N-tier machine learning-based architecture for DDoS attack detection

Thi-Hong Vuong[1], Cam-Van Nguyen Thi[1], and Quang-Thuy Ha[1]

Vietnam National University, Hanoi (VNU),
VNU-University of Engineering and Technology (UET),
No. 144, Xuan Thuy, Cau Giay, Hanoi, Vietnam
{hongvt57, vanntc, thuyhq}@vnu.edu.vn

Abstract. Distributed Denial of Service (DDoS) attack is a menace to network security that aims at exhausting the target networks with malicious traffic. With simple but powerful attack mechanisms, it introduces an immense threat to the current Internet community. In this paper, we propose a novel multi-tier architecture intrusion detection model based on a machine learning method that possibly detects DDoS attacks. We evaluate our model using the newly released dataset CICDDoS2019, which contains a comprehensive variety of DDoS attacks and address the gaps of the existing current datasets. Experimental results indicated that the proposed method is more efficient than other existing ones. The experiments demonstrated that the proposed model accurately recognize DDoS attacks outperforming the state-of-the-art by F1-score.

Keywords: DDoS attacks · CICDDoS2019 · machine learning methods · intrusion detection.

1 Introduction

Cyber security is a significant role in secure communication to prevent services from being paralyzed by network intrusions. Intruders often exploit popular rogue software to carry out multiple attacks against networked computer systems. The damage done in a cyber attack can range from a slight disruption in service to huge financial losses. Furthermore, today's escalation of Internet of Things (IoT) devices and services has dramatically changed our daily lives. A large number of advanced IoT technology-based applications have been successfully built and deployed, such as smart cities, smart health care, smart home and vehicle networks [2]. These systems more opportunities for attackers to easily break into the network.

Recently, intrusion detection systems (IDSs) detect and eliminate malicious activities in cyber security [21]. As the number of malicious attacks constantly increases exponentially, IDSs have a duty to deal with eliminating such attacks before they cause massive destruction on a large area of cyberspace. In the passive of time, these systems are designed and combined with machine learning

techniques to handle unauthorized use and access to network resources. According to [15], there are different techniques to propose detection and defense mechanisms such as machine learning, knowledge-based, and statistical. The statistical methods are not allowed to determine with certainty the normal network packet distribution. The machine learning approach is better than as they do not have any prior known data distribution, but defining the best feature-set is one of the main concerns for them [17].

There are two challenges for machine learning-based IDSs. Firstly, datasets were shortcomings and problems [16, 18, 23]. Machine learning models face a major challenge of having to develop a model from a limited set of data called training data sets. The ideal case is to look for the best models to classify intrusive and non-intrusive network activities that have the features such as high detection accuracy, low false positive rate (FPR), activation which is related to the IDS alert enhancement and IDS must be adaptable in relation to constantly changing network environments. Scale ability in relation to the challenges ahead is tracking increasingly complex and heterogeneous. IDSs cannot deal with it. In [12], it is challenging to develop such models with the above criteria in real life. On the other hand, Shiravi et al. [16], Singh and De [18] and Yu et al.[23] tried to develop DDoS dataset. But Iman et al. [15] showed that there are many shortcomings and problems, such as incomplete traffic, anonymized data, and out-dated attack scenarios, still researchers struggle to find comprehensive and valid dataset to test and evaluate their proposed detection and defense models. Therefore, having a suitable dataset is a significant challenge. Secondly, the model needs to identify new attacks. A different important issue of characteristics of the DDoS attacks can be manually set, controlled by the attacker, or it can be automated. Therefore, there is a need to identify new attacks and come up with new taxonomies in [15]. Detection of the attack is an important step to DDoS mitigation. Detection is very simple as the performance of the service or system degrades dramatically when an attack occurs. However, it is always challenging to differentiate malicious flows from legitimate flows.

In this paper, we propose a novel multi-tier architecture intrusion detection model base on the machine learning approach to resolve the above challenges. The proposed method use different level classifies to detect attacks. The novel proposed method present on the newly released dataset CICDDoS2019 [1][15], which remedies the shortcomings and limitations of previous datasets. We also compare the baseline methods such as Naive Bayes (NB), Support Vector Machine (SVM), Decision Tree (DT) in [7, 15] to indicate the efficacy of the proposed method on CICDDoS2019.

