Wireshark's simulator [8]. For data preprocessing, we utilized Python libraries, specifically NumPy and pandas, to clean and prepare the data before feeding it into our machine learning model. Figure 1 and Table 1 illustrates our neural network-based approach designed for detecting DIS attacks, where the data is encoded, tagged, and divided into training and testing sets. Each of these stages is discussed in detail in the subsequent sections of this study.

Table 1. Proposed solution step by step

Step Number	Description
Step No. 1	Start the simulation
Step No. 2	Perform the simulation with 3 different scenarios and collect the data
Step No. 3	Generate the .PCAP file using 6LoWPAN packet analyzer
Step No. 4	Open the .PCAP files in Wireshark for analysis
Step No. 5	Convert the .PCAP files to .CSV format
Step No. 6	Pre-process the data to prepare it for machine learning models
Step No. 7	Apply resampling techniques to create training and test sets
Step No. 8	Utilize Machine and Deep Learning algorithms to classify attacks and benign packets
Step No. 9	Develop LSTM, SVM, and DNN models for detecting DIS attacks
Step No. 10	Implement pseudo code to stop the Machine and Deep Learning phase and generate the three detection models for IoT environment attacks
Step No. 11	Send alarms to administrators along with log files to alert them of potential attacks



2.2. The Proposed Solution Steps

- Data Preparation: The dataset, containing both malicious and benign rows obtained from the DIS attack simulations, is prepared for further analysis.
- Machine and Deep Learning Phase: The prepared dataset is then used to train three different models: Long Short-Term Memory LSTM, Support Vector Machine SVM, and Deep Neural Network DNN. These models are trained through multiple processing and training steps.
- Model Creation: After completing the training process, the Machine and Deep Learning models are created, ready for the DIS detection procedure.

- DIS Detection Procedure: The trained models are applied to detect DIS attacks in the dataset. The detection procedure runs on the data to identify and classify potential attacks.
- Testing and Evaluation: The performance of the Machine and Deep Learning models in detecting DIS attacks is tested and evaluated to measure their accuracy and effectiveness.

The proposed approach outlines a systematic process to simulate DIS attacks, collect data, preprocess it, and apply Machine and Deep Learning models to detect and classify attacks and benign packets. The result consists of LSTM, SVM, and DNN models for detecting DIS attacks in an IoT environment. Alarms with accompanying log files are sent to administrators to ensure timely response and mitigation of potential threats.

2.3. DIS Attack Simulation and Analysis

2.3.1. Simulation Phase

In this phase, our objective is to generate the necessary data traffic, which will then be processed and input into our machine and Deep Learning model for detection purposes. To achieve this, we utilized the Cooja simulator [9] to simulate an IoT network both with and without the DIS Flooding attack. The targeted routing attack, DIS Flooding, was simulated in real-time, and various scenarios were analyzed to create a trustworthy dataset. Following the simulation, we generated a packet capture file, also known as a .PCAP file [10], which was further transformed into a .CSV file using the widely used traffic analyzer, Wireshark. This process ensured that we obtained reliable and suitable data for training and testing our machine and Deep Learning model to detect DIS attacks in the IoT environment.

2.3.1. Normal Simulation and Results

In this study, we utilized the baseline data obtained from normal simulation as shown to create a precise dataset for training our model. This dataset serves as a reference to compare the outcomes of the DIS attack in terms of power consumption, traffic data, and lost packets. By establishing a basic reference network, we were able to collect the necessary data required for our research.

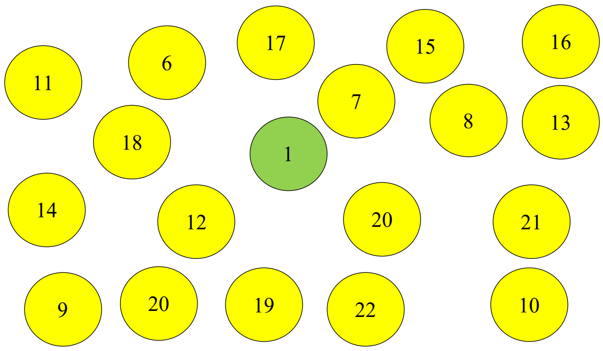


Figure 2. Normal IoT network map In Cooja

The primary objective was to gain insights into the impact of a malicious node within the regular network topology when implementing the DIS attack. By comparing the behavior of the network under normal conditions with the network's response during the attack, we aimed to understand the consequences and implications of the malicious node's actions. The configuration and the map of simulation are shown in Figure 2 and Table 2.

Table 2. Simulations configurations

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	100m×100m
MTU Size	1280Byte
Simulation Duration	60 minutes
No. of Sender Nodes	20
No. of Sink Node1	1
No. of repetitions	3

The purpose is to provide the unattached baseline data so that additional DIS attack simulation can be compared to it in terms of power consumption, traffic data, lost packets, and other characteristics. After the foundational reference network has been established, it will be possible to gather the baseline information for the research. It has already been established that our reference for the anticipated behavior of the nodes and all the results we have acquired from the typical simulation without the DIS attack are true. Therefore, DIS attack simulation can utilize its results as a standard. After five runs 1 hour each, our baseline simulations show no lost packets and no re-boots, as shown in Figure 3.

