A Recommender System to Detect Distributed Denial of Service Attacks with Network and Transport Layer Features

Kağan Özgün[a], Ayşe Tosun[b] and Mehmet Tahir Sandıkkaya[c]
Department of Computer Engineering, Istanbul Technical University, Istanbul, Turkey

Keywords: Distributed Denial of Service Attacks, Network Traffic, Attack Detection, LSTM, Gaussian Naive Bayes.

Abstract: Detecting Distributed Denial of Service (DDoS) attacks are crucial for ensuring the security of applications and computer networks. The ability to mitigate potential attacks before they happen could significantly reduce security costs. This study aims to address two research questions concerning the early detection of DDoS attacks. First, we explore the feasibility of detecting DDoS attacks in advance using machine learning approaches. Second, we focus on whether DDoS attacks could be successfully detected using a Long Short-Term Memory (LSTM) based approach. We have developed rule-based, Gaussian Naive Bayes (GNB), and LSTM models that were trained and assessed on two datasets, namely UNSW-NB15 and CIC-DDoS2019. The results of the experiments show that 82–99% of DDoS attacks can be successfully detected 300 seconds prior to their arrival using both GNB and LSTM models. The LSTM model, on the other hand, is significantly better at distinguishing attacks from benign packets. Additionally, incident response teams could utilize a two-level alert mechanism that ranks the attack detection results, and take actions such as blocking the traffic before the attack occurs if our proposed system generates a high risk alert.

1 INTRODUCTION

In information security, accessibility is ensuring system and data availability is a key aspect. Denial of Service (DoS) attacks poses a threat to accessibility and aim to disrupt a targeted system by overwhelming it with excessive requests or resource consumption. The ultimate goal is causing prolonged service disruption and potential financial losses (Masdari and Jalali, 2016). Subsequently, Distributed Denial of Service (DDoS) attacks leverage compromised devices, i.e., bots, distribute malicious traffic across multiple sources, and thereby, raise mitigation challenges (Vishwakarma and Jain, 2020). Analyzing DDoS attacks reveals that the frequency of incoming packets can be used to identify sub-categories (Masdari and Jalali, 2016). Packet sizes and headers also indicate the subcategories of these attacks.

Mitigation methods developed on a rule-based logic, namely Intrusion Detection Systems (IDS) (Liu and Lang, 2019), can be integrated into network security systems for early detection for effective incident response (Chan et al., 2004). This underscores the importance of early identification to address potential threats. While rule-based approaches have traditionally been the primary choice for attack detection, they lack the capability for attack forecasting. To address the dynamic nature of network data, adaptive methods that learn from historical data are essential. Deep learning (DL) approaches provide flexibility and effectiveness in handling evolving attack scenarios (LeCun et al., 2015). Studies utilizing DL models for DDoS attack detection report impressive accuracy scores ranging from 95% to 99% (Stiawan et al., 2021; Ramzy Shaaban et al., 2019; Cil et al., 2021).

Notably, time-based network data has led to studies employing the LSTM model for DDoS attack classification, achieving accuracy and F1-score rates above 95% and 90% respectively (Gaur and Kumar, 2022; Li and Lu, 2019; Zou et al., 2022). These promising results are often reported on one dataset representing a limited number of attacks, making it unrealistic to expect similar performance in real systems. Furthermore, a significant drawback in studies using DL or other machine learning (ML) methods is their focus on detecting attack-containing network packets only after they have entered the network. This

[a] https://orcid.org/0009-0002-5094-4168
[b] https://orcid.org/0000-0003-1859-7872
[c] https://orcid.org/0000-0002-9756-603X

Özgün, K., Tosun, A. and Sandıkkaya, M.
A Recommender System to Detect Distributed Denial of Service Attacks with Network and Transport Layer Features.
DOI: 10.5220/0012350100003648

In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 390-397
ISBN: 978-989-758-683-5; ISSN: 2184-4356

limitation hinders early detection based on the behavior of network traffic, a crucial aspect for real-world applicability and reaching more benefits than post-attack classification.

This paper aims to propose a DL-based recommender system for early detection of incoming DDoS attacks. This system can be integrated as a valuable component into Security Information and Event Management (SIEM) systems (Catillo et al., 2022) to warn the incident response team before an attack occurs. Our research questions are listed below:

- RQ1: To what extent can we detect DDoS attacks (k seconds) prior to their arrival by employing DL techniques and network traffic data?
- RQ2: How successful is an LSTM model in detecting DDoS attack datasets compared to other rule-based and ML-based approaches?

To address these questions, we propose a recommender system utilizing LSTM, GNB, and rule-based models for detecting DDoS attacks k seconds in advance. This system generates early alerts for likely attacks, facilitating practical integration into network incident response teams and allowing the ranking of alerts based on their criticality.

