A Review of the Distributed Denial of Services Attacks And Machine Learning Techniques

Kanwarpal Singh[1], Dr. Shashi Bhushan[2]
[1]M.Tech (Scholar), [2]Head of Deartment
Department of Information Security, Chandigarh Engineering College, Landran

Abstract – Currently, many companies and/or governments require a secure system and/or an accurate intrusion detection system (IDS) to defend their network services and the user's private information. In network security, developing an accurate detection system for distributed denial of service (DDoS) attacks is one of challenging tasks. DDoS attacks jam the network service of the target using multiple bots hijacked by crackers and send numerous packets to the target server. Servers of many companies and/or governments have been victims of the attacks. In such an attack, detecting the crackers is extremely difficult, because they only send a command by multiple bots from another network and then leave the bots quickly after command execute. DDoS attacks existed since mid-1980 and they are still the top most web security threat. Hence, mitigation of DDoS attacks is becoming very important. The distributed and dynamic nature of the DDoS attacks makes it more difficult to mitigate. In order to mitigate the DDoS attacks, several techniques have been proposed in the past by various researchers. However, most of the project research were focusing either on Application Layer or Network Layer and are mostly providing single layer of defence. In such scenario, hackers and attacker are taking advantage of the weakness of these mitigation techniques to launch the DDoS attack. In this layer based Denial-of-service attacks use legitimate HTTP requirements after implement of transport control protocol in three ways i.e. databases, Processor and Memory etc. In network Layer based on distributed denial of services sends the flood attack and USP and requests to the server and exhausts the bandwidth.

Keywords – DDoS attack, HTTP requirements, Network Layer and Application Layers.

I. INTRODUCTION

In past years, the news about distributed denial of serviceattack is rapidly increased around the world. Many services of companies and/or governments are victims of the attack. A hacker groups developed tools to execute DDoS attack very easily and sell them too many people. As the results, DDoS attacks became one of most harmful attacks in network security [4].

DDoS attack has produced severe damage to servers and would cause even greater intimidation to the development of new internet services. Traditionally, DDoS attacks are approved at the network layer such as flooding, SYN flood and USP flood which are called network layer DDoS attacks. We work on cyber security field.Cyber security is the body of technologies, processes and practices considered to protect system, computers, agenda and data from attack, break or unauthorized admission. In a compute situation, the term safety implies cyber safety. Organization and user's assets contain connected computing strategy, personnel, transportation, submission, services, telecommunications organizations the totality of diffused and stored data in the cyber atmosphere. Cyber security endeavours to ensure the achievement conservation of the safety property of the group and user's assets against relevant safety risks in the cyber atmosphere. The general safety objectives comprise the following [7]:

- Availability
- Integrity, which may take in authenticity and non-repudiation
- Discretion

Cyber safety involves protecting that information by avoiding, identify, and responding to attacks.

Internet Protocol

IPv6 is the most recent generation of the Internet Protocol (IP) defined by the Internet Engineering Task Force.Internet Protocol Version 6 is the latest version of Internet Protocol. It has been under development since the early 1990s. Other benefits of IPv6 include:

(i) No need for NAT (Network Address Translation) because there are enough IPv6 addresses for each device to have it's own address.
(ii) Configuration can be automatic.
(iii) Eliminates the challenge of private address collisions.
(iv) Improved multicast routing.
(v) A simplified packet header, which allows for more efficient forwarding.
(vi) Built-in authentication and privacy support through IPSec in the protocol.
(vii) Flexible options and extensions to the header format[9]

Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol used to facilitate communication over a network through an addressing system. It is currently the most popular Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 232 addresses (slightly over 4 billion addresses). Each device connecting to the Internet requires an IP address.

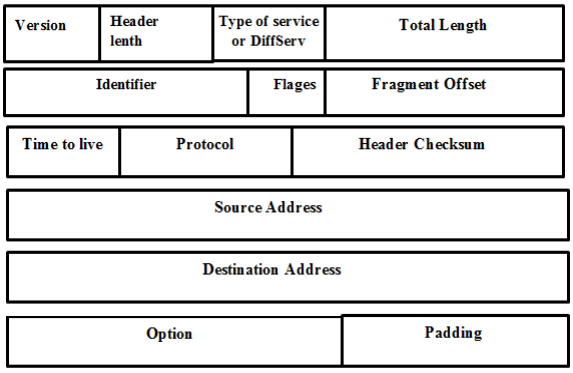

Fig 1. IPv6 and IPv4 Protoccols

That means that each device including cell phones, office phones, game consoles and computers each need their own IP address in order to connect and communicate over the Internet. With the ever-growing number of devices that need to connect to the Internet, it is no surprise that the amount of available IPv4 addresses will soon be exhausted. Already, there are more devices connected than there are routable IPv4 addresses. This is possible through a technology known as NAT (Network Address Translation) which allows multiple machines to appear as a single routable address. This comes with the cost of the complexity involved in supporting devices beployed behind a NAT device.