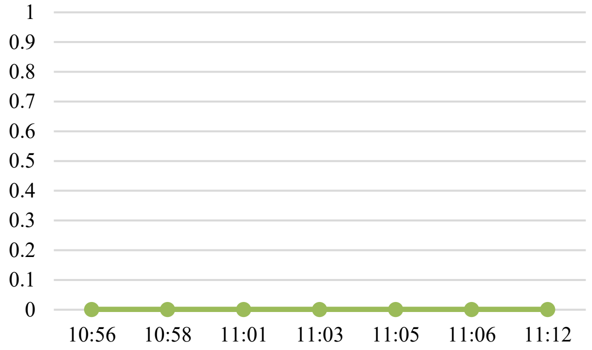


Figure 3. Graphical view of nodes lost packets

Furthermore, the average power also as shown in Figure 4. Consumption for all nodes is close to the mean of 1.074 MW. As can be seen in Figure 5, both radio listening and radio transmission consumes a consistent amount of power, with radio listening using more power than radio. It is evident that the impact of a DIS attack is primarily felt by systems near the infected nodes, particularly those within the attacker's radio range, the study demonstrates transmitting as expected given that nodes receive a variety of control messages throughout DODAG construction.

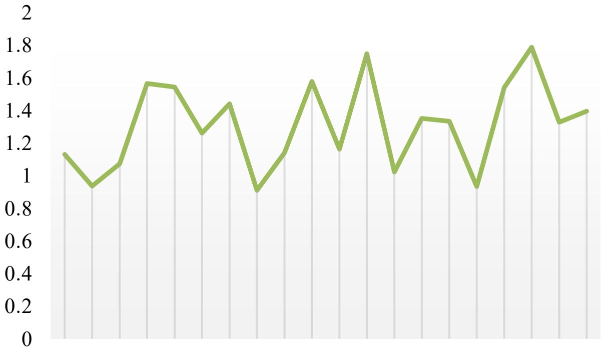


Figure 4. Graphical view of nodes power consumption (mw)

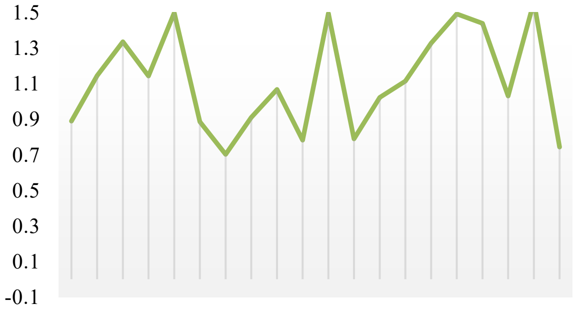


Figure 5. Graphical view of nodes radio consumption

Furthermore, the outcome is favorable when considering the packet loss metric. Throughout the simulation, we had zero packet loss, we adopted these results as our benchmark.

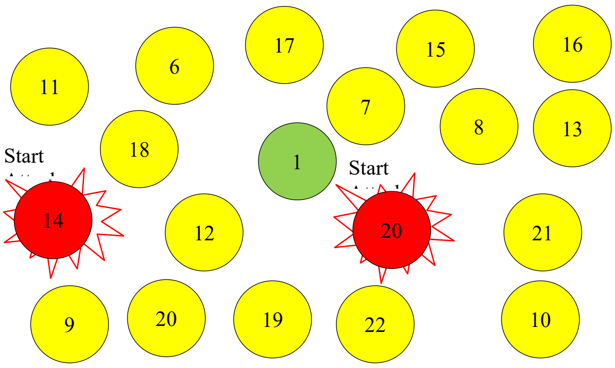


Figure 6. Simulating Malicious DIS attack node in IoT Networks

2.4. DIS Attack Simulation and Results

The DIS attack in this study targets IoT nodes through a flooding strike, intending to overwhelm the nodes and their connections. This type of flooding operation is classified as a denial-of-service attack DoS because its goal is to disrupt the service and disable surrounding nodes and the entire system [11]. Figure 6 illustrates the DIS attack map in the Cooja simulator, featuring two malicious nodes, leading to certain nodes exceeding 45 mw of energy usage. Additionally, both the radio listening and transmission cycles increase, and a total of 23 packets are lost by all nodes (Figure 7) within a 30-minutes timeframe. That nodes near the attacker experience heightened rates of power consumption, radio activity, and packet losses.

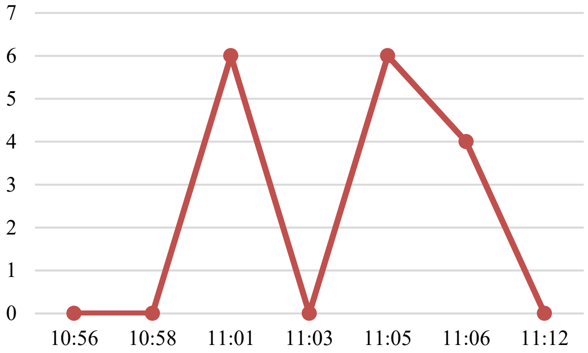


Figure 7. Graphical view of nodes lost packets during DIS attack

The subsequent graphs in Figure 8, 9, and 10 confirm a significant increase in the total energy consumption due to the DIS attack. As the attack commences, neighboring nodes of the malicious node are impacted.

