IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 11, November 2023

DOI: 10.17148/IJARCCE.2023.121101

A Hybrid Model for The Detection Of APA-DDoS Attacks Using Random Forest with Recurrent Neural Network

P.S. Ezekiel[1], O.E. Taylor[2]

Department of Computer Science, Rivers State University, Port Harcourt, Nigeria[1,2]

Abstract: The utilization of machine learning has significant importance in the identification and prevention of distributed denial of service (DDoS) attacks. Through the examination of network traffic patterns, machine learning algorithms possess the capability to detect anomalous activities that serve as indicators of a Distributed Denial of Service (DDoS) assault in a timely manner. This paper presents a novel hybrid approach for the detection of distributed denial-of-service (DDoS) attacks in network logs, leveraging the strengths of both Random Forest (RF) for feature extraction and Recurrent Neural Network (RNN) for classification. The proposed framework harnesses the discriminative power of RF in identifying salient features from the raw network log data, which are subsequently utilized as input for the RNN classifier. The Random Forest algorithm was employed to extract a comprehensive set of discriminative features from the network log data, enabling the model to capture intricate patterns indicative of DDoS attacks. These features were then employed as input to the RNN classifier, facilitating the utilization of sequential dependencies and temporal patterns within the log data. The hybrid model achieved exceptional performance, with an accuracy of 99.99%. Furthermore, the true positive rate was recorded at an impressive 99.99%, demonstrating the model's proficiency in correctly identifying actual instances of DDoS attacks. The false positive rate was exceptionally low, at 0.0001%, underscoring the model's robustness in minimizing misclassifications. This study represents a significant advancement in the field of DDoS attack detection, offering a powerful and accurate solution that effectively combines the strengths of Random Forest for feature extraction and RNN for classification. The hybrid model's outstanding performance metrics affirm its potential for deployment in real-world network security environments, providing a robust defense against DDoS attacks.

Keywords: Distributed Denial of service, Recurrent Neural Network, Random Forest Classifier, Network Logs.

I. INTRODUCTION

Distributed Denial of Service (DDoS) attacks present a substantial menace to network systems, as they concurrently target servers, websites, and network equipment [1]. These attacks have the capability to disrupt the network's infrastructure, thereby impacting all tiers of applications that experience high volumes of traffic and handle files from various origins. Consequently, this disruption results in diminished performance and temporary unavailability of services [2].

Detecting and mitigating Distributed Denial of Service (DDoS) attacks pose significant challenges, particularly in the context of Software-Defined Networking (SDN) systems [3]. Researchers have investigated multiple methodologies, such as machine learning, deep learning, and anomaly detection, in order to enhance the security of networks against distributed denial-of-service (DDoS) attacks [4] [5] [6]. Moreover, there has been a considerable amount of research conducted on the effects of Distributed Denial of Service (DDoS) attacks on new technologies like the Internet of Things (IoT) and cloud computing [7] [8].

The potential to interrupt essential systems, such as smart electric metre systems and transportation networks, highlights the severity of DDoS attacks [9]. Furthermore, the increasing occurrence and efficacy of Distributed Denial of Service (DDoS) attacks in wireless sensor networks and Internet of Things (IoT) contexts have generated apprehension [10] [11].

In order to tackle these issues, researchers have put forth novel techniques for detection and mitigation, including the utilisation of generative adversarial networks and deep autoencoder-based methodologies [12].

Furthermore, researchers have investigated the incorporation of sophisticated algorithms and intrusion detection systems as a means to bolster the robustness of network systems in the face of Distributed Denial of Service (DDoS) attacks [13]. The importance of these endeavours is emphasised by the possible consequences of Distributed Denial of Service (DDoS) attacks on vital network services, necessitating the development of resilient defence systems to protect against such vulnerabilities. [14] proposed an adaptive machine learning-based system for DDoS attack detection and mitigation in SDN-enabled Internet of Things (IoT) networks, utilizing multilayered feed-forwarding schemes to analyze network traffic features. Similarly, [15] introduced a hybrid deep learning approach, AE-MLP, for DDoS detection and

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 11, November 2023
DOI: 10.17148/IJARCCE.2023.121101

classification, demonstrating the use of Deep Learning (DL) techniques in detecting DDoS attacks. Furthermore, the security performance analysis of Low Earth Orbit (LEO) Satellite Constellation Networks (LSCNs) under DDoS attacks is an emerging area of study, indicating the evolving nature of DDoS attack research [16]. Additionally, the use of deep learning in OpenFlow-based SDN for DDoS attack detection and defense has been explored, highlighting the significance of advanced technologies in combating DDoS threats [17].

II. LITERATURE REVIEW

In [18], the paper proposed two distinct approaches for the detection of Distributed Denial of Service (DDoS) attacks within the context of Software-Defined Networking (SDN). One approach involved utilising the severity of a DDoS assault as a metric for detection. The second approach involved the utilisation of a Machine Learning (ML) methodology to improve the K-Nearest Neighbours (KNN) algorithm for the purpose of identifying and detecting Distributed Denial of Service (DDoS) attacks. The efficacy of the proposed K-nearest neighbours (KNN) method in identifying distributed denial-of-service (DDoS) attacks is substantiated by both theoretical analysis and experimental results obtained from a dataset. The findings indicated a high detection rate of 98% for DDoS attacks.

