International Journal of Computer Networks and Communications Security

VOL. 8, NO. 10, October 2020, 93–99
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

A Deep Learning based approach for DDoS attack detection in IoT-enabled smart environments

Umar Mohammed Badamasi[1], Sharjeel Khaliq[2], Omodolapo Babalola[3], Shafiu Musa[4], Tahir Iqbal[5]

[1, 4] Changchun University of Science and Technology China

[2] Government College University Faisalabad Pakistan

[3] Northwestern Polytechnical University Xian China

[5] Northeastern University Shenyang, Liaoning Province China

[1]umohammed4u@gmail.com, [2]musashafiu@gmail.com, [3]omodolapo.babalola@mail.nwpu.edu.cn

ABSTRACT

This research contributes to enhance the security of smart environments such as Internet-of-Things (IoT) network. IoT provides a big network to connect things around the world in concern to reduce human effort and to make a digitalized world more easily controllable. The heterogeneous and vulnerable nature of IoT network makes its environment a big target for cyber hackers. The ever-increasing nature of cyber threats as well as rapid development and growth of IoT infrastructure generates a severe need for the security of smart networks. One of the major threats that can take down the complete availability of targeted system is DDoS (Distributed Denial of Service) attack, which recently has attacked numerous IoT networks lead to enormous losses. Therefore, in order to secure IoT networks, the authors propose Deep Learning (DL) based Cuda-enabled Long-Short-Term-Memory (LSTM) technique with evaluation using latest CICDDoS2019 dataset for detection of DDoS attacks. The proposed system achieves highest accuracy of 99.60% and proves itself best as compared to current state-of-the-art solutions in the domain. Finally, we cross validate our results for the indication of unbiased performance.

Keywords: *IoT, DDoS, Deep Learning, LSTM, CICDDoS2019.*

1 INTRODUCTION

The growth of technology turned itself to the latest and emerging IoT paradigm, which makes connection of things everywhere in the world over the internet. The promising IoT technology aims to provide ease to our lives and society [1]. IoT comprises super computers as well as tiny devices or smart items that are networked together and without the interference of any human make connections all over the world through internet. IoT provides connections amongst diverse categories of smart things extending from super-computers to little objects that may consume very low processing power, therefore, it is a severe challenge to secure such a network and henceforward cyber-security is much ambiguous for the implementation in IoT network [2]. The IoT network comprises smart devices linked to the routers that make connections to the datacenters and clouds for communication. The defined architecture of IoT based network is depicted in Fig.1.

Moreover, with the several outstanding features, IoT environment is vulnerable to the major cyber threats and attacks. For this reason, the security of IoT enabled smart environments is a major concern. Major cyber-attacks can severely threaten the IoT network out of which one of the dangerous attack called Distributed Denial of Service (DDoS) attack [3]. It is a kind of attack, which can take down the entire availability of targeted system. These outbreaks can get success by exploiting multiple operating systems to compromise and use them as the bases of attack traffic. The compromised or exploited systems may include several devices as well as networks such as IoT, fog devices, and some more. Many techniques have been developed for securing IoT paradigm including Machine Learning (ML), Deep Learning (DL) [4]; Artificial Intelligence (AI) based Intrusion Detection System (IDS), and Intrusion Prevention System (IPS), etc.

IDS tends to be an efficient and very effective approach for performing network based attacks and threat detection [5]. Mostly, the current available IDS schemes are designed using ML based algorithms for model training and detection of cyber-attacks hitting different networks. Management of network-based security challenges involves three general approaches (i.e., threat-prevention, threat-detection as well as threat-mitigation). To make a security system or solution successful for securing IoT networks, all these three measures should be adopted perfectly. Diverse IDS approaches have been proposed using ML techniques. ML techniques have some limitations such as feature engineering problems outlined by the authors in [6]. To overcome these issues DL techniques have been adopted extensively.

IDS development based on DL techniques provides an advantage over traditional ML based solutions because they help to work over the challenge of appropriate feature engineering [7].

