Indonesian Journal of Electrical Engineering and Computer Science
Vol. 23, No. 2, August 2021, pp. 1068~1072
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v23.i2.pp1068-1072

Development of a new system to detect denial of service attack using machine learning classification

Mohammad M. Rasheed[1], Alaa K. Faieq[2], Ahmed A. Hashim[3]
[1,3]College of Engineering, University of Information Technology and Communications, Baghdad, Iraq
[2]Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq

Article Info

Article history:

Received May 5, 2021
Revised Jul 3, 2021
Accepted Jul 14, 2021

Keywords:

DoS attack
Machine learning
Network security

ABSTRACT

Denial of service (DoS) attack is among the most significant types of attacks in cyber security. The objective of this research is to introduce a new algorithm to distinguish normal service requests from the denial of service attacks. Our proposed approach can detect the denial of service attacks by the analysis of the packets sent from the client to the server, which depend on machine learning. Our algorithm collects different datasets of benign network traffic and different types of denial of service attacks, such as DDoS, DoS Hulk, DoS GoldenEye, DoS Slowhttptest, and DoS Slowloris, that were used for training. Moreover, our algorithm monitors the network every specific time to find denial of service attack. Our results show that the algorithm can detect the benign cases and distinguish the types of denial of service attack. Furthermore, the results could achieve 99 percentage of correct classification of all selected cases.

Corresponding Author:

Mohammad M. Rasheed
College of Engineering
University of Information Technology and Communications
Baghdad, Iraq
Email: mohammad.rasheed@uoitc.edu.iq

1. INTRODUCTION

During the recent years, denial of service (DoS) attacks has been often reported to target an increased number of internet sites. Transmission control protocol (TCP) synchronize (SYN) flooding is one of the most dominant types of these attacks [1]. Blazek *et al.* described an elevation in the frequency DoS attacks during this period, which can possibly cause various services to be disrupted, costing several millions to billions of dollars [2]. DOS attacks aim at ceasing the reception of minimal-performance services by the legitimate users, through the consumption of as largest amount of resources as possible as shown in Figure 1. TCP's three-way handshake is a procedure that is commonly utilized by TCP SYN flooding, particularly its limitation in maintaining half-open connections. The common candidate targets of this type of attacks include web, file transfer protocol (FTP), or mail servers, along with any other system with a connection to the internet and provision of TCP-based network services. The beginning of any TCP connection involves the expression of the client's willingness of establishing such a connection, which is indicated by a SYN message that is sent by the client to the server. As a reply, a synchronize (SYN) and acknowledge (ACK) SYN/ACK message is sent back by the server, confirming the receipt the initial SYN message and, simultaneously, commencing the reservation of an entry in the connection table and buffer space. Following such an exchange, the TCP connection is treated as half-open. An ACK message must be sent back to the server by the user to ensure that the TCP connection is completely established. During the TCP SYN flooding attack, enormous SYN messages with fake (spoofed) internet protocol (IP) addresses are sent to an

individual server (victim) by a certain attacker, among a high number of compromised users subjected to distributed DoS attacks. In spite of the reply sent by the server to SYN/ACK messages, absolutely no acknowledgment occurs by the client to these messages. Consequently, the resources of the server are consumed due to the occurrence of a large number of half-open connections. This process does not stop until the absolute consumption of the server's resources, leaving no more capability of accepting any other requests of TCP connection. End-system methods have been recently suggested to protect against SYN flooding attacks. Nonetheless, these methods necessitate that the end-systems be modified. They are also unable to provide protection against those attacks proceeding with full TCP handshaking [3]. Furthermore, the researchers are still questioning the potential overhead that such end-system methods are able to introduce. A continuous threat to networks and computers connected to the internet is still posed by DoS attacks. In the computer crime and security survey reported by the crime scene investigation/federal bureau of investigation (CSI/FBI), 42% of the participants reported DoS attacks as a major issue. Financial setbacks resulting from DoS attacks constituted the second largest cause of loss of revenue, immediately ranked after the proprietary information theft [4].

WikiLeaks reported that it was targeted by a distributed denial of service (DDoS) attack that lasted for over longer than one week. The website stated it was subjected to a traffic flood of 10 gigabits per second, causing slowness and unresponsiveness [5]. The research gap in this paper is applying machine learning algorithms to automatically the process of predicting Dos and DDoS attacks such as "DDoS", "DoS Hulk", "DoS GoldenEye", "DoS Slowhttptest" and "DoS Slowloris". The rest of the paper is organized as follows; Section 2 delineates the related work. Section 3 describes the system design. Section 4 provides the results. Section 5 is conclusions.