Table 1. Difference between Static and DHCP

Static IP	DHCP
Static IP is not really that complex as it simply means that the IP of a certain network element like a computer or router stays the same the same throughout.	Dynamic Host Configuration Protocol, abbreviated to DHCP,is a protocol for assigning free IP addresses to computers that are connected to the network.
There are limitations to using static IPs, not to mention that it is tiresome for the administrator, and dynamic IPs are used instead. [2]	Using DHCP is advantage for network administrators because it removes the repetitive task of assigning IP address to each computer on the network and when adding more units.

(i) DDoS attack in IPv6

Denial of service (DoS) attack is one of the major security threats to the IPv4 and IPv6 networks [18]. In DoS attacks, a victim host(s) can be denied from the services by wasting its resources and disrupt its communication with other neighboring hosts on same link. A targeted device is unable to process such large amount of network traffic and becomes unavailable or out of service. Moreover, when DoS attack is being attempted from large networks or systems then it is known as Distributed Denial of Service (DDoS) attacks.

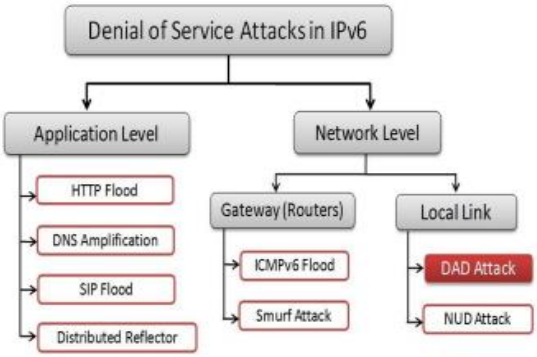

Fig 2. Taxanomy of DoS attacks in IPv6 Network[18]

In order to perform DDoS attack, an attackers uses various resources such as network nodes and Internet services which are distributed around the globe considered as botnets. Later, these botnets are used to launch the DDoS attack against the targeted victim.

Denial of Service (DoS) attacks in IPv6 network can be broadly classified into two main categories based on the attacked level such as; application level and network level. Further network level DoS attacks can be subdivided into gateway (router) and local link levels respectively. Figure 2 depicts the taxonomy of DoS attacks in IPv6 network.

II. RELATED WORK

Kamaljeet Kaur et al., 2016 [14] discussed with the anomaly based detection technique is a concept of a baseline for the network behaviour. Baseline can be considered as description of the type of network behaviour that can be accepted, any deviation from this baseline is considered as an anomaly. Therefore anomaly based intrusion detection uses machine learning techniques to detect whether a packet is intrusive or non-intrusive. It provides a systematic review of machine learning techniques used in DDoS attack detection.

Keisuke Kato et al., 2014 [10] described that the network security developing an accurate detection system for distributed denial of service (DDoS) attacks was one of challenging tasks. DDoS attacks jam the network service of the target using multiple bots hijacked by crackers and send numerous packets to the target server. Servers of many companies and/or governments have been victims of the attacks. In such an attack, detecting the crackers was extremely difficult, because they only send a command by multiple bots from another network and then leave the bots quickly after command execute. The proposed strategy was to develop an intelligent detection system for DDoS attacks by detecting patterns of DDoS attack using network packet analysis and utilizing machine learning techniques to study the patterns of DDoS attacks.

