International Journal of Engineering Innovation & Research
Volume 12, Issue 5, ISSN: 2277 – 5668

Review Paper on Denial of Service Attacks in SDN using Artificial Neural Network

Prateeksha Sahu[*], Onkar Nath Thakur and Rakesh Kumar Tiwari
Department of Computer Science and Engineering, Technocrats Institute of Technology and Science,
Bhopal, Madhya Pradesh, India.
[*]Corresponding author email id: prateeksha2706@gmail.com

Date of publication (dd/mm/yyyy): 10/10/2023

***Abstract* – Distributed Denial of Service (DDoS) attacks have been a serious cybercrime attack for decades and are one of the most disturbing areas of cyber security due to their disguising nature. Cisco predicted that attack frequency will be doubled from 7.9 million in 2018 to 15 million by 2023, and the financial hit of DDoS attacks on Information Technology (IT) services will cost from $300,000 to over $1,000,000 per hour. So, it is very important to handle DDoS attacks at the early stages. Various researchers focused on the problem of early detection of DDoS attacks in the SDN environment, but the performance of the actuators in the data plane was not discussed. Moreover, the deployment of the Intrusion Detection System (IDS) framework in high-speed networks reveals challenges concerning network monitoring issues and network security problems. This research begins with a qualitative analysis of various DDoS attacks, intending to present the best single feature for rapid DDoS detection based on a mathematical derivation. Then the study continues with qualitative analysis of the proposed feature by evaluating a framework consisting of a data generation module, various feature selection methods, various machine learning methods for binary classification of normal traffic and attack traffic, and a multi-label classification Artificial Neural Network (ANN) model for identifying different attacks through various extracted features.**

***Keywords* – Denial of service (DoS), Neural Network, Attack, Information Technology, Attack.**

I. Introduction

In this digital world, people rely on the Internet for every activity due to technological improvement. However, the same technology is misused by attackers to get unauthorized access to the network and the devices connected to the Internet, to gain information or to crash the network.

As per purples 2019 statistics [1], the network attack growth rate has been increasing for the last ten years, as shown in the following bar chart Figure 1. This report recognizes the security threats that could have a major impact on mission-critical applications used for day-to-day business operations.

Network attacks are any type of action that targets the entire network, individual system information, or network devices. Using various techniques attackers corrupt, update or delete data or information. The two main classifications of network attacks are passive and active types.

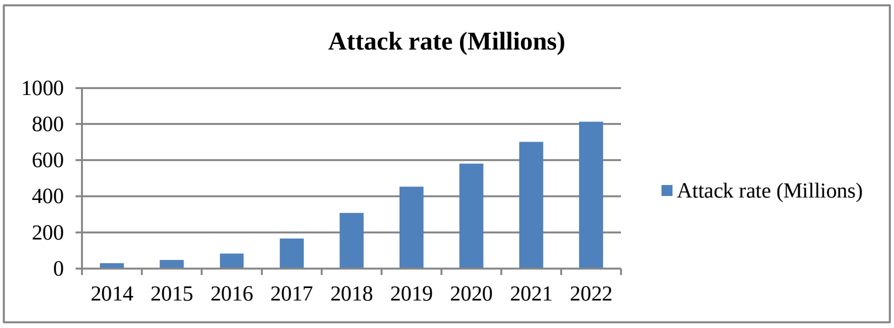

Fig. 1. Network Attack Growth.

Passive attackers can access the network to monitor or steal information without changing anything on the network. Active attackers not only gain access but also modify or delete the information on the network. Many common types of attacks are there in the computer Networks [2]. The following general risk factors can be used by the attackers to break through our network.

1. Unauthorized access: Accessing network information without proper permission is known as unauthorized access. This is due to a weak password, an already compromised account or a lack of security.
2. Denial of Service (DoS): DoS is meant to shutdown the server or the entire network, making service unavailable to its proposed users. Attackers send large volumes of packets to the target device to deactivate the server.
3. Man-in-the-middle: This type of attacker interrupts traffic, either within your system or from the outside. If the protocols are not protected in the network, the attacker can easily steal the network data, hijack the path or the session.
4. Code injection: Missed website communications are used by these attackers to make an API call and send harmful code instead of the expected information. If the receiver runs the code on the server, it is compromised by the attacker.
5. Privilege escalation: Once these types of attackers enter the network they expand their reach into the entire network: horizontally gaining access to adjacent devices and vertically to the higher level devices of the network.
6. Insider threat: It is originated within the targeted network. They have privileged authentication of the network, and they misuse the access. Security measures are not able to identify internal attackers.

