IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Detection of Multi-Vector DDoS Attack

Kunal Kumar Brahma[1*], Satyajit Sarmah[2], Chandan Kalita[3], Rajdeep Ghosh[4]

[1,2,3,4] Department of Information Technology, Gauhati University, Guwahati, India

Corresponding Author: kunalbrahma1@gmail.com, Tel.: 8486243433

DOI: https://doi.org/10.26438/ijcse/v7i6.847851 | Available online at: www.ijcseonline.org

Accepted: 09/Jun/2019, Published: 30/Jun/2019

***Abstract*— In this current technology driven society, internet has become a basic commodity for every individuals as well as organization. Due to the rapid increase of internet dependency of government offices, private company, or corporate sectors, security has become the main concern in all of these organizations. Attack over the network using stochastic approaches has created large chaos. The DDoS attack has created destruction and damages over the network since early 2000's. DDoS is known for its ability to fade the identity of the source of attack because of multiple address and flooding mechanism. Preventing the attack from its original source is quite difficult. This floods the whole system making the system of the particular sector to be crippled and can be remedied by early detection of the attack. In this work we try to detect the different DDoS attack vectors and classify it. The nature and its mechanism are studied to identify the type of attack. We use scikit learn, a machine learning approach to detect different forms of attacks.

Keywords*—*DDoS, vectors, Machine Learning, Confusion Matrix

I. Introduction

Nowadays, with the emerging cyber-attacks, detecting the origin of the source has become quite difficult. The attacks has grown and developed since the usage of widespread applications running online, which makes network security more important. Nowadays, due to more and more public availability, the internet has become as the main target of malicious attacks. Both the systems connected to the Internet and network devices comprising the Internet, can all be severely compromised by intrusions. Recently, internet flooding attacks like DoS, DDoS have posed catastrophic threats to network services.

A. DDOS Attack

A DDoS is a distributed network based attack to a system which is considered to be a high threat to the database servers and other network providing services of the victim. In this type of attack, an attacker can create multiple bots or zombies which operate from various uncharted systems that are unaware of the residing bot program. It can include various varieties of systems that can serve as slave in executing the DDoS. It has an attacker PC which controls a group of master systems that distributes the bot program to the slave systems for the purpose of DDoS attack towards the victim PC.

The significant increase of our dependency on Internet-based services in everyday life has intensified the survivability of networks. The resources like files or any application subjects that are mainly stored in computer systems require confidentiality, integrity, and availability. Because of extensive public availability, the Internet has become the main target of malicious attacks. The systems connected to the Internet and the network devices comprising the Internet, can all be severely affected by intrusions. The intrusion is defined as violation of security policy of system. During this process of intrusion, the victim's resources gets exposed or corrupted to paralyze the victims system. This is mainly done by attacker having personal grudge over any individual or company and the revenge being taken for the following reason.

To cope up with the situations of the multiple forms of DDoS attacks we have used a machine learning approach in this paper. The vectors for detection that was used was briefly studied based on its anomaly and behavior [1]. The attack having the highest percentage of accuracy was considered as the confirmed attack from host, which was done using Confusion Matrix.

II. Related Work

In this paper we have referred approaches of many research works that is related or similar to our work.

Amarpreet and Priya in their work describe how they managed to detect the DOS attack in VANET (Vehicular

AdHoc Network). To protect the VANET, they have used Enhanced Attack Packet Detection Algorithm (EAPDA). They have simulated the attack in NS2 and found the results in graph plot, where they found the number of false positive to be low. Their mechanism, didn't incorrectly detect any node as a malicious node as was done by existing schemes. This proved that EAPDA is more responsive and the verification was done with lesser delay which has also increased throughput. Then, they compared their results with the previous works on this [2].

Erwin Adi proposed the detection of HTTP DOS attack. For the attack traffic analysis conducted in this study he employed 4 machine learning techniques; Naïve Bayes, Decision Tree, JRip and Support Vector Machines. His study also evaluated and examined the instances of the traffic. The post result can be seen as, the host machine did not show any sign of resource depletion during the attack traffic generation, indicating that the observed resource parameters at the victim machine were not affected by the underlying host environment [3].

