IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DETECTION OF DDoS ATTACK USING HYBRID MACHINE LEARNING ALGORITHMS

[1]Keerthi M, [2] Manipi Manoj, [3]Kiran Kumar M, [4]Dakaraju ViswaTeja, [5]Sougandhika Narayan

[1,2,3,4]Undergraduates, Computer Science and Engineering, K S Institute of Technology,
Bengaluru, Karnataka, India-560109, Affiliated to VTU, Belagavi
[5]Assistant professor, Department of Computer Science and Engineering, K S Institute of Technology

Abstract*:* With great development in Science and Technology, the privacy and security of various organizations are condensed. Computer Intrusion and attack detection has always been a significant issue in networked environment. In most cases, there are two levels in which an intrusion may takes place i.e., in system level and the network level. Distributed Denial of Service is one of the network level attack. Distributed Denial of Service (DDoS) attack results in non-availability of services to the user. In case of organizations, this attack can result in a huge loss in terms of money or reputation since the clients of the organization cannot utilize the resources provided by that particular organization. The proposed solution to overcome this kind of attacks is, to monitor the network that is being attacked. The monitored network is analyzed and few parameters are considered from the analyzed network. These parameters are given as input data sets to machine learning algorithm for the classification of the data set. The algorithm classifies the data sets for the packets, causing the attack. These packets are then identified and terminated from the network that is being monitored.

Index Terms – **Minimet, Scapy, SVM, Wireshark.**

I. INTRODUCTION

The major threat in networking environment's is DDoS (Distributed Denial of Service) attack. The main aim of DDoS attacks is to prevent the legitimate user to access the service for a long time. In this attack, attacker tries to compromise the multiple numbers of hosts to send a huge amount of traffic intentionally towards a legitimate user. This leads to unavailability of service for large amount of time. A host which is under the attacker control is called bot. A group of controlled computers is known as botnet. In this, we have designed a DDoS detection mechanism based on machine learning techniques. In order to handle this DDoS attack, we have proposed a machine learning based model with Support Vector Machine (SVM). SVM is a kind of supervised learning technique. A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic. A botnet is a network of zombie computers programmed to receive commands without the owners' knowledge. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This, after all, will end up completely crashing a website for periods of time.

II. LITERATURE SURVEY

[1] Software-defined networking empowers network operators with more flexibility to program their networks. With SDN, network management moves from codifying functionality in terms of low-level device configurations to building software that facilitates network management.

[2] DDoS attacks have been the major threats for the Internet and can bring great loss to companies and governments. With the development of emerging technologies, such as cloud computing, Internet of things, artificial intelligence techniques, attackers can launch a huge volume of DDoS attacks with a lower cost, and it is much harder to detect and prevent DDoS attacks. In this paper to detect DDoS attacks, Naive Bayes and Random forest tree are used. In the paper, we survey on the latest progress on the DDoS attack detection using artificial intelligence techniques and give recommendations on artificial intelligence techniques to be used in DDoS attack detection and prevention.

[3] Intrusion Detection Systems (IDSs) are used to detect malicious actions on information systems such as computing and networking systems. Abnormal behaviours or activities on the network systems could be detected by security systems. But, conventional security systems such as anti-virus and firewall cannot be successful in many malicious actions. To overcome this problem, better and more intelligent IDS solutions are required. In this study, a hybrid approach was proposed to use to detect network attacks. Genetic Algorithm (GA) and K-Nearest Neighbor (KNN) methods were combined to model and detect the attacks. KNN was employed to classify the attacks and GA was used to select k neighbors of an attack sample. This hybrid system was first applied in intrusion detection field.

[4] A Distributed Denial of Service (DDoS) attack is a biggest threat to cyber security in SDN network. The attack will occur at the network layer or the application layer of the compromised systems that are connected to the network. In this paper we discuss the DDoS attacks from the traces of the traffic flow. We use different machine learning algorithms such as Naive Bayes, K-Nearest Neighbor, K-means and K-medoids to classify the traffic as normal and abnormal.