The rest of the paper is presented as follows. Section 2 describes the related work and reviews two approach of IDSs along with two detection mechanisms: signature-based attack detection and anomaly-based attack detection. Section 3 introduces our proposed framework, a brief description of the dataset, preprocess data, extract features and presents n-tier machine learning-based architecture for DDoS attack detection. Compared with the well-known methods and the state-

[1] https://www.unb.ca/cic/datasets/ddos-2019.html

of-the-art classification models, the experiment results of the proposed method are show in Section 4. Finally, the paper provides several conclusions and further work in Section 5.

2 Related Work

Attacks can be determined as examined by two approaches: signature-based detection, anomaly-based detection [3, 13]. While anomaly-based detection systems determine the traffic which has harmful content as result of the analysis of network traffic, signature-based detection systems examine based the previous data, which were recorded on the system and confirms the attack. Signature-based detection mechanisms rely on known DDoS attacks to identity the attack signatures [5, 6, 9]. It is successful in detecting known DDoS attacks. However, any variations in already existing attacks remain unnoticed by these detection mechanisms. Indeed, as the techniques unaware of the new signatures, they do not work for any new attack types that have not been seen previously. Anomaly-based detection mechanism can handle attacks with new signatures as well as newly appear attacks [1, 10, 19]. However, the selection of threshold value to differentiate between attack traffic and normal traffic is an open challenge for these techniques. There are lot of the other methods try to differentiate attack traffic and legitimate traffic based on the analysis and detection of anomalies in traffic flows [4, 8, 20].

There are the most recent and popular mechanisms that have been used for the detection of DDoS attacks in software-defined network environments [11, 14, 22]. Ye et al. in [11] proposed Support Vector Machine (SVM) classification algorithm to detect DDoS attack including UDP, TCP SYN and ICMP flood traffic. Rahman et al. in [14] used four machine learning techniques to detect DDoS under context of software-defined network. The experiments showed that the J48 has better accuracy in the baseline methods with two DDoS attack including TCP and ICMP floods. The three different machine learning algorithms: SVM, Navie Bayes (NB) and Neural Network to detect flow-table overflow attack were used in [22]. One of the challenges to detect application layer DDoS attacks is high similarity of attacks and benign behaviors. Therefore, there is a lack of available features to define as attacks. Indeed, many detection systems are not suitable to identify it. In addition, the previous proposed techniques that used public datasets to train anomaly detection systems suffer of several issues such as incomplete traffic, anonymized data and out of date attack scenarios. According to [7, 15], a comprehensive and valid dataset has a great impact on the evaluation of detection algorithms and techniques systems. Thus, to evaluate our proposed model, we use the newest public avaible dataset CICDDoS2019 [15]. The CICDDoS2019 dataset contain a comprehensive variety of DDoS attacks and address the gaps of the existing current datasets. With CICDDoS 2019, we approach an anomaly-based detection. In this paper, we propose n-tier machine learning-based architecture for DDoS attack detection.

3 Proposed Framework

According to [13], the basic structure of a DDoS attack has four different components such as attacker, multiple control masters or handlers, multiple slaves, agents or zombies and a victim or target machine. Different phases and characteristics of the DDoS attacks can be manually set, controlled by the attacker, or it can be automated. Therefore, there is a need to identify new attacks and come up with new taxonomies in [15]. We propose a novel n-tier machine learning-based architecture intrusion for DDoS attack detection as Fig 1. N-tier architecture intrusion detection model is also called as multiple classifier system that uses a set of classifiers as base machine learning techniques to build training data to classify unknown data. The proposed framework includes two phases. In the first phase, we preprocess CICDDoS2019 and select features. Then, feeding processing data into the second phase to build an attack model base on machine learning technique.