The DoS Prevention using automated mechanism with unsupervised learning by Eric Perraud, shows how he used machine learning approach to prevent DoS attack on automotive wireless connectivity unit in vehicles. His process of identifying the attacks is by using K-means clustering algorithm [4].

A brief description of detecting DDoS attack using k-Nearest Neighbor can be seen in a research work of Thwe and Thandar. This paper gives overview of how DDoS attack is detected and classified. This includes the study of nature of the attacks they found and then identifying the type of attack [4].

In 2017, Aqeel Sahi et. al., illustrates briefly about the detection and prevention of DDoS TCP Flood attack in a Cloud Environment. He used a new approach to walk through his work called as CS_DDoS, for the detection and prevention of DDoS TCP Flood attacks [5].

Harshita and Ruchikaa give a brief insight of detection of ICMP Flood in their work. They have used different methods and tools to check which different parameters ICMP DDoS Flood depends on [6].

Munazza Shabbir, et al., in their 2016 paper explains how they were able to detect the DDoS attack in Vehicular Ad-Hoc Network (VANET).They initiated the attacks with checking the number of packets being injected to each networks. After that, they analyzed the approximate number of packets in network during simulation time [7].

The DDoS detection for Ensemble-based multi-filter feature selection in cloud computing was achieved by performing an extensive experimental evaluation of their proposed method using intrusion detection benchmark dataset, NSL-KDD and decision tree classifier. This was done by Opeyemi Osanaiye et. al., in 2016. Their findings reported an effective reduce in the features of benchmark dataset from 41 to 13. It also suggests high classification accuracy with high reduction rate in comparison to other techniques performing classification [8].

III. METHODOLOGY

The basic method in our project relies on the process of attacking the server system (victim PC) in simulation mode by multiple attackers (zombies) in a DDoS attacking mechanism.

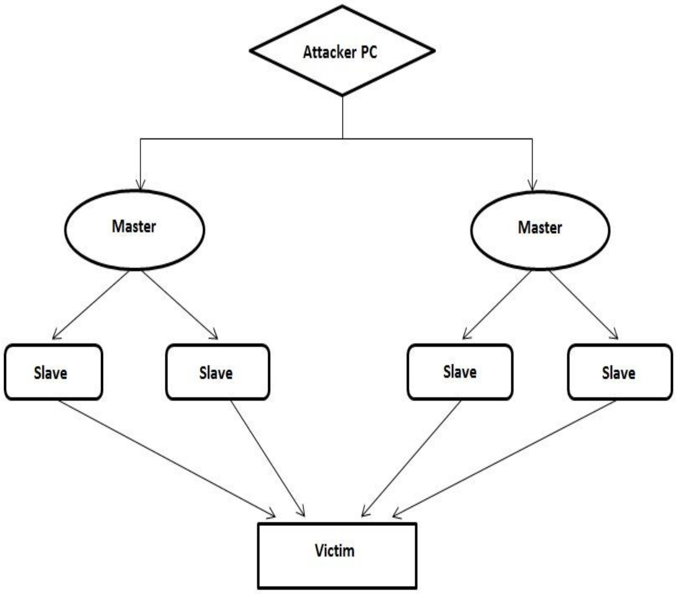


Fig.1: *Attack Mechanism*

As seen from above figure 1, the basic mechanism of the attack is initially from the attacker or the host. It then transmits the attacking vectors from the Masters to the multiple Slaves or Zombie PC's which are dormant and ready for attack. The slaves then attack in multiple quantity to the target or victim PC. This then results in large amount of DDoS flooding or achieving large amount of data's, resulting in the collapse of the victim PC.

Ultimately, the main goal of our work is to detect the DDoS attack and then identifying the type of attack that is being done in the victim PC. The attacking type is basically identified with the help of the Machine learning approach. We have basically used sklearn for the Machine Learning approach by using the Autoencoder Neural Network algorithm.

The 4 types of attacking vectors are selected for this project basically which includes SYN flooding, Ping flooding, http flooding and smurf attack. In the first phase we classify attacks with the help of scikit learn into two types namely; normal traffic and abnormal or attack traffic, where the percentage of accuracy has been found to be 93.5%. This was done with the help of Autoencoder Neural Network approach.