Figure 2 shows the McAfee [3] report of the last five-year statistics and it reveals that out of the top five attacks DoS and Man-in-middle are the prominent attacks in the traditional networks.

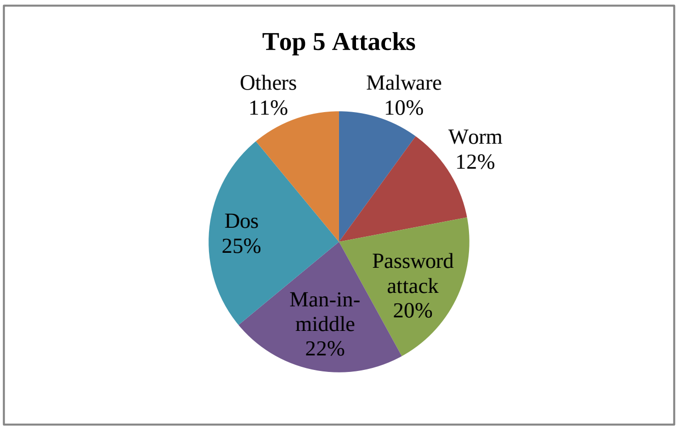

Fig. 2. McAfee statistics last five years average.

The following section will brief the different category of DoS and Man-in-middle attacks.

III. Literature Review

K. Muthamil Sudar et al. [1], SDN is an organization engineering that used to assemble, plan the equipment parts for all intents and purposes. We can powerfully change the settings of organization associations. In the conventional organization, it's impractical to change powerfully, on the grounds that it's a proper association. SDN is a decent methodology yet at the same time is helpless against DDoS assaults. The DDoS assault is threatening to the web. To forestall the DDoS assault, the AI calculation can be utilized. The DDoS assault is the various worked together frameworks that are utilized to focus on the specific server simultaneously. In SDN control layer is in the middle that connection with the application and foundation layer, where the gadgets in the framework layer constrained by the product. In this paper, we propose an AI procedure specifically Decision Tree and Support Vector Machine (SVM) to recognize noxious traffic. Our test result shows that the Decision Tree and Support Vector Machine (SVM) calculation gives better exactness and identification rate.

Muthamil Sudar et al. [2], SDN has as of late arisen as an organization worldview because of its high organization programmability and adaptability which can conquer the issue in customary organizations by decoupling the control plane from the information plane. The information plane will advance the parcels according to the choice made by the regulator in the control plane. This brought together control will assist with giving the theoretical perspective on the whole organization framework. Since the regulator is a center piece of SDN, it is more inclined for assaults and turns as a significant danger to the whole organization. Conveyed Denial of Service (DDoS) assault can then over-burden the SDN regulator and switch stream table which prompts an exhibition corrupt of the organization. To resolve this issue, we have sent two level security instruments. In level one, an entropy-based instrument is proposed to recognize the DDoS flooding assault in the beginning phase by briefly holding the specific stream. In level two, an AI based C4.5 procedure is proposed to distinguish the assault by breaking down extra elements and send a long-lasting caution to drop the bundles. The outcomes are examined with K-overlap approval strategy as far as responsiveness, particularity and precision.

Dong et al. [3], the Distributed Denial of Service (DDoS) assault has truly impeded organization accessibility for quite a long time and still there is no compelling safeguard system against it. Be that as it may, the arising Software Defined Networking (SDN) gives a better approach to revaluate the safeguard against DDoS assaults. In this paper, we propose two strategies to distinguish the DDoS assault in SDN. One strategy embraces the level of DDoS assault to distinguish the DDoS assault. The other technique utilizes the superior K-Nearest Neighbors (KNN) calculation in view of Machine Learning (ML) to find the DDoS assault. The aftereffects of the hypothetical investigation and the exploratory outcomes on datasets show that our proposed strategies can more readily distinguish the DDoS assault contrasted and different techniques.

Dong et al. [4], distributed computing have been generally taken on by scientists and industry. Notwithstandi--ng, inescapable acknowledgment of these novel systems administration standards has been hampered by the security dangers. Propels in the handling advances have helped aggressors in expanding the assaults as well, for example, the improvement of Denial of Service (DoS) assaults to appropriated DoS (DDoS) assaults which are rarely recognized by customary firewalls. In this paper, we present the condition of craft of the DDoS assaults in SDN and distributed computing situations. Particularly, we center around the investigation of SDN and distributed computing engineering. Plus, we likewise outline the examination works and open issues in distinguishing and handling the DDoS assaults.