Rida Anwar et al., 2016 [15] described that the Web servers, which host these online services, are the prime

targets for the hackers to perform Distributed Denial of Service (DDoS) attacks. Attackers release DDoS assaults on net servers in order to disrupt the offerings or to eat the network bandwidth. This makes legitimate users unable to access the web resources at times. DDoS attack compromise the availability of the service by means of utilizing the energy of thousands and thousands of zombies (compromised computers) below the manipulate of the bot masters. DDoS attacks happened since mid-1980 and they were motionless the top most web security threat. Hence, mitigation of DDoS attacks is becoming very important. The distributed and dynamic nature of the DDoS attacks makes it more difficult to mitigate. In order to moderate the DDoS attacks, several methods have been planned in the past by various academics. However, most of the project research were focusing either on Application Layer or Network Layer and are mostly providing single layer of defence.

Supriya Thakur et al., 2016[16] discussed in web services detect distributed denial of service attack is a constant critical risk to the internet. In application layer distributed denial of services attack is defined from the fewer layers. In this layer based Denial-of-service attacks use legitimate HTTP requirements after implement of transport control protocol in three ways i.e. databases, Processor and Memory etc. In network Layer based on distributed denial of services sends the flood attack and USP and requests to the server and exhausts the bandwidth. In previous work, in network layer based on DDoS attack send the SYN attack with ESVM.

Table 2: Related Work Summary

Author Name	Description	Techniques	Attacks
Kamaljeet et al., 2016	An intrusion detection uses machine learning techniques to detect whether a packet is intrusive or non-intrusive	ANN, SVM and Fuzzy Logics	DDoS
Keisuke Kato et al, 2014	Analyzed large numbers of network packets provided by the Center for Applied Internet Data Analysis and implemented the detection system using a support vector machine with the radial basis function (Gaussian) kernel	Support Vector Machine	DDoS
Rida Anwar et al.,	The first one is to describe various DDoS attack methods, and to present a systematic review and evaluation of the existing defense mechanisms. The second is to discuss a longer-term solution, dubbed the Internet-firewall approach, that attempts to intercept attack packets in the Internet core, well before reaching the victim.		
Supriya Thakur et al.,	In this layer based Denial-of-service attacks use legitimate HTTP requirements after implement of transport control protocol in three ways i.e. databases, Processor and Memory etc	ESVM	SYN

III. PREVENTION CLASSIFICATION TECHNIQUES

An intrusion detection system require administrator to include rules and signatures to detect attacks. Itrequires several man hours to test, create and deploy these signatures and again create new for unknown attacks.Anomaly based IDS based on machine learning technique provides the solution to this problem they help in generatinga system that can learn from data and provide prediction for the unseen data based on the learned data [5].Some of the commonly used machines learning techniques for DDOS attack detection:

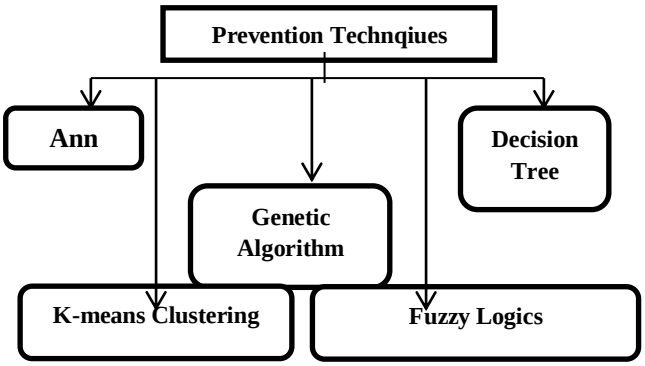

Fig 3. Prevention Techniques in DDoS attack

- **Artificial Neural Network:** Artificial Neural networks (ANNs) are a family group of models inspired by biological neural networks which are accustomed to estimate on a big number of inputs and are usually unknown. ANNs include an accumulation of processing elements interconnected together and aimed to transform some inputs to some desired outputs. In this, the Multilayer Perceptions MLP has been widely adopted neural network for intrusion detection in conventional systems. In NN based packets classification system, each component of the feature vector has one input node. Also, usually one output node is employed for each class to which an element might be assigned. The hidden nodes are linked to input nodes and some initial weight assigned to these connections. These weights are adjusted

during working out process. Back-propagation rule is among the learning algorithms employed for MLP based ANN [1].