2 RELATED WORK

In this section, we review relevant literature on SIEM systems and DDoS detection models. Catillo et al. (Catillo et al., 2022) developed a big data-operated SIEM system employing a semi-supervised deep Autoencoder model for anomaly detection in BG/L and Hadoop log records, and report recall of 96–99% and precision of 93–98%. Cinque et al. (Cinque et al., 2018) propose a rule-based SIEM system for air traffic data augmented with Latent Dirichlet Allocation, and report 90% precision and 93% recall in detecting anomalies.

Various works have addressed DDoS attack classification using ML methods (Wu et al., 2022; Halladay et al., 2022; Ramzy Shaaban et al., 2019; Cil et al., 2021) . We summarize studies utilizing the same datasets and algorithms with our research in Table 1. Each study uses different approaches for DDoS classification, either comparing the results of different DL methods or developing a better DL model by using different methods together. Boonchai et al. (Boonchai et al., 2022) compare the performance of DNN, Autoencoder, Logistic Regression, and Naïve Bayes models for DDoS classification, while the Autoencoder model outperforms all with 85% accuracy. Gaur and Kumar (Gaur and Kumar, 2022) explore binary and multi-classification approaches with LSTM layers, reporting accuracy values exceeding 99% and 98% respectively. In their study, the features in CIC-DDoS2019 dataset are grouped to increase the performance of the models. Zou et al. (Zou et al., 2022) propose FAMF-LSTM, a feature-attended multi-flow LSTM model, and outperform RNN and LSTM models with over 97% accuracy and 96% recall in two datasets. Li and Lu (Li and Lu, 2019) performed binary DDoS classification using an LSTM model and Bayesian approach, achieving 98% accuracy and 97% recall in their experiments.

3 METHODOLOGY

The methodological phase of the study is designed based on recommender system guidelines (Rezaimehr and Dadkhah, 2021) with specific details for DDoS detection.

3.1 Data Collection

Like in all data science studies, the development of recommender systems initiates with data collection and storing this acquired data. Datasets utilized in recommender systems are categorized as explicit or implicit, contingent upon the data collection method (Rezaimehr and Dadkhah, 2021). In our study's context, we employed two synthetically generated, and explicitly collected datasets that have been widely used in DDoS attack detection. The first of these datasets is a derived cyber-attack dataset released under the name UNSW-NB15 (Moustafa and Slay, 2015). The second dataset is CIC-DDoS2019 (Sharafaldin et al., 2019) which is specifically built out of known DDoS attack types.

UNSW-NB15. UNSW-NB15 dataset was created by the Cyber Range Lab at the University of New South Wales (UNSW) (Moustafa and Slay, 2015). The tool, IXIA PerfectStorm was used to automatically generate normal traffic data and synthetic attacks for modern networks. The raw network data in the established simulation environment has been recorded via the tcpdump tool, and is approximately 100GB. UNSW-NB15 includes nine different attack types apart from normal traffic data: Fuzzers, Analysis, Backdoors, DoS/DDoS, Exploits, Generic, Reconnaissance, Shellcode and Worms.

Argus and Bro-IDS tools were utilized to derive 49 different features from this dataset. The final dataset containing 49 columns and a total of 2,540,044 rows is shared as a CSV file in (Moustafa and Slay, 2015). In our study, we only need data

Table 1: Related works on DDoS attack detection.

Author	Model	Dataset	Performance
Proposed Method	LSTM	UNSW-NB15	0.83–0.82
		CIC-DDoS2019	0.99–0.99
(Zou et al., 2022)	FAMF-LSTM	BoT-IoT	0.99–1.00
		UNSW-NB15	0.97–0.96
(Boonchai et al., 2022)	DNN Autoencoder	CIC-DDoS2019	0.81–0.81
			0.85–0.85
(Gaur and Kumar, 2022)	LSTM (Binary)	CIC-DDoS2019	0.99–0.98
	LSTM (Multiclass)		0.98–0.98
(Li and Lu, 2019)	LSTM-BA	ISCX2012	0.98–0.97

[1] Metrics given as (Accuracy - Recall)

related to DoS attacks and benign network packets. Other attack categories were dropped from the dataset.

CIC-DDoS2019. CIC-DDoS2019 dataset, which was created at the Canadian Institute for Cybersecurity (CIC), University of New Brunswick (UNB), was generated specifically for research on DDoS attacks (Sharafaldin et al., 2019). While creating the simulation environment, the network data was generated by 25 different users using HTTP, HTTPS, FTP, SSH and email protocols on devices running different operating systems. Since the researchers aim to simulate subtypes of DDoS attacks, data belonging to 13 different DDoS attack types known as NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, TFTP and SYN are available in the dataset. The raw data contains 87 features and 70,619,331 rows of data.