Gu. Y. et al. [5], DDoS assault is an endeavor to make an internet based assistance inaccessible by overpowe--ring it with traffic from various sources. In this manner, it is important to propose a viable strategy to identify DDoS assault from enormous information deals. In any case, the current plans have a few limits, including that administered learning techniques, need huge quantities of named information and solo learning calculations have somewhat low recognition rate and high bogus positive rate. To handle these issues, this paper presents a semi-directed weighted k-implies location strategy. In particular, we first and foremost present a Hadoop-based cross breed highlight choice calculation to observe the best capabilities and propose a superior thickness based beginning group communities choice calculation to take care of the issue of exceptions and neighborhood ideal. Then, at that point, we give the Semi-directed K-implies calculation utilizing cross breed include choice (SKM-HFS) to distinguish assaults. At long last, we exploit DARPA DDoS dataset, CAIDA "DDoS assault 2007" dataset, CICIDS "DDoS assault 2017" dataset and genuine world dataset to do the check explore. The analysis results have shown that the proposed strategy outflanks the benchmark in the admiration of discovery execution and procedure for request inclination by likeness to an optimal arrangement (TOPSIS) assessment factor.

A. Raghavan et al. [6], viable and productive malware location is at the cutting edge of investigation into building secure advanced frameworks. Similarly as with numerous different fields, malware identification research has seen an emotional expansion in the utilization of AI calculations. One AI procedure that has been utilized broadly in the field of example matching overall and malware identification specifically is covered up Markov models (HMMs). Well preparation depends on a slope climb, and henceforth we can frequently work on a model via preparing on numerous occasions with various beginning qualities. In this exploration, we look at supported HMMs (utilizing AdaBoost) to HMMs prepared with numerous arbitrary restarts, with regards to malware discovery. These procedures are applied to an assortment of testing malware datasets. We observe that arbitrary restarts perform shockingly well in contrast with supporting. Just in the most troublesome "cold beginning" situations (where preparing information is seriously restricted) does supporting seem to offer adequate improvement to legitimize its higher computational expense in the scoring stage.

T. Young et al. [7], Profound learning techniques utilize numerous handling layers to learn various leveled portrayals of information and have created best in class brings about numerous areas. As of late, an assortment of model plans and techniques have bloomed with regards to regular language handling (NLP). In this paper, we audit critical profound learning related models and strategies that have been utilized for quite some time undertakings and give a stroll through of their development. We additionally sum up, investigate the different models and set forward an itemized comprehension of the past, present and eventual fate of profound learning in NLP.

X. Lei et al. [8], partition the patients' result expectation into two stages. The initial step is to separate the vital elements from the patients' numerous actual assessment markers. The subsequent advance is to utilize the critical elements separated from the initial step to anticipate the patients' results. To this end, we propose a model joining recursive component disposal with a cross-approval strategy and order calculation. In the initial step, we utilize the recursive element end calculation to rank the significance of all elements, and afterward remove the ideal elements subset utilizing cross-approval.

In the subsequent advance, we utilize four characterization calculations (support vector machine (SVM), C4.5 choice tree, arbitrary timberland (RF), and outrageous inclination helping (XGBoost)) to precisely anticipate patient results by utilizing their ideal elements subset. The chose model expectation execution assessment measurements are exactness, F1 measure, and region under recipient working trademark bend. The 10-overlay cross-approval shows that C4.5, RF, and XGBoost can accomplish awesome forecast outcomes with few highlights, and the classifier after recursive element disposal with cross-approval include determination has better forecast execution. Among the four classifiers, XGBoost has the best expectation execution, and its exactness, F1, and region under recipient working trademark bend (AUC) values are 94.36%, 0.875, and 0.927, separately, utilizing the ideal elements subset.

III. Denial of Service

Denials of service attacks are significant in networks than other areas that target the availability goal of security. The threats introduced by such attacks on continued service may be either accidental or malicious [9, 10].

Attack types: There are different types of Denial-of-Service attacks that occur in different forms such as transmission failures, flooding of numerous connection, echo-chargen, ping of death, smurf, syn flood, tear drop, redirection of traffic, DNS attacks etc. Transmissions fail for many reasons. One common reason could be, the line is cut or a noise can make a packet unrecognizable or deliverable. A communicating machine along the transmission path could fail due to hardware or software reasons or have gone for repair or testing. A machine could be overloaded or saturated and due to that it cannot accept packets, until it clears its packets. These problems could be temporary or automatically fixed. Some communication failures such as break in single communication line to a computer cannot be easily repaired, and can be fixed only by forming an alternative link or repairing the damaged one. This can be viewed from malicious stand point that anyone can sever, interrupt of overload capacity to deny service [9, 10].