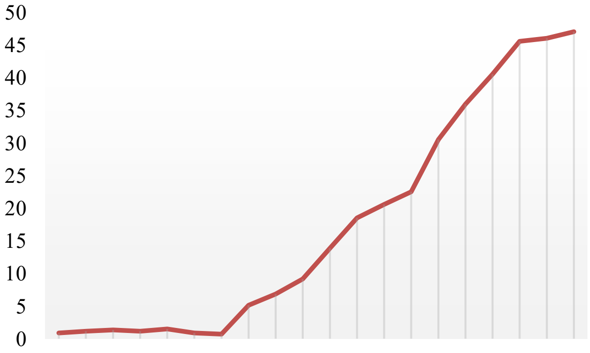


Figure 8. Graphical view of nodes power consumption during DIS attack (mw)

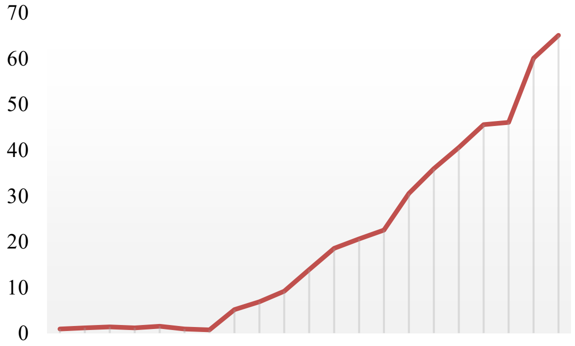


Figure 9. Nodes average lost packets during DIS attack

2.5. Dataset Coding

- Step 1: Dataset Loading and Preprocessing: In this step, we first imported the necessary libraries, including pandas [12], which allows us to efficiently manipulate data. Next, we proceeded to load the dataset from our specified file, which was in the CSV format, into a pandas Data Frame [13]. Then we structured the data in a tabular format, facilitating further processing.
- Step 2: Feature Extraction: Firstly, we computed the "DIS TRANSMISSION RATE / MS" feature, which provides us with valuable information about the rate of transmission of DIS messages per millisecond. This was

achieved by dividing the total number of DIS messages by the total time taken for transmission.

Next, we derived the "TAT" feature, which stands for "Time per Trusted Packet." By dividing the total transmission time by the number of trusted packets, we obtained the average transmission time per trusted packet. This metric offers insights into the efficiency of packet transmission during the RPL DIS attack. Furthermore, we counted the number of DIS control messages present in the dataset. This count was added as the "DIS Count" feature, which quantifies the occurrences of DIS control messages. These messages play a crucial role in understanding the dynamics of the attack. Lastly, we calculated the "TRATE / MS" feature, representing the overall transmission rate per millisecond.

• Step 3: Encoding DIS Control Messages as in Table 3.

Table 3. RPL control messages coding

Packet Information	ID
RPL Control (Destination Advertisement Object)	1
RPL Control (DODAG Information Solicitation)	2
RPL Control (DODAG Information Object)	3
ACK	4

To ensure consistency in data representation and facilitate further analysis, we encoded the various DIS control messages into numerical values. Specifically, we assigned numerical codes (1, 2, 3, and 4) to each type of RPL control message:

- (Destination Advertisement Object)
- (DODAG Information Solicitation)
- (DODAG Information Object), and ACK, respectively

By employing Label Encoding, we transformed these textual message names into corresponding numerical representations.

• Step 4: Saving the Processed Dataset: Upon the completion of feature extraction and encoding, we preserved the processed dataset, which now included the newly calculated features and encoded DIS control messages, we saved this dataset to a new CSV file. This file served as the foundation for our research paper, allowing us to present detailed insights into the RPL DIS attack and its associated features, we have provided a sample of our detection data set in the following Table 4.

Table 4. Sample of Dataset

No.	Time	Source	Destination	Length	Info	TRATE /MS	DIS Transmission Rate / MS	TAT = Total Transmission Time / Transmitted Packets	DIS Count	Label
1	1.301	18	9999	64	2	0.54578524	0.37135408	0.03234392	12983	1
2	0.475	2	9999	64	2	0.04344142	0.01482784	0.00099907	38	0
3	1.31	18	9999	64	2	0.52279605	0.30315553	0.03930165	13032	1
4	0.487	2	9999	64	2	0.04105705	0.01929529	0.00099952	38	0
5	1.318	18	9999	64	2	0.57527982	0.35557002	0.03367008	12893	1
6	0.499	2	9999	64	2	0.04720665	0.01068863	0.00099992	38	0
7	1.326	18	9999	64	2	0.50040472	0.34889721	0.03511814	12655	1
8	0.511	2	9999	64	2	0.04731116	0.01367734	0.00099913	38	0
9	1.334	18	9999	64	2	0.55967325	0.35408939	0.03032713	13230	1
10	1.935	18	9999	64	2	0.53448675	0.314864	0.03748553	13051	1
11	0.475	2	9999	64	2	0.04344142	0.01482784	0.00099907	38	0
12	2.019	18	9999	64	2	0.56908348	0.30152195	0.0375284	13135	1
13	1.935	18	9999	64	2	0.53448675	0.314864	0.03748553	13051	1
14	0.493	2	9999	64	2	0.04024781	0.01198719	0.00099964	38	0
15	0.499	2	9999	64	2	0.04720665	0.01068863	0.00099992	38	0

2.6. Machine and Deep Learning Models

Machine learning is a type of artificial intelligence (AI) that allows computers to learn without being explicitly programmed. Machine learning algorithms are trained on data, and they can then use that data to make predictions or decisions [14]. Deep learning is a subset of machine learning that uses artificial neural networks to learn from data. Artificial neural networks are inspired by the human brain, and they can be used to solve a wide variety of problems, including image recognition, natural language processing, and speech recognition [15]. The inputs, hidden layer, and output are the three main components of a neural network architecture as shown in Figure 10.