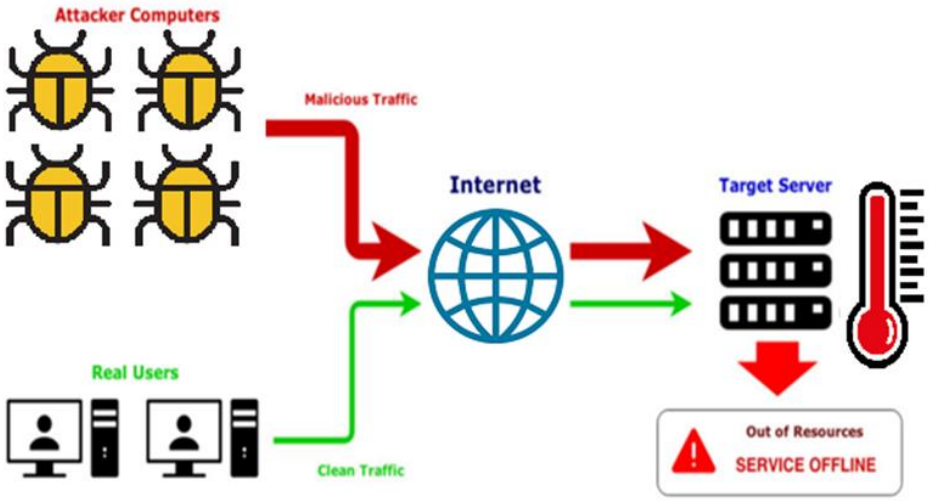

Figure 1. Malicious and clean traffic

2. RELATED WORK

Many studies have been involved in preventing DDoS attacks in recent times [6]. Such approaches are designed to aid a victim server to keep serving requests during the occurrence of attacks. Such approaches include those related to resource scaling, management, and relocation, as well as network-based mitigation methods specified by software. Moreover, there is several techniques solved abnormal attack [7]-[15], but this Dos attack need different technique to solve it. So that, we used different monitiring network attributs to distiquish between normal and abnormal attack, such as source and destination IPs, destination and source ports, type of attack and protocols, and more behavior of packet.

As a mechanism of action, DoS attacks overwhelm websites, clog network connections, and render servers unavailable [5]. Wang *et al.* [16] proposed a DoS attacks detection method that acts on the victim side, the model worked by monitoring the network traffic packets on the primary victim server. Xiao *et al.* [17] detected DDoS attacks toward a data center by employing correlation analysis. This approach benefits from the correlation of flow information within the data center. It confers a mechanism that depends on K-Nearest Neighbor with correlation and r-polling model for the reduction of the overhead caused by the high density of the training dataset. Kalkan and Alagöz [18] proposed a mechanism to detect and filter DDoS attacks, depending upon the score value calculated for each incoming packet. The authors suggested a

considerable increase in the success of system's behavior toward legal and attack packets. Decision on whether the packet is legal or not is decided by the mechanism. The utilized input attributes included IP address, port number, protocol type, packet size, time to live (TTL) value, and TCP flag. Our proposed technique is different from the above model in terms of environment. Our proposed system works by analyzing messages sent from the client to the server with history packets. After that, the proposed algorithm decides to drop or forward the packet.

An approach that employs the advanced all repeated patterns detection (ARPaD) Algorithm was previously introduced, allowing all repeated patterns in a sequence to be detected. The proposed method allows readily acquiring the results related to all IP prefixes in a sequence of hits. Therefore, the network administrator receives an alarm when a potential DDoS attack is being developed. The results are based on several experiments [19].

A method to preliminary detects DDoS attacks via the classification of network conditions was proposed by Nguyen and Choi in 2010 [20], where key features served for the selection of a number of variables. Furthermore, they utilized the -nearest neighbor (-NN) approach for the classification of network conditions into the phases of DDoS attack. Moreover, Tsai and Lin [21] described a novel approach, called the triangle area based nearest approach, for the detection of DDoS attacks, which resulted in the improvement of accuracy and false positive rate (FPR) values. The concept of the DDoS attack and its influences on network traffic was introduced by Bhange *et al.* [22] in 2012. The authors investigated this attack via the analysis of network traffic the distribution, with the aim of distinguishing abnormal from normal network behavior. A highly sophisticated method for the detection of DoS attack, utilizing MCA, was introduced by Tan *et al.* in 2014 [23], proposing a novel detection system that depends on MCA for the protection of online services against DoS attacks. Also in 2014, a mathematical model was developed for the estimation of the combined influences of DDoS attack pattern and network environment on the attack. The model was designed by initially capturing the adjustment behaviors that belong to the victim TCPs congestion window.

