http://www.jctjournals.com

ISSN(ONLINE):2278 – 3814

Volume-11, Issue-1, January 2022

JOURNAL OF COMPUTING TECHNOLOGIES (JCT)

International Journal

Page Number: 01-06

A Bird Eye On Cyber Security Problems

Arjun Choursiya [1],Prof.Anuradha Deolase[2],
[1]M.Tech Scholar, [2]Assistant Professor,
[1,2]Department of cyber security
[1,2]Vikrant Institute of Technology & Management, Mohow Indore l(M.P), INDIA,
[1] Carjun2224@gmail.com, [2]anuradhadeolase@vitmindore.com

***Abstract*— In this survey paper discuss on DDoS attacks are the most destructive attacks that interrupt the safe operation of essential services delivered by the internet community's different organizations. DDOS stands for Distributed Denial Of Service attacks. These attacks are becoming more complex and expected to expand in number day after day, rendering detecting and combating these threats challenging. Hence, an advanced intrusion detection system (IDS) is required to identify and recognize an- anomalous internet traffic behaviour. Within this article the process is supported on the latest dataset containing the current form of DDoS attacks including (HTTP flood, SIDDoS). This study combines well-known grouping methods such as Naïve Bayes, Multilayer Perceptron (MLP), and SVM, Decision trees.**

Keywords—Component accuracy, Precision, Selectivity, Sensitivity, Specificity, Confusion Matrix (C.M.) Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) etc.

I. INTRODUCTION

Denial of Service attacks drains a specified program's web bandwidth but also information measures, restricting it from providing service to users with authenticated traffic. DDoS (Distributed Denial of Service) attacks are becoming more widespread. As seen in Figure 1, cyber-attacks acquire access to a large number of compromised systems, known as a "botnet," and then conduct simultaneous attacks on the victim machine. DDoS attacks are changing but also increasing in volume, frequency, as well as complexity in combination with the development and growth of transformative Internet technologies. Organizations confront optimal network risks that might have a significant effect on their activities, including downtime, data leaks, or even payment demands from hackers. Behavior for DDoS mitigation should be undertaken in the occurrence of DDoS attacks, as recommended below. Before any mitigation strategies can be implemented, DDoS attacks should first be detected. DDoS operations were first detected by traffic volume using criteria they had designed. This strategy seems to have drifted behind the dynamic and developing nature of DDoS attacks.

In risk assessment, traditional manual approaches have low accuracy but significant latency. Threats may be caught more rapidly and precisely using machine learning techniques such as Naive Bayesian, KNN, and Random Forest. Professional specialists or specific feature selection algorithms should identify features for categorization in machine learning (ML)[20]. Feature extraction, on the other hand, is an important aspect of deep learning (DL). Convolutional neural networks (CNN), as well as recurrent neural networks (RNN), are deep learning models that learn multiple levels of data interpretation from a huge volume of classification techniques using a succession of nonlinear processing layers. As a result, deep learning (DL) may be a useful method for detecting DDoS.

Numerous kinds of network assaults arrive with expansion of computing networks, particularly the internet. International ransom ware virus called Wannacry has newly stopped internet services in around 156 countries. As per Kaspersky lab results throughout the fourth quarter, Botnet aided attacks were aimed at assets in nearly 69 countries. The final quarter also experienced the largest DDoSbased Botnet attack that lasts roughly 15.5 days 371 hours Crackers or dark hackers are constantly creating new forms of multilayered DDoS attacksthat happen mainly on a OSI network and application layer. Such attacks have used the spoofed IP addresses to confound source detection and conduct a huge-scale attack. These attacks are quite huge, as the attack traffic absolutely consumes the network spectrum at the peak, thus reducing the legal packets. Ironically, the victims are government entities, finance companies, defense forces and military agencies. Famous sites such as facebook, twitter, wiki leaks etc, had become victims of DDoS that also observed interruptions in routine maintenance resulting in financial failures, depletion of service and lack of access.

