The Scientific Temper (2025) Vol. 16 (2): 3839-3847

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2025.16.2.15

https://scientifictemper.com/

RESEARCH ARTICLE

RRFSE: RNN biased random forest and SVM ensemble for RPL DDoS in IoT-WSN environment

R. Sakthiraman*, L. Arockiam

Abstract

Distributed denial of service (DDoS) attacks have significantly impacted network performance and stability in the internet of things (IoT) wireless sensor networks (WSNs) that utilize the routing protocol for low-power and lossy networks (RPL). These attacks cause severe network degradation or failure by flooding network nodes with malicious traffic, which interferes with communication. This study presents an ensemble of machine-learning techniques to detect DDoS attacks in RPL-based IoT-WSN systems, including an RNN-biased random forest (RF) and support vector machine (SVM) classifier. The recurrent neural network (RNN) is used to identify attack sequences by capturing temporal patterns in network data. A Random Forest classifier integrates these temporal features and employs many decision trees to improve detection accuracy. An SVM is used to greatly enhance the detecting process. It differentiates between attack and legitimate traffic using robust decision boundaries. The ensemble model improves overall performance in detecting DDoS attacks with greater accuracy, fewer false positives, and improved flexibility in changing attack plans by utilizing the advantages of each technique. Despite the resource limitations present in IoT-WSN environments, experimental results show that this ensemble technique is effective in real-time detection. This approach offers an effective defense against DDoS attacks for Internet of Things networks, guaranteeing dependable communication in networks with limited power and resources.

Keywords: Internet of things, Wireless sensor network, Recurrent neural network, Random forest, Support vector machine, DDOS attack.

Introduction

Wireless sensor networks (WSNs) that make use of the routing protocol for low-power and lossy networks (RPL) have become widely used as a result of the internet of things' (IoT) evolution. Applications like industrial automation, environmental monitoring, and smart cities depend on these networks. However, because of their intrinsic resource limitations, they are vulnerable to a number of security risks, most notably distributed denial of service (DDoS) attacks. Adversaries use these attacks to overload network nodes with traffic, which significantly reduces network performance and, in extreme situations, causes network failure.

Recent studies have underscored the severity of DDoS attacks on IoT networks. For instance, (Xie *et al*., 2023) highlighted that DDoS attacks are among the most dangerous threats to IoT networks, capable of denying legitimate services by flooding the network with malicious traffic. The study demonstrated that machine learning models, particularly random forests, achieved high accuracy (99.32%) in detecting various types of DDoS traffic.

To enhance the resilience of RPL-based IoT-WSNs against DDoS attacks, integrating machine learning techniques has emerged as a promising approach. Recurrent neural networks (RNNs) are adept at capturing temporal patterns in network traffic, making them suitable for identifying attack sequences. Random forest classifiers, known for their robustness and high accuracy, can effectively handle the temporal features extracted by RNNs. Support vector machines (SVMs) further contribute by establishing clear decision boundaries between legitimate and malicious traffic. The ensemble of these techniques leverages their individual strengths, resulting in improved detection accuracy, reduced false positives, and adaptability to evolving attack strategies.

Department of Computer Science, St. Joseph's College (Autonomous), (*Affiliated to Bharathidasan University*), Tiruchirappalli – 620002, India.

***Corresponding Author:** R. Sakthiraman, Department of Computer Science, St. Joseph's College (Autonomous), (Affiliated to Bharathidasan University), Tiruchirappalli – 620002, India., E-Mail: chandransakthi887@gmail.com

How to cite this article: Sakthiraman, R., Arockiam, L. (2025). RRFSE: RNN biased random forest and SVM ensemble for RPL DDoS in IoT-WSN environment. The Scientific Temper, **16**(2):3839-3847.

Doi: 10.58414/SCIENTIFICTEMPER.2025.16.2.15

Source of support: Nil

Conflict of interest: None.

Received: 21/01/2025 **Accepted:** 19/02/2025 **Published** : 20/03/2025

This study builds upon existing research by presenting an ensemble model that combines RNNs, random forests, and SVMs to detect DDoS attacks in RPL-based IoT-WSN systems. The proposed approach aims to ensure reliable communication in networks with limited power and resources, thereby enhancing the overall security and stability of IoT deployments.

Related Works

An intrusion detection system (IDS) based on conditional tabular generative adversarial networks (CTGAN) for detecting DDoS and DoS attacks in IoT networks (Alabsi *et al*., 2023). The CTGAN is used to generate synthetic network traffic resembling legitimate data, which enhances the training of machine learning and deep learning classifiers. The proposed IDS, tested on the Bot-IoT dataset, showed improved accuracy, precision, recall, and F1 score in detecting malicious traffic. The authors suggest refining CTGAN models, integrating additional anomaly detection techniques, and testing the IDS on real-time IoT environments to enhance its robustness.