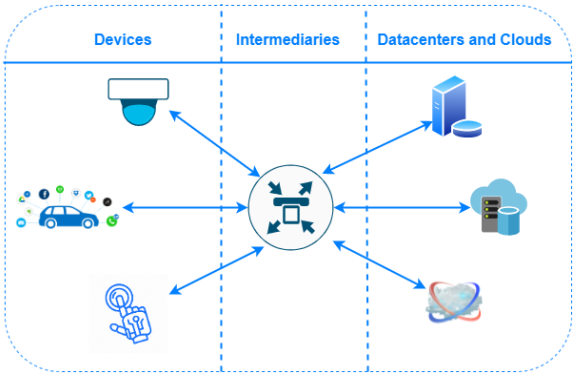

Fig. 1. IoT Network

On the other hand, the most important challenges of DL are highlighted as the lack of transparency in DL based security applications as well as the DL models are more vulnerable to adversarial attacks [7][8]. Still, DL based security solutions are more efficient and provide high accuracy with low rate of false alarms in many cases. As the IoT paradigm is more attractive target for attackers to spread on DDoS attack due to its rapid growth and extensive adoption. Therefore, in this research, we work to secure IoT network from emerging DDoS threats. We propose an efficient state-of-the-art DL based DDoS detection scheme for the detection and classification of malicious or compromised network traffic inside an IoT network.

Using LSTM-enabled DL classifier, we effectively perform detection of several DDoS attacks targeting IoT networks, our dataset include diverse categories of DDoS attacks for the assessment in our experimentation, classified in two main categories (i.e., Reflection attacks and Exploitation attacks) with multiple sub-categories, whereas classification and differentiation of these malicious intents from the authentic traffic in network. The main contributions of our research work are manifold:

- The authors employed latest and up-to-date openly available dataset of realistic network traffic namely CICDDoS2019.
- Construction of LSTM-enabled deep model for DL based threat detection method comprising multi-class attack classifications in the network of IoT achieving highest accuracy with lowest False Positives Rate (FPR).
- Further, we have cross-validated our work for showing unbiased results using 3-fold cross validation.
- In addition, we have compared our model performance with existing state-of-the-art researches.

Remaining sections of article are organized as following: Section 2 carries out the study of related work. Section 3 discusses the proposed methodology in detail. In Section 4, we present main implementation and experimental setups along with dataset description and algorithm structure. Results and discussion are illustrated in Section 5. Finally, we conclude our work with future indications in Section 6.

2 RELATED WORK

For proving the significance of our work, in this section, we have discussed different works of researchers along with their achievements in the domain. The authors [9] introduced the algorithms in which they provides the correct and incorrect intrusion detection lacking operator input system having the capability of identification and random environment which is changing timely. The basic objective of an algorithm is to have the accuracy of 34% in all the detection intrusion systems, which have recognized quantities of intrusions accomplished packets. The two tired negative determination process utilized to decline the affected packets by co-stimulation. The artificial neural network via intrusion detection provided by the work in [10] that uses the Artificial Neural Network (ANN) technique, ANN have the ability to distinguish the normal packets and the malicious ones. The main objective of ANN is to reduce the false positive rate, which is less than 2%. The ANN is using both the Cyber traffic analyzer and conventional network traffic. The basic demonstration of false positive rate has been increasing and decreasing and it is less than 2%.

Researchers in [11] proposed a Gated Recurrent Unit Recurrent Neural Network (GRU-RNN) has enabled the intrusion detection systems for SDNs. However, the proposed system has been tested using the oldest NSL-KDD dataset, the accuracy rate achieved by the model is very low (i.e., 89%) with only six features. The experiment results shows that the suggested model does not perform well for the attack classification in networks. The accuracy rate that proposed by the f model is 80%, TPR of the GRU-DNN is 90% and the FPR is 10%. These algorithms has higher TPR and lower FPR compared to other algorithms. The research [12] proposed a fog-assisted software defined networking (SDN) driven intrusion detection/prevention system (IDPS) for IoT networks. By using the SDN control, a collocated fog computational arrangement with IoT network equips proposed IDPS for timely identification of various attack models in near real time for effective neutralization. Using UNSW-NB15 dataset, the TN rate of all four classifiers above 90% for all window sizes, and it considered as a good performer. This paper [13] proposed the sFlow and adaptive polling based sampling with Snort Intrusion Detection System (IDS) and deep learning based model, which helps to lower down the various types of prevalent DDoS attacks inside the IoT network. When sFlow based implementation compared with adaptive polling then the evaluation rate of the proposed system shows the 95% of True Positive rate that is higher detection accuracy and it shows less than 4% of False Positive rate. The DNN model with sFlow class achieved the accuracy rate of 91% with FPR of 4% and F measure values of 88.10%. In [14], the researchers initiated the Clort in addition of NIDS snort, which is the greatest for offloading pattern matching on GPU. The major objective of this method is less power consumption and throughput in IoTs. Clort is efficient than GPU because of its consistency which consumed 33% less energy and 25% faster throughput.