- **Fuzzy Logics**: Fuzzy logic is based on fuzzy set theory which works on reasoning. Techniques based on fuzziness have been used for anomaly detection. The concept of fuzzy logic lets an object to fit in to different classes simultaneously.It designed a fuzzy logic system to detect exhaustion attacks in IEEE 802.1.5.4 MAC layer. It uses an anomaly based approach and operates in a distributed manner. They strengthened their scheme by two parameters of attack detection namely energy decay rate and attack detection rate. They distinguish attack scenario from the impact of traffic load on network behaviour [11].
- **Decision Tree**: Decision tree algorithm is one of the predictive modelling techniques used in data mining, statistics and machine learning for classification. In this a decision tree is used to sort the instances from root node to leaf node. The dataset is learnt and modelled in algorithm therefore whenever a new data item is given for classification it will be classified as learned from the previous dataset. Decision tree algorithm can also be used for detecting DDoS attacks[3].
- **Genetic Algorithm:** Genetic algorithm is a process of natural selection that associates with larger class of evolutionary algorithm. GA is a search method that identifies an approximate solution to optimization tasks. GA algorithm based intrusion detection system is used to detect intrusion based on past behaviour. In this method a profile is created for the normal behaviour. Based on this profile GA learns and takes the decision for the unseen patterns. GA also used to develop rules for network intrusion. A typical genetic algorithm requires a genetic representation of solution and a fitness function to evaluate solution [6].
- **K-means clustering:** K-Means clustering is a method of partitioning the dataset into k clusters in which each set belongs to cluster with the nearest mean. It planned a method for proactive detection of DDoS attack by exploiting its construction. Procedures of DDoS attacks are analysed and select variables based on these features. Then perform the cluster analysis of proactive detection of attack. The results are evaluated using 2000 DARPA intrusion detection. The consequence shows that each stage of attack setup is separated well and detects predecessors of DDoS attack as well as attack itself [12].

Table 3. Comparison between Technique used in Distributed Denial of Attacks

Parameters	Techniques Used	DDoS Attacks	Issues
Auto-Correlation Function	Service Level Agreement	Yes	Traffic increases
Probability and Detection Rate	Filteration Method	Yes	Congestion Rate increases
Throughput	Check point	Yes	Delay increases

Table 4. Performance Parameters

Author Name	Year	Parameters			
		FPR	FNR	Acc	Entropy
Seo, J et al.,	2005	✓	✓	X	X
Jin Li et al.,	2010	✓	✓	✓	X
Jae-Hyun Jun et al.,	2011	X	X	X	✓
Ramamoorthi, A	2011	X	X	✓	X
V. Akilandeswari	2012	✓	✓	✓	X
Young-Tae Han	2012	X	X	X	X
Mohamed Karim	2012	X	X	X	X
Ali, Amer Nizar	2012	X	X	X	X
Kato, Keisuke	2014	✓	✓	X	X
Barati, Mehdi	2014	✓	✓	X	X
Yuri G. Dantas	2014	X	X	X	X
Rashmi v. et al.,	2015	X	X	X	X
Kaur Kamaljeet et al.,	2016	X	X	X	X
Rida Anwar et al.,	2016	X	X	X	X
Thakur, Supriya et al.,	2016	X	X	X	X
Qiao Yan, et al.,	2015	X	X	X	X
Rehman, S. U et al.,	2016	X	X	X	X

The above 4 table defined that the performance parameters like FAR (false positive rate) , FNR (false negative rate) and accuracy and entropy.

IV. ISSUES IN DDoS ATTACK

DDoS attack is an accepted growth from the SYN Flood [17]. The idea belated this attack is converging Internet linking bandwidth of many categories of machinery upon

one or a few machines. This way it is likely to use a large array of smaller widely distributed computers to create the big flood effect [12]. Usually, the attacker installs his remote attack database on weakly protected processors using Trojan horses and intrusion methods, and then coordinates the attack from all the different computers at once. This makes, brute force flood of malicious "nonsense" Internet traffic to marsh and devour the objective server's or its network connection bandwidth. This means packet flood contends with, and overwhelms, the network's valid traffic so that "good packets" have a low probability of enduring the flood[8].

Avoid the distribution denial of service attacks with optimization techniques and some others:

(i) The firewall state table may be overwhelmed, causing reboots, or worse.

(ii) It locks up and making the DDoS attack effective from the attacker's perspective.

The service is no longer available to legitimate users.

For in-depth security analysis purposes, however, relying on samples is a serious concession; you miss a large piece of information as you only receive one packet out of a thousand, or worse. A flow analytics device has to evaluate the behavior of a traffic stream over a longer time period to be sure something is wrong, and to avoid false positives.