In the study [19], the authors presented a novel framework for the detection of distributed denial-of-service (DDoS) attacks in the context of 5G and beyond-5G (B5G) networks. This framework was designed to be both composite and efficient, addressing the need for robust and effective detection mechanisms in these advanced network environments. The detection framework that was proposed comprises a composite multilayer perceptron that was integrated with an effective feature extraction algorithm. This framework was designed not only to identify the occurrence of a DDoS assault but also to determine the specific sort of DDoS attack that was experienced. Upon the conclusion of the simulations and subsequent evaluation of the proposed framework using a dataset acknowledged by the industry, the findings indicated that the framework possesses the capability to effectively identify Distributed Denial of Service (DDoS) attacks. The accuracy score achieved by the framework was notably high, reaching 99.66%, while the associated loss was little, measuring at 0.011.

In [20], a novel approach for detecting Distributed Denial of Service (DDoS) attacks was proposed, which relies on analysing traffic changes. Additionally, two machine learning models were developed to effectively identify and classify DDoS attacks. In order to assess the efficacy of the two machine learning models, a substantial dataset is generated using DDoS simulators BoNeSi and Slow HTTP Test. This dataset is then merged with the CICDDoS2019 dataset to evaluate the accuracy of identification and classification, as well as the efficiency of the algorithms. The findings of our study demonstrated that the long short-term memory model that was proposed achieved an identification accuracy of 98.9%. This performance surpasses that of the other four prominent learning models discussed in most relevant literatures. The convolutional neural network that has been proposed exhibits a classification accuracy of up to 99.9%.

In a study conducted by [21], an experiment was conducted using the CICDDoS2019 dataset, which encompasses several DDoS attacks types that emerged in 2019. The results of the experiment revealed a detection success rate of 99.99% for attacks on network traffic, while the classification accuracy for different attack types reached 94.57%. The achieved high accuracy values demonstrated the efficacy of utilising deep learning models for countering DDoS attacks.

In [22], the author proposed a versatile and modular framework that enabled the detection and mitigation of Low-Rate Distributed Denial of Service (LR-DDoS) attacks inside Software-Defined Networking (SDN) environments. In our architecture, we focus on training the intrusion detection system (IDS) by employing six distinct machine learning (ML) models, namely J48, Random Tree, REP Tree, Random Forest, Multi-Layer Perceptron (MLP), and Support Vector Machines (SVM). To assess the effectiveness of these models, their performance was evaluated using the Canadian Institute of Cybersecurity (CIC) DoS dataset. The evaluation results indicate that the proposed approach successfully achieves a detection rate of 95%, even in the presence of challenges associated with detecting Low-Rate Denial-of-Service (LR-DoS) attacks.

The authors in the paper [23], introduced a way for transforming network traffic data into image format. They proceeded to train a ResNet model, which is considered a cutting-edge convolutional neural network, using the converted data. The methodology described in this study achieved a high level of accuracy, specifically 99.99%, in detecting Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks using binary classification. In addition, the approach presented in this study demonstrated an average precision of 87% in identifying eleven distinct types of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack patterns. This performance surpassed the current state-of-the-art by 9%.

[24] identified and analysed instances of distributed denial-of-service (DDoS) attacks on financial institutions by use of Banking Dataset. In this study, a variety of classification methods were employed to forecast DDOS attacks. We have included additional intricacy to the structure of generic models in order to enhance their performance. The study additionally, employed the support vector machine (SVM), K-Nearest Neighbors' (KNN), and random forest algorithms (RF). The Support Vector Machine (SVM) achieved a classification accuracy of 99.5% in detecting Distributed Denial

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 11, November 2023

DOI: 10.17148/IJARCCE.2023.121101

of Service (DDoS) attacks. On the other hand, the K-Nearest Neighbours (KNN) algorithm and Random Forest (RF) algorithm achieved accuracy rates of 97.5% and 98.74% respectively for the same task.

In study [25], the authors employed a machine learning technique to distinguish between benign traffic and DDoS assault traffic. The primary contribution of this study is in the identification of hitherto unexplored features that can be utilised for the detection of Distributed Denial of Service (DDoS) attacks. The dataset was generated by logging novel information into a CSV file, which was then utilised to train machine learning algorithms for Software-Defined Networking (SDN). Previous studies on DDoS attack detection have utilised either non-SDN datasets or have not made their research data publicly available. The categorization task is executed using a unique hybrid machine learning model. The findings indicated that the hybrid approach of combining the Support Vector classifier with Random Forest (SVC-RF) yielded the most accurate classification of traffic, achieving a testing accuracy of 98.8%. Furthermore, this model demonstrated a notably low false alarm rate.

The study conducted by [26] introduces a novel approach to anomaly intrusion detection and prevention by employing a reinforcement learning technique within an agent-based system. The system employs two agents: the initial agent is responsible for launching attacks on the network system, while the second agent is tasked with detecting and categorising these attacks into various types, namely normal, denial-of-service (DoS), probe, unauthorized-to-local (U2L), and unauthorized-to-remote (U2R) attacks. The orange line in the system diagram represents the reward received by the attacking agent, while the blue line represents the reward obtained by the agent responsible for the detection of intrusion attacks. The attacking agent was rewarded a cumulative total of 5, but the defending agent was rewarded a cumulative total of 95. This implies that the defensive agents exhibit enhanced performance in identifying and categorising attacks executed by the offensive agent. Additionally, the graphic illustrates the loss values incurred by the agent throughout the training process. During the training process, it is observed that every agent exhibits a loss value that is less than 0.5. The agent achieved accuracy rates for each individual assault. The accuracy rates for the several categories are as follows: normal at 0.79%, DoS at 0.94%, R2L at 0.88%, Probe at 0.94%, and U2R at 0.99%.