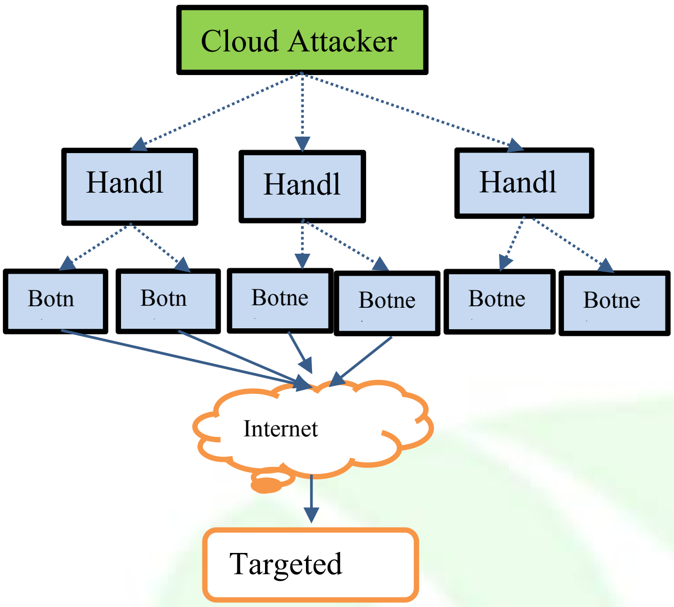

Fig. 1. - Cloud Denial of Service (DoS) attack

Machine learning (ML), as well as deep learning (DL), have both been found to be completely effective in detecting DDoS attacks. Algorithms are, however, taught to detect only examples selected from the training set's distribution models. As a result, individuals may perform in situations where they have never learned. The Open Set Recognition (OSR) challenge is about figuring out what one doesn't know. Because DDoS intrusion technologies develop, resulting in shifting traffic parameters, this issue has a significant influence on DDoS attack detection. Malicious node attacks could not only prevent access to network resources but also result in major risks and harm. A Denial of Service (DoS) attack, for example, prevents genuine end-users from using network resources by overflowing the target system by propagating widely and finally paralyzing it. TCP/SYN Flood, Ping Flood, UDP Flood, and Distributed Denial of Service are all examples of DoS assaults (DDoS). Several compromised malicious activities attack a single target in a DDoS attack[25].

The next section discusses the previous work that is presented by different researchers. After that discuss the proposed method for Distributed Denial of Service (DDoS) attack detection in section III. Section IV discusses the simulation and result of the proposed method. Last but not least discuss the conclusion in section V.

II. LITERATURE SURVEY

Kshirsagar, D., & Kumar, S. (2021), In this research work, presented a feature selection based framework using flter-based feature selection techniques with threshold and achieves signifcant performance to detect DDoS attacks. The framework obtains reduced features of 36, 14, 36, 25, and 18 for the detection of Portmap, SYN, NetBIOS, MSSQL, and LDAP attacks respectively. The system provides an improved accuracy of 99.9569, 99.9948, and 99.9930% for the detection of Portmap, MSSQL, and LDAP attacks respectively with J48 using reduced features. The system also outperforms in FAR for the detection of LDAP, Portmap, and MSSQL attacks with model built-up time. The validation of the proposed framework on KDD Cup 1999 dataset provides improved DR of 99.8884% with a minimum model built-up time of 6.71 s, using 16 reduced features for the binary classifcation. The system achieves a signifcant performance compared to the relevant existing feature selection methods used for intrusion detection on KDD Cup 1999 and CICDoS2019 datasets[1].

