International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V68I11P113

Volume 68 Issue 11, 83-85, November 2020
© 2020 Seventh Sense Research Group®

Review Article

A Survey on DDoS Attack Detection Methods Employing Intelligent Techniques

Vinayak P R[1], Gripsy Paul [2]

[1,2]Department of Computer Science and Engineering, Adi Shankara Institute of Engineering and Technology
Kalady, Kerala, India

Received Date: 14 October 2020
Revised Date: 22 November 2020
Accepted Date: 24 November 2020

Abstract *- The Distributed denial-of-service (DDOS) attacks target network resources to disable the websites or services through overloading the resources with a large amount of traffic. The arrival of intelligent systems such as machine learning-based techniques and deep learning techniques have improved the automatic detection of such attacks. The machine-learning-based techniques such as support vector machine (SVM), decision tree, or Na¨ıve Bayes (NB) can efficiently use for classification. CNN or other techniques can also use for constructing deep neural networks to detect attacks. In this paper, we discuss in detail various DDoS attack detection methods.*

Keywords *- attack detection, DDoS, deep learning, machine learning, network security*

I. INTRODUCTION

Nowadays, cyber-attacks increased hugely. Various techniques had implemented to protect communication systems and services from attackers. Denial of service (DoS), code injection, memory corruption, SQL injection, gain information, overflow, bypass something, etc., are the most powerful cyber-attacks in today's world.

A website [20] has reported over 123450 vulnerabilities. Cyber-attacks reduce communication devices' performance, steal confidential data, money, and threaten people using attacks like ransomware. However, the distributed denial-of-service (DDoS) attack [9] [10] [11] [12] is the most common and powerful attacks performed by overflowing or overloading the network resources and services. The attack rejects the benefits or services to standard or legitimate (authorized) users. The DDoS attack method is a type of DoS [14] attack, and it is an incredibly powerful attack, and it is very challenging to defend. The targeted system is overloaded or flooded by attackers, such as malicious users or malicious programs from different sources. Thus detection and prevention of the attack become difficult.

The resource depletion and the bandwidth depletion DDoS attack are the main kinds of DDoS attacks [13]. In the bandwidth depletion attack, unwanted/malicious traffic overflows or flood the system. The resource depletion type is another attack type; it tie-up or depletes the services and resources available to the system [13]. The machine-learning-based techniques [21] and deep learning-based techniques provide intelligent recognition of DDoS attacks. In this paper, we describe in detail various DDoS attack discovery methods.

We describe the following sections through this paper: Section II discusses the existing studies related to the DDoS attack and detection methods. In section III, we discuss the detection methods and their relevance. Finally, Section IV describes the conclusions of our survey.

II. LITERATURE SURVEY

A method for detecting the DDoS attack on Software-Defined-Networking (SDN) has been described in the paper [1]. In this method, they describe two methods for detecting the DDoS attack. K-Nearest Neighbor (KNN) based approach and degree of DDoS attack had used to detect the attack. Besides, they discuss different types of attacks, such as flood attacks, Coremelt attacks, and authentication server attacks. They have studied SDN features such as flow size, flow rate, flow duration, and flow length. The first method (machine-learning-based approach) has achieved a precision of 0.993 and recall of 0.994. The other method has achieved a precision of 0.985 and a recall of 0.987.

Another machine-learning-based approach for mitigating and detecting low rate DDoS attacks has described in [2]. They implemented the architecture to detect the attacks in SDN environments. Their proposed framework consists of two main modules, an Intrusion Detection System and Intrusion Prevention System. The framework detects HTTP flows, manages potential attackers list, creates the flow rules for mitigating, and the ML model identifies flow and classifies malicious flow. They trained multiple machine learning models. The IDS module detects flows using different trained ML models. Also, they have achieved an accuracy of 95%.

C4.5 algorithm based DDoS attack detection method had described in [3]. They linked their method to signature detection technologies. Signature-based systems recognize intrusion by recognizing patterns that match the signatures of well-known attacks or threats. By using this approach, updating the knowledge base without changing existing or pre-defined rules is possible. The C4.5 algorithm achieved an F-measure of 0.988 on classification. The F-measure of

Naive Bayesian and K-means are 0.914 and 0.959, respectively. Thus, the C4.5 algorithm provides a better classification in their study.

A backpropagation neural network-based DoS attack recognition method had described in [4]. The frame length, CPU usage, and flow rate are the parameters used in their method. Also, explains symptoms and examples of DoS attack. They had used non-attack data and attacked data to train the network. Their approach obtained an accuracy of 96.2%.