3.2 Pre-Processing Data

In this study, we conducted several pre-processing steps to enhance the efficiency of our LSTM model for DDoS attack detection. First, categorical features in both datasets were converted into binary features using the one-hot encoding method. Subsequently, we normalized all numerical features to mitigate the risk of overfitting. To identify the most effective features for attack detection and reduce training costs, we trained an LSTM model with four layers, including dropout and dense layers. The top 10 features selected for both datasets are available in our GitHub repository (Ozgun, 2023).

Given that DDoS attacks typically target specific entities from multiple sources acting as bots, we implemented additional pre-processing steps to predict attacks occurring k seconds later. This involved distinguishing prior packets from the same source and targeting the same destination address. To achieve this, we applied a grouping strategy, grouping packets based on network addresses, utilizing a sliding window approach to prevent overlooking attacks from new sources.

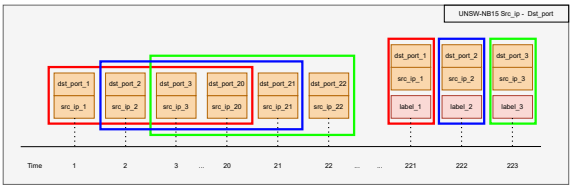

Figure 1: UNSW-NB15 (Source IP - Destination Port) Rule Based Data Preparation.

During model training, we divided the input data into mini-batches containing 50, 100, 150, and 200 packets. A sliding window was applied during the mini-batch creation phase to preserve the time-series structure of the data within each mini-batch. These mini-batch groups were employed to detect DDoS attacks in time series data after 300, 600, 1200, 1800, 2400, and 3000 packets. With an average of 100 ms between each packet, our models could detect attacks roughly 30, 60, 120, 180, 240, and 300 seconds in advance.

The grouping of packets based on network addresses was crucial for the success of our approach. For the UNSW-NB15 dataset, source IP–destination port and destination IP–destination port were used for grouping, while for the CIC-DDoS2019 dataset, source IP–destination IP was employed. This innovative approach allowed us to create a three-dimensional array that fits the LSTM model framework, enabling the model to consider reconnaissance attacks and providing a more comprehensive analysis of DDoS scenarios.

For Rule-Based Model. In the rule-based model, classification decisions are based solely on the source and destination addresses of the packets. The mini-batches and sliding windows are visually depicted in Figure 1, where different colors represent distinct elements. It is crucial to highlight that classification oc-

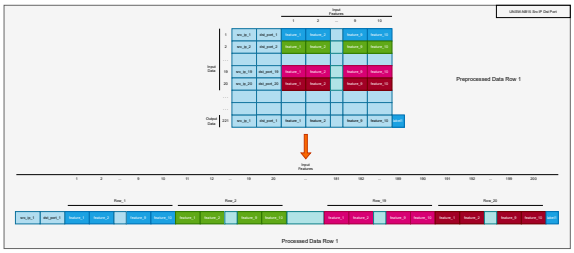

Figure 2: UNSW-NB15 (Source IP - Destination Port) Gaussian Naive Bayes Data Preparation.

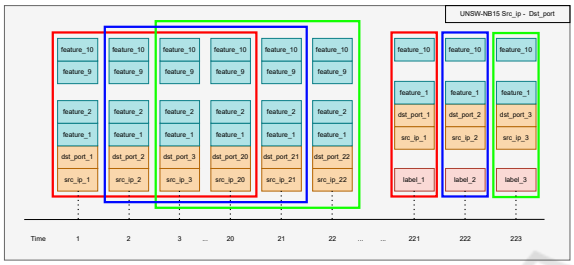

Figure 3: UNSW-NB15 (Source IP - Destination Port) LSTM Data Preparation.

curs for a given packet when it shares the same source IP and destination port as the first packet within its corresponding window. For instance, packets at the first and 221st seconds must have identical IP addresses and ports to undergo classification.

For GNB Model. In addition to grouping based on source and destination addresses, the GNB model was trained using the top 10 selected features. However, the GNB model inherently cannot process three-dimensional data. Consequently, the data within each group had to be concatenated to create a row vector. Figure 2 visually represents the structure of data from the UNSW-NB15 dataset in a mini-batch of 20 packets, illustrating the concatenation of different packets to form a row vector of 1×200. The output is derived from the packet at the 221st second.

For LSTM Model. The LSTM model is capable of handling arrays larger than two dimensions, so the GNB model's operation of concatenating the data was not performed. Instead, the three-dimensional data was directly fed as the input to the LSTM model, after the grouping process as we did in the other models. Figure 3 illustrates this process for UNSW-NB15.