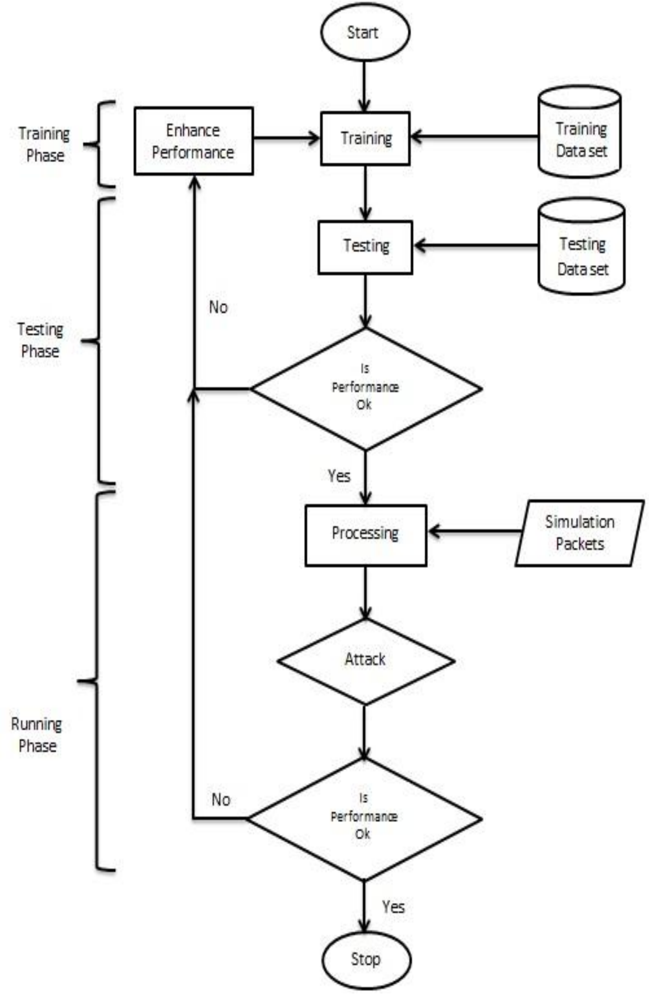


Fig.2: *Flow Chart for system*

As shown in the figure 2, during the training phase, the data generated for the attack is trained. After the training phase, the data is then tested for its performance whether it's ok to be used further. During the running phase, the data is used for processing if the performance comes out to be ok. If it's not then, the data is enhanced or modified. The packets generated during the simulation from attacks are also used for processing. The processed data's are then used for attack to get an enhanced and better performance. If the performance comes to be sound then it is further processed and if it's not then, the data is trained to enhance its performance.

IV. EXPERIMENT

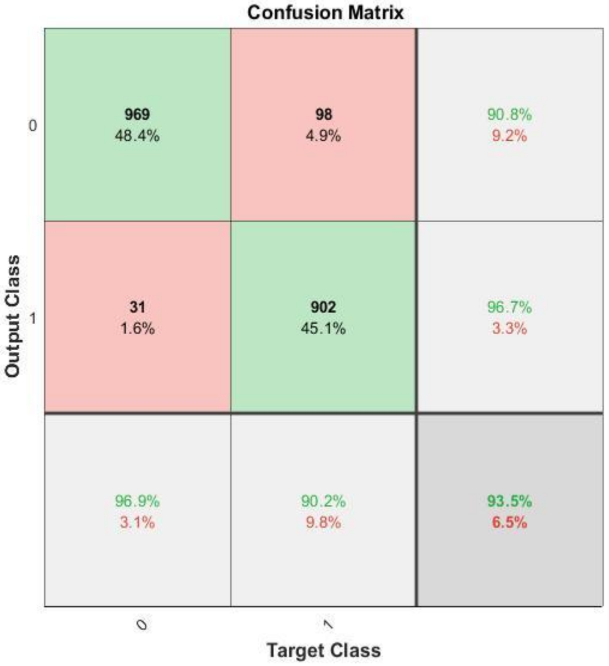
The process for calculating the accuracy was basically done with the help of confusion matrix. Confusion Matrix is done with the help of the four basic parameters True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). With these four parameters we have calculated the Precision, Sensitivity, Specificity and F-score. And finally we have calculated the Accuracy. The formulas of this Precision, Sensitivity, Specificity and F-score are;