• Inputs: The inputs are the data that is fed into the neural network. This data can be anything from images to text to audio [16].

• Hidden layer: The hidden layer is the part of the neural network where the learning takes place. The neurons in the hidden layer learn to extract features from the input data [16].

• Output: The output is the result of the neural network's learning. This output can be a prediction, a classification, or a decision.

The number of inputs, hidden layers, and outputs can vary depending on the problem that the neural network is trying to solve [17].

• Support Vector Machines (SVM): SVM is a supervised machine learning algorithm used for classification tasks, In the context of our work, we used features extracted from network traffic data to train an SVM classifiers work well for binary classification problems, helping us distinguish between normal and attack traffic [18].

• Long Short-Term Memory (LSTM): LSTM is a type of recurrent neural network (RNN) that excels in handling sequential data, we used LSTM to model the temporal patterns in network traffic data, LSTM networks can capture dependencies over time, making them suitable for detecting attack sequences or abnormal traffic patterns for our case [19].

- Deep Neural Networks (DNN): DNNs are a broader category of neural networks that include multiple hidden layers. They are useful for complex pattern recognition and feature extraction, In the context of our work, DNN are employed to automatically learn and extract relevant features from network traffic data [20].

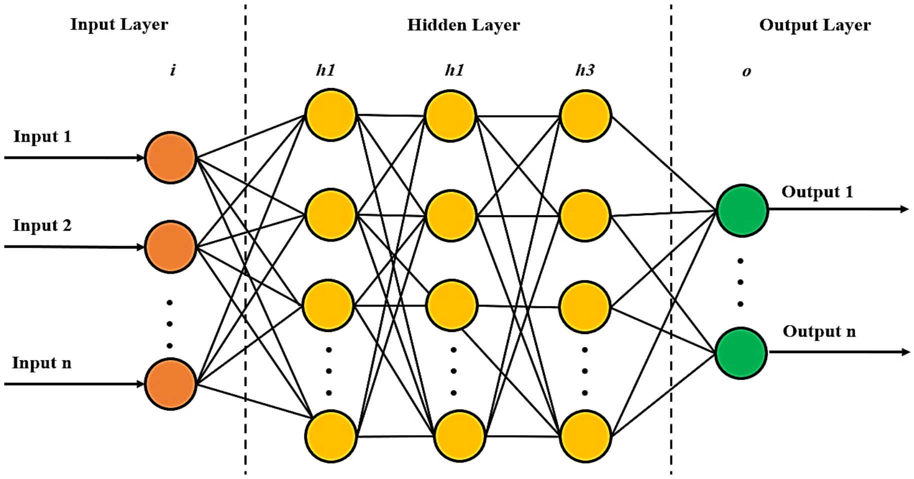


Figure 10. Neural Network Architecture

The strength of each model, namely the Long Short-Term Memory LSTM, Support Vector Machine SVM, and Deep Neural Network DNN, is strategically utilized in the proposed solution. The LSTM model excels at capturing temporal dependencies and patterns, making it particularly adept at handling sequential data prevalent in network traffic [21]. The SVM model, known for its ability to find optimal decision boundaries, complements the LSTM by effectively handling feature classification and separation [22]. Finally, the DNN model, with its deep architecture, is capable of learning intricate representations, enabling it to detect subtle and complex attack patterns [23-24].

Through extensive training with the pre-processed data, each of these models has acquired the ability to distinguish between normal network behavior and abnormal patterns indicative of DIS attacks. Their collective strength and complementary capabilities contribute to the creation of a robust and reliable DIS attack detection approach. By incorporating this combination of machine and deep learning models, the proposed solution becomes a comprehensive defense mechanism against DIS flooding attacks in the IoT environment. Such an advanced defense system ensures the security and integrity of IoT networks, guarding against potential service disruptions and mitigating the damage caused by malicious activities. Importantly, the real-time detection capability of the solution allows for swift and proactive responses to emerging threats, enhancing the overall resilience and protection of IoT infrastructures.

3. RESULTS AND DISCUSSION

3.1. Proposed Solution Outcomes

Our method for detecting DIS attacks in the IoT environment starts with a dataset containing multiple inputs and corresponding outputs, with each class associated with labels (0, 1) denoting normal and attack instances, respectively. During the training phase, the three models (LSTM, SVM, and DNN) are trained using the dataset's inputs and outputs. In this process, a training sample is fed into each model, allowing them to learn and generate predictions for similar data, which are then utilized for classifying the test dataset during the testing phase. Various functions and parameters are employed to construct and optimize the models, ensuring their effectiveness in the proposed solution. To evaluate the accuracy of the models in the classification study, several metrics are employed, including Mean Squared Error M.S.E, Mean Absolute Error M.A.E, Root Mean Squared Error R.M.S.E, and R-Squared R2, also known as the coefficient of determination. These metrics provide valuable insights into the models' performance and their ability to accurately classify the DIS attack dataset.