III. METHODLOGY

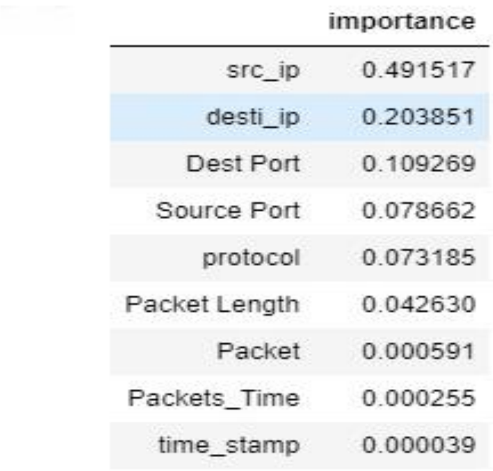
Initially, the system of the victim is being monitored for incoming and outgoing packets by a monitoring tool called Wireshark. Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

The monitored packets are being captured and are converted into a csv file in order to make it easier for the user to just enter the path of the file as an input to the machine learning algorithm that is SVM (Support Vector Machine). This input is given in terms of command line interface. Experimental results show that SVMs achieve significantly higher search accuracy than traditional query refinement schemes after just three to four rounds of relevance feedback.

The machine learning algorithm classifies the input data into 0 and 1. 0 if there is no attack and 1 if there is a attack happening.

Since the input data to the algorithm is the live data captured by the monitoring tool, there can be a lot of parameters to be considered while classifying them, which is time taking process and a bit tedious for the algorithm as well. So, the parameters are considered based on their importance during classification.

For example, from the below figures source_ip has more importance while causing the attack compared to other parameters.



	importance
src_ip	0.491517
desti_ip	0.203851
Dest Port	0.109269
Source Port	0.078662
protocol	0.073185
Packet Length	0.042630
Packet	0.000591
Packets_Time	0.000255
time_stamp	0.000039

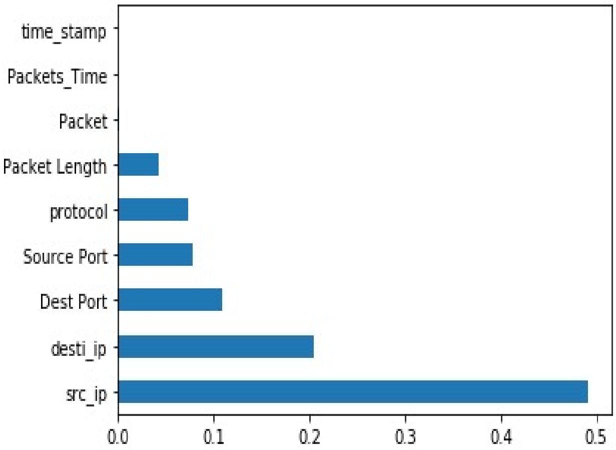
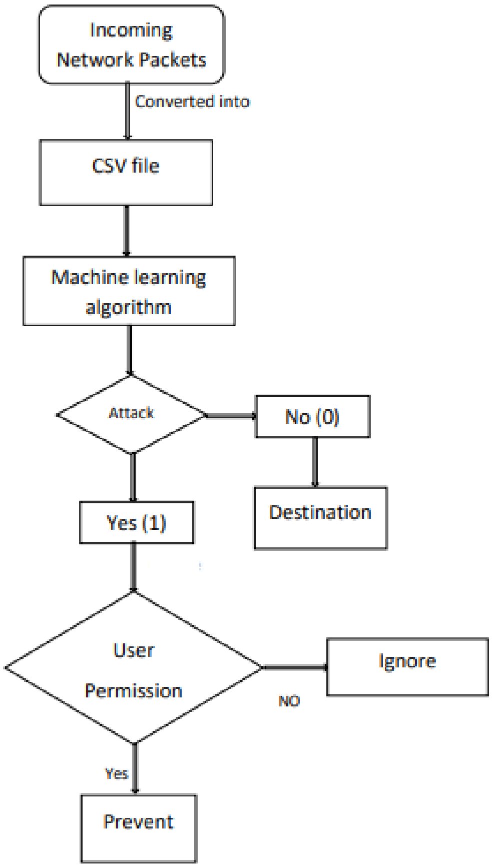


Figure 1: Importance of the parameters.