Erhan, D., & Anarim, E. (2020). In this research work, presented the AMP method for DDoS detection that uses the MP algorithm. Researcher also introduce the characteristic feature vector generated from a combination of multiple one-dimensional traffific attributes. Furthermore, in this study, adaptation to the traffific data to the MP algorithm is provided by creating dictionaries from the training dataset. Because there is no recent study that uses the MP algorithm in the detection of DDoS attacks, the proposed methodology is compared with the MPMP and Wavelet methods. Researcher practice these methods using CAIDA and BOUN datasets. The experimental results show that the AMP method performs better with higher CID values comparing with the Wavelet and the MPMP approaches. Additionally, in this study, a hybrid intrusion detection framework is proposed that combines the abnormality indicator values obtained from different dictionaries. The abnormality indicator values are combined with an intelligent decision mechanism that uses ANN. MPMP and Wavelet methods are designed for only anomaly detection. Researcher also include these methods in our Hybrid framework by combining them with the decision module utilizing the abnormality indicator vectors obtained for each traffific attribute vector. Evaluation results show that the hybrid detection framework using the AMP approach performs better than MPMP and Wavelet-based methods for all traffific classes, including attack-free traffific class[2].

Chen, Y. W.,* et. al *(2020 June), In this research work, presented, a multi-layer DDoS detection system based on machine learning to prevent DDoS attacks in IoT gateway. We extract features of four types of DDoS attacks, including sensor data flood, ICMP flood, SYN flood, and UDP flood and make these features to be numerical. We launch DDoS attacks from eight smart poles as a real IoT scenario and show that our multi-layer DDoS detection system can distinguish normal packets and DDoS attack packets from IoT devices accurately. Our proposed system can detect DDoS attacks with high accuracy. The F1-score is over 97%. When abnormal packets are detected, the IP addresses and MAC addresses of the malicious devices are sent to the SDN controller. The SDN controller adds these IP addresses, and MAC addresses into blacklists and sets the rules for SDN switches from the blacklists. The devices in the blacklists are blocked immediately in the SDN switches. In this way, our proposed multi-layer DDoS detection system not only detects the DDoS attacks but also blocks the malicious devices [3].

Rahman, O., et.al (2019, July). , In this research work, presented an SDN framework to detect and protect the controller and the OF switch from DDoS attacks. This framework involves training a machine learning model with captured data to predict DDoS attacks. The prediction is then used by our mitigation script to make decisions in our SDN network.Researchers evaluated SVM, K-NN, J48, and Random Forest with online captured data. Our experiment results showed J48 to be the most suitable classifier for our network [4].

Yang, L., et.al. (2018, October) This research work presented, an SDN framework to identify and defend against DDoS attacks. This framework consists of 2 parts which are traffic collection module, attack identification module and flow table delivery module. Traffic collection module extracts traffic characteristics to prepare for traffic identification. Currently, we have applied SVM to DDoS traffic identification. The experiment results on the KDD99 dataset show the effectiveness. This classification model is deployed on the simulated SDN environment for campus network as a DDoS detection module. All traffic is identified by this model. If attack traffic is identified, the controller will discard packets according to the predefined rule. If the packet is not attacked, the forwarding policy will be executed normally[5].

Meti, N., et.al (2017, September). This research work presented Software Defined Networking is an emerging architecture which is ideal for the high-bandwidth, dynamic nature of today's applications as it is not only dynamic but also easily manageable, cost-effective and adaptable. SDN aims at allowing network engineers and administrators to respond quickly to the rapidly changing business requirements. This paper provides security to SDN controller. It shows how DDoS attacks can be detected by classifying the incoming requests using machine learning algorithms. The implementation of IDS in SDN using machine learning algorithms has shown better results. We implement the proposed mechanism using Mininet and Ryu controller. Results show the effectiveness of the solution by trying it on different topologies. SVM algorithm proves to be a better choice for implementing IDS in SDN as it as highest accuracy and recall and a decent precision value among all the three algorithms considered [6].

Barki, L., et. al (2016, September) (2017) This research work presented, Software Defined Network (SDN) is an emerging architecture that is dynamic, manageable, cost effective and adaptable, making it ideal for high bandwidth, dynamic nature of todays applications. The goal of SDN is to allow network engineers and administrators to respond quickly to changing business requirements. This paper provides security to SDN controller. Further paper shows how DDoS attacks can be detected by classifying the incoming requests using various machine learning algorithms. The implementation of IDS in SDN using machine learning algorithms has shown better results. We implement the proposed mechanism using Mininet and POX controller. Results show the effectiveness of the solution by trying it on different topologies [7].

