iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Security Analysis of Distributed Denial of Service Attacks Using Machine Learning a Survey

Sunita[1], Abhishek Kajal[2]
[1]Mtech. Student Department of Computer Science & Engineering
[2]Asst. Professor Guru Jembheshwar University of Science & Technology, Hisar, India

Abstract: ***Denial of service attack is the major problem in cyber network. DoS/DDoS attacks make the system performance slow. This paper discusses about DoS/DDoS attack detection algorithm and its various versions used for providing the security to the system. Each algorithm has many disadvantages like long training time, high computational cost, and adjustment of weight. Many researchers have also proposed hybrid technique with evolutionary algorithm to improve the performance of cyber system.***
Keywords : Denial of Service, Distributed Denial of Service, Artificial Neural Network, User Datagram Protocol, Internet Control Message Protocol. Multilayer Perceptron.

I. INTRODUCTION

Cyber attacks are an experiment to disturb,damage or gain unauthorized access to a computer system or network. A cyber attack is carefully misuse of computer systems, technology-dependent enterprises and networks. Cyber attacks to use malicious code to change computer code or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity lose. Cyber attacks are a criminal act using a computer that occurs over the Internet. The Internet has become the source of multiple types of crime and different ways to perform these crimes. Cyber security involves preventing, detecting, and responding to cyber incident. The rest of paper is organized as follows: In section II, types of attack are discussed, Distributed denial of service of attack, Problem face due to DDoS attack, Machine learning techniques in section III. In section IV conclusion is given.

II. TYPES OF ATTACK

Malware: is type of computer code that has a malicious intent. Malware is often used to destroy something on a computer or to steal private information.

Viruses: Viruses are a type of attack that makes a computer"sick". They infect a computer just like a real virus that infects a person. Viruses replicate themselves, and they survive by attaching to other programs or files.

Spyware: Spyware is also used to steal confidential information. Spyware is capable of recording, keystrokes, which means that the attacker can view password that the victim enters into the computer.

Worms: Worms replicates themselves many times to fulfill nefarious surviving all by themselves, and not only do they replicate on a single computer host, but also they can replicate across the whole network of computers.

Password attack: focus on cracking a victim's password so that the attacker might obtain access to a secured system.

Brute Force attack: is executed when an attacker tries to use all possible combinations of letters, numbers and symbols to enter a correct password.

Dictionary attack: occurs when an attacker utilizes a dictionary in an attempt to crack a password. Essentially a word of the dictionary is input into the password field to try to guess the password.

Denial of service attacks: Is a special form of cyber attack that focused on the interruption of a network service. This is obtained when an attacker sends large amount of traffic or data through the target network until the network becomes overloaded.

III. DISTRIBUTED DENIAL OF SERVICE ATTACK:

A DDoS attack arises from a regular DoS attack in it there are multiple computers involved. The computers work together by means of the internet to send traffic to the target network [1].

A distributed denial of service attack is an attack in which various computer system attack a target such as a server website or other network resource cause a denial of service for users of the targeted resource.

[2] The Difference between DoS and DDoS Attack.

A Denial of Service attack is different from a DDoS attack. One computer and one Internet connection to flood a targeted system or

resource is used by the denial of service attack. The DDoS attack uses various computers and Internet connections to flood the targeted system resource.

A. Types of ddos attack

There are different types of DDoS attacks. Most attacks include the following:

Traffic attacks: Traffic flooding attack sends a huge volume of TCP, UDP and ICPM packets to the target system. Legitimate requests are getting lost and the attacks may be accompanied by malware exploitation. UDP flood attacks are initiated by sending a large number of UDP packets to random ports on a remote host. On receiving the packets, target system looks the destination ports to identify the applications waiting on the port.

ICMP flood: overflows the target resource with ICMP Echo Request packets, generally send the multiple packets as fast as possible without waiting for the acknowledgement. This type of attack can consume both outgoing and incoming bandwidth.

1) Bandwidth attacks: overloads the target with massive amounts of junk data. This results in a loss of network bandwidth or resources may lead to a complete denial of service.
2) Application attacks: Application-layer data messages are depleted resources in the application layer, leaving the target's system services unreachable.
3) Volume Based Attacks. Includes ICMP floods packets, IP spoofed-packet UDP floods packets.
4) Protocol Attacks: Includes fragmented packet attacks, Ping of Death, SYN floods Smurf DDoS and more. In SYN FLOOD the attacker sends multiple packets but does not send the Acknowledgement back to the server. The connections are half opened and half closed those consuming server resources.