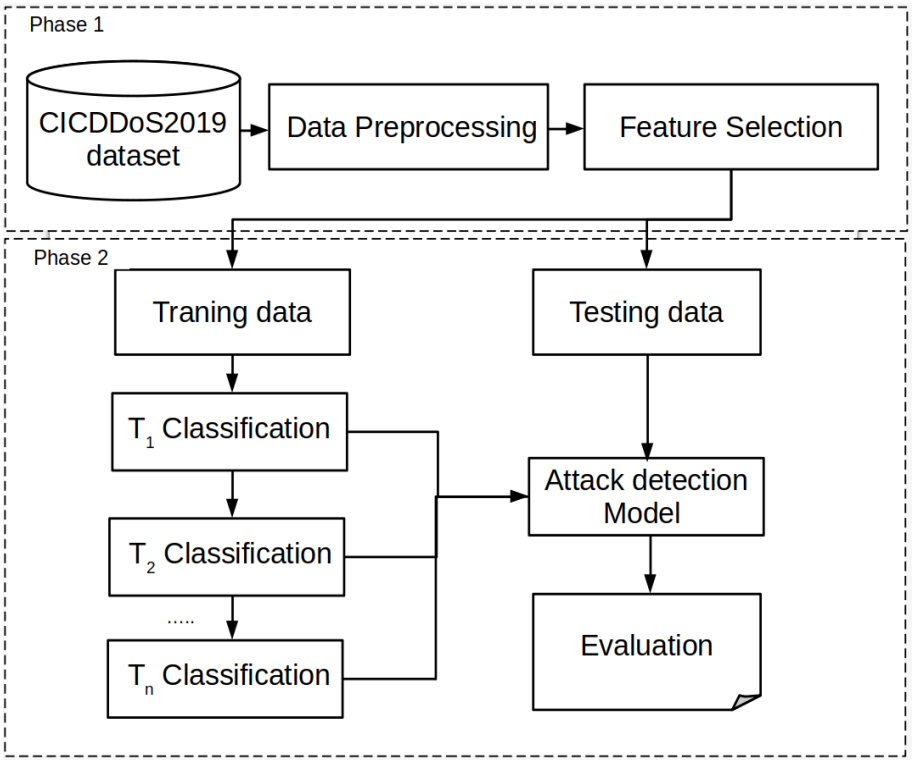

Fig. 1. The general flowchart of the proposed method. Given CICDDoS2019 dataset, preprocess data and extract features in the first phase. In the second phase, use n-tier classification architecture and evaluate for DDoS attack detection model.

3.1 Dataset Preprocessing

The first phase before training the IDS models is to preprocess the dataset to make it more suitable for the training phase and avoid the overfitting problem. The steps are taken for preprocessing as follows:

- The CICDDoS2019 dataset contains the socket information such as scoure IP, destination IP, flowID, etc. The original dataset includes 88 features when removed to all socket features. One-hot encoding scheme is used convert the labeled string to numerical values.
- In the CICDDoS2019, the following class labels are employed: UDP, BENIGN, UDP-Lag, SYN, MSSQL, NetBIOS, LDAP. According to [15], the capturing period for the training day on January 12th started at 10:30 and ended at 17:15, and for the testing day on March 11th started at 09:40 and ended at 17:35. The statistics of CICDDoS2019 with 7 class labels details in Table 1.
- The class labels in CICDDoS2019 were classified on terms of reflection-based and exploitation-based attacks [15]. Because of imbalanced class labels, we group the class labels into 4 based on the two above terms of attacks: 1 (UDP, UDP-Lag, SYN), 2 (NetBIOS, LDAP), 3 BENIGN, and 4 MSSQL in Table 2.

Table 1. Detail statistics CICDDoS2019 with seven class labels

Label	Training day Jan 12th	Percentage	Testing day Mar 11th	Percentage
UDP	3134645	19,67%	3867155	19,17%
BENIGN	56863	0,36%	56965	0,28%
UDPLag	366461	2,30%	1873	0,01%
SYN	1582289	9,93%	4891500	24,24%
MSSQL	4522492	28,38%	5787453	28,68%
NetBIOS	4093279	25,69%	3657497	18,13%
LDAP	2179930	13,68%	1915122	9,49%
Total	15935959	100%	20177565	100%