3.3 Recommender Engine

Once essential data-related procedures are executed, the next phase is building a recommendation engine. In our study's context, we assessed three different classification-based methods to build our engine for DDoS attack detection. This section provides details on the models' designs and training/test procedures.

Rule-Based Model. We employed a rule-based model, a common method in attack detection, to assess its effectiveness in comparison to LSTM and GNB models. Rule-based models, popular among network security experts, assess packets based on source and destination addresses, flagging an attack if packet numbers surpass a set threshold. While experts can often set effective limits through observation, this approach is prone to human error, especially when done by non-experts, and can be easily deceived. In our rule-based model, determining the threshold for labeling a packet as an attack is crucial. A threshold of one flags all subsequent packets as attacks, leading to numerous false positives. Conversely, a very high threshold, like 200, may result in missing attacks and generating high false negatives. We opted for two thresholds, three and five, indicating attack criticality. If there are more than three but less than 6 packets with the same source and destination addresses within our mini-batch data, subsequent packets are labeled as potentially containing a DDoS attack (Level 1). If there are more than five such packets, we label it as a Level 2 attack. Fewer than three packets are marked as benign.

GNB Model. GNB model is used as the base ML model in our study. Unlike the rule-based model, since features other than the source IP/port and destination IP/port information are used as input, a more efficient attack detection would be made by processing the data of the reconnaissance process, especially before the attack starts. GNB model has been reported to produce effective attack detection in datasets containing known attack types and network movements (Belavagi and Muniyal, 2016). For this reason, we utilize this model as a simple and robust alternative to the LSTM model. Within the scope of our study, we implemented the GNB model in the Python *sklearn* library. We have divided the datasets as 70% train and 30% test. We kept the same grouping used in the rule-based model to perform detection on the same data instances over three models.

LSTM Model. We developed a LSTM-based model, known for its efficacy in handling time-series data (Siami-Namini et al., 2019). Unlike GNB, LSTM does not impose specific data distributions, and unlike rule-based models, it accommodates information from multiple features in multi-dimensional forms. LSTM, with its various memory types, processes historical data and adapts to changing data in deep learning approaches (Van Houdt et al., 2020), making it suitable for detecting attacks k seconds in advance by observing prior packets over time. Our proposed LSTM model comprises four layers: LSTM layer

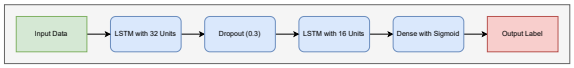

Figure 4: LSTM Model Structure.

with 32 units, enabling the model to learn from input data and maintain memory of previous inputs. Dropout layer to prevent overfitting by randomly deactivating neurons during training, enhancing model robustness (Sanjar et al., 2020). Additional LSTM layer with 16 units, capturing complex temporal patterns in the data. Dense layer with a sigmoid activation function for binary classification, determining the presence of an attack in the received packet. This architecture is designed to effectively handle time-series data, capture temporal dependencies, prevent overfitting, and make binary classifications related to DDoS attacks. Fig. 4 shows the general structure of our model. The training and test splits as well as grouping of data are the same as those described in the GNB models.

3.4 Ranking

The system introduces a two-level alert mechanism for incident response teams instead of providing binary results for detecting attacks k seconds in advance. Level 1 packets signify a likelihood of containing attacks, while Level 2 packets are considered high-risk, indicating a very probable attack. Benign packets are classified as safe, indicating no attacks. The ranking is based on posterior probabilities generated by the models during classification. In GNB and LSTM models, a Level 1 alert is triggered when the posterior probability falls between 51% and 75%, while a Level 2 alert is generated for probabilities exceeding 75%. The rule-based model, not producing probabilities, relies on the count of packages in mini-batches from the same source and going to the same destination. In this context, more than three packages prompt a Level 1 alert, while more than five packets trigger a Level 2 alarm.

4 RESULTS

In total, 144 different experiments were performed with combinations of two different datasets, three different models, two different data grouping approaches and 24 different experimental configurations due to mini-batch sizes and detection windows (k seconds). In order to discuss the results more effectively, a sample is reported in this section: Three models, two datasets, two different groupings with two mini-batch sizes (100 and 200 packets) and three detection windows (60 and 300 seconds).