In the study conducted by [27], a sophisticated method was proposed for the identification of behavioural bootnet attacks. This system leveraged on the Random Forest Classifier and Principal Component Analysis (PCA) techniques. The initial step of the system involved utilising a dataset comprised of botnet information, which was employed in the development of a resilient model for the purpose of identifying Bootnet attacks. The dataset underwent preprocessing using the pandas software, which is commonly employed for data cleaning purposes. Principal Component Analysis (PCA) was employed to reduce the dimensionality of the dataset in order to mitigate the issue of data imbalance. The principal component analysis (PCA) outcome was utilised as the input for the random forest classifier. The random forest classifier was trained with a total of 1000 estimators. The outcome of the model demonstrates a highly encouraging level of accuracy, approximately reaching 99%.

III. DESIGN METHODOLOGY

This section describes the components of the system architecture and how they are interconnected. Figure 1 shows the architecture of the system architecture.

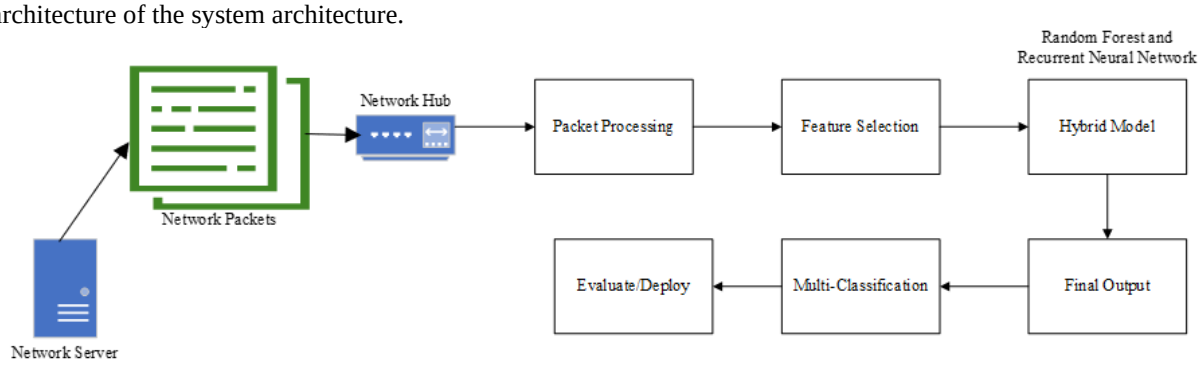

Figure 1: Architectural design of the proposed system

Network Server: The Network Server is the brains of the operation, controlling how information travels between nodes. It connects the network hardware to the monitoring software. It takes in data from various network log sources and forwards them on.

Network Hub: The Network Hub collects and organizes data from various network log sources. It makes sure the information is structured and sorted in the right way for further examination. This part is essential for the system's smooth operation as it controls the flow of information.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 11, November 2023

DOI: 10.17148/IJARCCE.2023.121101

Packet Processing: Packet Processing is the process of inspecting and analyzing data packets in a network in search of irregularities. This section filters incoming information using methods like traffic profiling, anomaly detection, and signature-based detection to identify possible DDoS attacks.

Feature Selection: Feature Selection is the procedure of picking out useful characteristics from the data collected in the network logs. This feature aids in data extraction that can reveal the presence of DoS attacks. It helps narrow down the data to its most relevant aspects for analysis. Random Forest classifier was used for the feature selection. The feature importance was calculated averaging the drop in impurity over the number of trees in the forest.

Assumption

Let *N* denote the number of trees in the Random Forest classifier and *F* denote the number of features in the dataset. Let t denote the node and *i* denote the tree. The feature importance can be calculated using the Gini function G(t) and the number of samples.

$$I(f,t) = n_t * G(t) - n_{left} * G(t_{left}) - n_{right} * G(t_{right}) \quad \text{Eqn. 1.}$$

Where $(t_{left})\ and\ t_{right}$ represent the left and right child notes after the split, n_{left} and n_{right} represent the number of samples in each child node, and $G(t_{left})\ and\ G(t_{right})$ represents the Gini impurities of the left and right child nodes. The summation of the total important features.

$$I(f) = \frac{1}{N} \sum_{i=1}^{N} \sum_t I\,(f,t,i) \quad \text{Eqn. 2.}$$

The normalized feature importance that sum up to 1 can be seen in Eqn. 3

$$I_{norm}\,(f) = \frac{I\,(f)}{\sum_j I(j)} \quad \text{Eqn. 3.}$$

Hybrid Model: The extracted feature of the Random Forest Classifier was used as input to feed the Recurrent Neural Network (RNN) architecture. This was utilized to have an improved number of false positive and negative values.

Final Output: The Final Output component summarizes the analysis done in the preceding sections. A comprehensive report of potential DDoS attacks and their characteristics is generated. This output is essential for making well-informed decisions about network security.

Multi Classification: The system's ability to multi-classify detected attacks into distinct groups according to their characteristics is called "multi-classification." This feature makes sure the system can tell the difference between common types of DDoS attacks like UDP floods, SYN floods, and HTTP floods.