All the works have been achieved distinct ratio of standard metrics with average 4% of FPR and 95% of accuracy but no more than this. One of the latest research even showed highest FPR, which is 10% as discussed previously. Our model works on these metrics for better performance and provide improved results.

3 PROPOSED METHODOLOGY

This section describes the proposed methodology along with its significance and novelty. Since DDoS attacks are very frequent and severe to any network, there is a drastic need to come up with a solution to tackle these attacks. Many techniques have been proposed for securing networks from DDoS attacks; however, existing schemes generate high false alarms. Therefore, this article propose an efficient, robust, and scalable solution for multi-classification of DDoS attacks. The Fig.2 briefly illustrates the architecture of our proposed scheme.

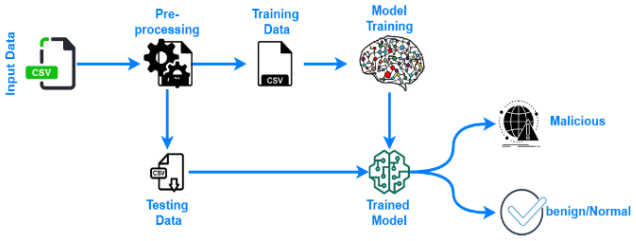

Fig. 2. Proposed model Architecture

The proposed mechanism is based on GPU enabled Cuda-LSTM assisted framework for performing the detection of sophisticated multi-vector DDoS attacks in IoTs.

4 IMPLEMENTATION AND EXPERIMENTS

This section briefly illustrates the experimental environment along with dataset; it will then be followed by description of evaluation metrics used for performance measurement of proposed model. Finally, the explanation of algorithm structure of our model is discussed.

A. Practical environment and Dataset

For the implementation of python libraries, we have used Anaconda environment, employed our model using Keras on Tensorflow package, and utilized DL algorithms. The specification of experimental setup are as follows: the system contains 64-bit OS with GPU based seven score processors and 16 GB of RAM in windows 10. This research is conducted using publically available up-to-date dataset of realistic network traffic named as CICDDoS2019 [15]. The captured traffic is of two types, the malicious, benign, malicious traffic contains traces of evolving DDoS attacks that are commonly found in networks, and the benign traffic comprises normal routine traffic for model training against classification of normal and attack instances. The data is captured in (PCAPS) format, which reflects the true and real world data. Those PCAPs also includes network traffic analysis captured using CICFlowMeter-V3 combined with categorized labelled flows. While building the dataset as described by the authors, they had focused on realistic traffic by keeping it on the highest priority. Twenty-five users were targeted as in the testbed for capturing overall traffic coming from them; the users were operating on traffic based on protocols like FTP, HTTP,

SSH, HTTPs, and including the email protocols for generation of dataset. The constructed dataset contains 86 of traffic features in total with the column containing labels to the traffic. The authors aimed that the best of 86 features were extracted for best training of model and achievement of highest detection scores.