RQ1. In order to answer our first RQ, we have analyzed LSTM and GNB models' performance presented in Table 2. Please note that we have analyzed the findings on Level 1 scores only because this level indicates that any packet with more than 50% probability is labelled as attack. Experiments show that network traffic data can be used to effectively detect 80-99% DDoS attacks (recall rates) 30 to 300 seconds in advance. The precision rates also show that the models produce very low false positives while detecting the attacks. When we examine Table 2 in detail, it is seen that both GNB and LSTM models distinguish attacks from benign packets in CIC-DDoS2019 dataset successfully, although this is an attack-intensive dataset. F1-scores of 96%–99% with GNB and 97%–99% with LSTM are reported for detecting attacks. The rates are similar for detecting benign packets, although LSTM is slightly better in detecting benign packets in terms of recall and F1-score. For UNSW-NB15 dataset, which is a dataset with 10% attack data, we observe that the LSTM model outperforms GNB in detecting attacks: An accuracy rate of 81–83%, and an F1-score of 78–81% are achieved for detecting the packets that contain an attack. Furthermore, we have assessed the impact of mini-batch size and k seconds on the performance of the LSTM model for both datasets.

We have seen that increasing the mini-batch size slightly improves the performance, whereas increasing k value does not necessarily affect the findings. For instance, in UNSW-NB15, using mini-batch size of 20 packets and detecting attacks 60 seconds in advance gives us an F1-score of 82%, whereas mini-batch size of 100 packets and detecting 60 seconds in advance gives an F1-score of 85% in case of Level 1 attacks. However, mini-batch size of 200 and k value of 60 or k value of 300 both give F1-scores of 85% and recall 77–79% for benign and attack packets, respectively. Thus, we report higher mini-batch values and three packet counts in Table 2. We recommend choosing the k value as 300 seconds in order to give the network security teams the necessary time for intervention, as it has been seen as the most appropriate configuration for both the accuracy of the recommender made and for sending notifications in advance of the required time.

RQ2. We compare the models' performance with each other to answer this RQ. Overall, LSTM outperforms other models in distinguishing attacks from other packets on both datasets with varying attack rates. The rule-based model manages to achieve 59–99% F1-Score for attacks but poorly performs for be-

nign packets in terms of F1-score on both datasets. The F1-score of attacks drops from 99% to 59% when we observe UNSWNB-15 dataset, as this model tends to classify majority of the packets as attack. This shows us the problem with the rule-based models due to false positive rates. When we look at the results of GNB model in Table 2, we observe an opposite scenario on UNSWNB-15 dataset: 70% F1-score is reported for benign packets, whereas the F1-score rates are very low (1%) for detecting the attacks. This indicates that GNB model is not able to detect attack packets in the context of our experimental design. When we look at the results on CIC-DDoS2019 dataset, the model reaches F1-scores above 96% for detecting attacks, and around 81% for detecting benign packets. Additionally, when we examine the precision and recall values, we can say that GNB is much more successful than the rule-based model, especially on CIC-DDoS2019 dataset. Upon scrutinizing the outcomes of the LSTM model, it becomes evident that it consistently outperforms other models in distinguishing both classes in the datasets. We observe an F1-score of over 78% and 97% for detecting attacks in two datasets, UNSW-NB15 and CIC-DDoS2019 respectively.

When we assess our findings with respect to their consistency (Avazpour et al., 2014), we can interpret that the results of the experiments conducted on UNSW-NB15 dataset, which is closer to real-life network traffic, are more realistic, and LSTM shows its effectiveness on this dataset. We need further experiments to prove LSTM model's stability on real-life data, but our offline analysis gives useful insights on its potential.

5 DISCUSSION

Level-Based Analysis. Our recommender system offers a two-level alert mechanism, prioritizing likely attacks for efficient incident response. Table 2 illustrates model performance for both alert levels. Since each packet has a single label (benign/attack) in both datasets, evaluating the performance involves categorizing packets into Level 1 or Level 2 attacks based on algorithmic posterior probabilities. A Level 1 attack is identified if the probability exceeds 50%, and a Level 2 attack is declared if the probability is above 75%. LSTM's Level 2 alert performance exhibits lower recall but higher precision compared to Level 1, indicating conservative but mostly accurate detection. In a real-life scenario, prioritizing Level 2 alerts can aid incident response teams in preemptive actions like traffic blocking before an attack unfolds. The conservative nature of Level 2 alerts, with lower false positives, aligns with expert decisions. Although delaying action on Level 1 alerts may miss some incoming attacks within the next 300 seconds, configuring the recommender system to generate forecasts and monitor alert level changes can address this concern. Neither rule-based nor GNB can provide such a ranking system in our study. Rule-based lacks probabilities, and GNB produces probabilities close to zero or one for selected datasets.

Training Configurations. The experimental phase of the study starts by trying different split rates for training, testing and validation. In addition to the presented results, two other split rates are evaluated for the LSTM model. One of them is split as 60%, 20%, 20% respectively for train, validation and testing. The other one is similarly split into 60, 30, 10. We observe that using a validation set improves detecting benign packets in CIC-DDoS2019, as the benign packets represent a minority class in this dataset, and tuning the parameters using a validation set generates a more successful model. However, since we cannot build the GNB model using a train-validation-test split, the results of these different training configurations were excluded from the experiments. We continued with 70% train and 30% test data while reporting this study.