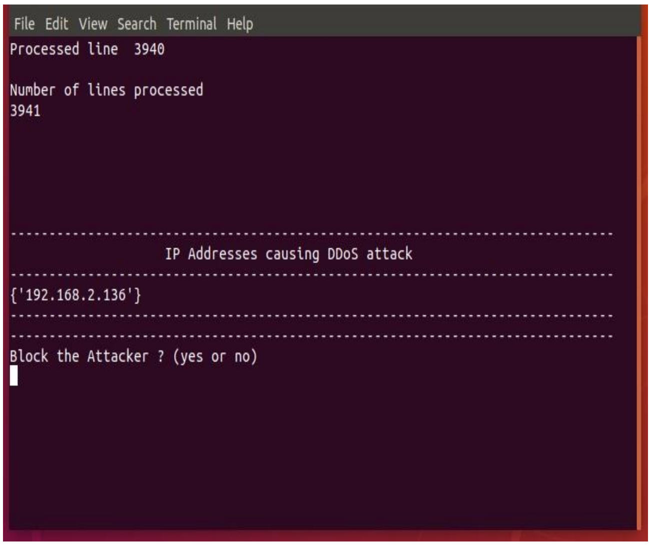
In case if there is no attack (0) happening, the packet is being transferred to the destination. In case of attack, the user is sent with an alert message to the mentioned E-mail id. The user is returned with the ip address of the attacker. And also the user is asked whether they want to block the detected ip address causing the attack. If yes, the address is blocked and the victim does not receive any kind of packets from the blocked address. Therefore, the victim's system is being prevented from the attacker.

FLOW DIAGRAM:



IV. RESULTS

At the end, the algorithm returns the ip address of the attacker and blocks the attacker on the insistence of the user.



```
Processed line  3940

Number of lines processed
3941




--------------------------------------------------------------------------------
                     IP Addresses causing DDoS attack
--------------------------------------------------------------------------------
{'192.168.2.136'}
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Block the Attacker ? (yes or no)
```

Figure 2. Returning the ip address of the attacker

V. CONCLUSION

The evolution of DDoS attacks shows no signs of slowing. They keep growing in volume and frequency, today most commonly involving a “blended” or “hybrid” approach. Without early threat detection and traffic profiling systems, it’s impossible to know they’re here. In fact, chances to know about it only when the website slows to a halt or crashes. This is especially true for sophisticated attacks, which use a blended approach and target multiple levels simultaneously. These attacks target data, applications, and infrastructure simultaneously to increase the chances of success. To prevent such attacks, we have proposed a solution where it uses a machine learning technique to detect the attack and prevent the attack by blocking the attacker’s address causing it.

VI. REFERENCES

[1] Kreutz, Diego, et al. "Software-defined networking: A comprehensive survey." Proceedings of the IEEE 103.1 (2015): 14-76.

[2] DDoS detection and prevention based on artificial intelligence techniques Boyang Zhang ; Tao Zhang ; Zhijian Yu 2017 3rd IEEE International Conference on Computer and Communications (ICCC)

[3] Yavuz CANBAY and Seref SAGIROGLU, “A Hybrid Method for Intrusion Detection” In IEEE 14th International Conference on Machine Learning and Applications”,2015.

[4] Barki, Lohit, et al. "Detection of distributed denial of service attacks in software defined networks." Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on. IEEE, 2016.

[5] Saurav Nanda, Faheem Zafari, CasimerDeCusatis, Eric Wedaa and Baijian Yang, “Predicting Network Attack Patterns in SDN using Machine Learning Approach”,In IEEE Conference on Network Virtualization and Software Defined Networks (NFVSDN),2016.

[6] https://www.kaggle.com/devendra416/ddos-datasets

[7] https://www.kaggle.com/nirajvermafcb/support-vector-machine-detail-analysis

[8] https://tools.kali.org/information-gathering/hping3