N. Dayal et al (2017, January), Researcher presented an attack model in this overview to detect and categorise different DDoS attack possibilities in SDN. Various DDoS assaults were also carried out in the SDN environment with the aid of the hyenae attack tool, employing a few of the most common traditional DDoS attack tactics. Researchers discovered that although volumetric assaults have a significant effect on the data plane because they concentrate on consuming data plane bandwidth, they have little influence on the controller. The effect is only evident during the assault phase. Protocol exploitation attacks, on the other hand, have little impact on network capacity. They concentrate on the use of various device resources like TCAM, logical port, and so on. These strikes have the potential to be devastating to the controller both during and after the attack. In reality, TCP SYN flood and HTTP flood assaults may put the controller to a halt[8]

Yadav, S., et.al (2015, September) In this research work, A Logistic Regression framework was suggested to design regular user searching behavior to detect any incoming application layer DDoS attack traffic. A variety of features were developed to distinguish between an attacker and a normal user when simulating user behavior. Classification methods from a newly constructed feature set were combined with those from an existing feature set to produce an optimal or nearly optimal result. Our method was tested on real-world traffic obtained from web server logs and attack traffic generated in a sandbox environment. Multiple datasets, both real world as well as computer developed, were used to evaluate the proposed technique. With an average Detection Rate of 98.64 percent and a False Positive Rate of 1.41 percent, the test findings demonstrate that the proposed scheme is impactful at distinguishing attack traffic from regular traffic[9].

III. CLASSIFICATION OF DDOS

Automated, exploited disadvantage, attack rate dynamics, source address applicability, spoofing methodologies as well as the effect on victim kinds as well as persistence are some of the factors used to categorise DDoS attacks. High-Rate Flooding (HRF) DDoS attacks on computing and networking resources are examined in this thesis. During the attack, it utilises a legitimate connection. The attack can be launched with a smaller number of connections.

- In the sluggish DoS assault, there is a low traffic quantity as well as bandwidth use. It's impossible to detect by typical defense systems. Detection of slow DoS assaults has been proposed using a variety of methods [8,9]. Slow DoS attacks have previously been detected using SDN and machine learning-based methodologies [12].
- This study proposes a slow DoS classifier based on deep learning and flows data. The use of deep neural network categorization on flow data for the identification of slow HTTP DoS is innovative in this work. In comparison to the host-based slow DoS attack detection, the suggested technique provides the following benefits.
- To prevent sluggish DoS attacks, a network gateway can gather and analyse traffic flow information, allowing a preventive solution to be activated before the attack traffic reaches the target.
- It is possible to utilise the slow DoS classifier on any web server, regardless of operating system or host, without changing any server configuration settings. Web-based services, such as citizen services, cloud-based services, banking, as well as financial services, are increasingly popular in today's service industry.
- Slow DDoS attacks on web servers in these contexts could have a devastating impact. The suggested approach can be used to identify and prevent slow HTTP DoS in these contexts because it focuses on web applications.

An impactful quantitative assessment to distinguish normal traffic from attack and surge of legitimate access is provided by traffic features such as source IP address, source port, as well as target port. This method was chosen because it is the most impactful method for achieving the thesis's objective. The source IP address is the most important factor in determining the randomness of the traffic that arrives. This chapter also discusses a method for calculating the entropy of the source IP address. There aren't many attack traffic traces, but the Center for Applied Internet Data Analysis (CAIDA) dataset is. Real-time traffic traces from the institute of engineering (IOE) webserver were used to conduct the research's practical aspects.