There are mainly three types of DDoS attacks [3]: Bandwidth (Throughput Attacks), Protocol Attacks, Software Vulnerability Attacks, Bandwidth (Throughput Attacks) attacks are those attack in which the bandwidth of users disable (exhausted) by flooding the traffic towards victim. Bandwidth/Throughput attacks are of two types: flooding attack and amplification attack.

Protocol Attacks DoS attacks based on protocol features take advantage of certain standard protocol features. For example several Distributed Denial of Service Attack Detection Techniques All rights reserved by www.ijsrd.com 200 attacks exploit the fact that IP source addresses can be spoofed. Example of such attack is: 1 DNS Name Server Attack Several types of DoS attacks have focused on DNS, and many of these involve attacking DNS cache on name servers. An attacker who owns a name server may coerce a victim name server into caching false records by querying the victim about the attacker's own site. A vulnerable victim name server would then refer to the rogue server and cache the answer [4] Software Vulnerability Attacks In these types of attack attacker get the benefit of software vulnerabilities. These attacks are of three types- Land Attack, Ping of Death Attack, Fragmentation Attack and Teardrop Attack.

The basic idea of log-based trace back is that each router stores the information (digests, signature, or even the packet itself) of network traffic through it. Once an attack is detected, the victim queries the upstream routers by checking whether they are logged the attack packet in question or not. If the attack packet's information is found in a given router's memory, then that router is deemed to be part of the attack path. Obviously, the major challenge in Distributed Denial of Service Attack Detection Techniques (IJSRD/Vol. 4/Issue 05/2016/051) All rights reserved by www.ijsrd.com 202 log-based trace back schemes is the storage space requirement at the intermediate routers [5]. Hash based IP trace back can trace even a single IP packet provided, the copy of the packet, its destination and approximate time of the packet's reception at the victim are available.

B. Problem Faced Due To Ddos Attack:

1) Rapid consumption of bandwidth, computational resources, processor time or disk space.
2) Disruption of routing information.
3) Disruption of physical network components or resource in short time interval.
4) Sudden spike or maxing out of the processor's usage.
5) Multiple errors triggered in interconnected machines.

C. Machine learning techniques

[6] Network-based IDS (NIDS) commonly detects attacks such as worms, scans, DoS attacks, botnets, and other types of attacks. Network IDSs are normally categorized based on the detection method as one of two types: signature-based or anomaly-based detection. Signature-based, also known as rule- or misuse-based [7] detects an attack by comparing well-known attack signatures, or

patterns, with the monitored traffic. A match generates an alarm for a potential attack. This type has fast detection time, detects most known attacks [8] normally has a low false positive rate, i.e., it does not signal an alarm for legitimate traffic. On the other hand, an anomaly-based IDS, also known as behavior-based, operates by comparing the network traffic behavior against previous "normal" traffic behavior. Any deviation in the comparison is considered to be a sign of an attack. The system acquires a normal traffic profile, usually through training, and monitors the traffic for any change with the normal profile [9]. The normal traffic behavior is classified into two types [8] standard and trained. The standard is based on standard protocols and rules such as TCP handshaking connection [10] set up and how the attacker could perform a half connection attack. The trained traffic is used to calculate a threshold value for future detection. Anomaly detection can detect unknown attacks; however it generally produces higher (1) false positive rates than signature-based systems.

1) Artificial neural network
2) Support vector machine
3) Fuzzy logic
4) Decision tree
5) Genetic algorithm
6) Naive bayes
7) Kmean clustering

Artificial neural network: ANN are a family of group of models inspired by biological neural networks which are confirmed to estimate one big number of inputs and are usually unknown ANN include processing elements interconnected together and aimed to transform some inputs to some desire output. In ANN three layers are used input layer, hidden layer and output layer. Input layer is used to input the data hidden layer process the data out layer gives the output.[11] presented a neural network for DDoS attack detection to analysis the server resource and network traffic and they use the learning vector quantification(LVQ)for post anomaly detection. [12] Introduced a neural network based attack classification to detect different attacks. The author focuses on separating flash crowd event from denial of service attack.

SVM: Support vector machines are supervised learning models that related with learning algorithms and investigate data used for classification and regression analysis. Given a set of training examples, each marked as belonging to one or two categories, an SVM training algorithm builds a model that assigns new examples to one category or other, making it a non-probabilistic binary linear classifier. An SVM model represents examples as points in space, mapped so that the examples of the other categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and estimated a category which it belongs based on which side of the gap they fall.

Fuzzy logic: fuzzy logic is based on fuzzy set theory which works on reasoning. Technique based on fuzziness has been used for anomaly detection. The concept of fuzzy logic lets an object to fit in to different classes simultaneously. [13] Designed a fuzzy logic based system for identifying the intrusion with in a network. They use the automated strategy for generation of fuzzy rules, which are obtained from the definite rules using frequent items. When data are not labeled, supervised learning is not possible, and an unsupervised learning approach is required, which attempts to find natural clustering of the data to groups, and then map new data to these formed groups.