Evaluate and Deploy: The function of this subsystem is to evaluate the effectiveness of the detection mechanism. To evaluate the system's efficacy, the false positive rate, and the response time, it must be put through a battery of tests mimicking actual attacks.

IV. RESULTS AND DISCUSSION

The version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal Productions from the IEEE LaTeX style files.

The experimental result is made up of two phases. The first phase has to do with the exploratory data analysis, and feature extraction. This second phase has to do with the training of the RNN model using the extracted features.

A. Exploratory Data Analysis

For performing analysis, pandas, seaborn, and matplotlib library was used in conducting analysis on the dataset. The analysis was conducted so that a proper insight on the dataset before training the LSTM model can be seen. The analysis phases are checking if the dataset contains some nan and duplicate values. Pandas data was used in achieving this. Secondly, a bar chart was plotted to check if the number of classes (different types of the D attacks on network system)

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 11, November 2023

DOI: 10.17148/IJARCCE.2023.121101

have the same number of instances. The bar chat in Figure 2 shows that the number of instances of each of the different types of DDoS attacks are different. From the bar chart, it is seen clearly that the number of instances of the different classes of the DDoS attacks are not the same. That simply make the dataset imbalance, this simply means that if the data imbalance is not solved, the RNN classifier will produce high rate of false positive and negative. To solve the data imbalance problem, random over sampling needs to be performed. This was achieved using an over-sampling technique called RandomOverSampler. This was used this to down sample the dataset, making all the classes have equal number of instances. The down sampled data can be seen in the bar chart in Figure 3. Figure 4 shows the correlation matrix of the features that are correlated.

Finally, the most important features was extracted from the dataset by using the Random forest Classifier (RF). The RF classifier was used in ranking the features of the dataset. Table 1 shows the extracted features (The most important features), and Figure 5 shows the visualized plot of the important features.

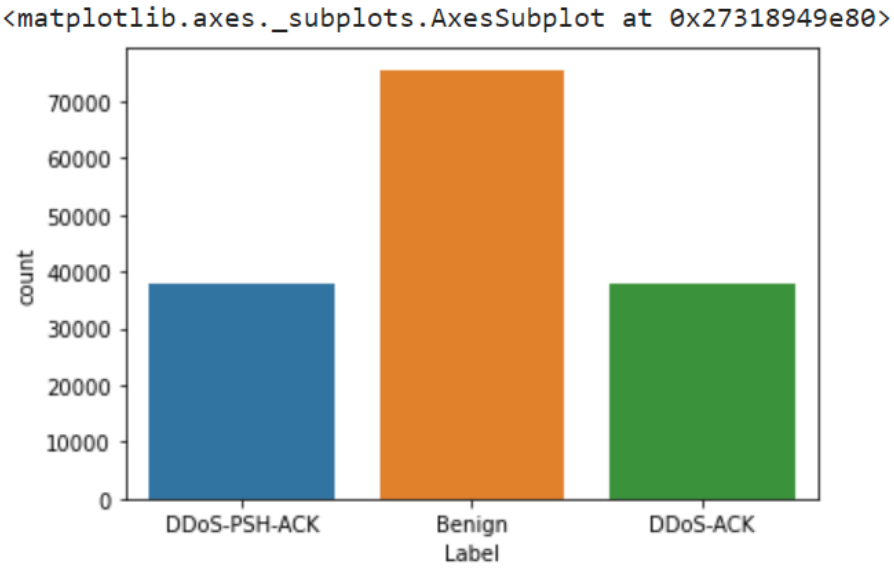

Figure 2: Bar chart of the imbalance class.

From the diagram, it is seen clearly that the number of instances of the target class are different. The class with the highest number of instances is that of the Benign class.

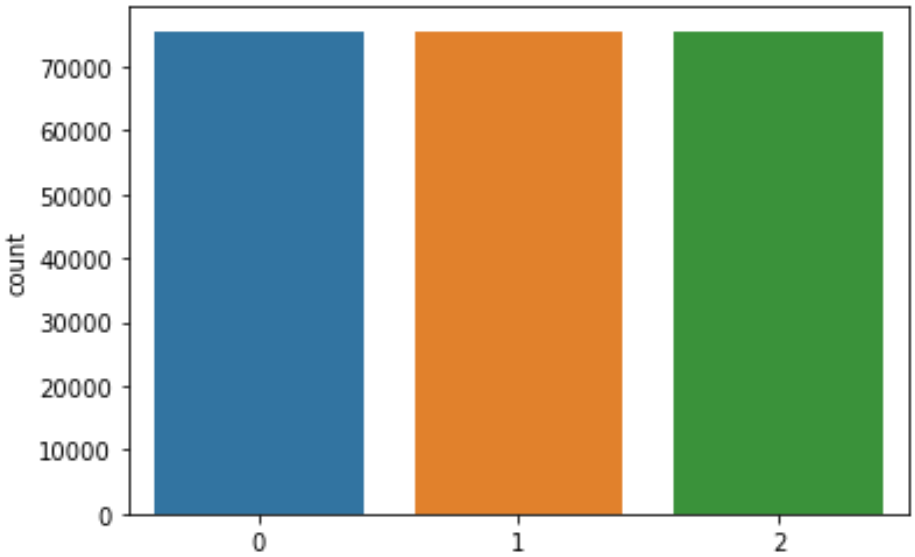

Figure 3: Bar chart of the imbalance class.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 11, November 2023

DOI: 10.17148/IJARCCE.2023.121101

From the diagram, it is seen clearly that the number of instances of the target class are the same.