The initial focus is on the LSTM model, which undergoes rigorous training and evaluation following the process shown in Figure 11. the LSTM model's training and testing R-square errors, RMSE, MSE, and MAE are presented for the binary. Classification of the DIS attack dataset, all of these metrics indicate satisfactory results, confirming the LSTM model's effectiveness in detecting DIS attacks in the IoT environment.

Next, the SVM model is integrated into the analysis, following the same training and evaluation process outlined in Figure 12 The results for the SVM model's training and testing RMSE, MSE, and MAE metrics are illustrated in a graph. These metrics provide crucial insights into the SVM model's performance, demonstrating its accuracy and reliability in detecting and classifying DIS attacks in IoT network.

Additionally, the DNN model is incorporated into the analysis, following the training and assessment procedure depicted in Figure 13 The results for the DNN model's training and testing R-square errors, RMSE, MSE, and MAE metrics are presented in another graph. This visualization showcases the effectiveness of the DNN model in accurately detecting and classifying DIS attacks in the IoT environment, emphasizing its significance in enhancing the security of IoT networks.

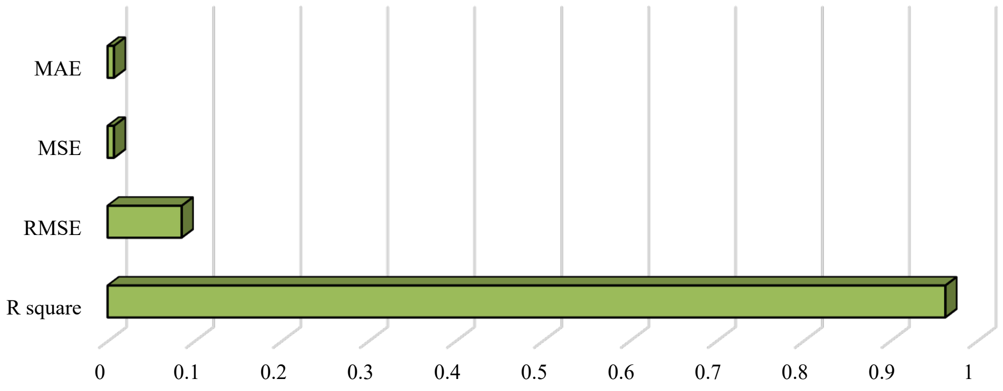


Figure 11. LSTM Model Effectiveness: Graphical Interpretation of Outcomes

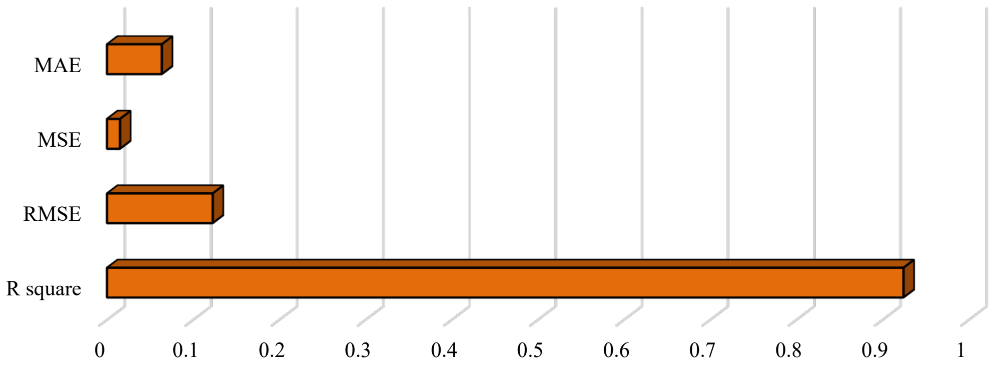


Figure 12. SVM Model Effectiveness: Graphical Interpretation of Outcomes

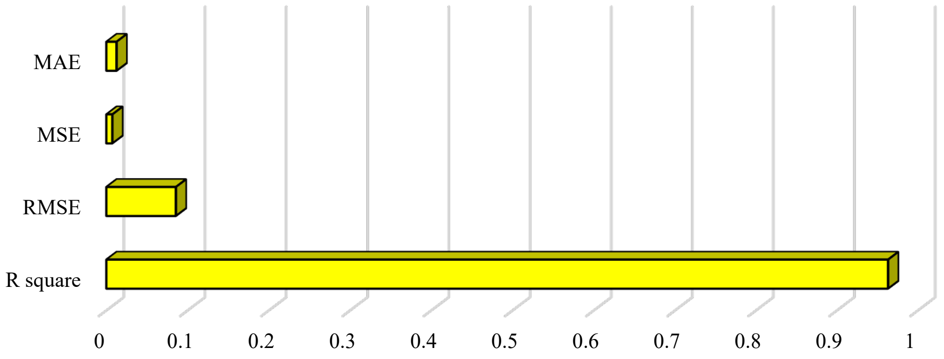


Figure 13. DNN Model Effectiveness: Graphical Interpretation of Outcomes

3.2. Comparison of the Used Models

The effectiveness of the proposed strategy is evaluated by comparing the LSTM model with other models and approaches. Figure 15 presents a performance comparison between the LSTM model and two other models DNN and SVM), illustrating that the LSTM model outperforms them in terms of accuracy, precision, and R-square score. The LSTM model's superior performance highlights its efficacy in accurately detecting and classifying DIS attacks in the IoT environment.