Grouping Strategy. While performing data processing operations in the analysis part of the study, two different grouping strategies were applied on each dataset. These strategies simply consider grouping the packets coming from the same source IP or going to the same destination IP. For the UNSW-NB15 dataset, we also added the destination port next to the IP information during grouping because we have observed that adding this information increases the performance of attack detection. Overall, a grouping strategy is necessary to build time-series based models and to detect incoming attacks in advance. However, we cannot clearly say which information in the grouping matters the most. Both source IP and destination IP based groupings report similar performance in detecting attacks 300 seconds in advance. The decision of which information to use in a grouping should be made according to the traffic data structure.

6 CONCLUSION

We have designed and implemented a recommender system that can be used as part of SIEM systems, with a specific focus on detecting DDoS attacks k seconds in advance. We have trained LSTM, GNB, and rule-based models to answer our two RQs.

Table 2: Performance of rule-based, GNB and LSTM models.

	Dataset	Group By[1]	Alert Level	Config[2]	Accuracy	Recall[3]	Precision[3]	F1 Score[3]
Rule-based model	UNSW-NB15	dstip-dport	Level 1	100 / 60	0.56	0.15 / 0.97	0.85 / 0.53	0.25 / 0.69
	UNSW-NB15	dstip-dport	Level 2	100 / 60	0.58	0.19 / 0.95	0.81 / 0.54	0.31 / 0.64
	UNSW-NB15	srcip-dport	Level 1	100 / 60	0.50	0.28 / 0.72	0.50 / 0.50	0.36 / 0.59
	UNSW-NB15	srcip-dport	Level 2	100 / 60	0.50	0.29 / 0.71	0.50 / 0.50	0.24 / 0.60
	UNSW-NB15	dstip-dport	Level 1	200 / 300	0.53	0.09 / 0.99	0.95 / 0.51	0.16 / 0.67
	UNSW-NB15	dstip-dport	Level 2	200 / 300	0.55	0.14 / 0.99	0.95 / 0.52	0.24 / 0.68
	UNSW-NB15	srcip-dport	Level 1	200 / 300	0.49	0.19 / 0.80	0.51 / 0.49	0.28 / 0.61
	UNSW-NB15	srcip-dport	Level 2	200 / 300	0.49	0.19 / 0.80	0.51 / 0.49	0.28 / 0.61
	CIC-DDoS2019	dstip	Level 1	100 / 60	0.95	0.08 / 0.99	0.98 / 0.95	0.08 / 0.98
	CIC-DDoS2019	dstip	Level 2	100 / 60	0.96	0.08 / 0.99	0.95 / 0.96	0.14 / 0.98
	CIC-DDoS2019	srcip	Level 1	100 / 60	0.91	0.03 / 0.99	0.99 / 0.91	0.06 / 0.96
	CIC-DDoS2019	srcip	Level 2	100 / 60	0.92	0.05 / 0.99	0.96 / 0.92	0.10 / 0.96
	CIC-DDoS2019	dstip	Level 1	200 / 300	0.96	0.02 / 0.99	0.93 / 0.96	0.03 / 0.99
	CIC-DDoS2019	dstip	Level 2	200 / 300	0.96	0.03 / 0.99	0.93 / 0.96	0.06 / 0.98
	CIC-DDoS2019	srcip	Level 1	200 / 300	0.93	0.01 / 0.99	0.99 / 0.93	0.02 / 0.99
	CIC-DDoS2019	srcip	Level 2	200 / 300	0.93	0.02 / 0.99	0.99 / 0.93	0.03 / 0.96
Gaussian Naïve Bayes model	UNSW-NB15	dstip-dport	Level 1	100 / 60	0.54	0.99 / 0.01	0.54 / 0.97	0.70 / 0.01
	UNSW-NB15	dstip-dport	Level 2	100 / 60	0.54	0.99 / 0.01	0.54 / 0.97	0.70 / 0.01
	UNSW-NB15	dstip-dport	Level 1	200 / 300	0.56	0.99 / 0.01	0.56 / 0.94	0.72 / 0.01
	UNSW-NB15	dstip-dport	Level 2	200 / 300	0.56	0.99 / 0.01	0.56 / 0.94	0.72 / 0.01
	UNSW-NB15	srcip-dport	Level 1	100 / 60	0.54	0.99 / 0.01	0.54 / 0.97	0.70 / 0.01
	UNSW-NB15	srcip-dport	Level 2	100 / 60	0.54	0.99 / 0.01	0.54 / 0.97	0.70 / 0.01
	UNSW-NB15	srcip-dport	Level 1	200 / 300	0.56	0.99 / 0.01	0.56 / 0.95	0.72 / 0.01