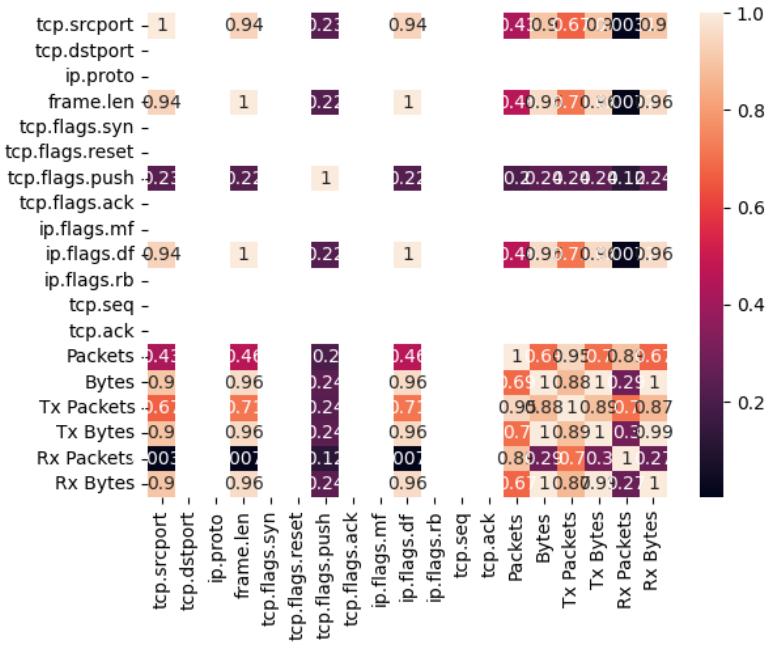

Figure 4: Correlation Matrix

The correlation matrix displays the features of the dataset that are correlated.

Table 1: Extracted Features

	Features	Important_Features
8	tcp.flags.push	0.255143
15	frame.time	0.222767
21	Rx Bytes	0.094308
2	tcp.srcport	0.093496
17	Bytes	0.089306
11	ip.flags.df	0.080300
19	Tx Bytes	0.066526
5	frame.len	0.047294
18	Tx Packets	0.027264
16	Packets	0.015311

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 11, November 2023

DOI: 10.17148/IJARCCE.2023.121101

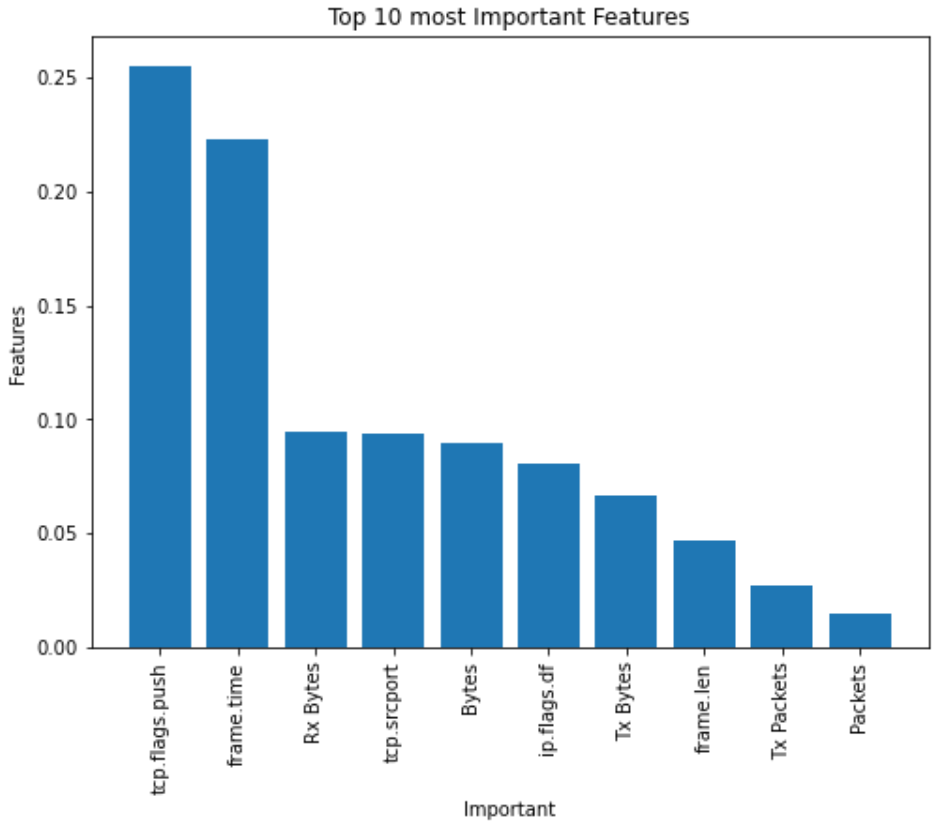

Figure 5: Extracted Features

B. Model Parameter Tuning and Training

This section describes the parameters and the processes used in training the RNN model for the detection of DDoS attacks on network logs. The RNN model was trained by fine tuning it's hyper parameters. The fine-tuned parameters of the RNN model has three layers, one input layer with input neuron of 256, a hidden layer with an input neural of 256, and finally the output layer with dense layer 5. The hyper parameters used here are relu and softmax for activation functions, optimizer = 'adam', and loss ='categorical_consentropy', batch_size=64, and epoch =7. The result of the LSTM model for both training and evaluation can be seen in Table 2. The evaluation of the LSTM model was validated on a test data. The evaluation matrix used are classification report and confusion matrix. The graphical analysis of Table 2 can be seen in Figure 6 and Figure 7. The classification report of the can be seen in Figure 4.6 and the confusion matrix can be seen in Figure 8.