While the LSTM model excels in accuracy and precision, the SVM model demonstrates superiority in terms of training time, measured in epochs, and overall model complexity, including the number of neurons and layers. The SVM model's efficiency in terms of training time and complexity makes it a viable option for certain scenarios where quick response times and simpler model structures are preferred. In conclusion, the LSTM model is the optimal choice when high accuracy and precision are of utmost importance, while the SVM model provides advantages in terms of training time and model complexity in specific use cases. The comparison results aid in selecting the most suitable model for detecting and addressing DIS attacks based on specific requirements and priorities.

Furthermore, we conducted experiments to compare the accuracy of SVM, LSTM, and DNN models, as shown in Figure 14 The experiment data was utilized to evaluate the performance of these three different machine and Deep learning models in terms of categorization accuracy, particularly in the context of resource management. Notably, the results of the experiments indicate that the LSTM classifier significantly outperforms the other models when it comes to identifying DIS attacks. Its superior accuracy in detecting and classifying DIS attacks underscores its effectiveness in providing robust and reliable security solutions for resource constrained IoT environments.

The comparison analysis conclusively underscores the suitability of the Long Short-Term Memory (LSTM) model as the optimal choice for effectively identifying and mitigating Distributed Denial of Service (DIS) attacks within the intricate landscape of Internet of Things (IoT) networks. The LSTM model's ability to capture and comprehend intricate temporal dependencies and patterns within data streams makes it exquisitely attuned to the dynamic and evolving nature of DIS attacks. This level of sophistication empowers IoT networks to not only detect these attacks promptly but also to undertake precise measures for their mitigation.

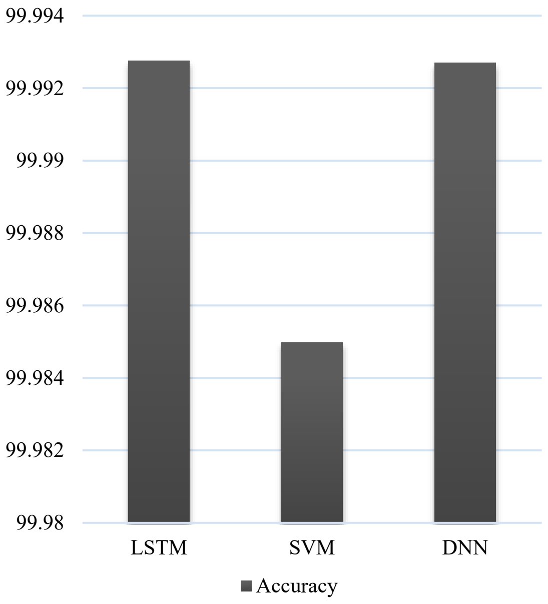


Figure 14. Comparative Analysis of LSTM, SVM, and DNN Accuracy

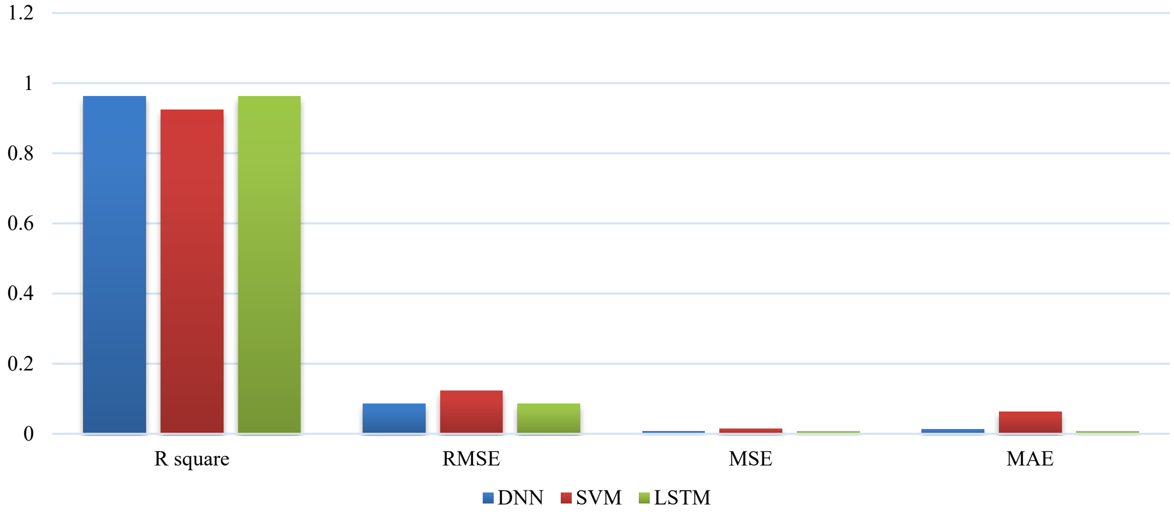


Figure 15. DNN Model Effectiveness: Graphical Interpretation of Outcomes

4. CONCLUSION

In conclusion, this paper introduces a significant advancement in IoT security, featuring a specialized Intrusion Detection System (IDS) designed to detect RPL Protocol DIS Flooding attacks. The meticulous analysis and comparison of three distinct machine and deep learning algorithms not only pinpoint the most effective detection method but also emphasize energy efficiency, crucial for resource constrained IoT devices. This dual focus on robust security and energy conservation is especially pertinent in IoT environments. The proposed IDS model's effectiveness is rigorously validated through extensive real-world simulations and testing, ensuring its practical applicability in authentic IoT scenarios.