Table 2. Detail statistics CICDDoS2019 with group class labels

Label	Training day Jan 12th	Percentage	Testing day Mar 11th	Percentage
(1) UDP , UDP-Lag, SYN	5083395	31,90%	8760528	43,42%
(2) BENIGN	56863	0,36%	56965	0,28%
(3) NetBIOS , LDAP	6273209	39,37%	5572619	27,62%
(4) MSSQL	4522492	28,38%	5787453	28,68%
Total	15935959	100%	20177565	100%

3.2 Feature Selection

In the feature selection, we focus on selecting the best features to predict DDoS attacks instead of all features in the original data. The Random Forest Regressor was used to calculate the importance of each feature among 88 features in the dataset [15]. We select a subset of 24 features from the original CICDDoS2019 dataset to train our learning model as in Table 3.

Table 3. Feature set used in the Intrusion Detection System

1 Fwd Packet Length Max	13 Subflow Fwd Bytes
2 Fwd Packet Length Min	14 Destination Port
3 Min Packet Length	15 Protocol
4 Max Packet Length	16 Packet Length Std
5 Average Packet Size	17 Flow Duration
6 FWD Packets/s	18 Fwd IAT Total
7 Fwd Header Length	19 ACK Flag Count
8 Fwd Header Length 1	20 Init_Win_Bytes_Forward
9 Min_Seg_Size_Forward	21 Flow IAT Mean
10 Total Length of Fwd Packet	22 Flow IAT Max
11 Fwd Packet Length Std	23 Fwd IAT Mean
12 Flow IAT Min	24 Fwd IAT Max

3.3 Multi-tier architecture intrusion detection model

We propose a n-tier classification architecture for DDoS attacks detection. The pseudo-code of the proposed method for attack detection shown in Algorithm 1. In the one step, we used binary classifiers T_1, T_2,..., T_n to classify the input traffic into normal and malicious types by Random Forest (RF). Then, these learner outputs are integrated for the second step to detect DDoS attacks as multi-class classification framework.

Algorithm 1 N-tier architecture intrusion detection model

1: Input: CICDDoS2019 atfer preprocessing and extracting
   D= $(x_1, y_1), (x_2, y_2), ...(x_n, y_n)$, n learning datasets
2: Step 1: Learn binary classifier
3: **for** Each class label **do**
4: Implement RF for attacked or normal classification
5: T_i Classification, i: attack class label
6: Save T_i classification model
7: **end for**
8: Step 2: Learn N-tier classifier
9: Integrate T_i classification model into n-tier classifier
10: Classify x_j as attacked or normal
11: Evaluate model

4 Experiments

4.1 Evaluation metrics

In this experiment, we have evaluated the effectiveness of our IDS with the use of the Confusion Matrix as shown in Table 4 below:

Table 4. Confusion Matrix

	Predicted Attack	**Predicted Normal**
Actual Attack	True Positive (TP)	False Negative (FN)
Actual Normal	False Positve (FP)	True Negative (TN)

- True positive (TP): the number of rightly recognized malicious code.
- True negative (TN): the number of rightly recognized benign code.
- False positive (FP): the number of incorrectly identified Benign code, when a detector recognizes a benign code as a Malware.
- False negative (FN): the number of incorrectly recognized malicious code, when a detector recognizes a Malware as a benign code

We use precision (P), recall (R) and F1 score (F1) to evaluate the proposed framework with the baseline methods. P, R, F1 are define in Eq.1, 2, 3.

$$P = \frac{TP}{TP + FP} \tag{1}$$

$$R = \frac{TP}{TP + TN} \tag{2}$$

$$F1 = 2 * \frac{P * R}{P + R} \tag{3}$$

4.2 Experiment Cases

We present the proposed method with two cases and compare it with the baseline methods such as NB, SVM, DT in [7, 15]. In the first experiment case, the proposed method is implemented on the CICDDoS2019 with seven class labels as the following in Table 1. In the second experiment case, we implement the proposed method above dataset with group labels in Table 2. We use the training day for training data, and 20 percentage of the testing day for testing data for the proposed method and baseline methods.

(a) Comparison with the baseline methods on CICDDoS2019 in Table 1
The experiments indicated that the proposed method is more efficient than the baseline methods in Table 5. The performance of the proposed framework overall measure such as P, R, and F1-score is higher than the comparison methods. F1-score of the proposed method is extremely

higher than NB from 30 % to 90 % on labels. The results know that F1-score is higher than SVM and DT from 5 % to 30 % on labels in Fig 2.