This research presents a novel intrusion detection model integrating CNN with reciprocal points learning (RPL), an open-set recognition (OSR) technique (Shieh *et al*., 2024). The model aims to detect both known and unknown DDoS attacks by effectively learning attack patterns and distinguishing malicious traffic. The CNN-RPL model achieved high accuracy in detecting known attacks using the CICIDS2017 dataset and the highest accuracy against unknown attacks in the CICDDoS2019 dataset. The model's performance might degrade with highly sophisticated adversarial attacks that can evade OSR-based detection. Additionally, its reliance on deep learning increases computational demands. The study recommends enhancing the model's adaptability to evolving DDoS attack patterns and integrating incremental learning techniques to improve real-time attack detection.

This work introduces a hybrid deep learning-based IDS for RPL-based IoT networks. The approach combines supervised deep artificial neural networks (DANN) and semi-supervised deep autoencoders (DAE) to classify known and unknown attacks (Al Sawafi *et al*., 2023). Additionally, the study introduces a new dataset, IoTR-DS, which simulates three RPL-specific attacks (DIS, Rank, and Wormhole). The IoTR-DS dataset contributed to better attack detection in RPL-based IoT environments. Future research could expand the dataset with additional IoT attack scenarios, improve model efficiency for real-time detection, and explore federated learning for distributed attack detection.

The Proposed work presents a discrete event system (DES)-based IDS to detect rank and version number attacks in RPL-based IoT networks (Ray *et al*., 2023). The model utilizes an active probing technique that differentiates normal and malicious network behavior, ensuring minimal computational overhead. The centralized nature of the IDS may introduce single points of failure, and the approach might not be effective against more sophisticated attacks like Sybil or botnet-based DDoS. The authors propose extending the framework to support decentralized IDS models, integrating more attack types, and improving energy efficiency further by optimizing event monitoring techniques.

This paper provides a comprehensive review and taxonomy of attack detection approaches targeting the RPL protocol in IoT networks. It categorizes various attacks, including resource-based attacks like Hello flooding and version number attacks (VNA), and discusses existing detection and mitigation strategies (Alfriehat N *et al*., 2024). The authors recommend developing more robust detection mechanisms that can handle indirect and sophisticated attacks, ensuring the reliability of RPL-based IoT networks.

This paper explores the use of dimensionality reduction techniques to enhance the timely detection of DDoS attacks in IoT networks. By reducing the feature space, (Kumari *et al*., 2024) the proposed method aims to improve the efficiency and accuracy of machine learning models in identifying malicious activities. The study highlights that selecting appropriate features for reduction is critical and may vary across different IoT environments, potentially affecting the model's performance. The authors suggest investigating adaptive feature selection methods to enhance the generalizability of the detection system across diverse IoT scenarios.

In the study, routing techniques for WSNs utilizing blockchain and reinforcement learning are reviewed. Secure routing protocols that take trust values and hostile nodes into account are covered. (Rukmani et.al.,2024) Energy-efficient routing strategies and their security implications are examined in the paper. Numerous strategies for detecting rogue nodes and enhancing routing effectiveness are investigated.

The study focuses on identifying knee arthritis. A better classification method based on SVM is suggested. (Hemamalini et.al.,2024) The effectiveness of hyperparameter tuning is increased using Cuckoo search optimization. The model's performance is improved by reducing classification errors. Significant improvements in classification performance are demonstrated by the experimental results. F1 score, recall, accuracy, and precision are all improved by the method

The researchers developed an anomaly-based intrusion detection system (IDS) that combines Convolutional Neural Networks (CNN) with a Multi-Objective Enhanced Capuchin Search Algorithm to detect intrusions in IoT networks (Asgharzadeh *et al*., 2023). The system aims to identify anomalies in network traffic that may indicate potential attacks. The proposed IDS achieved high detection rates and demonstrated robustness in identifying various types of intrusions within IoT environments.

This paper proposes a trust-based anomaly detection scheme that utilizes a hybrid deep learning model, combining sequence prediction and deep learning techniques, to mitigate routing attacks in IoT networks. The model focuses on detecting anomalies in routing behaviors to identify potential attacks (Ahmadi K *et al*., 2024). The scheme effectively detected various routing attacks, including black-hole attacks, DIS flooding attacks, version number attacks, and decreased rank attacks, thereby enhancing the security of IoT networks (Table 1).