	UNSW-NB15	srcip-dport	Level 2	200 / 300	0.56	0.99 / 0.01	0.56 / 0.95	0.72 / 0.01
	CIC-DDoS2019	dstip	Level 1	100 / 60	0.98	0.80 / 0.99	0.99 / 0.97	0.89 / 0.99
	CIC-DDoS2019	dstip	Level 2	100 / 60	0.98	0.80 / 0.99	0.99 / 0.97	0.89 / 0.99
	CIC-DDoS2019	dstip	Level 1	200 / 300	0.98	0.77 / 0.99	0.99 / 0.97	0.87 / 0.99
	CIC-DDoS2019	dstip	Level 2	200 / 300	0.98	0.77 / 0.99	0.99 / 0.97	0.87 / 0.99
	CIC-DDoS2019	srcip	Level 1	100 / 60	0.94	0.71 / 0.99	0.99 / 0.93	0.83 / 0.96
	CIC-DDoS2019	srcip	Level 2	100 / 60	0.94	0.71 / 0.99	0.99 / 0.93	0.83 / 0.96
	CIC-DDoS2019	srcip	Level 1	200 / 300	0.94	0.68 / 0.99	0.99 / 0.93	0.81 / 0.96
	CIC-DDoS2019	srcip	Level 2	200 / 300	0.94	0.68 / 0.99	0.99 / 0.93	0.81 / 0.96
LSTM model	UNSW-NB15	dstip-dport	Level 1	100 / 60	0.82	0.84 / 0.80	0.83 / 0.81	0.84 / 0.81
	UNSW-NB15	dstip-dport	Level 2	100 / 60	0.82	0.92 / 0.71	0.79 / 0.88	0.85 / 0.78
	UNSW-NB15	dstip-dport	Level 1	200 / 300	0.82	0.79 / 0.85	0.87 / 0.76	0.83 / 0.80
	UNSW-NB15	dstip-dport	Level 2	200 / 300	0.83	0.89 / 0.75	0.82 / 0.85	0.85 / 0.79
	UNSW-NB15	srcip-dport	Level 1	100 / 60	0.82	0.84 / 0.80	0.83 / 0.81	0.84 / 0.81
	UNSW-NB15	srcip-dport	Level 2	100 / 60	0.81	0.91 / 0.70	0.78 / 0.87	0.84 / 0.78
	UNSW-NB15	srcip-dport	Level 1	200 / 300	0.83	0.83 / 0.82	0.85 / 0.79	0.84 / 0.81
	UNSW-NB15	srcip-dport	Level 2	200 / 300	0.83	0.90 / 0.74	0.81 / 0.85	0.85 / 0.79
	CIC-DDoS2019	dstip	Level 1	100 / 60	0.99	0.92 / 0.99	0.99 / 0.99	0.96 / 0.99
	CIC-DDoS2019	dstip	Level 2	100 / 60	0.99	0.93 / 0.99	0.99 / 0.99	0.96 / 0.99
	CIC-DDoS2019	dstip	Level 1	200 / 300	0.96	0.61 / 0.99	0.99 / 0.96	0.76 / 0.99
	CIC-DDoS2019	dstip	Level 2	200 / 300	0.97	0.70 / 0.99	0.99 / 0.97	0.82 / 0.99
	CIC-DDoS2019	srcip	Level 1	100 / 60	0.98	0.90 / 0.99	0.99 / 0.97	0.95 / 0.99
	CIC-DDoS2019	srcip	Level 2	100 / 60	0.98	0.91 / 0.99	0.99 / 0.97	0.95 / 0.99
	CIC-DDoS2019	srcip	Level 1	200 / 300	0.96	0.77 / 0.99	0.99 / 0.95	0.87 / 0.97
	CIC-DDoS2019	srcip	Level 2	200 / 300	0.96	0.79 / 0.99	0.99 / 0.95	0.88 / 0.98

[1] **dstip-dport**: Destination IP - Destination Port. **srcip-dport**: Source IP - Destination Port.
[2] Packet count used / detection for next k seconds
[3] Metrics given as (normal / attack)

As a result of our experiments, we have successfully managed to propose a system that runs with an LSTM-based model and is capable of detecting 82% of DDoS attacks 300 seconds in advance. We chose to use two different datasets from the literature and intentionally picked these with different characteristics in terms of attack traffic density. However they both are synthetically generated, and in turn, we could not fully observe how the performance of our proposed model would be in real life. As a future work of this study, running similar models on network data collected from real environments will be pursued. Ad-

ditionally, using this as an SIEM system component designed for detecting DDoS attacks in a real-life system, and evaluating its performance together with the experts could be future research directions. This way, we could evaluate how such systems reduce network security costs and benefit to incident response teams.