The experiments show that the proposed method is more efficient on labels such as SYN, BENIGN, UDP, MSSQL and NetBIOS from 60 % to 99 %. However, the proposed method also limited detection labels as UDPLag and LDAP. Because the UPDLag percentage is extremely smaller only 2,30 % on training data. It is not enough to learn for DDoS attack detection. LDAP percentage also is smaller than others only 13,68 %. To improve the efficiency of the proposed framework, we group the class labels into four labels as Table 2. After grouping, the percentage of class labels is approximate each other except BENIGN.

Table 5. Comparison the baseline methods of seven class labels

Measure	NB			SVM			DT			**Proposed Method**		
	P	R	F1	P	R	F1	P	R	F1	P	R	F1
UDP	0,951	0,027	0,053	0,974	0,477	0,641	0,986	0,497	0,661	0,982	0,526	**0,685**
BENIGN	0,078	0,100	0,087	0,939	0,464	0,621	0,989	0,912	0,949	0,995	0,992	**0,993**
UDPLag	0,000	0,000	0,000	0,000	0,000	0,000	0,002	0,316	0,004	0,843	0,178	**0,294**
SYN	0,983	0,099	0,179	0,991	0,548	0,706	1,000	0,953	0,976	0,860	0,998	**0,924**
MSSQL	0,000	0,000	0,000	0,444	0,869	0,588	0,512	0,626	0,563	0,506	0,698	**0,587**
NetBIOS	0,002	0,000	0,000	0,205	0,225	0,215	0,375	0,555	0,447	0,511	0,630	**0,564**
LDAP	0,108	1,000	0,195	0,000	0,000	0,000	0,507	0,198	0,284	0,622	0,286	**0,392**

(b) Comparison with the baseline methods on CICDDoS2019 in Table 2

The proposed framework is implemented on CICDDoS2019 after grouping labels with the same term. The result of experiments indicated that the proposed method on grouping labels is the best on both P, R and F1-score than the baseline methods in Table 6. F1-score of (1 UDP, UDP-Lag, SYN), (2 BENIGN), (3 NetBIOS, LDAP) and (4 MSSQL) are about 87,6 %, 99,3 %, 67,8 % and 53 %, correspondingly. The results demonstrated that the proposed framework accurately recognize DDoS attacks outperforming the baseline methods in Fig 3. Indeed, by the grouping labels, the efficiency of the proposed method is better.

Table 6. Comparison with the baseline methods of four class labels

Measure	NB			SVM			DT			**Proposed Method**		
	P	R	F1	P	R	F1	P	R	F1	P	R	F1
1	0,790	0,004	0,008	0,988	0,459	0,627	0,997	0,704	0,825	0,995	0,782	**0,876**
2	0,030	0,104	0,047	0,979	0,495	0,658	0,991	0,918	0,953	0,995	0,991	**0,993**
3	0,016	0,000	0,000	0,472	0,956	0,632	0,457	0,680	0,547	0,587	0,803	**0,678**
4	0,288	0,999	0,447	0,535	0,099	0,167	0,589	0,482	0,530	0,589	0,482	**0,530**

