IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DETECTION OF DDOS ATTACKS USING HYBRID MACHINE LEARNING ALGORITHMS

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

[1,2,3,4]Student, [5]Assistant Professor,
[1,2,3,4,5]Department of Computer Science & Engineering,
[1,2,3,4,5]K S Institute of Technology, Bengaluru – 560109, Karnataka, India

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 algorithms 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, SOM, 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 hybrid machine learning techniques.

In order to handle this DDoS attack, we have proposed a combination of two machine learning based model with Support Vector Machine (SVM) and Self Organized Map (SOM). SVM is a kind of supervised learning technique whereas SOM is a kind of unsupervised 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 and 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 behaviors 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 Neighbour, K-means and K-medoids to classify the traffic as normal and abnormal.

III. Existing System

Existing models focus on DDoS attacks and victim attributes, but do not focus on botnet attributes, and botnet becomes the main technology of DDoS organization and management.

The key goal of distributed denial of service is to compile multiple systems and form botnets using infected zombies/agents over the Internet. The purpose is to attack a specific target or network with different types of packets. The infected system is controlled remotely by an attacker or a self-installed Trojan.

i) Saied proposed their model using artificial neural network algorithm to detect TCP, UDP and ICMP DDoS attacks, distinguished real traffic from DDoS attacks, and conducted in-depth training on the algorithm by using real cases generated by existing popular DDoS tools and DDoS attack modes.

ii) Saurav Nanda used Bayesian Network and achieved an accuracy of 91.68 % which indicates that out of 278,598 attacks, their model was able to accurately predict 254,834 attacks.

iii) Ahmad Y. Javaid used deep learning methods to detect the DDoS attack in SDN environment. They had collected the traffic from home wireless network (HWN) scenario. And they got 96.65% accuracy.

iv) S. Ramanauskait proposed a DDoS attack model. The modeling results of different botnet allocation strategies show that the success of DDoS depends on attack dynamics.

IV. Proposed System

In order to handle this DDoS attack, we have proposed a combination of two machine learning based model with Support Vector Machine (SVM) and Self Organized Map (SOM). SVM is a kind of supervised learning technique where as SOM is a kind of unsupervised learning technique. Initially, we are going to implement the SVM and SOM. And from the references and different sample datasets claims that SOM works well for the attack classification compared to the SVM. In order to improve the performance, we are jointly implementing both SVM and SOM, which shows the better detection rate, accuracy and false rate compared to separate implementation. In this section, we discussed about working of two algorithms and our proposed hybrid machine learning algorithm.

Initially the network is monitored and the statistical data is sent for classification, which in turn forms a dataset for the proposed system. The data set is initially passed into SVM where the data is classified on basis of the protocols as shown in Figure.1, from the output of SVM the attack probability is determined if there is a possibility of attack the packet data is set with termination policies and the packet is terminated from being attacked. If the output data doesn't have probability of attack but little bit suspicious is sent to SOM for further classification, which in turn classifies the data and termination policies are set for the data that leads for possibility of attacks.

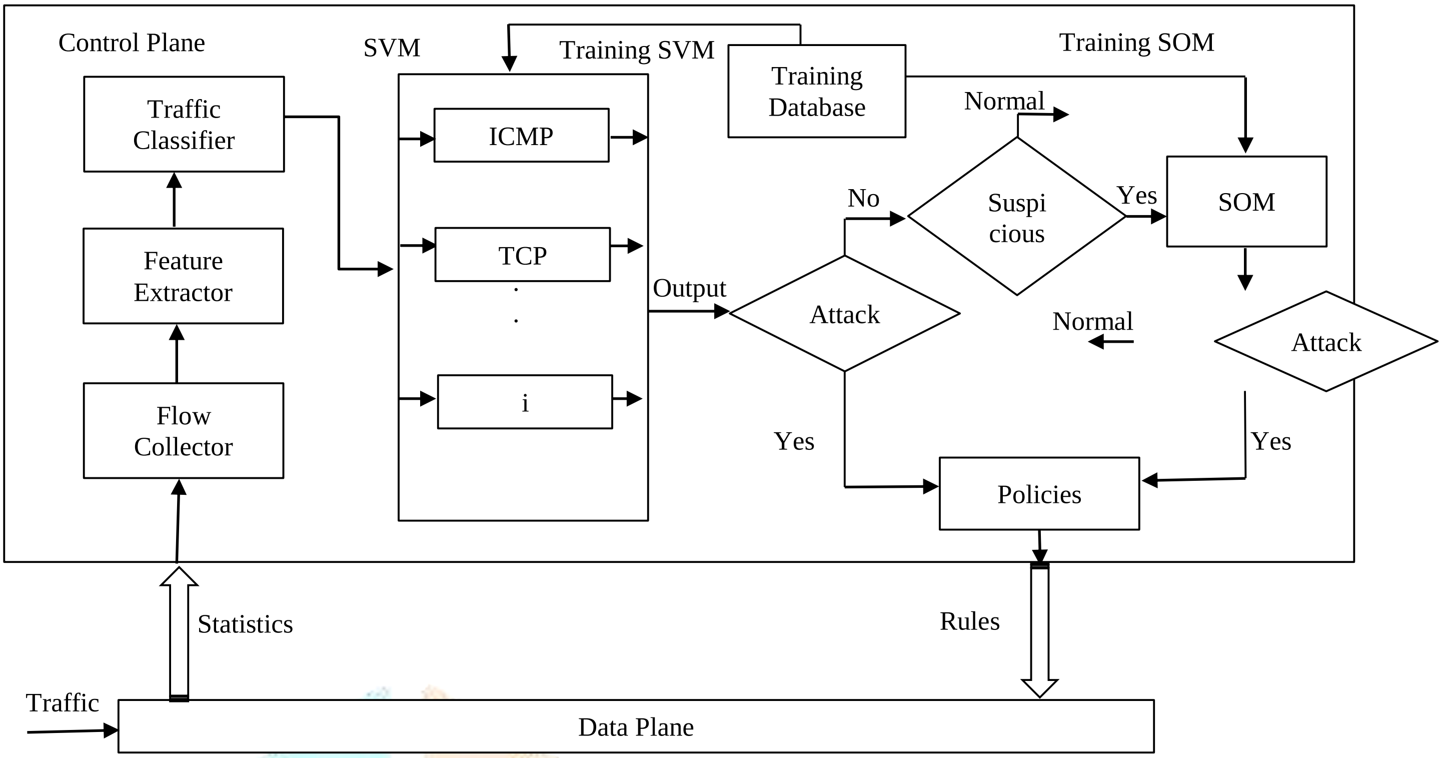

Fig.1 Proposed SVMs-SOM Mechanism

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.