A decision tree is a tree-like structures or model of decisions and its possible importance, including chance of event outcomes, resource costs, and utility of the resource. DDoS attacks are measured using decision tree algorithms.

Genetic Algorithm: a genetic algorithm (GA) is a meta heuristic activated by the process of natural selection that belongs to the broad class of evolutionary algorithms (EA). Genetic algorithms are used to generate high-quality solutions to optimization and search problems by depending on bio-inspired operators such as mutation, crossover and selection. In a genetic algorithm, a population of candidate solutions to an optimization problem is developed to get better solutions. Each candidate solution has a set of properties (its chromosomes or genotype) which can be mutated and changed; traditionally, solutions are represented in binary as strings of zero and one, but other encodings are also possible.

The solution usually starts from an arbitrarily generated individuals from a population, and is an iterative process, with the population in each iteration called a generation. In each generation, the fitness of every individual in the population is evaluated; the fitness is the value of the objective function in the optimization problem. The more fit individuals are randomly selected from the most frequently used population and each individual's genome is changed to form a new generation. The new generation of candidate solutions is then used in the next iteration of the algorithm. When a maximum number of generations have been produced then the algorithm exits or a satisfactory fitness level has been arrived for the population.

NAIVE BAYES: Naïve Bayes is a technique for constructing classifiers: that assign class labels to problem instances where the class labels are drawn from some finite set. It is a family of algorithms based on common principle value of a particular feature is independent of the value of any other feature, given the class variable. Akilandeswari and shalinie [12] had introduced a probabilistic neural network based attack traffic classification to detect different DDoS attacks. The authors focus on separating flash crowd event from denial of service attacks. Mouhammd Alkasassbeh [14] compiles new dataset that consist of dos attacks in different network layers. DDoS attacks are detected using three techniques Multilayer Perceptron (MLP), Naive Bayes and Random Forest. MLP showed the highest accuracy rate.

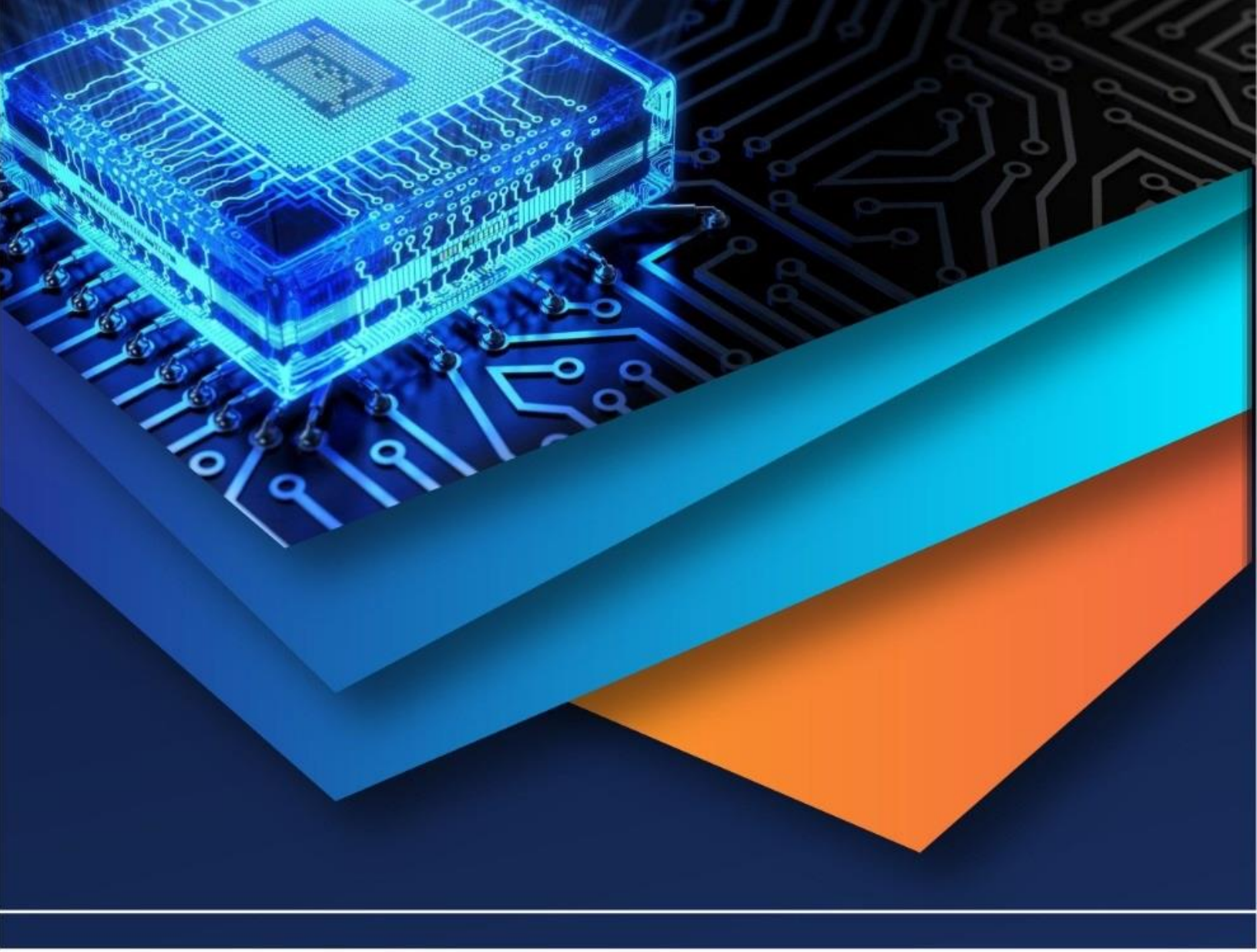
K-means clustering: is a way of partitioning the dataset into k clusters. In which each data set belongs to cluster which have nearest mean. Keunsoo Lee & JuhyunKim [15] proposed a method for Proactive detection of DDoS attack by exploiting its architecture. Procedures of DDoS attacks are analyzed and select variables based on these features. Then perform the cluster analysis of proactive detection of attack.The results are evaluated using 2000 DARPA instruction detection the result shows that each stage of attack scenario is partitioned well and detects precursors of DDoS attack as well as attack itself.