$$\text{Precision} = \frac{TP}{TP + FP} = 90.2\%$$

$$\text{Sensitivity} = \frac{TP}{TP + FN} = 96.7\%$$

$$\text{Specificity} = \frac{TN}{FP + TN} = 90.81\%$$

$$\text{F-score} = \frac{2*TP}{2*TP + FP + FN} = 96.9\%$$



	0	1	
0	969 48.4%	98 4.9%	90.8% 9.2%
1	31 1.6%	902 45.1%	96.7% 3.3%
	96.9% 3.1%	90.2% 9.8%	93.5% 6.5%

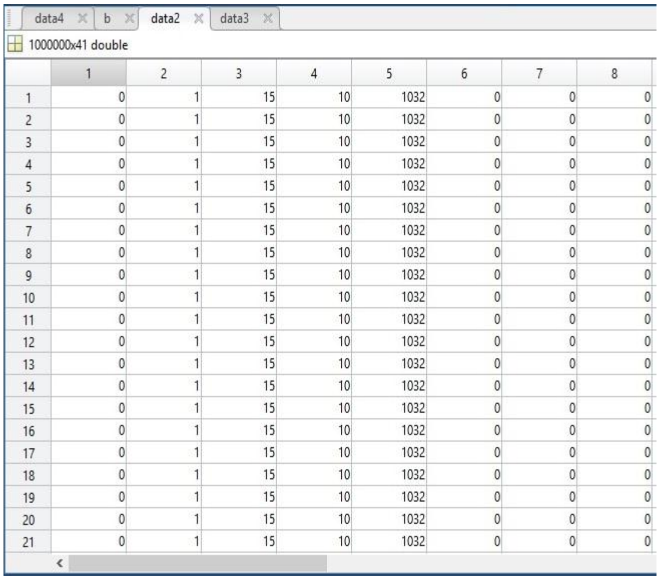
Fig.3. *Confusion Matrix in First Phase*

After the classification of data's in 2 classes the accuracy of data was calculated for the confusion matrix using the formula;

$$\text{Accuracy} = \frac{\text{TP + TN}}{\text{TP + TN + FP + FN}} = 93.5\%$$

Using the formula for accuracy, the total accuracy of the attack type generated from 10,00,000 datasets is found out to be 93.5%. Hence, the accuracy of data generated was found appropriate for the type of DDoS attack.

Tools/Environment/Experimental Platform: MATLAB is a platform independent programming language. It allows different types of features which includes algorithms, implementations, graph plots, matrix generations, data etc. During the whole project for data classification, training, and testing windows 8.1 Operating System is used and the attacks are performed in Kali Rolling Linux and Ubuntu 16.04 LTS Linux environment. Figure 4 is a snapshot of the 10,00,000 data generation of a dataset in MATLAB.



1000000x41 double

	1	2	3	4	5	6	7	8
1	0	1	15	10	1032	0	0	0
2	0	1	15	10	1032	0	0	0
3	0	1	15	10	1032	0	0	0
4	0	1	15	10	1032	0	0	0
5	0	1	15	10	1032	0	0	0
6	0	1	15	10	1032	0	0	0
7	0	1	15	10	1032	0	0	0
8	0	1	15	10	1032	0	0	0
9	0	1	15	10	1032	0	0	0
10	0	1	15	10	1032	0	0	0
11	0	1	15	10	1032	0	0	0
12	0	1	15	10	1032	0	0	0
13	0	1	15	10	1032	0	0	0
14	0	1	15	10	1032	0	0	0
15	0	1	15	10	1032	0	0	0
16	0	1	15	10	1032	0	0	0
17	0	1	15	10	1032	0	0	0
18	0	1	15	10	1032	0	0	0
19	0	1	15	10	1032	0	0	0
20	0	1	15	10	1032	0	0	0
21	0	1	15	10	1032	0	0	0

Fig.4. *Data generation*

V. RESULTS AND DISCUSSION

We have trained a computer system to know the anomalies in a network for the DDoS attack. To do so we have trained 4 different 10,00,000 data values from the KDD dataset. Then,we have tested the system in preliminary phase. In preliminary phase the data having highest value tested will be considered the type of attack. After that, using the confusion matrix we have found out the accuracy to be 93.5%.