REFERENCES

Avazpour, I., Pitakrat, T., Grunske, L., and Grundy, J. (2014). Dimensions and Metrics for Evaluating Recommendation Systems. In Robillard, M. P., Maalej, W., Walker, R. J., and Zimmermann, T., editors, *Recommendation Systems in Software Engineering*, pages 245–273. Springer Berlin Heidelberg, Berlin, Heidelberg.

Belavagi, M. C. and Muniyal, B. (2016). Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection. *Procedia Computer Science*, 89:117–123.

Boonchai, J., Kitchat, K., and Nonsiri, S. (2022). The Classification of DDoS Attacks Using Deep Learning Techniques. In *2022 7th International Conference on Business and Industrial Research (ICBIR)*, pages 544–550.

Catillo, M., Pecchia, A., and Villano, U. (2022). AutoLog: Anomaly detection by deep autoencoding of system logs. *Expert Systems with Applications*, 191:116263.

Chan, A., Ng, W., Yeung, D., and Tsang, C. (2004). Refinement of rule-based intrusion detection system for denial of service attacks by support vector machine. In *Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.04EX826)*, pages 4252–4256.

Cil, A. E., Yildiz, K., and Buldu, A. (2021). Detection of ddos attacks with feed forward based deep neural network model. *Expert Systems with Applications*, 169:114520.

Cinque, M., Cotroneo, D., and Pecchia, A. (2018). Challenges and Directions in Security Information and Event Management (SIEM). In *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, pages 95–99.

Gaur, V. and Kumar, R. (2022). DDoSLSTM: Detection of Distributed Denial of Service Attacks on IoT Devices using LSTM Model. In *2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, pages 01–07.

Halladay, J., Cullen, D., Briner, N., Warren, J., Fye, K., Basnet, R., Bergen, J., and Doleck, T. (2022). Detection and Characterization of DDoS Attacks Using Time-Based Features. *IEEE Access*, pages 49794–49807.

LeCun, Y., Bengio, Y., and Hinton, G. (2015). Deep learning. *Nature*, pages 436–444.

Li, Y. and Lu, Y. (2019). LSTM-BA: DDoS Detection Approach Combining LSTM and Bayes. In *2019 Seventh International Conference on Advanced Cloud and Big Data (CBD)*, pages 180–185.

Liu, H. and Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences*, 9(20).

Masdari, M. and Jalali, M. (2016). A survey and taxonomy of DoS attacks in cloud computing. *Security and Communication Networks*, pages 3724–3751.

Moustafa, N. and Slay, J. (2015). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 Military Communications and Information Systems Conference (MilCIS)*, pages 1–6.

Ozgun, K. (2023). A Recommender System to Detect Distributed Denial of Service Attacks with Network and Transport Layer Features. https://github.com/kaganozgun/dos-prediction-with-lstm.

Ramzy Shaaban, A., Abdelwaness, E., and Hussein, M. (2019). TCP and HTTP Flood DDOS Attack Analysis and Detection for space ground Network. In *2019 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, pages 1–6.

Rezaimehr, F. and Dadkhah, C. (2021). A survey of attack detection approaches in collaborative filtering recommender systems. *Artif Intell Rev*, pages 2011–2066.

Sanjar, K., Rehman, A., Paul, A., and JeongHong, K. (2020). Weight Dropout for Preventing Neural Networks from Overfitting. In *2020 8th International Conference on Orange Technology (ICOT)*, pages 1–4.

Sharafaldin, I., Lashkari, A. H., Hakak, S., and Ghorbani, A. A. (2019). Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. In *IEEE 53rd International Carnahan Conference on Security Technology*, pages 1–6.

Siami-Namini, S., Tavakoli, N., and Namin, A. S. (2019). The Performance of LSTM and BiLSTM in Forecasting Time Series. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 3285–3292.

Stiawan, D., Suryani, M. E., Susanto, Idris, M. Y., Aldalaien, M. N., Alsharif, N., and Budiarto, R. (2021). Ping Flood Attack Pattern Recognition Using a K-Means Algorithm in an Internet of Things (IoT) Network. *IEEE Access*, pages 116475–116484.

Van Houdt, G., Mosquera, C., and Nápoles, G. (2020). A review on the long short-term memory model. *Artificial Intelligence Review*, 53(8):5929–5955.

Vishwakarma, R. and Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication Systems*, 73(1):3–25.

Wu, Z., Zhang, H., Wang, P., and Sun, Z. (2022). RTIDS: A Robust Transformer-Based Approach for Intrusion Detection System. *IEEE Access*, pages 64375–64387.

Zou, L., Wei, Y., Ma, L., and Leng, S. (2022). Feature-Attended Multi-Flow LSTM for Anomaly Detection in Internet of Things. In *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1–6.