Based on the deep learning technique, the DDoS discovery method for a software-defined network (SDN) has been described in [5]. Their detection method includes mainly three modules: traffic classifier, feature extractor, and traffic collector and flow installer. By examining the message type, the reason for the arrival of the packets can easily detect. Also, they listed the description of a total of 68 features. It consists of features extracted for UDF flows, TCP flows, and ICMP flows. The features reduced using the Stacked Autoencoder (SAE). The Traffic classifier classifies traffic. For attack class and normal class classification, they obtained an accuracy of 99.82%. Besides, the method achieved an accuracy of 95.65% on individual class classification.

Another deep-learning-based model using a convolutional neural network (CNN) for DDoS detection scheme had explained in [6]. During the preprocessing phase, Z-score normalization has used and performed dimensional reconstruction. Then, they developed the deep-learning-based ensemble model. Their method achieved a detection accuracy of 99.48%.

An interesting DDoS attack recognition for smart grid networks using auto-encoder-based feature learning was described in [7]. They proposed a scheme for feature encoding using various encoders levels, i.e., shallow encoders and deep auto-encoders. Unsupervised learning was performed. The method of using that kind of auto-encoders is the specialty of this method. Besides, they used a multiple kernel learning approach. Their proposed method had obtained an average accuracy: 93% and achieved 97% accuracy on a dataset.

Another big area of DDoS detection is the Botnet DDoS discovery methods. In [8] analyzed the DDoS recognition using several machine learning (ML) approaches. Different approaches such as Artificial Neural Network, SVM, Unsupervised Learning (USML), Na¨ıve Bayes (NB), and Decision Tree are used and described different bots Agobot, DSNX bots, Q8 bots, SDBot, etc. On the performance analysis using different models on both datasets, the USML approach achieved greater accuracy than other classifiers. The technique achieved 94.78% accuracy on a dataset and 98.08% accuracy on another dataset.

We studied various existing approaches for DDoS attack detection. Machine learning methods and Deep learning models have been incorporated for developing the attack detection systems. The state-of-the-art detection mechanisms make the classification and detection task easy. The summary of the papers we studied has shown in Table 1.

Table 1. Summary Of Analysed Papers

Article	Description	Performance
[1]	KNN and degree of DDoS had used to detect the attack	Precision:0.993,and Recall:0.994
[2]	ML model identifies flow and classifies the malicious flow	Accuracy: 95%
[3]	C4.5 algorithm based DDoS attack detection	F-measure: 0.988
[4]	BPNN based DoS detection	Accuracy: 96.2%
[5]	Deep learning-based DDoS detection for SDN	For attack and normal class, Accuracy:99.82% For individual class classification, Accuracy: 95.65%
[6]	CNN based DDoS detection	Accuracy: 99.48%
[7]	DDoS detection for the smart grid. Auto-encoders and multiple kernel-based	Accuracy: 97%
[8]	Botnet DDoS detection, the unsupervised model, provides better results	Accuracy:98.08%

III. DISCUSSION

In this survey, we studied various deep-learning-based and machine-learning-based DDoS attack detection methods and their performance. Various techniques, such as ANN, SVM, Na¨ıve Bayes (NB), Unsupervised Learning, Decision Tree (DT), CNN, etc., are used to develop the threat detection system. Many of them provide good results.

The detection mechanisms are powerful, and many methods produce results greater than 90%. Many studies described various features for developing the detection system. The usage of deep learning models improves the attack classification and detection process by selecting the features automatically. Analysis of different datasets produces different results. Thus it points to the need for highly scalable and more reliable, and more robust classification models.

This area requires more accurate, highly scalable, and high-speed threat detection mechanisms. The Accuracy and detection speed is the highly prioritized performance index. Therefore, highly used and comparatively new techniques such as CNN [17], Recurrent Neural Networks (RNN) [18] [19], Attention Techniques [15], or Graph-based techniques [16] can be incorporated to analyze the problem in different aspects using different features. Many of these techniques are highly using for text-based analysis, and some techniques are also used in attack detection; however, more analysis will make more satisfying results.

IV. CONCLUSION

Availability of network resources is a highly important factor along with other safety and privacy indexes in cyberspace. We analyzed and studied various state-of-the-art DDoS detection techniques. Machine learning and deep learning-based models improve the detection accuracy. We believe that more detailed analysis using the latest deep-learning techniques will increase the system's detection accuracy and performance. Also, the detection time is an essential factor for this problem. Most accurate and quick detection mechanisms are always crucial in threat detection systems.