Failures also could occur due to the non-functioning of routers, circuit boards, firewalls, monitoring devices, storage devices and switches, for which age, factory flaws, power surges, heat and tampering can be the reasons. Such component failures may cause the entire network to fail. Even-though such failures are almost natural occurrences, one should also think about the possibilities of them being induced. Flooding is the most common type of attack reported to CERT/CC. It involves sending of an excessive amount of packets to the destination causing an excessive amount of end point, too much of bandwidth consumption, and hogging of a link. Both single source against single destination and multiple sources against multiple destinations are common [11].

There are different packet types that are used for attacks by attack tools. There are different types of flooding attacks that are carried out practically. The most common ones are TCP flooding, where a stream of TCP packets with various flags set are sent to the victim IP address. Syn, ACK and RST are the most common types of flags that are used for this kind of attack. UDP flooding is another kind of flooding attack where stream of UDP packets are sent to the victim IP address [12].

IV. Distributed Denial of Service (DDOS)

DDoS attacks are two stage attacks constructed by the attackers for multiplying the effect. The first stage concentrates on planting an unnoticeable Trojan horse that may be named for a popular editor or utility on a target machine. The same may be subsequently repeated on many targets, thus making the targets systems as zombies [13]. Then a signal is sent to all zombies to launch the attack, and the victim is led to defend ‘n’ attacks from ‘n’ number of zombies, each targeting with different kind of attacks such as syn, smurf, all acting at once. DDoS attacks are considered serious due to their nature of being launched through scripts, where one can easily write procedures for planting Trojan horse to launch one or all the attacks [14, 15]. At the outset, these attacks can be divided into two broad categories as agent handler model and Internet Relay Chat model (IRC). The agent handler model gets further divided into client-handler communication and agent-handler communication, and the IRC model gets divided to secret/private channel and public channel.

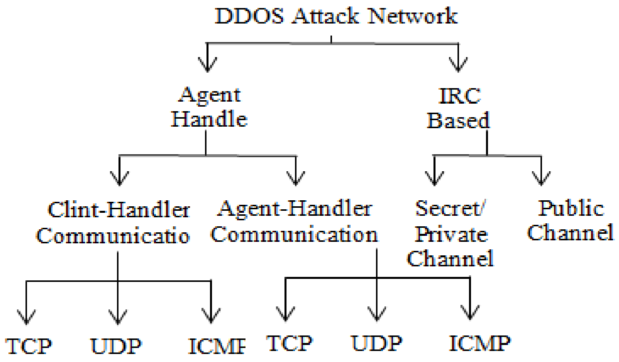

Fig. 3. DDoS Attack Network.

V. Artificial Neural Network

In Artificial Intelligence, a machine learning subset is called deep learning, which has the potential of learning unstructured or unsupervised data. Input layer, output layer and hidden layers are the essential components of the DNN framework. The proposed DNN framework is specified in Figure 4.

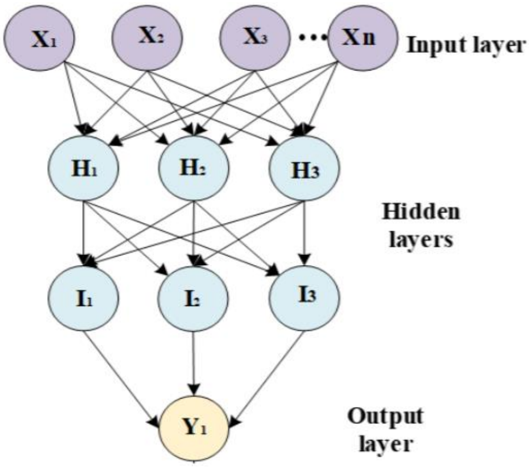

Fig. 4. Artificial Intelligence Architecture.

DNN indicates the type of ML (Machine Learning) while the system utilizes many layers of nodes to derive high-level functions from input information. It means transforming the data into a more creative and abstract component. Nodes are little parts of the system, and they are like neurons of the human brain. When a stimulus hits them, a process takes place in these nodes. Some of them are connected and marked, and some are not, but in general, nodes are grouped into layers [16]. The system must process layers of data between the input and output to solve a task. Creative and analytical components of information are analyzed and grouped to ensure that the object is identified correctly. The creation of neural network is inspired by the working of human brain and its functions. Artificial intelligence and machine learning, which is a subset of AI, play an essential part in its functionality. It starts working when a developer enters data and builds a machine learning algorithm, mostly using the “if ... else ...” principle of building a program. The deep neural network does not only work according to the algorithm but also can predict a solution for a task and make conclusions using its previous experience.