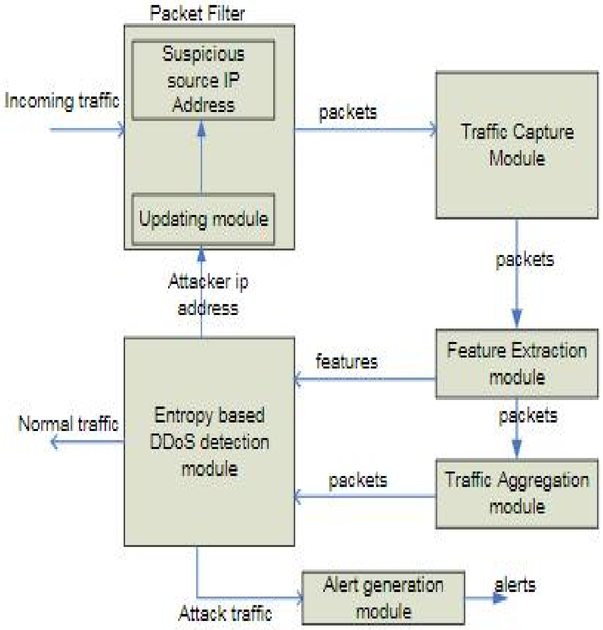

Fig. 2 Block Diagram of DDoS detection System

The above figure 2 shows the traffic and its intensity and discusses the entropy-based DDoS detection module.

IV. CONCLUSION

In this survey paper, as Attack techniques continue to lead, the companies today have to face various threats. DDoS attacks are increasing day by day and their main aim is to harm the every level in the data center of the organization. Smart Companies take steps not only to defend from the attacks ,but also find the origin of the attack. This article attention is on the matter that to take effective counter steps against DDoS attacks. It is shown in the paper that there are various detection and mitigation mechanisms to prevent the network from various kinds of DDoS attacks. In future some different techniques can be used to detect and mitigate the effect of DDoS attack, like detection technique integrated pattern of matching method with wire shark and mitigation using Access control lists(ACL) with trace route or using a Firewall. So this paper give a survey about various kinds of DDoS attacks and how to handle them. It helps to give a basic idea of the techniques to the reader who wants to get started his research work from network security.

[1] Kshirsagar, Deepak, and Sandeep Kumar. "A feature reduction based reflected and exploited DDoS attacks detection system." Journal of Ambient Intelligence and Humanized Computing (2021): 1-13.

[2] Erhan, Derya, and Emın Anarim. "Hybrid DDoS detection framework using matching pursuit algorithm." IEEE Access 8 (2020): 118912-118923.

[3] Chen, Yi-Wen, Jang-Ping Sheu, Yung-Ching Kuo, and Nguyen Van Cuong. "Design and implementation of IoT DDoS attacks detection system based on machine learning." In 2020 European Conference on Networks and Communications (EuCNC), pp. 122-127. IEEE, 2020.

[4] Rahman, Obaid, Mohammad Ali Gauhar Quraishi, and Chung-Horng Lung. "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.

[5] Yang, Lingfeng, and Hui Zhao. "DDoS attack identification and defense using SDN based on machine learning method." In 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN), pp. 174-178. IEEE, 2018.

[6] Meti, Nisharani, D. G. Narayan, and V. P. Baligar. "Detection of distributed denial of service attacks using machine learning algorithms in software defined networks." In 2017 international conference on advances in computing, communications and informatics (ICACCI), pp. 1366-1371. IEEE, 2017.

[7] Barki, Lohit, Amrit Shidling, Nisharani Meti, D. G. Narayan, and Mohammed Moin Mulla. "Detection of distributed denial of service attacks in software defined networks." In 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2576-2581. IEEE, 2016.

[8] Dayal, Neelam, and Shashank Srivastava. "Analyzing the behavior of DDoS attacks to identify DDoS detection features in SDN." In 2017 9th International Conference on Communication Systems and Networks (COMSNETS), pp. 274-281. IEEE, 2017

[9] Hsieh, Chang-Jung, and Ting-Yuan Chan. "Detection DDoS attacks based on the neural network using Apache Spark." In 2016 international conference on applied system innovation (ICASI), pp. 1-4. IEEE, 2016.

[10] Buragohain, Chaitanya, and Nabajyoti Medhi. "FlowTrApp: An SDN based architecture for DDoS attack detection and mitigation in data centers." In 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), pp. 519-524. IEEE, 2016.