REFERENCES

[1] Shi Dong and Mudar Sarem. Ddos attack detection method based on improved knn with the degree of ddos attack in software-defined networks. IEEE Access, 8 (2019) 5039–5048.

[2] Jesus Arturo P'erez-D'ıaz, Ismael Amezcua Valdovinos, Kim-Kwang Raymond Choo, and Dakai Zhu. Flexible sdn-based architecture for identifying and mitigating low-rate ddos attacks using machine learning. IEEE Access, 8 (2020) 155859–155872.

[3] Marwane Zekri, Said El Kafhali, Noureddine Aboutabit, and Youssef Saadi. Ddos attack detection using machine learning techniques in cloud computing environments. In 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), IEEE.(2017) 1–7.

[4] Monika Khandelwal, Deepak Kumar Gupta, and Pradeep Bhale. Dos attack detection technique using a backpropagation neural network. In 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE. (2016) 1064–1068.

[5] Quamar Niyaz, Weiqing Sun, and Ahmad Y Javaid. A deep learning-based ddos detection system in software-defined networking (sdn). arXiv preprint arXiv:1611.07400, (2016).

[6] Shahzeb Haider, Adnan Akhunzada, Ghufran Ahmed, and Mohsin Raza. Deep learning-based ensemble convolutional neural network solution for distributed denial of service detection in sdns. In 2019 UK/China Emerging Technologies (UCET), IEEE. (2019) 1–4.

[7] Shan Ali and Yuancheng Li. Learning multilevel auto-encoders for ddos attack detection in the smart grid network. IEEE Access, 7:108647–108659, (2019).

[8] Tong Anh Tuan, Hoang Viet Long, Raghvendra Kumar, Ishaani Priyadarshini, Nguyen Thi Kim Son, et al. Performance evaluation of botnet ddos attack detection using machine learning. Evolutionary Intelligence, (2019) 1–12.

[9] Bing Wang, Yao Zheng, Wenjing Lou, and Y Thomas Hou. Ddos attack protection in the era of cloud computing and software-defined networking. Computer Networks, 81 (2015) 308–319.

[10] Alan Saied, Richard E Overall, and Tomasz Radzik. Detection of known and unknown ddos attacks using artificial neural networks. Neurocomputing, 172 (2016) 385–393.

[11] Yonghao Gu, Kaiyue Li, Zhenyang Guo, and Yongfei Wang. Semisupervised k-means ddos detection method using a hybrid feature selection algorithm. IEEE Access, 7 (2019) 64351–64365.

[12] Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak, and Ali A Ghorbani. Developing realistically distributed denial of service (ddos) attack dataset and taxonomy. In 2019 International Carnahan Conference on Security Technology (ICCST), 1–8. IEEE. (2019).

[13] Stephen Specht and Ruby Lee. Taxonomies of distributed denial of service networks, attacks, tools, and countermeasures. CEL2003-03, Princeton University, Princeton, NJ, USA, (2003).

[14] Heng Zhang, Peng Cheng, Ling Shi, and Jiming Chen. Optimal dos attack scheduling in a wireless networked control system. IEEE Transactions on Control Systems Technology, 24(3) (2015) 843–852.

[15] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. Advances in neural information processing systems, 30 (2017) 5998–6008.

[16] Liang Yao, Chengsheng Mao, and Yuan Luo. Graph convolutional networks for text classification. In Proceedings of the AAAI Conference on Artificial Intelligence, 33(2019) 7370–7377.

[17] Yoon Kim. Convolutional neural networks for sentence classification. arXiv preprint arXiv:1408.5882, 2014.

[18] Mike Schuster and Kuldip K Paliwal. Bidirectional recurrent neural networks. IEEE transactions on Signal Processing, 45(11) (1997) 2673–2681.

[19] Junyoung Chung, Caglar Gulcehre, KyungHyun Cho, and Yoshua Bengio. Empirical evaluation of gated recurrent neural networks on sequence modeling. arXiv preprint arXiv:1412.3555, (2014).

[20] CVE Details. [online]. Available: https://www.cvedetails.com/

[21] FY Osisanwo, JET Akinsola, O Awodele, JO Hinmikaiye, O Olakanmi, and J Akinjobi. Supervised machine learning algorithms: classification and comparison. International Journal of Computer Trends and Technology (IJCTT), 48(3) (2017) 128–138.