Background

Fuzzy Logic

Fuzzy logic is an intelligent decision-making approach that effectively handles uncertainty and imprecise data, making it particularly useful in intrusion detection for IoT networks. Unlike traditional binary classification techniques, fuzzy logic enables systems to interpret ambiguous inputs and make approximate reasoning decisions. In the context of DDoS attack detection, fuzzy logic evaluates key network parameters such as traffic volume, packet rate, latency, and error rate to determine abnormal patterns. Studies such as (Javaheri D *et al*., 2023) have shown that fuzzy logic-based anomaly detection outperforms rigid threshold-based systems by reducing false positives and enhancing detection accuracy. By incorporating fuzzy membership functions, the system can dynamically adjust to varying traffic conditions, making it more adaptable to evolving cyber threats. However, fuzzy logic alone may struggle with complex, high-dimensional data, which necessitates hybrid approaches integrating machine learning models for improved performance.

Long Short-Term Memory

Long short-term memory (LSTM) is a specialized type of recurrent neural network (RNN) designed to capture long-term dependencies in sequential data. In IoT-WSN environments, LSTMs have proven highly effective in detecting DDoS attacks by analyzing temporal patterns in network traffic (Suleiman *et al*., 2023). Unlike traditional neural networks, LSTMs use memory cells to retain critical historical information while mitigating issues like vanishing gradients. This capability allows LSTMs to identify sophisticated attack patterns that span multiple time steps. Several studies have highlighted the advantages of LSTMs in network security, demonstrating their ability to differentiate between normal and malicious traffic with high accuracy (Gopali S *et al*., 2024). However, the computational complexity of LSTM models can be a challenge in resource-constrained IoT environments. To address this, optimized variants like attention-based LSTMs and hybrid models combining LSTMs with feature selection techniques have been explored to improve efficiency and reduce processing overhead.

Multi-Dimension Random Forest (MDRF)

Multi-dimension random forest (MDRF) is an advanced ensemble learning approach that extends traditional random forest models by incorporating feature grouping and dimensionality reduction. In our previous work, we proposed MDRF to enhance DDoS attack detection by segmenting input features into multiple dimensions,

Table 1: Existing methods table

Author & Year	*Findings*	*Limitations*	*Future work*
Alabsi *et al*. (2023)	Proposed a Conditional Tabular Generative Adversarial Network (CTGAN)-based IDS to detect DDoS/DoS attacks in IoT. Demonstrated improved classification performance using synthetic data.	Heavy reliance on synthetic data quality; may not generalize well to real-world environments.	Improve CTGAN models and integrate additional anomaly detection methods.
Shieh *et al*. (2024)	Developed CNN-RPL (Convolutional Neural Network with Reciprocal Points Learning) to detect known and unknown DDoS attacks, achieving 99.93% accuracy on known attacks and 98.51% on unknown ones	Vulnerable to adversarial attacks; deep learning models require high computational resources	Enhance adaptability to evolving DDoS attacks and integrate incremental learning
Ray *et al*. (2023)	Introduced a Discrete Event System (DES)-based IDS with active probing to detect rank and version number attacks in RPL networks. Achieved over 99% detection accuracy.	Centralized IDS can introduce single points of failure; may not be effective against sophisticated attack variations	Develop decentralized IDS models and optimize energy efficiency
Sharma *et al*. (2024)	Provided a taxonomy of RPL attacks and reviewed existing detection approaches. Identified gaps in current security measures	Existing detection methods struggle with indirect attacks and network congestion manipulation	Develop robust mechanisms to address indirect and sophisticated attack strategies.
Mansour *et al*. (2023)	Proposed a trust-based anomaly detection scheme using hybrid deep learning models to mitigate IoT routing attacks. Successfully detected black-hole, DIS flooding, and rank attacks.	Dependence on trust metrics introduces delays in detection; performance can be affected by dynamic network changes	Explore adaptive trust-based IDS models with real-time responsiveness

thereby improving classification accuracy while reducing computational cost. This method groups similar features together, allowing the model to analyze complex attack patterns more effectively. Compared to conventional random forests, MDRF demonstrated superior performance in detecting RPL-based IoT attacks, achieving higher true positive rates and fewer false alarms. However, one limitation of MDRF is its reliance on predefined feature groups, which may not generalize well to unseen attack patterns. Future improvements include integrating adaptive feature selection methods to further enhance model flexibility and robustness in dynamic IoT environments.

Custom-made Support Vector Machine (CSVM)

Custom-made support vector machine (CSVM) is an optimized version of the traditional SVM model, designed specifically for IoT-WSN intrusion detection. Unlike conventional SVMs, which rely on predefined kernel functions, CSVM dynamically selects the most suitable hyperplane by leveraging domain-specific feature selection techniques. This customization allows CSVM to effectively classify high-dimensional network traffic data, distinguishing between legitimate and malicious packets with higher precision. In our implementation, CSVM integrates feature selection outputs from MDRF to enhance its classification capabilities. Experimental results indicate that CSVM improves detection rates while reducing false positives compared to standard SVM approaches. However, the model's effectiveness is influenced by the quality of selected features, highlighting the need for continuous feature optimization. Future research aims to integrate deep learning techniques with CSVM to further enhance its adaptability to evolving DDoS attack patterns.