Furthermore, the integration of a trust-based security mechanism within the IDS enhances its defensive capabilities against sophisticated cyber threats. For future work, it would be beneficial to explore the scalability of the proposed IDS system across various IoT platforms and network sizes, ensuring its adaptability and effectiveness in diverse environments. Additionally, investigating the integration of real-time adaptive learning algorithms could further enhance the IDS's capability to dynamically respond to evolving cyber threats. Another promising avenue is the exploration of collaborative security approaches, where multiple IoT devices work in synergy to improve overall network security. Finally, considering the rapid advancement in IoT technologies, continual assessment, and refinement of the IDS to cater to emerging IoT standards and protocols will be crucial for maintaining its relevance and efficacy in the face of new challenges. This paper not only addresses a critical security challenge but also lays a foundation for ongoing research and advancements in the dynamic field of IoT security.

REFERENCES

[1] M.A. Albreem, A.M. Sheikh, M.H. Alsharif, et al., "Green Internet of Things (GIoT): Applications, Practices, Awareness, and Challenges", IEEE Access, Vol. 9, pp. 38833-38858, 2021.

[2] A.H.M Aman, N. Shaari, "Internet of Things Energy System: Smart Applications, Technology Advancement, and Open Issues", International Journal of Energy Research, Vol. 45, No. 6, pp. 8389-8419, 2021.

[3] E. Jarmouni, A. Mouhsen, M. Lamhaemmedi, A. Krari, "Management of Battery Charging and Discharging in a Photovoltaic System with Variable Power Demand Using Artificial Neural Networks", E3S Web of Conferences, 2021.

[4] M.N. Khan, A. Rao, S. Camtepe, "Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey", IEEE Internet of Things Journal, Vol. 8, No. 6, pp. 4132-4156, 2021.

[5] J.V.V. Sobral, J.J.P.C. Rodrigues, R.A.L. Rabelo, et al., "Routing Protocols for Low Power and Lossy Networks in Internet of Things Applications", Sensors, Vol. 19, No. 9, p. 2144, 2019.

[6] G. Simoglou, G. Violettas, S. Petridou, et al., "Intrusion Detection Systems for RPL Security: A Comparative Analysis", Computers and Security, Vol. 104, p. 102219, 2021.

[7] A. Krari, A. Hajami, E. Jarmouni, "Detecting the RPL Version Number Attack in IoT Networks using Deep Learning Models", International Journal of Advanced Computer Science and Applications, Vol. 14, No. 10, 2023.

[8] A. Krari, A. Hajami, E. Jarmouni, "Study and Analysis of RPL Performance Routing Protocol under Various Attacks", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 49, Vol. 13, No. 4, pp. 152-161, December 2021.

[9] A. Mahmud, F. Hossain, T.A. Choity, et al., "Simulation and Comparison of RPL, 6LoWPAN, and CoAP Protocols Using Cooja Simulator", International Joint Conference on Computational Intelligence, pp. 317-326, 2019.

[10] W. Song, M. Beshley, K. Przystupa, et al., "A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection", Sensors, Vol. 20, No. 6, p. 1637, 2020.

[11] W. Zhijun, L. Wenjing, L. Liang, et al., "Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey", IEEE Access, Vol. 8, p. 43920, 2020.

[12] M. Lovric, T. Duricic, H. Hussain, et al., "PyChemFlow: An Automated Pre-Processing Pipeline in Python for Reproducible Machine Learning on Chemical Data", ChemRxiv, Theoretical and Computational Chemistry, V. 1, 2023.

[13] P. Sinthong, M.J. Carey, "Exploratory Data Analysis with Database-backed Dataframes: A Case Study on Airbnb Data", 2021 IEEE International Conference on Big Data (Big Data), 2021.

[14] R. Sil, A. Roy, B. Bhushan, et al., "Artificial Intelligence and Machine Learning based Legal Application: The State-of-the-Art and Future Research Trends", The 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2019.

[15] H. Kim, "Deep Learning", Artificial Intelligence for 6G, pp. 247-303, 2022.

[16] O.I. Abiodun, M.U. Kiru, A. Jantan, et al., "Comprehensive Review of Artificial Neural Network Applications to Pattern Recognition", IEEE Access, Vol. 7, pp. 158820-158846, 2019.

[17] P. Singh, S.K. Borgohain, A.K. Sarkar, et al., "Feed-Forward Deep Neural Network (FFDNN)-Based Deep Features for Static Malware Detection", International Journal of Intelligent Systems, pp. 1-20, 2023.