3. SYSTEM DESIGN

Machine learning [24] is integral part of artificial intelligence that based on improving results through learning and experience. J48 represents an open-source Java implementation of the C4.5 algorithm in the Weka data-mining tool. C4.5 is software that is used to produce a decision tree depending on a labeled input dataset. C4.5 is commonly described as a statistical classifier, given the possibility of using the decision trees it generates for the purpose of classification [25]. Our proposed method adopts the machine learning classifies algorithm of type J48. The selected training samples include the benign and DDoS, DoS Hulk, DoS GoldenEye, DoS Slowhttptest and DoS Slowloris samples, captured by Sharafaldin *et al.* [26]. The proposed method contains benign and DoS attacks as network traffic samples. We tested the network in different behavioral of attack. So that, we know every label, when the network was ready, we captured it by using CICFlowMeter. The dataset labeled for every captured, we captured five of different the DoS attack dataset and one of benign dataset; we used this data set for training. Moreover, every sample includes many attributes, such as source and destination IPs, destination and source ports, type of attack and protocols, and more behavior of packet. The number of attributes for every sample is saved as a CSV file, is 79. We used 14400 samples for training and testing, 9600 samples for training and 4800 samples for testing. The training dataset we called it in the flowchart diagram as shown in Figure 1 is "first dataset". The testing dataset we called it in the flowchart diagram as shown in Figure 1 is "second dataset". In the training part, we divided 9600 for each of the benign and DDoS, DoS Hulk, DoS GoldenEye, DoS Slowhttptest, and DoS Slowloris, so each included 1600 samples. In the testing part, we divided 4800 for each of the benign and DDoS, DoS Hulk, DoS GoldenEye, DoS Slowhttptest, and DoS Slowloris, so each included 800 samples. The algorithm monitors the network to read 78 attributes without label attribute because it used for testing. When the number of samples is monitored by the algorithm and should reaches to 800 samples, the algorithm saves them as a second dataset without label. The algorithm changes and tests the label. The algorithm changed the sequence of the label (SoL) that starts from "benign", "DDoS", "DoS Hulk", "DoS GoldenEye", "DoS Slowhttptest" and ends with "DoS Slowloris". After that, the algorithm finds the best result label (BRL), depending on the label that was changed as shown in Figure 2. If the high accuracy is labeled as benign, the algorithm continues to capture a new dataset; otherwise, it sends a warning of an attack, with the type of that attack. Approaches that include statistical analysis, machine learning, and data mining can be used in the detection of DDoS attack.

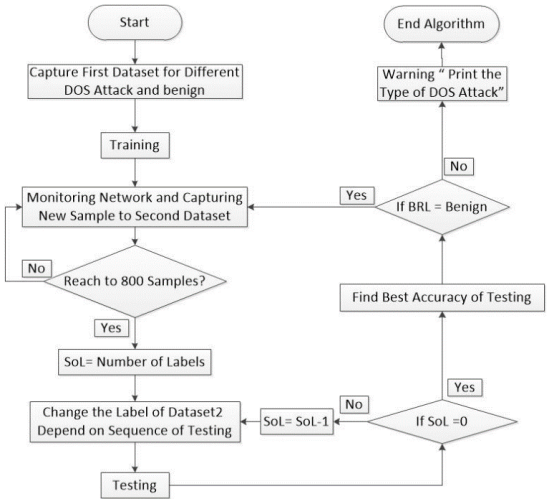

Figure 2. Flowchart diagram of proposed system

4. RESULTS

We tested our algorithm based on the samples that were collected with six datasets as shown in Table 1. The first tested result was that of the benign samples; the result stated that 782 samples are benign. Moreover, the algorithm classified 3 samples as DDoS, 2 as Dos Hulk, 2 as DoS GoldenEye, 10 as DoS Slowhttptest, and 1 as DoS Slowloris; where the classification accuracy of benign was 97.7 percentage.

The second tested result was that of the DDoS samples, where 798 samples were classify as DDoS. However, the algorithm also showed an incorrect classification, where it classified 2 samples as benign, where the classification accuracy of DDoS was 99.8 percentage. The third tested result was that of the DoS Hulk samples. The algorithm classified 799 samples as DoS Hulk. However, 1 sample was classified as benign; the classification accuracy for DoS Hulk was 99.9 percentage. The fourth tested was DoS GoldenEye, it was 800 samples; the classification accuracy was 100 percentage.

The fifth tested was DoS Slowhttptest, it was 794 of 800 samples were correctly classified; the accuracy was 99.3 percentage. However, 6 samples were incorrectly classified, among which 4 as DoS Slowloris and 1 sample as each of DoS GoldenEye and benign. Finally, the sixth tested was DoS Slowhttptest, it was 794 of 800 samples were correctly classified; the accuracy was 99.3 percentage. However, 6 samples were incorrectly classified, among which 4 as DoS Slowhttptest and 2 as benign.

Table 1. Result of proposed system

Type of Sample	Number of Samples	Benign	DDoS	DoS Hulk	DoS GoldenEye	DoS Slowhttptest	DoS Slowloris	Correct Classification
Benign	800	782	3	2	2	10	1	97.8%
DDoS	800	2	798	0	0	0	0	99.8%
DoS Hulk	800	1	0	799	0	0	0	99.9%
DoS GoldenEye	800	0	0	0	800	0	0	100%
DoS Slowhttptest	800	1	0	0	1	794	4	99.3%
DoS Slowloris	800	2	0	0	0	4	794	99.3%
Total of Correct Classification								99.3%

5. CONCLUSIONS

Our proposed machine learning classifier algorithm is of the type J48. We selected benign and DDoS, DoS Hulk, DoS GoldenEye, DoS Slowhttptest and DoS Slowloris samples for tested our proposed system. They were captured by using CICFlowMeter, five labeled as having one type of the five DoS labels, while one had the label of benign. Moreover, every sample included many attributes, including the source and destination IPs, destination and source ports, type of attack and protocols, and more behavior of packet. The formed collectively 79 attributes for every sample, which were saved as a CSV file. We tested our algorithm based on the samples collected with six datasets. Our results or all the selected cases showed the accuracy of proposed system was 99 percentage of correct classification. In the future work, we will test our algorithm in various mobile attacks such as scareware and SMS.

REFERENCES

[1] V. A. Siris and F. Papagalou "Application of anomaly detection algorithms for detecting SYN flooding attacks," in *IEEE Global Telecommunications Conference GLOBECOM* '04, 2004, pp. 2050–2054, doi: 10.1109/GLOCOM.2004.1378372

[2] R. B. Blazek, H. Kim, B. Rozovskii, A. Tartakovsky, "A novel approach to detection of denial-of-service attacks via adaptive sequential and batch sequential change-point detection methods," in: *Proceedings of IEEE Workshop on Systems, Man, and Cybernetics Information Assurance*, June 2001.

[3] G. R. Zargar and T. Baghaie, "Category Based Intrusion Detection Using PCA," *International Journal of Information Security*, vol. 3, no. 4, pp. 259-271, 2012, doi: 10.4236/jis.2012.34033.

[4] W. W. Streilein, D. J. Fried, and R. K. Cunninggham, "Detecting flood-based denial-of-service attacks with SNMP/RMON," in *Proceedings of the Workshop on Statistical and Machine. Learning Techniques in Computer Intrusion Detection, George Mason University*, September 2003.

[5] R. Thandeeswaran and M. A. S. Durai, "Bi-level user authentication for enriching legitimates and eradicating duplicates in cloud infrastructure," *International Journal of Computer Aided Engineering and Technology*, vol. 12, no. 1, pp. 95-112, 2020, doi: 10.1504/ijcaet.2020.103836.

[6] M. Arshi, M. Nasreen, and K. Madhavi, "A Survey of DDOS Attacks Using Machine Learning Techniques," *E3S Web Conf.*, 2020, doi: 10.1051/e3sconf/202018401052.

[7] M. M. Rasheed, N. M. Norwawi, O. Ghazali, and M. K. Faaeq, "Detection algorithm for internet worms scanning that used user datagram protocol," *IJICS*, vol. 11, no. 1, 2019, doi: /10.1504/IJICS.2019.096847.

[8] M. M. Rasheed and M. K. Faaeq, "Behavioral Detection of Scanning Worm in Cyber Defense," in *Proceedings of the Future Technologies Conference (FTC) 2018, Springer International Publishing*, 2018, pp. 214–225, doi: 10.1007/978-3-030-02683-7_16.

[9] N. S. Rao, K. C. Sekharaiah, and A. A. Rao, "A survey of distributed denial-of-service (DDoS) defence techniques in ISP domains," in *Innovations in Computer Science and Engineering*, vol. 32, pp. 221–230, 2019.