Proposed Method

Proposed "RNN biased random forest and SVM ensemble for RPL DDoS in IoT-WSN Environment" method consists of three innovative functional modules namely Fuzzy DDoS Attention Model, FDAM infused Long Short-Term Memory (FLSTM), and FLSTM Multi-dimensional Random Forest Customized SVM Composite. Construction methodologies, functionalities, and the purposes of these modules are presented in this section in a transparent way in this section.

Fuzzy DDoS Attention Model (FDAM)

FDAM module is used to perform a preliminary evaluation of the key parameters such as traffic volume, packet rate, network latency, error rate, and energy consumption. FDAM method analyzes the rate of change in the standard flow of these parameters and sets an attention flag α as the output. If a notable change in the flow is detected, FDAM sets $\alpha = 1$, otherwise sets $\alpha = 0$.

Let $V_t, P_t, L_t E_t$ and J_t be the traffic volume, packet ratio, network latency, error rate, and energy consumption, respectively at timestamp t. Let $K = \{\kappa_1, \kappa_2, \kappa_3, \kappa_4, \kappa_5\}$ be the set of flow variations of the pivotal parameters traffic volume, packet rate, network latency, error rate, and energy consumption between timestamps t and $t-1$.

In FDAM, a privileged equation is contrived to compute the variations of the input parameters. Let X_t be the value of an input parameter at timestamp t, X_{t-1} be the input value at timestamp $t-1$, X_{min} be the minimum possible value of the parameter, and X_{max} be the maximum possible value of the parameter, then the variation κ_x is computed by the following equation.

$$\kappa_x = \left(\frac{100}{X_{max} - X_{min}} \right) \times \left| X_t - X_{t-1} \right| \times 10^{-2} \qquad \text{Equation (1)}$$

where X can be substituted by any input parameter such as $V_t, P_t, L_t E_t$ and J_t to compute corresponding κ_x.

The fuzzy anomaly average K_{avg} for the variations of the perceived input parameters are computed by the following formula.

$$K_{avg} = \frac{1}{n} \sum_{1=1}^{n} \kappa_i \qquad \text{Equation (2)}$$

where n refers to the number of input parameters perceived which is equal to 5 for the current FDAM version.

The attention flag α is determined by Equation 3

$$\alpha = \begin{cases} \text{1 if } K_{avg} \geq \frac{1}{2} \vee \forall i = 1 \rightarrow 5 \text{ if } (\ _i \geq \quad) \\ 0 \text{ otherwise} \end{cases} \qquad \text{Equation (3)}$$

A flowchart for FDAM functionality is illustrated in Figure 1.

Through this way, the proposed FDAM sets the attention flag α to 1 if the anomaly average is above 50% if a single parameter anomaly variation is greater than or equal to 75%. This Attention flag is further used by the chronological modules.

FDAM-infused Long Short-Term Memory (FLSTM)

A standard LSTM model is optimized to incorporate the attention flag which is obtained from the FDAM module. Regula equations for the input gate, candidate cell state, cell state update, hidden state, output gate and forget gate are customized for FLSTM as follows.

Input Gate:

$$i_t = \sigma\left(w_i \cdot \left[h_{t-1}, x_t \right] + \alpha \cdot b_i \right). \qquad \text{Equation (4)}$$

Candidate Cell State:

$$\tilde{C}_t = \tanh\left(w_c \cdot \left[h_{t-1}, x_t \right] + \alpha \cdot b_c \right) \qquad \text{Equation (5)}$$

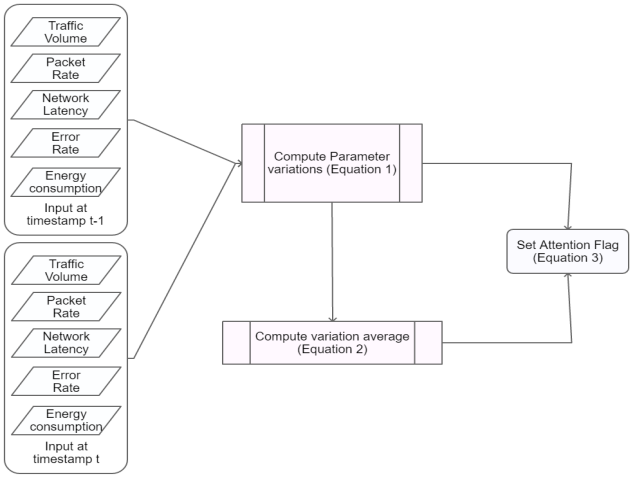

Figure 1: FDAM flowchart

Cell State Update

$$C_t = f_t \odot \mathrm{C}_{t-1} + i_t \odot \tilde{C}_t \qquad \text{Equation (6)}$$