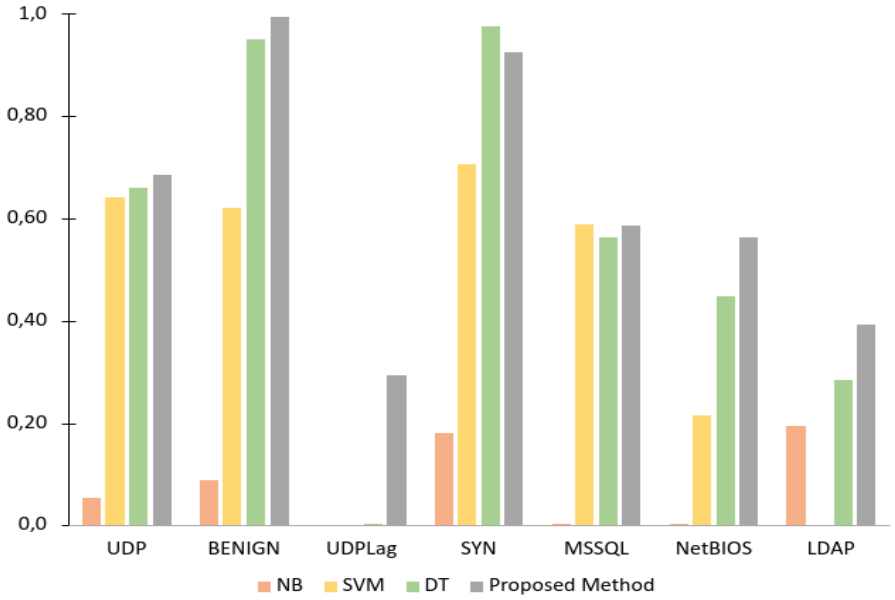

Fig. 2. Comparison the baseline methods on F1-score with seven class labels

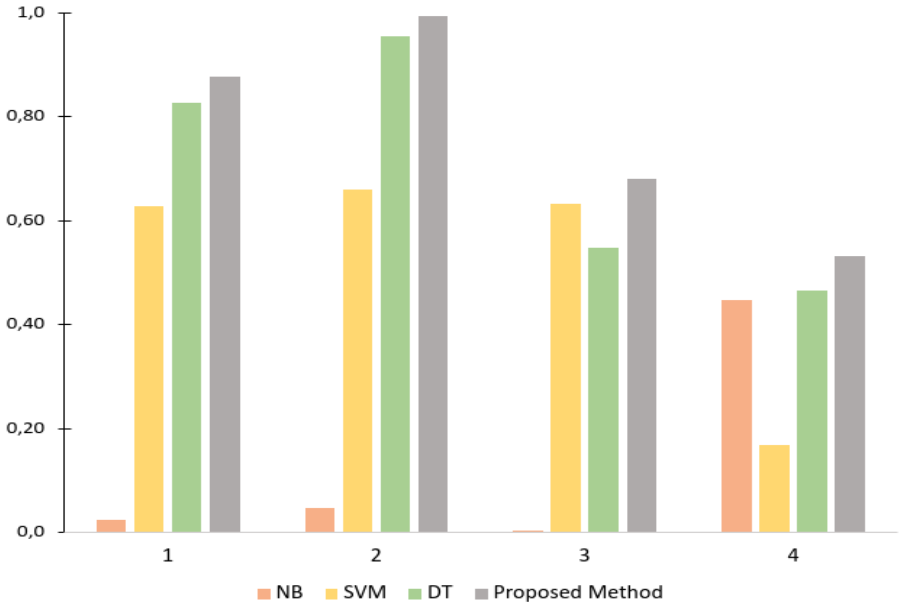

Fig. 3. Comparison the baseline methods on F1-score with four class labels

5 Conclusions

In the paper, we propose a novel n-tier machine learning-based architecture for DDoS attack detection. We used the new released CICDDoS2019 dataset which contains comprehensive and most recently DDoS types of attacks. The experiments indicated that the proposed method gives the highest evaluation metrics in terms of F1-score compared to the existing well known classical machine learning techniques. In work future, we will test the performance of our proposed model on other datasets. Furthermore, we perhaps extend our work to a deep learning architecture for DDoS attack detection.