B. Performance Metrics

The measurement of our proposed DL based DDoS detection model is evaluated using different standard performance metrics such as Accuracy, Precision, Recall, F1-score, and some more. For the standard metrics, the equations are given as following:

$$\textbf{Accuracy} = \frac{\mathcal{TP}+\mathcal{TN}}{\mathcal{TP}+\mathcal{TN}+\mathcal{FP}+\mathcal{FN}} \quad (1)$$

$$\textbf{Precision} = \frac{\mathcal{TP}}{\mathcal{TP}+\mathcal{FP}} \quad (2)$$

$$\textbf{Recall} = \frac{\mathcal{TP}}{\mathcal{TP}+\mathcal{FN}} \quad (3)$$

$$\textbf{F1-Score} = 2X \frac{\mathcal{TP}}{\mathcal{TP}+\mathcal{FN}} \quad (4)$$

Where TP, TN, FP, and FN stand for true positives, true negatives, false positives, and false negatives, in the same order.

C. Structure of Algorithm

In this subsection, we demonstrate the algorithm structure of our DL-based model as given in **Table I.** The model is constructed using following layers and neurons for enhanced performance. Total number of LSTM layers deployed in the model are three in actual, and three layers of dense are used afterwards, the model comprises one dropout layer as well as one output layer. The model is employed using GPU-enabled system for cu-LSTM model, which contains 200 neurons in the first layer. The second layer of the model is composed of 100 neurons. The next layers such as third layer of our proposed model comprises
80 neurons. For first two layers, the return sequence is true and for the last one it is false. Additionally, the dense or fully connected layers are used in construction of model, which sequentially comprises 80, 70, and 50 neurons respectively. The model used RELU as its activation function, and for loss function, it has employed categorical cross entropy. The model uses ADAMAX for optimization purpose and it is employed using batch-size of 64 and 5 epochs are set as total number of iterations. The last layer of proposed architecture encompasses four neurons in total; one from them represents benign-class, and the other three are used for the organization of multi-class DDoS attacks.

Table-I	**Cu-LSTM Structure**			
LAYERS	**LS-LAYERS**	**F-CONNECTED**	**DRO UP-OUT**	**OUTPUT**
	3	3	1	1
NEURONS	200,100,80	80,70,50	0.3	4
ACTIVATION FUNCTION	RELU			SOFTMAX
LOSS FUNCTION	CATEGORICAL CROSSENTROPY			
OPTIMIZER	ADAMAX			
BATCH SIZE	64			
EPOCHS	5			

5 RESULTS AND DISCUSSION

DL models are implemented using the environments as discussed in the previous section. This section briefly explains the conducted results after the evaluation of model on the mentioned dataset. For the evaluation and measurement of model performance, following metrics are used:

(i) The Confusion matrix (CM) is the classifier metric that holds overall information regarding the results,
(ii) True Positive Rate (TPR) is the metric that is used to measure the ratio of correct predictions,
(iii) The metric named as False Positive Rate (FPR) reflects the ratio of instances categorized in class x, but belongs to a diverse class, alongside all the occurrences not belonging to class x,
(iv) Recall is one of the metrics which represents the ratio of illustrations that are appropriately predicted as true, and
(v) Precision is the metric that evaluates the likelihood of the positive prediction to be correct.

In what tracks, we deliberately demonstrate the consequences from the investigation of our Cuda-LSTM-enabled DDoS detection

architecture; the CM of our model is displayed in Fig.3.

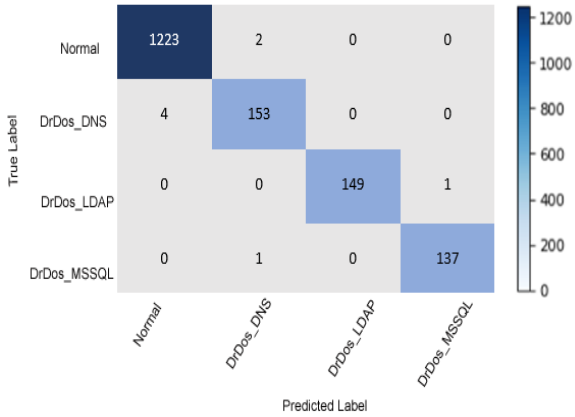

Fig. 3. Confusion Matrix

By using the CM effectively, we have calculated values of Accuracy along with the ratio of (TPR), True Negative Rate also written as (TNR), and Matthews Correlation Coefficient also written as (MCC). The results to the mentioned metrics are illustrated in Fig.4.