Hidden State

$$h_t = o_t \odot \tanh\left(C_t \circ \frac{\alpha}{2}\right) \qquad \text{Equation (7)}$$

Output Gate

$$o_t = \sigma\left(w_o \cdot \left[h_{t-1}, x_t\right] + \alpha \cdot b_o\right) \qquad \text{Equation (8)}$$

Forget Gate

$$f_t = \sigma\left(w_f \cdot \left[h_{t-1}, x_t\right] + \alpha \cdot b_f\right) \qquad \text{Equation (9)}$$

FLSTM is contrived in a way that includes an additional control mechanism to selectively enable or disable the biases based on the attention flag α in its computations. Biases in neural networks are typically used to adjust the outputs of the gates and improve the flexibility of the model in learning patterns. In FLSTM, the binary type attention flag acts as a switch to determine whether these biases are applied in each gate. When the attention flag is active, the biases contribute to the calculations, allowing the FLSTM to leverage additional learnable parameters for better performance. Conversely, when the flag is inactive, the biases are excluded, simplifying the model and potentially reducing overfitting or computational overhead. This modification provides dynamic control over the LSTM network's complexity, making FLSTM as adaptable for scenarios that require fine-tuning of computational or model capacity. FLSTM generates an anomaly prediction ω_L based on the input parameters and the attention flag provided by FDAM. The output ω_L is used in the subsequent module FLMRFCS to conclude the final decision about whether the arrived network transaction is a DDoS attack or not.

FLSTMs offer several advantages that make them highly versatile and efficient for sequence modeling tasks. By incorporating an attention flag mechanism, they provide dynamic control over model complexity, allowing biases to be selectively enabled or disabled. This flexibility enhances the model's ability to learn complex patterns when needed, while also simplifying it to reduce the risk of overfitting in scenarios with limited data or less complexity. The adaptability to varying resource constraints makes FLSTM particularly useful for deployment in resource-limited environments, such as IoT and wireless sensor nodes. In addition, the ability to fine-tune the inclusion of biases during training or deployment adds another layer of flexibility, enabling real-time adjustments to meet evolving requirements. This dynamic control also aids in improving interpretability, as it allows researchers to study the impact of biases on gate functions and overall performance. These features make FLSTM a powerful and adaptable tool for applications ranging from natural language processing to sensor data analysis. FLSTM architecture is provided in Figure 2.

FLSTM Multi-dimensional Random Forest Customized SVM Composite (FLMRFCS)

This module involves determining the number of features in a typical network transaction, which depends on factors such as the communication protocol, routing protocol, network architecture, and the hardware components involved. The features are organized into a set, and feature groups are created in a separate set. Unlike a standard random forest model, the modified decision random forest (MDRF) approach divides all input features into separate groups to improve performance metrics like true positives, true negatives, and accuracy. Each group contains a specific number of features, and if a group has fewer features than required, padding is applied to ensure that all groups are filled appropriately. This approach helps in better organizing the features and optimizing the model's performance during the classification process.

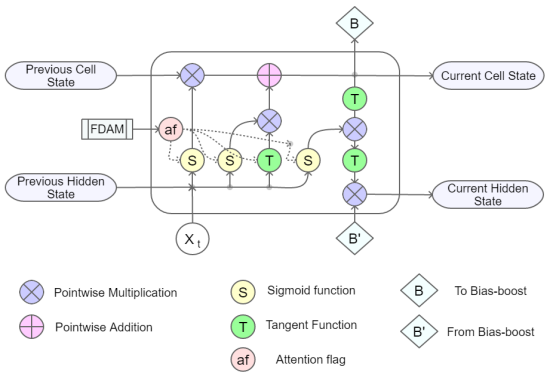

Figure 2: FLSTM architecture

The modified decision random forest - dimensionality reduction (MDRF-DR) algorithm enhances the performance of the standard random forest model by focusing on improving feature relevance and reducing the dimensionality of the input data. It does so by evaluating each feature in terms of its contribution to the classification process. Specifically, the algorithm identifies features that are deemed "beneficial," meaning those that significantly contribute to improving model accuracy, true positives, and true negatives.

Features that contribute less than 50% to the model's effectiveness are considered to be of lower value, and these are eliminated from the feature set. This process of eliminating less beneficial features helps in reducing the computational complexity of the model, thus making it more efficient while maintaining or even improving its predictive power. The remaining set of beneficial features, referred to as the beneficial multi-dimension random forest set is then passed to the next functional module for further processing.

This dimensionality reduction not only simplifies the model but also ensures that only the most relevant features are used in subsequent decision-making, helping the algorithm focus on the data that has the most predictive power. By removing less useful features, the MDRF-DR algorithm can achieve better generalization, faster training times, and potentially higher accuracy in detecting patterns, particularly in complex datasets like IoT and WSN data.