V. CONCLUSION

DoS attack reasons either disruption or degradation on victim's shared resources, as a result avoiding appropriate users from their access right on those resources. DoS attack may objective on a specific component of computer, entire computer system, certain networking infrastructure, or even entire Internet infrastructure. Attacks can be either by exploits the natural weakness of a system, which is known as logical attacks or overloading the victim with high volume of traffic, which is called flooding attacks. A distributed form of DoS attack called DDoS attack, which is generated by many compromised machines to coordinately hit a victim. DDoS attacks are adversarial and constantly evolving. In this paper we have analysed various machine learning techniques for DDoS detection. Request and Network layer DDoS attacks are effectively generated and distinguished by described that the various approach used in real time difference detection system. An apparent vision of the DDoS attack is attained and discussed numerous techniques along with their pros and cons to prevent and alleviate these attacks. Due to an alarming increase in DDoS attacks, internet security from these attacks becomes vulnerable issue. Having clarified view of the attack, effective countermeasures can be implemented to fight against these attacks.

VI. REFERENCES

[1]. Seo, Jungtaek, Cheolho Lee, Taeshik Shon, Kyu-Hyung Cho, and Jongsub Moon. "A new DDoS detection model using multiple SVMs and TRA." In *Embedded and Ubiquitous Computing–EUC 2005 Workshops*, pp. 976-985. Springer Berlin/Heidelberg, 2005.

[2]. Bahl, Pradeep. "System and method of assigning and reclaiming static addresses through the dynamic host configuration protocol." U.S. Patent 6,957,276, issued October 18, 2005.

[3]. Jin li Yong liu," DDoS attack detection based on neural network", IEEE 2010, pp: 196-199.

[4]. J. Jun, H. Oh, and S. Kim, "DDoS flooding attack detection through a step-by-step investigation," pp: 04, 2011.

[5]. Ramamoorthi, A., T. Subbulakshmi, and S. Mercy Shalinie. "Real time detection and classification of DDoS attacks using enhanced SVM with string kernels." In Recent Trends in Information Technology (ICRTIT), 2011 International Conference on, pp: 91-96. IEEE, 2011.

[6]. V. Akilandeswari," Probabilistic Neural Network based attack traffic classification", IEEE fourth international conference on advance computing 2012.

[7]. Y. Han, M. Kim, and H. Park, "Vulnerability of Small Networks for the TTL Expiry DDoS Attack," pp: 147–149, 2012.

[8]. Mohamed Karim Aroua & Belhassen Zouari,"A distributed and coordinated massive DDoS attack detection and response approach",2012 IEEE 36th international conference on computer software and applications workshops pp: 230-235.

[9]. Ali, Amer Nizar Abu. "Comparison study between IPV4 & IPV6." International Journal of Computer Science Issues 9, no. 3 (2012): 314-317.

[10]. Kato, Keisuke, and Vitaly Klyuev. "An Intelligent DDoS Attack Detection System Using Packet Analysis and Support Vector Machine." IJICR (2014), pp: 478-485.

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

[12]. Yuri G. Dantas,"A selective defense for application layer DDoS attacks", 2014 IEEE joint intelligence and security informatics conference", pp: 75-82.

[13]. Rashmi v. Deshmukh and Kailas k. Davadkar ,"Understanding DDOS attack and its effect in cloud environment", Procedia computer science 49(2015) pp: 202-210.

[14]. Kaur Kamaljeet et al., "A Review on Various Machine Learning Techniques for the Detection of DDoS Attacks", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Issue 9, September 2016.

[15]. Rida Anwar, Shruti Gorasia ," Detection and Classification of Distributed Denial of Service (DDoS) Attack", International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 4 Issue I, January 2016.

[16]. Thakur, Supriya, Er Amritpal Kaur, and Banur SVIET. "Run Time Exposure and Classification of Flood Attack using Genetic and Enhance Support Vector Machine." International Academy of Engineering and Medical Research, 2016 Volume-1, ISSUE-3.

[17]. Qiao Yan, F. Richard Yu, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges", IEEE communication surveys & tutorials, vol. 18, no. 1, first quarter 2016.

[18]. Rehman, S. U., & Manickam, S. (2016). Denial of Service Attack in IPv6 Duplicate Address Detection Process. *International Journal of Advanced Computer Science & Applications*, *7*, 232-238.