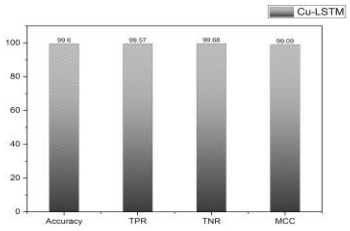

Fig.4. Accuracy, TPR, TNR, and MCC

TNR represents the ratio of perfectly classified negatives that means the superior the value, the enhanced the presentation of the system. MCC denotes to the interrelationship among true and expected occurrences in binary classification, which states that greater values (in between (minus) 1 and (plus) 1) produce better presentation in expressions of estimated results. To show the performance of proposed model on standard metrics, the proportions of precision, recall, and F1-score are described in Fig.5.

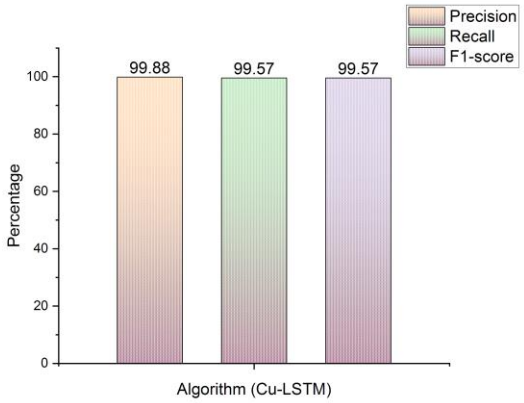

Fig. 5. Precision, Recall, and F1-score

Furthermore, we have also evaluated our proposed architecture using more other properties for extensive analysis, the metrics such as False Negative Rate (FNR), False Positive Rate (FPR), False Discovery Rate (FDR), and False Omission Rate (FOR) are also used, as exposed in Fig.6 with the result of outcomes.

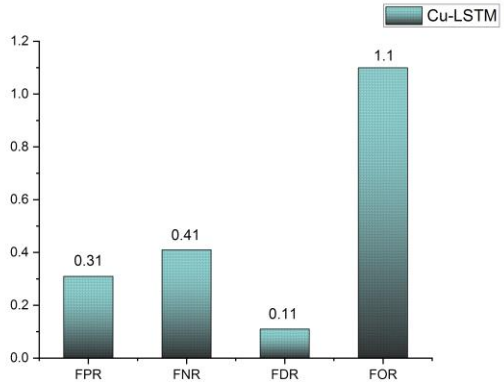

Fig. 6. FPR, FNR, FDR, and FOR

The False Negative Rate (FNR) composed of the samples that were positive but classified incorrectly. FPR is the classifier also known as False Alarm Rate (FAR), exemplifies the proportion among the imperfectly categorized negative illustrations to the exact amount of negative illustrations. False Discovery Rate (FDR) as well as False Omission Rate (FOR) processes supplement the positive and negative predicted values, respectively. The values of FPR, FNR, FOR, and FDR are in the range of zero and one which is suitable for the detection of DDoS in various IoT devices.

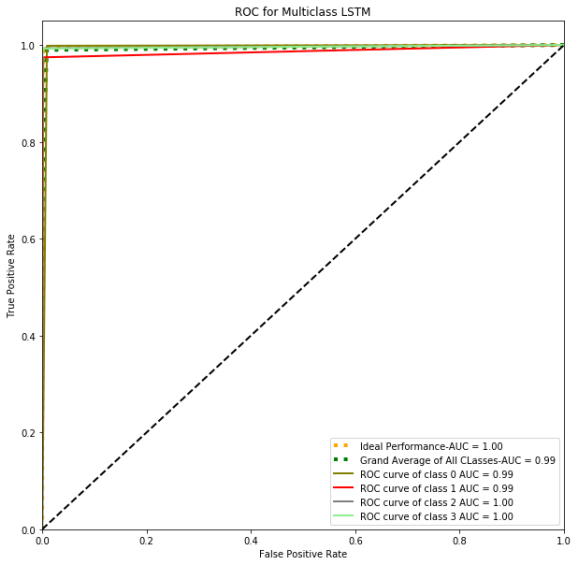

Fig. 7. ROC Curve

As above-mentioned, the ROC curve exemplifies the association between the ratios of False Positives (FP) and True Positives (TP). As described in Fig.7, the line representation to each class nearby x-axis displays its great performance.