The classification support vector machine (CSVM) model employs supervised learning, although no labeled dataset is directly used. Instead, the Wireshark-assisted hypervisor output provides DDoS attack labels for each network transaction occurring within a specific internet of things - wireless sensor networks (IoT-WSN) environment. The feature selection process from the modified decision random forest (MDRF) model is inherited by the CSVM, with the assumption that the beneficial random forests are more likely to contain the most impactful features from the input data. The process begins by defining an empty feature set that will be used by the CSVM module. Selected features from the MDRF model are added to this set through a predefined method. Once the features are selected, the number of features chosen is determined, and a hyperplane with one less dimension than the number of selected features is initialized for the CSVM. The CSVM then uses a hyperplane selection algorithm to evaluate all possible combinations of feature pairs (X-Y axis features). This selection process aims to enhance the model's ability to classify correctly, specifically improving performance metrics such as the true positive rate (TPR) and reducing the false positive rate (FPR). By selecting the optimal features and adjusting the hyperplane accordingly, the CSVM model strives to maximize classification accuracy in detecting DDoS attacks.

FLMRFCS uses the output ω_R fetched from the MDRF module, and the output ω_S from CSVM module, along with FSLTM output ω_L to determine the DDoS attack status as in the following algorithm.

Algorithm: FLMRFCS

Input: $\omega_R, \omega_S,$ and ω_L

Output: DDoS status

Step 1: Let ω_T be the central tendency coefficient

Step 2: Let ω_Q be the normalized output quotient

Step 3: Read ω_R from MDRF

Step 4: Read ω_S from CSVM

Step 5: Read ω_L from FLSTM

Step 6: Compute $\omega_T = \omega_R + \left(\frac{\omega_S - \omega_R}{2}\right)$

Step 7: Compute $\omega_Q = \omega_L + \left(\frac{\omega_T - \omega_L}{2}\right)$

Step 8: $Output = \begin{cases} DDoS\ if\ \omega_Q > \frac{1}{2} \\ Not\ DDos\ otherwise \end{cases}$

Step 9: return Output

Step 10: Repeat process from Step 3 until network halt

A comprehensive flow diagram of proposed RRFSE method is illustrated in Figure 3.

Experimental Setup

The proposed RRFSE method is implemented on a computer equipped with an Intel i7 processor, 16 GB of memory, and 1TB of storage. To obtain real-time IoT-WSN data and perform DDoS detection, a server leased from i2k2.com is used. This server is integrated with the industrial-standard Wireshark network tracing tool to assess the performance of various methods discussed in the study. A custom user interface (UI) is developed to upload programming scripts to the server, allowing interaction with both the server and Wireshark to retrieve performance metrics. The UI is built using Visual Studio IDE. The network scripts and communication with the Wireshark software are developed in C++ 20.0. As the entire system relies on real-time network data, pre-existing datasets are not used. During the training phase, performance is recorded every 7% increment of data until 70%, while in the testing phase, performance metrics are logged for every 3% of data until 30%, adhering to a 70:30 training-to-testing ratio throughout the experiments.

Results and Discussion

The results of the proposed RRFSE method approach are displayed in the tables below alongside the outcomes

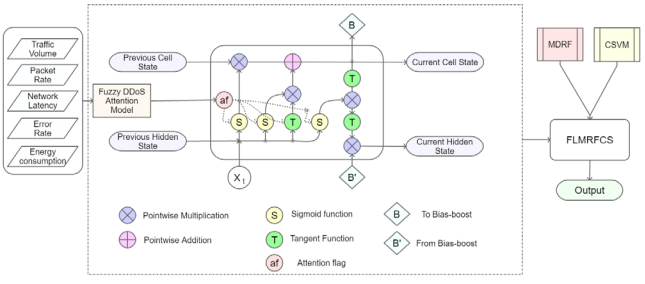

Figure 3: RRFSE workflow diagram

from other models that are currently in use, which include conditional tabular generative (CTG), hybrid deep learning intrusion detection (HDLID), novel energy-efficient scheme for discrete event modeling (NEESDEM), and unknown ddos reciprocal points learning (UDRPL). Every evolution metric, including sensitivity, specificity, accuracy, precision, F-score, and G-mean, exhibits a notable improvement.

As Table 2 shows, the suggested RRFSE approach achieved 98.92% accuracy when compared to current techniques. Table 3 demonstrates that the RRFSE method performed better than the precision by 98.81%. RRFSE receives a 99.02% in the sensitivity (Table 4). The specificity attained in Table 5 is 98.81%, but the F score metrics in Table 6 reach 98.92%. In the end, Table 7 displays the G-mean value of 98.99%.

Compared with various approaches presently in usage, including the conditional tabular generative (CTG), hybrid deep learning intrusion detection (HDLID), novel energy-efficient scheme for discrete event modelling (NEESDEM), and unknown DDoS reciprocal points learning (UDRPL). Figure 4 indicates the visual appearance of the outcomes of the proposed RRFSE method approach. It is clear from the preceding graph that the RRFSE methodology performs better than the existing methods in every evaluation metric.

Table 2: Accuracy (%)

Data (%)	*UDRPL*	*HDLID*	*NEESDEM*	*CTGA*	*RRFSE*
3	96.99	95.75	97.91	98.17	98.92
6	96.95	95.64	97.85	98.17	98.97
9	96.99	95.71	97.88	98.14	99.04
12	97.03	95.64	97.89	98.19	98.99
15	97.04	95.67	97.95	98.19	99.03
18	96.99	95.71	97.92	98.14	98.96
21	97.03	95.71	97.92	98.12	98.96
24	96.92	95.71	97.89	98.14	99.01
27	97.03	95.67	97.91	98.13	98.99
30	96.97	95.71	97.93	98.10	98.92

Table 3: Precision(%)

Data (%)	*UDRPL*	*HDLID*	*NEESDEM*	*CTGA*	*RRFSE*
3	98.05	96.05	97.04	97.82	98.81
6	97.94	95.97	96.91	97.76	98.86
9	97.91	96.08	96.99	97.76	98.89
12	98.02	95.94	97.04	97.84	98.89
15	98.07	95.94	97.04	97.79	98.95
18	97.91	96.02	96.94	97.71	98.89
21	98.05	95.94	96.96	97.79	98.84
24	97.94	95.97	97.02	97.82	98.89
27	97.99	95.99	96.94	97.74	98.92
30	97.91	95.99	97.04	97.71	98.81

Table 4: Sensitivity (%)

Data (%)	*UDRPL*	*HDLID*	*NEESDEM*	*CTGA*	*RRFSE*
3	96.01	95.47	98.75	98.52	99.02
6	96.04	95.34	98.77	98.57	99.08
9	96.14	95.37	98.74	98.51	99.19
12	96.12	95.37	98.72	98.52	99.08
15	96.09	95.42	98.83	98.57	99.11
18	96.14	95.42	98.88	98.57	99.02
21	96.09	95.49	98.85	98.43	99.08
24	95.99	95.47	98.75	98.46	99.13
27	96.14	95.37	98.85	98.51	99.05
30	96.11	95.45	98.80	98.49	99.02

Table 5: Specificity (%)

Data (%)	*UDRPL*	*HDLID*	*NEESDEM*	*CTGA*	*RRFSE*
3	98.00	96.02	97.09	97.83	98.81
6	97.90	95.94	96.97	97.78	98.87
9	97.87	96.05	97.04	97.78	98.90
12	97.98	95.92	97.09	97.86	98.89
15	98.03	95.92	97.10	97.81	98.95
18	97.87	96.00	96.99	97.73	98.89
21	98.01	95.92	97.02	97.80	98.84
24	97.90	95.95	97.07	97.83	98.89
27	97.95	95.97	96.99	97.75	98.92
30	97.87	95.97	97.10	97.73	98.81

Table 6: FScore (%)

Data (%)	*UDRPL*	*HDLID*	*NEESDEM*	*CTGA*	*RRFSE*
3	97.02	95.76	97.89	98.17	98.92
6	96.98	95.65	97.83	98.16	98.97
9	97.02	95.72	97.86	98.14	99.04
12	97.06	95.65	97.87	98.18	98.98
15	97.07	95.68	97.93	98.18	99.03
18	97.02	95.72	97.90	98.14	98.96
21	97.06	95.72	97.90	98.11	98.96
24	96.95	95.72	97.87	98.14	99.01
27	97.06	95.68	97.88	98.12	98.99
30	97.00	95.72	97.91	98.10	98.92

Table 7: GMean (%)

Data (%)	*UDRPL*	*HDLID*	*NEESDEM*	*CTGA*	*RRFSE*
3	97.00	95.75	97.92	98.17	98.92
6	96.96	95.64	97.86	98.17	98.97
9	97.00	95.71	97.89	98.15	99.04
12	97.04	95.64	97.90	98.19	98.99
15	97.06	95.67	97.96	98.19	99.03
18	97.00	95.71	97.93	98.15	98.96
21	97.04	95.71	97.93	98.12	98.96
24	96.94	95.71	97.90	98.15	99.01
27	97.04	95.67	97.92	98.13	98.99
30	96.99	95.71	97.94	98.11	98.92

Figure 4: Graphical representation of RRFSE Method

Conclusion

The suggested ensemble approach for identifying DDoS attacks in RPL-based IoT WSNs that combines RNN, BRF, and SVM provides a practical way to deal with the increasing threat of DDoS in IoT contexts. Each of these models contributes unique benefits to raise the overall reliability, resilience, and accuracy of detection. Time-dependent dependencies and trends in network traffic are captured by RNN's effective sequential data analysis, which is crucial for identifying complex DDoS attacks that change over time. The model's robustness is enhanced by BRF, which uses several decision trees that are capable of handling both small and large datasets. This ensures that there are few false positives despite identifying complex attack patterns.SVM helps by classifying data according to a margin of separation, which improves precision by assisting in the identification of harmful or unusual network behaviors in features with high dimensions.

Acknowledgment

I Sincerely acknowledge the Head of the department, Dr. L. Arockiam, Head and Associate Professor, Department of Computer Science and Principal of this Institution, for providing the facility to complete this paper successfully.

References

Ahmadi, K., & Javidan, R. (2024). A Trust Based Anomaly Detection Scheme Using a Hybrid Deep Learning Model for IoT Routing Attacks Mitigation. *IET Information Security*, *2024*(1), 4449798.

Alabsi, B. A., Anbar, M., & Rihan, S. D. A. (2023). Conditional tabular generative adversarial based intrusion detection system for detecting ddos and dos attacks on the internet of things networks. *Sensors*, *23*(12), 5644.

Al Sawafi, Yahya, Abderezak Touzene, and Rachid Hedjam. "Hybrid deep learning-based intrusion detection system for RPL IoT networks." *Journal of Sensor and Actuator Networks* 12, no. 2 (2023): 21.

Alfriehat, N., Anbar, M., Aladaileh, M., Hasbullah, I., Shurbaji, T. A., Karuppayah, S., & Almomani, A. (2024). RPL-based attack detection approaches in IoT networks: review and taxonomy. *Artificial Intelligence Review*, *57*(9), 248.

Asgharzadeh, H., Ghaffari, A., Masdari, M., & Gharehchopogh, F. S. (2023). Anomaly-based intrusion detection system in the Internet of Things using a convolutional neural network and multi-objective enhanced Capuchin Search Algorithm. *Journal of Parallel and Distributed Computing*, *175*, 1-21.

Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., & Draheim, D. (2023). Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. *Engineering Applications of Artificial Intelligence*, *123*, 106432.

Dheepika, P. S., & Umadevi, V. (2024). An optimized approach for detection and mitigation of DDoS attack cloud using an ensembled deep learning approach. The Scientific Temper, 15(03), 2579-2587

Gopali, S., & Siami Namin, A. (2022). Deep learning-based time-series analysis for detecting anomalies in internet of things. *Electronics*, *11*(19), 3205.

Hemamalini, G., & Maniraj, V. (2024). Enhanced optimization based support vector machine classification approach for the detection of knee arthritis. The Scientific Temper, 15(spl-1), 97-106.

Javaheri, D., Gorgin, S., Lee, J. A., & Masdari, M. (2023). Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives. *Information Sciences*, *626*, 315-338.

Jenifer, R. R., & Prakash, V. S. J. (2023). Detecting denial of sleep attacks by analysis of wireless sensor networks and the

Internet of Things. The Scientific Temper, 14(04), 1412-1418.

Kumari, P., & Jain, A. K. (2024). Timely detection of DDoS attacks in IoT with dimensionality reduction. *Cluster Computing*, *27*(6), 7869-7887.

Ray, D., Bhale, P., Biswas, S., Mitra, P., & Nandi, S. (2023). A novel energy-efficient scheme for rpl attacker identification in IoT networks using discrete event modeling. IEEE Access, 11, 77267-77291.

Rekha, R., & Sundaram, P. M. (2024). Enhanced malicious node identification in WSNs with directed acyclic graphs and RC4-based encryption. The Scientific Temper, 15(spl-1), 182-190.

Rukmani, A., & Jayanthi, C. (2024). Trust and security in wireless sensor networks: A literature review of approaches for malicious node detection. The Scientific Temper, 15(spl-1), 338-347.

Shakya, S., & Abbas, R. (2024). A Comparative Analysis of Machine Learning Models for DDoS Detection in IoT Networks. *arXiv preprint arXiv:2411.05890*.

Shieh, C. S., Ho, F. A., Horng, M. F., Nguyen, T. T., & Chakrabarti, P. (2024). Open-set recognition in unknown ddos attacks detection with reciprocal points learning. *IEEE Access*.

Shukla, P., Krishna, C. R., & Patil, N. V. (2024). SDDA-IoT: storm-based distributed detection approach for IoT network traffic-based DDoS attacks. *Cluster Computing*, *27*(5), 6397-6424.

Suleiman, M. B., Robinson, R., & Kiru, M. U. Long-Short Term Memory Network Based Model for Reverse Brute Force Attack Detection.

Xie, Y. (2023). Machine learning-based DDoS detection for IoT networks. *Applied and Computational Engineering*, *29*, 99-107.