References

1. Abdelsayed, S., Glimsholt, D., Leckie, C., Ryan, S., Shami, S.: An efficient filter for denial-of-service bandwidth attacks. In: GLOBECOM'03. IEEE Global Telecommunications Conference (IEEE Cat. No. 03CH37489). vol. 3, pp. 1353–1357. IEEE (2003)
2. Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer networks **54**(15), 2787–2805 (2010)
3. Aytaç, T., Aydın, M.A., Zaim, A.H.: Detection ddos attacks using machine learning methods
4. Barford, P., Kline, J., Plonka, D., Ron, A.: A signal analysis of network traffic anomalies. In: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment. pp. 71–82 (2002)
5. Cabrera, J.B., Lewis, L., Qin, X., Lee, W., Prasanth, R.K., Ravichandran, B., Mehra, R.K.: Proactive detection of distributed denial of service attacks using mib traffic variables-a feasibility study. In: 2001 IEEE/IFIP International Symposium on Integrated Network Management Proceedings. Integrated Network Management VII. Integrated Management Strategies for the New Millennium (Cat. No. 01EX470). pp. 609–622. IEEE (2001)
6. Cheng, C.M., Kung, H., Tan, K.S.: Use of spectral analysis in defense against dos attacks. In: Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE. vol. 3, pp. 2143–2148. IEEE (2002)
7. Elsayed, M.S., Le-Khac, N.A., Dev, S., Jurcut, A.D.: Ddosnet: A deep-learning model for detecting network attacks. In: 2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM). pp. 391–396. IEEE (2020)
8. Huang, Y., Pullen, J.M.: Countering denial-of-service attacks using congestion triggered packet sampling and filtering. In: Proceedings Tenth International Conference on Computer Communications and Networks (Cat. No. 01EX495). pp. 490–494. IEEE (2001)
9. Hussain, A., Heidemann, J., Papadopoulos, C.: Identification of repeated denial of service attacks. In: Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications. pp. 1–15. Citeseer (2006)
10. Jow, J., Xiao, Y., Han, W.: A survey of intrusion detection systems in smart grid. International Journal of Sensor Networks **23**(3), 170–186 (2017)
11. Karan, B., Narayan, D., Hiremath, P.: Detection of ddos attacks in software defined networks. In: 2018 3rd International Conference on Computational Systems and

Information Technology for Sustainable Solutions (CSITSS). pp. 265–270. IEEE (2018)
12. Kumar, G., Thakur, K., Ayyagari, M.R.: Mlesidss: machine learning-based ensembles for intrusion detection systems—a review. The Journal of Supercomputing pp. 1–34 (2020)
13. Mahjabin, T., Xiao, Y., Sun, G., Jiang, W.: A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks **13**(12), 1550147717741463 (2017)
14. Rahman, O., Quraishi, M.A.G., Lung, C.H.: Ddos attacks detection and mitigation in sdn using machine learning. In: 2019 IEEE World Congress on Services (SERVICES). vol. 2642, pp. 184–189. IEEE (2019)
15. Sharafaldin, I., Lashkari, A.H., Hakak, S., Ghorbani, A.A.: Developing realistic distributed denial of service (ddos) attack dataset and taxonomy. In: 2019 International Carnahan Conference on Security Technology (ICCST). pp. 1–8 (2019)
16. Shiravi, A., Shiravi, H., Tavallaee, M., Ghorbani, A.A.: Toward developing a systematic approach to generate benchmark datasets for intrusion detection. computers & security **31**(3), 357–374 (2012)
17. Shuyuan Jin, Yeung, D.S.: A covariance analysis model for ddos attack detection. In: 2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577). vol. 4, pp. 1882–1886 Vol.4 (2004)
18. Singh, K.J., De, T.: An approach of ddos attack detection using classifiers. In: Emerging Research in Computing, Information, Communication and Applications, pp. 429–437. Springer (2015)
19. Sun, B., Xiao, Y., Wang, R.: Detection of fraudulent usage in wireless networks. IEEE Transactions on Vehicular Technology **56**(6), 3912–3923 (2007)
20. Talpade, R., Kim, G., Khurana, S.: Nomad: Traffic-based network monitoring framework for anomaly detection. In: Proceedings IEEE International Symposium on Computers and Communications (Cat. No. PR00250). pp. 442–451. IEEE (1999)
21. Tama, B.A., Rhee, K.H.: An extensive empirical evaluation of classifier ensembles for intrusion detection task. Computer Systems Science and Engineering **32**(2), 149–158 (2017)
22. Ye, J., Cheng, X., Zhu, J., Feng, L., Song, L.: A ddos attack detection method based on svm in software defined network. Security and Communication Networks **2018** (2018)
23. Yu, S., Zhou, W., Jia, W., Guo, S., Xiang, Y., Tang, F.: Discriminating ddos attacks from flash crowds using flow correlation coefficient. IEEE transactions on parallel and distributed systems **23**(6), 1073–1080 (2011)