Table 2: Simulation of the Model on 10 Steps

Epoch 1/10
63851/63851 [==============================] - 329s 5ms/step - loss: 0.0124 - accuracy: 0.9963 - val_loss: 0.0011 - val_accuracy: 0.9999
Epoch 2/10
63851/63851 [==============================] - 367s 6ms/step - loss: 8.1246e-04 - accuracy: 0.9999 - val_loss: 6.7327e-04 - val_accuracy: 0.9999
Epoch 3/10
63851/63851 [==============================] - 409s 6ms/step - loss: 0.0012 - accuracy: 0.9999 - val_loss: 9.5968e-04 - val_accuracy: 0.9999
Epoch 4/10
63851/63851 [==============================] - 383s 6ms/step - loss: 8.6852e-04 - accuracy: 0.9999 - val_loss: 8.3973e-04 - val_accuracy: 0.9999

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 11, November 2023

DOI: 10.17148/IJARCCE.2023.121101

Epoch 5/10
63851/63851 [==========] - 518s 8ms/step - loss: 0.0015 - accuracy: 0.9999 - val_loss: 5.7470e-04 - val_accuracy: 1.0000
Epoch 6/10
63851/63851 [==========] - 513s 8ms/step - loss: 0.0012 - accuracy: 0.9999 - val_loss: 7.7087e-04 - val_accuracy: 0.9999
Epoch 7/10
63851/63851 [==========] - 504s 8ms/step - loss: 9.4816e-04 - accuracy: 1.0000 - val_loss: 7.3796e-04 - val_accuracy: 0.9999
Epoch 8/10
63851/63851 [==========] - 489s 8ms/step - loss: 0.0011 - accuracy: 1.0000 - val_loss: 5.6745e-04 - val_accuracy: 1.0000
Epoch 9/10
63851/63851 [==========] - 636s 10ms/step - loss: 8.5152e-04 - accuracy: 1.0000 - val_loss: 0.0036 - val_accuracy: 1.0000
Epoch 10/10
63851/63851 [==========] - 395s 6ms/step - loss: 0.0020 - accuracy: 1.0000 - val_loss: 4.4836e-04 - val_accuracy: 1.0000

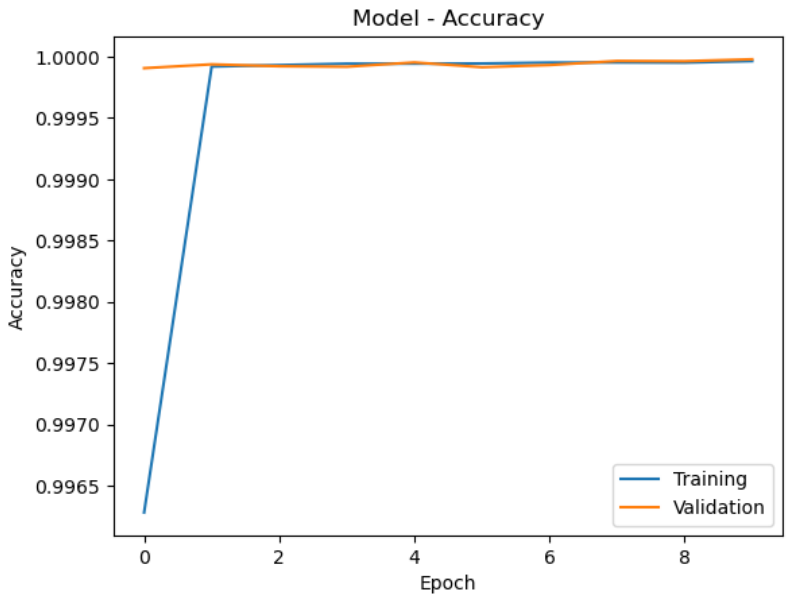

Figure 6: Training Accuracy for Both Training and Validation.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 11, November 2023

DOI: 10.17148/IJARCCE.2023.121101

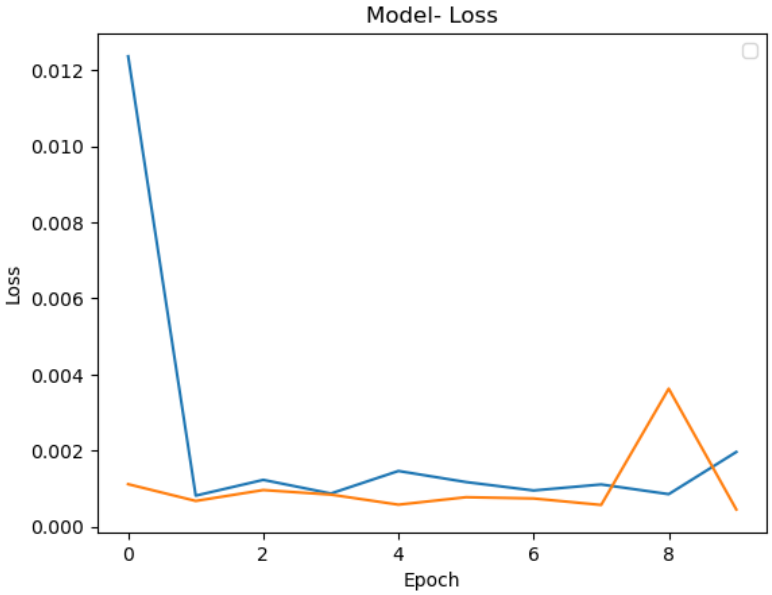

Figure 7: Loss values for training and Validation.