VI. Conclusion

SDN offers a centralized controller and dynamic programming environment to improve network performance than the existing traditional networks. However, the control plane and the data plane are vulnerable to the most common IP Spoofing and DDoS flooding attacks. The existing research proposals are implemented with statistical-based methods, knowledge based, learning-based models, and entropy-based approaches to detect and mitigate IP spoofing and DDoS flooding attacks in SDN. The main goal of this research will has to present a method to improve the accuracy in detection of DDoS attacks in software defined networks controller. Also, the delay in detecting the attacks must be small so that there is enough time to mitigate the attack before the controller is made unreachable or slowed down.

References

[1] K. Muthamil Sudar, M. Beulah and P. Deepalakshmi, “Detection of distributed denial of service attacks in SDN using machine learning techniques”, International Conference on Computer Communication and Informatics (ICCCI), Jan. 27-29, 2021, Coimbatore, India.

[2] Muthamil Sudar, K., & Deepalakshmi, P. (2020). A two level security mechanism to detect a DDoS flooding attack in software-defined networks using entropy-based and C4. 5 technique. Journal of High Speed Networks, (Preprint), 1- 22.

[3] Dong, S., & Sarem, M. (2019). DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks. IEEE Access, 8, 5039-5048.

[4] Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access, 7, 80813- 80828.

[5] Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semisupervised K-means DDoS detection method using hybrid feature selection algorithm. IEEE Access, 7, 64351- 64365.

[6] A. Raghavan, F.D. Troia, and M. Stamp, "Hidden Markov models with random restarts versus boosting for malware detection," *J. Comput. Virol. Hacking Techn.*, vol. 15, no. 2, pp. 97107, Jun. 2019.

[7] T. Young, D. Hazarika, S. Poria, and E. Cambria, "Recent trends in deep learning based natural language processing [review article]," *IEEE Comput. Intell. Mag.*, vol. 13, no. 3, pp. 5575, Aug. 2018.

[8] X. Lei and Y. Xie, "Improved XGBoost model based on genetic algorithm for hypertension recipe recognition," *Comput. Sci*, vol. 45, pp. 476481, 2018.

[9] Y. Guo, Y. Liu, A. Oerlemans, S. Lao, S. Wu, and M. S. Lew, "Deep learning for visual understanding: A review," Neurocomputing, vol. 187, pp. 2748, Apr. 2016.

[10] Abduvaliyev, A., Pathan, A.S.K., Zhou, J., Roman, R., and Wong, W.C. “On the vital areas of intrusion detection systems in Wireless Sensor Networks”, IEEE Communications Surveys & Tutorials, Vol. 15, Issue 3, pp. no. 1223-1237, 2015.

[11] Abubakar, A.I., Chiroma, H., Muaz, S.A., and Ila, L.B. “A review of the advances in cyber security benchmark datasets for evaluating data-driven based Intrusion detection systems”, Procedia Computer Science, Vol. 62, pp. no. 221–227, 2015.

[12] Bay, S.D., Kibler, D., Pazzani, M.J., and Smyth, P. (2015), “The UCI KDD archive of large data sets for data mining research and experimentation”, ACM SIGKDD Explorations Newsletter, Vol. 2, Issue 2, pp. no. 81–85, 2015.

[13] Aburomman, A.A. and Reaz, M.B.I. “A novel SVM-kNN-PSO ensemble method for Intrusion Detection System. Applied Soft Computing”, Vol. 38, pp. no. 360–372, 2015.

[14] Pedro Casas, JohanMazel and Philippe Owezarski “Unsupervised network intrusion detection systems: detecting the unknown without knowledge”, Elsevier Computer Communications, Vol. 35, Issue 7, pp. no. 772 – 783, 2012.

[15] Carlos A. Catania, Facundo Bromberg and Carlos García Garino “An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection”, Elsevier Expert Systems with Applications, Vol. 39, Issue 2, pp. no. 1822–1829, 2012.

[16] Xie, B. & Zhang, Q., “Application-layer anomaly detection based on application-layer protocols' keywords”, Computer Science and Network Technology (ICCSNT), 2nd International Conference on, pp. 2131-2135, 2012.

Author’s Profile

First Author
Prateeksha Sahu, Department of Computer Science and Engineering, Technocrats Institute of Technology and Science, Bhopal, Madhya Pradesh, India.

Second Author
Onkar Nath Thakur, Department of Computer Science and Engineering, Technocrats Institute of Technology and Science, Bhopal, Madhya Pradesh, India.

Third Author
Rakesh Kumar Tiwari, Department of Computer Science and Engineering, Technocrats Institute of Technology and Science, Bhopal, Madhya Pradesh, India.