Table 2: Results of the 3-folds of proposed scheme

	Accuracy	**Precision**	**Recall**	**F1-Score**
3-Folds	**Cu-LSTM**	**Cu-LSTM**	**Cu-LSTM**	**Cu-LSTM**
1	99.44	100	99.24	99.24
2	99.62	99.80	99.68	99.68
3	99.74	99.85	99.80	99.80
Avg.	99.60	99.88	99.57	99.57

Finally, Table II illustrates the results of overall three folds for showing unbiased results of our proposed scheme according to latest detection schemes provided in section II. The unbiased cross-validation of results clearly displays the scalability and effectiveness of our Cuda-LSTM-enabled architecture associated to other existing solutions.

6 CONCLUSION

Deep learning as an intuitive method is an answer for the DDoS detection issue that exists for IoT networks. Through the proposition of a robust multiclass classification model conspire by means of a GPU-empowered Long-short-term-memory (LSTM) based model by testing its efficiency for the recently distributed DDoS dataset with IoT based organization traffic; we have had the ability to demonstrate the performance of our proposed model. The capacity of the classifier in multi-class for DDoS attacks was demonstrated by the overall ratio of nearly 99.5% measures including results of accuracy, precision, recall and F1 score. In the multiclass characterization, the classifier declared the detection accuracy of above 99.6% for DDoS threats. The outcomes are noteworthy and warrant further exploration in this area of online protection for IoT or smart infrastructures.

7 REFERENCES

[1] L. Coetzee and J. Eksteen, "The Internet of Things-promise for the future? An introduction," in IST-Africa Conference Proceedings, 2011, 2011, pp. 1-9.

[2] A. Chadd, "DDoS attacks: past, present and future," Network Security, vol. 2018, pp. 13-15, 2018.

[3] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, pp. 80-84, 2017.

[4] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," in 2017 IEEE International Conference on Smart Computing (SMARTCOMP), 2017, pp. 1-8.

[5] Roopak, Monika, Gui Yun Tian, and Jonathon Chambers. "Deep learning models for cyber security in IoT networks." 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2019.

[6] W. Guo, D. Mu, J. Xu, P. Su, G. Wang, and X. Xing, "Lemna: Explaining deep learning based security applications," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 364–379, ACM, 2018.

[7] Ibitoye, Olakunle, Omair Shafiq, and Ashraf Matrawy. "Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks." 2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2019.

[8] Javeed, Danish, et al. "An Efficient Approach of Threat Hunting Using Memory Forensics." International Journal of Computer Networks and Communications Security 8.5 (2020): 37-45.

[9] M. E. Pamukov and V. K. Poulkov, "Multiple negative selection algorithm: Improving detection error rates in IoT intrusion detection systems," 2017 9th IEEE International

Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Bucharest, 2017, pp. 543-547

[10] A. Shenfield, D. Day, and A. Ayesh, "Intelligent intrusion detection systems using artificia," Neural networks, ICT Express. 4. 10.1016/j.icte.2018.04.003

[11] Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2018, June). Deep recurrent neural network for intrusion detection in sdn-based networks. In 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft) (pp. 202-206). IEEE.

[12] Khan, Tahir Ullah. "Internet of Things (IOT) Systems and its Security Challenges." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 8.12 (2019).

[13] Ujjan, R. M. A., Pervez, Z., Dahal, K., Bashir, A. K., Mumtaz, R., & González, J. (2020). Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. Future Generation Computer Systems, 111, 763-779.

[14] C. Stylianopoulos, L. Johansson, O. Olsson, and M. Almgren, "CLort: High Throughput and Low Energy Network Intrusion Detection of IoT Devices with Embedded GPUs," 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, 10.1007/978-3-030-03638-6_12.

[15] Sharafaldin, Iman, et al. "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy." 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019.