Classification_Report

	precision	recall	f1-score	support
DDoS-PSH-ACK	1.00	1.00	1.00	15075
Benign	1.00	1.00	1.00	15162
DDoS-ack	1.00	1.00	1.00	15123
accuracy			1.00	45360
macro avg	1.00	1.00	1.00	45360
weighted avg	1.00	1.00	1.00	45360

Figure 8: Classification Report

```
([<matplotlib.axis.YTick at 0x2731b79e2e0>,
  <matplotlib.axis.YTick at 0x273184c9df0>,
  <matplotlib.axis.YTick at 0x2731878a7f0>],
 [Text(0, 0.5, 'DDoS-PSH-ACK'),
  Text(0, 1.5, 'Benign'),
  Text(0, 2.5, 'DDoS-ack')])
```

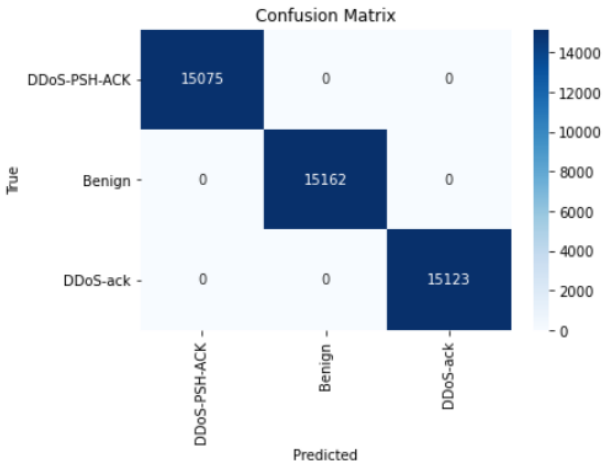

Figure 9: Confusion Matrix

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 11, November 2023
DOI: 10.17148/IJARCCE.2023.121101

V. CONCLUSION

The heading of the Acknowledgment section and the References section must not be numbered. Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template.

The hybrid model incorporating Random Forest for feature extraction and a Recurrent Neural Network (RNN) classifier for the detection of DDoS attacks on network logs has demonstrated exceptional performance. The model achieved an impressive accuracy of 99.99%, showcasing its remarkable capability in accurately discerning between normal network traffic and malicious DDoS attacks. Furthermore, the model exhibited outstanding precision in identifying true positives, with a rate of 99.99%. This indicates its proficiency in correctly classifying instances of DDoS attacks, crucial for timely response and mitigation. The false positive rate, standing at an incredibly low 0.0001%, underlines the model's precision in minimizing the occurrence of false alarms, which is essential for reducing unnecessary resource allocation and maintaining operational efficiency.

The integration of Random Forest for feature extraction and RNN for classification has proven to be a synergistic approach, harnessing the strengths of both algorithms to achieve exceptional results. Random Forest's proficiency in discerning relevant features from network logs provided a rich and discriminative feature set for the RNN classifier, enhancing its ability to make accurate predictions. This hybrid model represents a significant advancement in DDoS attack detection, showcasing the potential for combining traditional machine learning techniques with deep learning approaches. Its high accuracy, coupled with an impressive true positive rate and minimal false positives, instills confidence in its real-world applicability and effectiveness in safeguarding network infrastructures against DDoS threats. As such, this model stands as a promising tool for enhancing network security and resilience in the face of evolving cyber threats.

REFERENCES

[1] C. Shieh, T. Nguyen, W. Lin, W. Lai, M. Horng, & D. Miu, "Detection of adversarial ddos attacks using symmetric defense generative adversarial networks", Electronics, vol. 11, no. 13, p. 1977, 2022. https://doi.org/10.3390/electronics11131977

[2] "Ensemble dos attack detection with iot integration algorithm", International Journal of Emerging Trends in Engineering Research, vol. 8, no. 9, p. 6342-6346, 2020. https://doi.org/10.30534/ijeter/2020/230892020

[3] S. N. and K. Archana, "Detecting distributed denial of service (ddos) in sd-iot environment with enhanced firefly algorithm and convolution neural network", Optical and Quantum Electronics, vol. 55, no. 5, 2023. https://doi.org/10.1007/s11082-023-04553-x

[4] M. Munir, I. Ardiansyah, J. Santoso, A. Mustopa, & S. Mulyatun, "Detection and mitigation of distributed denial of service attacks on network architecture software defined networking using the naive bayes algorithm", Journal of Information System Management (Joism), vol. 3, no. 2, p. 51-55, 2022. https://doi.org/10.24076/joism.2022v3i2.656

[5] M. Ibrahim, A. Salawi, S. Alghamdi, N. Alkenani, A. Almuntashiri, R. Alghamdiet al., "Anomaly detection to counter ddos attacks on smart electric meter systems", International Journal of Cryptocurrency Research, vol. 2, no. 1, p. 12-18, 2022. https://doi.org/10.51483/ijccr.2.1.2022.12-18