VI. CONCLUSION AND FUTURE SCOPE

In this work, we have classified the normal and abnormal traffic from the dataset, and also tried to detect different types of attack by studying its nature and behaviour. For detection of various attacks, we used machine learning approaches and we have computed the accuracy. In future we will train and test more numbers of attack to detect large vectors of DDoS attack and know about it as fast as we can from the system and be more precise and accurately.

REFERENCES

[1] Krishna Modi, Prof. Abdul Quadir Md., "*Detection and Prevention of DDoS Cloud using Double-TCP Mechanism and HMM-Architecture*", Vol.**3**,No.**2**,pp.**113–120**, April **2014**,

[2] Amarpreet Singh, Priya Sharma, "*A novel mechanism for detecting DOS attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA)*", IEEE Transaction, Proceedings of 2015 RAECS UIET Panjab University Chandigarh 21-22nd December **2015**.

[3] Erwin Adi, "*Distributed denial-of-service attacks against HTTP/2 services*", pp.**79–86, 2016**.

[4] Eric Perraud "*Machine Learning Algorithm of Detection of DOS Attack on an Automotive Telmatic Unit*" International Journal of Computer Networks & Communications (IJCNC) Vol.**11**, No.**1, 27-43**, January **2019**

[5] Thwe Thwe Oo, Thandar Phyu, "Statistical Anomaly Detection of DDoS Attacks Using K-Nearest Neighbour", International Journal of Computer & Communication Engineering Research (IJCCER) Volume.**2**, Issue.**1** January **2014**.

[6] Aqueel Sahi, D.Lai, Yan Li, Mohammed Diykh, "*An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment*", IEEE Access, pp.**1-13**, Vol.**5**, April**2017**.

[7] Harshita, Ruchikaa Nayyar, "*Detection of ICMP Flood DDOS Attack*", International Journal of Computer Science Trends and Technology (IJCST), Vol.**5,** Issue.**2**, pp.**199-205**,March-April**2017**.

[8] Munazza Shabbir, Muazzam A. Khan,Umair Shafiq Khan, Nazar A. Saqib "*Detection and Prevention of Denial of Service Attacks in VANET*", International Conference on Computational Science and Computational Intelligence, pp.**970-974**, **2016.**

[9] Opeyemi Osanaiye, Haibin Cai, Kim-Kwang Raymond Choo, Ali Dehghantanha, Zheng Xu and Mqhele Dlodlo, "Ensemble-based multi-filter feature selection method for DDOS Detection in Cloud Computing", EURASIP Journal on Wireless Communication and Networking, pp.**1-10**, **2016**.

Authors Profile

Kunal Kumar Brahma is an M.Tech student in Department of Information Technology, Gauhati University. He has done his B.Tech in Computer Science and Engineering from Royal School of Engineering and Technology, Royal Global University. His areas of interest is Computer Networks and Intrusion Detection.

Satyajit Sarmah is an Assistant Professor in the department of Information Technology, Gauhati University. He has done his PhD in wireless Networking from the department of Information Technology, Gauhati University. Satyajit Sarmah completed his MTech in Information Technology from Tezpur University, Assam. His reaserch areas are Computer Networks, Network security etc..

Chandan Kalita currently works as an Assistant Professor in the department of Information Technology, Gauhati University. His research work is in file system, non-volatile memory. His recent research interest are distributed file system, NOSQL, Big Data, key value storage etc.

Rajdeep Ghosh is an Assistant Professor in the department of Information Technology, Gauhati University. He did his B.Tech and M.Tech in IT from Assam University, Silchar. His area of research includes Machine Learning, Signal Processing, Brain Computer Interface, Quantum Computing and Soft Computing.