[10] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021, doi: 10.1109/ACCESS.2021.3056614.

[11] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods*," IEEE Access*, vol. 7, pp. 51691–51713, 2019, doi: 10.1109/ACCESS.2019.2908998.

[12] M. M. Rasheed, S. Badrawi, M. K. Faaeq, and A. K. Faieq, "Detecting and optimizing internet worm traffic signature," *2017 8th Int. Conf. on Inf. Tec. (ICIT)*, May 2017, doi: 10.1109/ICITECH.2017.8079961.

[13] A. Zulhilmi, S. A. Mostafa, B. A. Khalaf, A. Mustapha, and S. S. Tenah, "A comparison of three machine learning algorithms in the classification of network intrusion," in *Proceedings of the International Conference on Advances in Cyber Security*, Penang, Malaysia, July 2020, pp. 313–324.

[14] M. Ring, S. Wunderlich, D. Grüdl, D. Landes, and A. Hotho, "Flow-based benchmark data sets for intrusion detection," *Proc. of the 16th European Conf. on Cyber Warfare and Security*, Dublin, Ireland, 2017, pp. 361-369.

[15] M. M. Rasheed, A. K. Faieq, and A. A. Hashim, "Android Botnet Detection Using Machine Learning," *Ingénierie des Systèmes D Information*, vol. 25, no. 1, pp. 127–130, Feb. 2020, doi: 10.18280/isi.250117.

[16] J. Wang, R. C.-W. Phan, J. N. Whitley, and D. J. Parish, "Augmented Attack Tree Modeling of Distributed Denial of Services and Tree Based Attack Detection Method," *presented at the 2010 IEEE 10th International Conference on Computer and Information Technology (CIT)*, Jun. 2010, https://doi.org/10.1109/CIT.2010.185.

[17] P. Xiao, W. Qu, H. Qi and Z. Li, "Detecting DDoS attacks against data center with correlation analysis," *Comput. Commun.*, vol. 67, pp. 66–74, 2015, doi: 10.1016/j.comcom.2015.06.012.

[18] K. Kalkan and F. Alagöz, "A distributed filtering mechanism against DDoS attacks: ScoreForCore," *Comput. Netw.*, vol. 108, pp. 199–209, 2016, doi: 10.1016/j.comnet.2016.08.023.

[19] K. Xylogiannopoulos, P. Karampelas, and R. Alhajj, "Early DDoS Detection Based on Data Mining Techniques," *IFIP Int.l Workshop on Inf. Security Theory and Practice*, 2014, pp. 190–199, doi: 10.1007/978-3-662-43826-8_15.

[20] H. V. Nguyen and Y. Choi, "Proactive detection of DDoS attacksutilizing k-NN classifier in an anti-DDoS framework*," Int. Journal of Electrical, Computer, and Systems Engineering*, vol.4, no. 4, pp. 247–252, 2010.

[21] C. F. Tsai and C. Y. Lin, "A triangle area based nearest neighbors approach to intrusion detection," Pattern Recognition, vol. 43, no. 1, pp. 222–229, 2010, doi: 10.1016/j.patcog.2009.05.017.

[22] A. Bhange, A. Syad, and S. Singh Thakur, "DDoS attacks impact on network traffic and its detection approach," *International Journal of Computer Applications*, vol. 40, no.11, pp. 36–40,2012 doi: 10.5120/5011-7332.

[23] Z. Y. Tan, A. Jamdagni, X. J. He, P. Nanda, and R. P. Liu, "A system for denial-of-service attack detection based onmultivariate correlation analysis," *IEEE Transactions on Paralleland Distributed Systems*, vol. 25, no. 2, pp.447–456, 2014, doi: 10.1109/TPDS.2013.146.

[24] C. Grosan and A. Abraham, "Machine Learning," *Intelligent Systems. Intelligent Systems Reference Library*, vol. 17, 2011, doi: 10.1007/978-3-642-21004-4_10.

[25] P. Chandrasekar, K. Qian, H. Shahriar, and P. Bhattacharya, "Improving the Prediction Accuracy of Decision Tree Mining with Data Preprocessing," presented at *the 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, Jul. 2017, doi: 10.1109/COMPSAC.2017.146.

[26] I. Sharafaldin, A. Habibi Lashkari, and A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," *4th International Conference on Information Systems Security and Privacy (ICISSP)*, Portugal, January 2018.