[6] C. Li, Y. Wu, X. Yuan, Z. Sun, W. Wang, X. Liet al., "Detection and defense of ddos attack–based on deep learning in openflow-based sdn", International Journal of Communication Systems, vol. 31, no. 5, 2018. https://doi.org/10.1002/dac.3497

[7] A. Anggrawan, R. Azhar, B. Triwijoyo, & M. Mayadi, "Developing application in anticipating ddos attacks on server computer machines", Matrik Jurnal Manajemen Teknik Informatika Dan Rekayasa Komputer, vol. 20, no. 2, p. 427-434, 2021. https://doi.org/10.30812/matrik.v20i2.410

[8] M. Parimala*, "Shield advanced mitigation system of distributed denial of service attack in integration of internet of things and cloud computing environment", International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 2, p. 1300-1306, 2019. https://doi.org/10.35940/ijitee.a4841.129219

[9] H. Amari, L. Khoukhi, & L. Belguith, "Prediction and detection model for hierarchical software-defined vehicular network",, 2022. https://doi.org/10.1109/lcn53696.2022.9843483

[10] M. Khan, M. Nasralla, M. Umar, N. Ghani-Ur-Rehman, S. Khan, & N. Choudhury, "An efficient multilevel probabilistic model for abnormal traffic detection in wireless sensor networks", Sensors, vol. 22, no. 2, p. 410, 2022. https://doi.org/10.3390/s22020410

[11] F. Hussain, S. Abbas, M. Husnain, U. Fayyaz, F. Shahzad, & G. Shah, "Iot dos and ddos attack detection using resnet",, 2020. https://doi.org/10.1109/inmic50486.2020.9318216

[12] S. Sindian and S. Sindian, "An enhanced deep autoencoder-based approach for ddos attack detection", Wseas Transactions on Systems and Control, vol. 15, p. 716-724, 2020. https://doi.org/10.37394/23203.2020.15.72

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 11, November 2023
DOI: 10.17148/IJARCCE.2023.121101

[13] A. Abdulrahman and M. Ibrahem, "Evaluation of ddos attacks detection in a new intrusion dataset based on classification algorithms", Iraqi Journal of Information & Communications Technology, vol. 1, no. 3, p. 49-55, 2019. https://doi.org/10.31987/ijict.1.3.40

[14] M. Aslam, D. Ye, A. Tariq, M. Asad, M. Hanif, D. Ndziet al., "Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for sdn-enabled iot", Sensors, vol. 22, no. 7, p. 2697, 2022. https://doi.org/10.3390/s22072697

[15] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, & S. Camtepe, "Ae-mlp: a hybrid deep learning approach for ddos detection and classification", Ieee Access, vol. 9, p. 146810-146821, 2021. https://doi.org/10.1109/access.2021.3123791

[16] Y. Zhang, Y. Wang, Y. Hu, Z. Lin, Y. Zhai, L. Wanget al., "Security performance analysis of leo satellite constellation networks under ddos attack", Sensors, vol. 22, no. 19, p. 7286, 2022. https://doi.org/10.3390/s22197286

[17] C. Li, Y. Wu, X. Yuan, Z. Sun, W. Wang, X. Liet al., "Detection and defense of ddos attack–based on deep learning in openflow-based sdn", International Journal of Communication Systems, vol. 31, no. 5, 2018. https://doi.org/10.1002/dac.3497

[18] Dong, S., & Sarem, M. (2019). DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks. *IEEE Access*, *8*, 5039-5048.

[19] Amaizu, G. C., Nwakanma, C. I., Bhardwaj, S., Lee, J. M., & Kim, D. S. (2021). Composite and efficient DDoS attack detection framework for B5G networks. *Computer Networks*, *188*, 107871.

[20]. Jia, Y., Zhong, F., Alrawais, A., Gong, B., & Cheng, X. (2020). Flowguard: An intelligent edge defense mechanism against IoT DDoS attacks. *IEEE Internet of Things Journal*, *7*(10), 9552-9562.

[21]. Cil, A. E., Yildiz, K., & Buldu, A. (2021). Detection of DDoS attacks with feed forward based deep neural network model. *Expert Systems with Applications*, *169*, 114520.

[22]. Perez-Diaz, J. A., Valdovinos, I. A., Choo, K. K. R., & Zhu, D. (2020). A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access*, *8*, 155859-155872.

[23]. Hussain, F., Abbas, S. G., Husnain, M., Fayyaz, U. U., Shahzad, F., & Shah, G. A. (2020, November). IoT DoS and DDoS attack detection using ResNet. In *2020 IEEE 23rd International Multitopic Conference (INMIC)* (pp. 1-6). IEEE.

[24]. Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., ... & Shafiq, M. (2022). Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. *Sustainability*, *14*(14), 8374.

[25]. Ahuja, N., Singal, G., Mukhopadhyay, D., & Kumar, N. (2021). Automated DDOS attack detection in software defined networking. *Journal of Network and Computer Applications*, *187*, 103108.

[26]. Taylor, O. E., Ezekiel, P. S., & Igiri, C. G. Anomaly-Based Intrusion Detection/Prevention System using Deep Reinforcement Learning Algorithm. *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, 10(1), 58-65.

[27]. Taylor, O. E., & Ezekiel, P. S. (2022). A smart system for detecting behavioural botnet attacks using random forest classifier with principal component analysis. *European Journal of Artificial Intelligence and Machine Learning*, *1*(2), 11-16.