[18] K.M. Abuali, L. Nissirat, A. Al Samawi, A. "Advancing Network Security with AI: SVM-Based Deep Learning for Intrusion Detection", Sensors, Vol. 23, No. 21, p. 8959, 2023.

[19] S. Alsudani, A. Ghazikhani, "Enhancing Intrusion Detection with LSTM Recurrent Neural Network Optimized by Emperor Penguin Algorithm", Wasit Journal of Computer and Mathematics Science, pp. 67-78, 2023.

[20] G. Li, J. Wang, Y. Wang, "An In-Situ Visual Analytics Framework for Deep Neural Networks", IEEE Transactions on Visualization and Computer Graphics, pp. 1-17, 2023.

[21] R. Wazirali, E. Yaghoubi, M.S.S. Abujazar, "State-of-the-art Review on Energy and Load Forecasting in Microgrids Using Artificial Neural Networks, Machine Learning, and Deep Learning Techniques", Electric Power Systems Research, Vol. 225, p. 109792, 2023.

[22] D. Diaz Bedoya, M. Gonzalez Rodriguez, J.M. Clairand, et al., "Forecasting Univariate Solar Irradiance using Machine learning models: A case study of two Andean Cities", Energy Conversion and Management, Vol. 296, p. 117618, 2023.

[23] M.A. Al Ghamdi, "A Fine-Grained System Driven of Attacks Over Several New Representation Techniques Using Machine Learning", IEEE Access, Vol. 11, pp. 96615-96625, 2023.

[24] M.H. Ibrahem, M.H. Abdulameer, "Age Face Invariant Recognition Model Based on VGG Face Based DNN and Support Vector Classifier", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 54, Vol. 15, No. 1, pp. 232-240, March 2023.

BIOGRAPHIES

Name: **Ayoub**
Surname: **Krari**
Birthday: 10.08.1996
Birthplace: Settat, Morocco
Bachelor: Network and Technologies of Telecommunications, Department of Mathematics and Computer Science, Faculty of Science and Technology, Hassan I University, Settat, Morocco, 2017

Master: Telecommunications System and Network Engineering, University of Sultan Moulay Slimane, Beni Mellal, Morocco, Since 2019
Doctorate: Student, Internet of Things Routing Security, VETE Laboratory, Faculty of Science and Technologies, Hassan I University, Settat, Morocco, Since 2019
The Last Scientific Position: Systems and Security Engineer at the Ministry of National Education, Morocco, Since 2020
Research Interests: Internet of Things, Security, AI
Scientific Publications: 5 Papers

Name: **Abdelmajid**
Surname: **Hajami**
Birthday: 26.04.1975
Birthplace: Errachidia, Morocco
Bachelor: Informatics, Mathematic and Informatics Department, Faculty of Sciences and Technology, Hassan I University, Settat, Morocco, 2004
Master: Networks, Telecommunications and Multimedia, Department of Networks and Telecoms, National Higher School of Computer Science and Systems Analysis, Mohamed V University, Rabat, Morocco, 2006
Doctorate: Networks, Telecommunications and Multimedia, Department of Networks and Telecoms, National Higher School of Computer Science and Systems Analysis, Mohamed V University, Rabat, Morocco, 2011
The Last Scientific Position: Prof., Department of Applied Physics, Faculty of Sciences and Technology, Hassan I University, Settat, Morocco, Since 2011
Research Interests: Security, Networks, Bio-Informatics
Scientific Publications: 62 Papers, 2 Books, 2 Projects, 3 Theses
Scientific Memberships: MIR Lab National Higher School of Computer Science and Systems Analysis, Mohamed V University, Rabat, Morocco

Name: **Ezzitouni**
Surname: **Jarmouni**
Birthday: 11.02.1994
Birthplace: Settat, Morocco
Bachelor: Physics, Department of Physics, Faculty Science and Technology, Hassan I University, Settat, Morocco, 2011
Master: Electrical Engineering, Faculty of Science and Technology, Hassan I University, Settat, Morocco, 2019
Doctorate: Student, Smart Grids, Renewable Energy and Artificial Intelligence, Laboratory of Radiation-Matter, and Instrumentation (RMI), Faculty of Sciences and Technology, Hassan I University, Settat, Morocco, Since 2019
The Last Scientific Position: Teacher, Ministry of Education, Morocco, Since 2020
Research Interests: Smart Grids, Renewable Energy, Artificial Intelligence
Scientific Publications: 8 Papers

Name: **Kaoutar**
Surname: **Errakha**
Birthday: 18.09.1989
Birthplace: Settat, Morocco
Bachelor: Computer engineering, Department of Mathematics and Computer Science, Hassan I University, National Schools of Applied Sciences, Settat, Morocco, Since 2012
Master: Engineer in Computer Engineering, UH1, National Schools of Applied Sciences, Khouribga, Morocco, 2014
Doctorate: Student, Artificial Intelligence and Recommendation System, Computer Science, Networks, Mobility and Modeling, Faculty of Science and Technology, Hassan I University, Settat, Morocco, Since 2021
The Last Scientific Position: Engineer in Computer Engineering, National Schools of Applied Sciences, Khouribga, Morocco, Since 2014
Research Interests: Artificial Intelligence, Recommendation Systems, Machine Learning
Scientific Publications: 3 Papers