[11] Xiao, Peng, Zhiyang Li, Heng Qi, Wenyu Qu, and Haisheng Yu. "An efficient DDoS detection with bloom filter in sdn." In 2016 IEEE Trustcom/BigDataSE/ISPA, pp. 1-6. IEEE, 2016.

[12] Yadav, Satyajit, and Selvakumar Subramanian. "Detection of Application Layer DDoS attack by feature learning using Stacked AutoEncoder." In 2016 international conference on computational techniques in information and communication technologies (icctict), pp. 361-366. IEEE, 2016.

[13] Wang, Rui, Zhiping Jia, and Lei Ju. "An entropy-based distributed DDoS detection mechanism in software-defined networking." In 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1, pp. 310-317. IEEE, 2015.

[14] Zhao, Teng, Dan Chia-Tien Lo, and Kai Qian. "A neural-network-based DDoS detection system using Hadoop and HBase." In 2015 IEEE 17th International Conference on High-Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, pp. 1326-1331. IEEE, 2015.

[15] Yadav, Satyajit, and S. Selvakumar. "Detection of application-layer DDoS attack by modeling user behavior using logistic regression." In 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), pp. 1-6. IEEE, 2015.

[16] Balkanli, Eray, A. Nur Zincir-Heywood, and Malcolm I. Heywood. "Feature selection for robust backscatter DDoS detection." In 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), pp. 611-618. IEEE, 2015.

[17] Badve, Omkar P., Brij B. Gupta, Shingo Yamaguchi, and Zhaolong Gou. "DDoS detection and filtering technique in cloud environment using GARCH model." In 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), pp. 584-586. IEEE, 2015.

[18] Kokila, R. T., S. Thamarai Selvi, and Kannan Govindarajan. "DDoS detection and analysis in SDN-based environment using support vector machine classifier." In 2014 Sixth International Conference on Advanced Computing (ICoAC), pp. 205-210. IEEE, 2014.

[19] Kokila, R. T., S. Thamarai Selvi, and Kannan Govindarajan. "DDoS detection and analysis in SDN-based environment using support vector machine classifier." In 2014 Sixth International Conference on Advanced Computing (ICoAC), pp. 205-210. IEEE, 2014.

[20] Choi, Junho, Chang Choi, Byeongkyu Ko, and Pankoo Kim. "A method of DDoS attack detection using HTTP packet pattern and rule engine in the cloud computing environment." Soft Computing 18, no. 9 (2014): 1697-1703.

[21] Barati, Mehdi, Azizol Abdullah, Nur Izura Udzir, Ramlan Mahmod, and Norwati Mustapha. "Distributed Denial of Service detection using hybrid machine learning technique." In 2014 International Symposium on Biometrics and Security Technologies (ISBAST), pp. 268-273. IEEE, 2014.

[22] Sharma, Shachi, and Pranay Yadav. "Removal of fixed valued impulse noise by improved Trimmed Mean Median filter." In 2014 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-8. IEEE, 2014.

[23] Yadav, Pranay, and Parool Singh. "Color impulse noise removal by modified alpha trimmed median mean filter for FVIN." In 2014 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-8. IEEE, 2014.

[24] Yadav, Pranay. "Color image noise removal by modified adaptive threshold median filter for RVIN." In 2015 International Conference on Electronic Design, Computer Networks & Automated Verification (EDCAV), pp. 175-180. IEEE, 2015.

[25] 5.Yadav, Pranay, Shachi Sharma, Prayag Tiwari, Nilanjan Dey, Amira S. Ashour, and Gia Nhu Nguyen. "A Modified Hybrid Structure for Next Generation Super High-Speed Communication Using TDLTE and Wi-Max." In the Internet of Things and Big Data Analytics Toward Next-Generation Intelligence, pp. 525-549. Springer, Cham, 2018.

[26] Sharma, Bharti, Sachin Kumar, Prayag Tiwari, Pranay Yadav, and Marina I. Nezhurina. "ANN-based short-term traffic flow forecasting in undithe vided two-lane highway." Journal of Big Data 5, no. 1 (2018): 1-16