IV. CONCLUSION

After going through the paper we concluded that there are many solutions of cyber attack each solution have advantage and disadvantage machine learning has long training time and calculations are very complex. DOS/SDDoS attacks are major threats in cyber networks. This paper enables better understanding of the problem and good security administrator.

REFERENCES

[1] P. Gudadhe and S. Nimbhorkar, “A Survey Paper on Detection of Denial of Service Attack on Wireless Network,” IEEE, Vol.4, Issue11, pp.2373-2376, 2015.
[2] F.Lau,,S.H. Rubin, M. H.Smith and L. Trajkovic,“Distributed Denial of Service Attacks,”Natural Sciences and Engineering Research Council Grant 21684499, 2002.
[3] A. Sachdeva1 and B. Parashar, “ Distributed Denial of Service Attack Detection Techniques ,” International Journal for Scientific Research & Development| Vol. 4, Issue 05, 2016 | ISSN (online): 2321-0613
[4] C.Douligeris and A. Mitrokotsa, “DDoS attacks and defense mechanisms: classification and state-of-the-art,”
[5] G.Florance, “Survey of IP Traceback Methods in Distributed Denial of Service (DDoS) Attacks,” International Journal of Innovative Research in Science, Engineering and Technology,Vol. 4, Issue 7, July 2015.
[6] M. Alenezi and M. J. Reed, “Methodologies for detecting DoS/DDoS attacks against network servers,” The Seventh International Conference on Systems and Networks Communications, ICSNC 2012 .
[7] F. Dressler, G. Munz, and G. Carle, “Attack detection using cooperating autonomous detection systems (CATS), ” Wilhelm- Schickard Institute of Computer Science, Computer Networks and Internet, 2004.
[8] S. A. Khayam, et al., “A survey of anomaley-based intrusion detection systems,” School of Electrical Engineering and Computer Science (SEECS), National University of Sciences & Technology (NUST)2009.
[9] N.Ye, Secure computer and network systems: modeling, analysis and design: Wiley, 2008.
[10] R. W. Stevens, TCP/IP illustrated, Volume 1: The protocols: Addison-Wesley Professional, 1994.
[11] Jin li yong liu, “DDoS Attack Detection Based on Neural Network,” IEEE, 2010, pp. 196-199.
[12] V. Akilandeswari, “Probabilistic Neural Network Based Attack Traffic classification,” IEEE, fourth international conference on advance computing, 2012.
[13] R. Shanmugavadivu, “network Intrusion Detection System using Fuzzy Logic,” Indian Journal of Computer science & Engineering, Vol. 2, No. 1.
[14] M. Alkasassbeh, G. A. Naymat, “Detecting Distributed De3nial of Service attack using Data Mining Techniques,” Intenational journal of Advanced Computer Science and application , Vol. 7, No. 1, 2016.
[15] K.Lee, J. Kim and S. Kim, “DDoS Attack Detection Method using Cluster Analysis,” Expert System With application, Vol. 34, Issue 3, 2008.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY