www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12595-12598

Survey on Data Mining and IP Traceback Technique in DDoS Attack

Aakriti Aggarwal[1] Ankur Gupta[2]

[1]Research Scholar Electronics Dept., [2]H.O.D, Assistant Proff. Electronics Dept
Gita Institute of Management and Technology
Kurukshetra University
INDIA
aakriti.aggrwal@gmail.com

Abstract-Denial of Service (DoS) attack is presently a very serious threat for the Internet security. These attacks attempts to exhaust victim's resources e.g. CPU cycles, memory or network bandwidth. Thus disturb the consistent access of services to the user. When DoS attacks are formed by multiple distributed computer it is called as distributed denial of service (DDoS) attack. DDoS attacks can weaken computing and communication power of its victim within a short period of time. Because of seriousness of the problem many defense mechanisms have been proposed to encounter the attack. In this paper, two types of techniques for DDoS attacks and their countermeasure are given so that a better understanding of attack can be achieved.

Keywords - DoS attacks; DDoS attacks; data mining; IP traceback.

INTRODUCTION

DoS attack exploit internet to aim web services [10]. This attack is intended to prevent the legitimate user from accessing a specific network resources or degrade normal services for legitimate user by sending useless packets (traffic to victim) to suppress the services and connection Denial of Service attack aims to disallow a victim (host, router or whole network) can be launched in any ways. One method is by exploiting system design weaknesses and another method of launching is by imposing computational intensive task on victim such as encryption and decryption and secret computation [1]. However flooding based Distributed Denial of Service (DDoS) attack do not rely on particular network protocol or system weakness. Instead DDoS simply exploit huge resources between internet and victim. In this attack sufficient numbers of compromised hosts are collected to send junk packets towards the victim at the same time. The degree of traffic is high enough that a victim cannot afford it and becomes paralyzed.

The key reason behind this occurrence of huge attack is that the network security community does not have efficient & capacity or bandwidth. Denial of Service attack are prevails from several years. Previously single source attacks were countered and by simple several defense mechanisms source of those attacks were rejected or blocked but with the massive growth of internet from last decade a large number of vulnerable systems are currently available to attack.

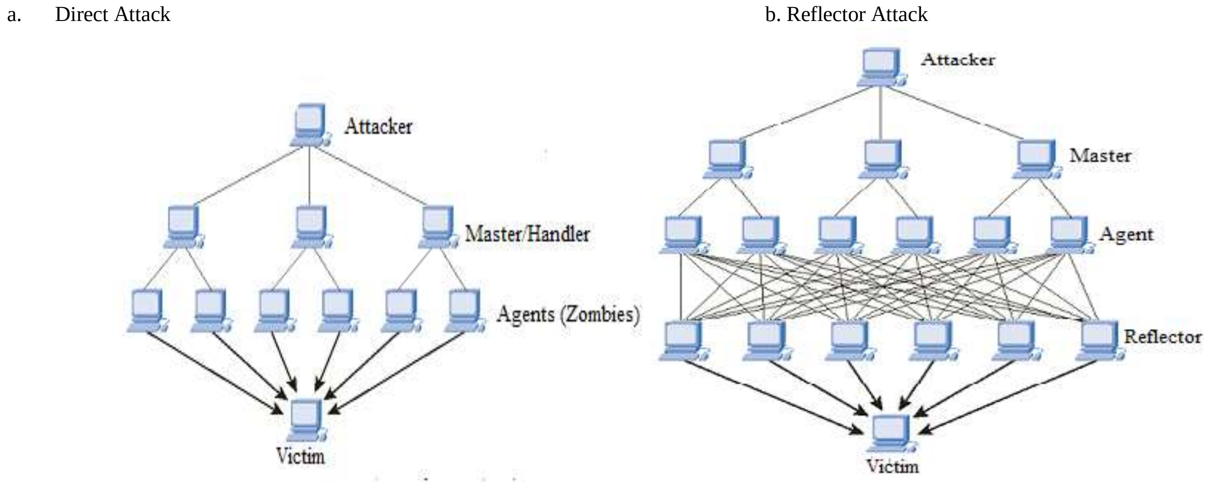
effective defense mechanism to locate attackers as it is easy for attackers now to disguise them by taking advantage of vulnerabilities of World Wide Web such as dynamic, anonymous and stateless nature. [5] [7]

Rest of this paper firstly describe the architecture of DDoS attack its elements. Then a brief of defense mechanism of the attack is stated and finally paper ends with comparison of two different approaches to defend DDoS attack.

ARCHITECTURE AND DDOS STRATEGY

There are mainly two types of flooding based Distributed Denial of Service (DDoS) attack namely Direct attack and Reflector attack or indirect attack [1].

Figure no. 1- Direct and Reflector Attack


a. Direct Attack

b. Reflector Attack

a. Direct Attack- In direct attack attacker fixes up to send a large number of attack packets directly towards a victim. Attack packets can be TCP, ICMP, UDP or mixture of them. Before launch of direct attack, attacker firstly sets up a DDoS attack network consist of attacking host, master or handler or zombies.

b. Reflector Attack- It is an indirect attack which uses intermediate nodes known as reflectors as attack launchers. Attacker sends packets to reflector with the packets indiscribed source address to a victim address which requires responses. Without realizing that the packets are actually fake the reflector returns response packets to the victim. Hence attack packets firstly reflected in the form of normal attack towards victim and cause the attack. Figure 1 clearly shows the reflector attack.

DDoS attack composed of four elements mainly [4]

- Real Attacker - This initiates all process.
- The master -These are compromised host which control multiple agents with the special program running on them.
- Reflector/Zombie- These are compromised host that are responsible for generating a stream of packets towards the intended victim.
- Victim – The ultimate target.

I. LITURATURE SURVEY

Intrusion response consists of many sub mechanisms like hash based IP traceback, centre track, ICMP traceback and many more. Likewise intrusion consist of many other techniques i.e. data mining, rate limiting etc.. Here we are concerned about these two defense mechanisms of DDoS attack. Literature surveys of both of these techniques are presented below.

[19] For HTTP botnet detection author proposed association rule based data mining approach. In today's cyber world botnet is the widespread and highly dangerous among all threats. In botnet for delivery of various network threats and malicious activities such as spamming, ID theft and spoofing, a group of compromised computers connected through the internet mainly the host i.e. the liable host are accessed remotely and controlled by a master. Updation and command of botnet can be done through command and control centre. Data mining technique unable us to automatically detect characteristics from huge amount of data, which the traditional signature based methods could not perform.

[17] Identifying attacks source by some mechanism for mitigation of attack at its origin is referred as trace back in DDoS defense. Implementing this method is not easy because of many factors like easy spoofing of source IP addresses and stateless nature of IP routing without knowing the complete path and many more. In this paper three different IP traceback mechanisms are given i.e. Probabilistic Packet Marking (PPM), Deterministic Packet Marking (DPM), and Packet Logging.

[16][18] To implement a traceback scheme author calculated entropy variations of network traffic. Difference of entropy values between normal traffic and DDoS traffic is firstly calculated for the detection of an attack. If the attack is present or detected by this difference in traffic values then tarceback is initialize towards its upstream routers. This proposed method for detection of DDoS attack has advantages over traditional approaches like scalability and storage requirement in victim or intermediate router. Only short term information is stored in it i.e. entropy values of successive time interval to detect the DDoS attack.

[15] Presented that DDoS attacks are large scale attacks launch from a huge number of compromised hosts called zombies, major threat to internet services. Extremely popular and common websites such as Amazon, Yahoo and CNN are among the well known victims of DDoS attacks. Large number of companies which transact online faces the considerable loss as they are being immensely targeted to DDoS attack. Therefore keeping this issue in mind, author presented various significant areas where data mining techniques can be used as strong candidate for detection and prevention of DDoS attack.

[14] For detection and traceback of low rate DDoS attack author presented a mechanism, where low rates attacks are often similar to normal traffic and have such ability to hide their attack related identities in the aggregate traffic. For the detection of low rate DDoS attack two new information matrices were introduced which are generalized entropy metric and information distance metric. In this method, difference between authorized or genuine and attack traffic is calculated through the proposed information matrices which are capable to detect the attack in prior hopes earlier than the counts mentioned in proposed schemes. Detection

accuracy of the system is enhanced by these information matrices and effectively able of identifying low rate DDoS attacks by reducing false positive rate.

[13] The two categories of data mining methods are supervise and unsupervised technique. Training data is used to predict a hidden function in supervised data mining technique. This training data have input variables and output classes. The output of this method can predict a class of the input variables. Classification and prediction are the examples of supervise mining. Unsupervised data mining is a method for identifications of hidden patterns from a given set of data without introducing training data. Clustering and associative rule mining are the examples of unsupervised mining. Data mining is a versatile field that makes use of analysis tool from statistical model machine learning method for discovery of previously unknown, pattern and relationships in large data sets, which are used for finding hackers and preserving privacy.

[12] Based on data mining technique author introduced a DDoS detection system. Distributed denial of service attack is a very serious risk/ threat for the stability of the internet. This paper presents the nature of this attack and its detection method which is recently introduced based on data mining model. In this FCM (Fuzzy C Means) that is a cluster algorithm and apriori association algorithm are used for extraction of network traffic model and network protocol status model. For the detection of attack a threshold is set and based on this threshold value results are calculated. The outcomes shows that by this method DDoS attack can be detected swiftly and efficiently.

[11] Data mining is becoming continuing technology in as different as using historical data for the prediction of the success of marketing campaigns, looking for the templates in network traffic for discovery of illegal activities or analyzing sequences. For knowledge discovery in data base data mining is an important part. KDDs is an iterative process of the important extraction of the information from data and can be applied for development of secure system infrastructure. It includes several steps beginning from collection of raw data and ending in creation of new knowledge. Data mining is used in many areas like engineering, biomedicine, finance and cyber security.

[9] In probabilistic packet marking (PPM) when packet moves from source to destination, every router insert its IP address probabilistically into it. The procedure relies on the presumption that attack packets are more frequent then non attack or legitimate packets. After the detection of attack, victim request adequate range of packets to rebuilt the path up to the attack source through embedded information within the packets. There are no particular fields described in an IP packet for markings. This system has some major cons, like it is justifiable just for direct attacks.

[8] Uses cluster analysis method for the detection of the DDoS attack. This attack generate huge amount of packets by a large number of agents and can easily exhaust communication and computing resources of a victim within a short span of time. This paper proposed a technique for pro-active detection of DDoS attack by taking benefits from its architecture which consist of selection of handlers and agents, communication and compromise and initialization of attack. Focus is on the procedures on which DDoS attacks are based and then select variables build on these features. Pro-active detection of attack is achieved after the cluster analysis. This paper exercises with 2000 DARPA data set for checking the new methods. The result comes out to be that each face of attack scenario is portioned well and detection of DDoS attack can be done.

[6] Introduce a combine data mining approach for the detection of DDoS attacks as this attack causes serious damage hence, a reliable detection and appropriate response mechanisms are necessary. Existing security mechanisms do not provide affective defense against DDoS attacks. For modeling the traffic pattern of normal and distinct attacks, this proposes a combine data mining approach. For selection of a relevant attributes this method uses the automated feature selection mechanism. The building of classifier is done with hypothetically selected attribute through the neural network. The result of this experiment shows that this method can provide the best performance on real network in comparison with any other single data mining approaches.

[3] In deterministic packet marking (DPM), the router place its IP packets deterministically into the IP packets. This scheme was launched to overcome the drawbacks of probabilistic packet marking. This technique on intermediate routers has easy implementation and needs less computational overheads. Yet, it also has the limitations such as packets are marked only by first entry or ingress edge router with the information. So, it require even additional packets to reconstruct the attack path. This technique is less effective than traditional schemes.

[2] In this approach of ICMP messaging routers are programmed to send ICMP messages together with network traffic. Path information such as source address, destination address and the authentication parameters etc. are contained by the ICMP packets. One ICMP messaging packets is sent by router for every 2000 packets passing through it if working on this scheme i.e. with a proportion of 0.005 percent of network traffic a traceback message is sent.

CONCLUSION

Undoubtedly DDoS attacks can cause serious problems in the internet. So the defense mechanisms are introduced. After examining various data mining and IP traceback schemes we can conclude that data mining technique is much better than IP traceback technique in ways like data mining methods can process large amount of data, readymade algorithms are available and modeling and estimation f traffic is easy, do not require marking of packets and many more. We have not presented all existing traceback techniques but major schemes like PPM, DPM, ICMP messaging are given. A perfect technique can never be designed but focus should be made for designing of such scheme which can overcome shortcomings to an extent.

REFRENCES

[1] Chang R.K.C., “Defending against flooding based distributed denial of service attacks: A tutorial,”, Computer Journal. IEEE Communication Magazine, vol. 40, no. 10, pp. 42-51, (2002).

[2] H.F. Lipson, “Tracking and Tracing Cyber Attacks: Technical Challenges and Global Policy Issues,” CERT Coordination Center, Special Report: CMU/SEI-2002-SR-009 (2002)

[3] Belenky and N. Ansari, “IP Traceback with Deterministic Packet Marking,” IEEE Comm. Letters, vol. 7, no. 4, pp. 162-164, April (2003).

[4] Christos Douligeris, Aikaterini Mitrokotsa, “DDoS attacks and defense mechanisms: A Classification and state of –the-art,” Computer Networks 44, pp. 643-666 (2004)

[5] Patrikakis, M.Masikos, O.Zouraraki, “Distributed Denial of Service Attacks,” The Internet Protocol J., vol. 7, no. 4, pp. 13-35, (2004).

[6] Mihui Kim, Hyunjung Na, Kijoon Chae, Hyochan Bang and Jungchan Na, “A Combined Data Mining Approach for DDoS Attack Dtetection,” ICOIN 2004, LNCS 3090, c Springer- Verlag Berlin Heidelberg, pp. 943-950 (2004).

[7] T.Peng, C. Leckie, R.M. Rao, K. "Servey of network-based defense mechanism countering the DoS and DDoS problem," ACM Computing Survey, 39, 3:1-3:42 (2007).

[8] Lee, Juhyun Kim, Ki Hoon Kwon, Younggoo Han, Sehun Kim, "DDoS attack detection method using Cluster analysis," Expert System with Applications 34, pp. 1659-1665 (2008).

[9] M. T. Goodrich, "Probabilistic Packet Marking for Large- Scale IP Traceback," IEEE/ ACM Trans. Networking, vol. 16, no. 1, pp. 15-24, Feb. (2008).

[10] V.Chandola, A.Banerjee,, V.Kumar, "Anomaly detection : A survey," ACM Computing Survey, 41, 15: 1-15: 58. (2009).

[11] P. Sundari, Dr. K. Thangadurai, "An Empirical Study on Data Mining Applications," Global Journal of Computer Science and Technology, vol. 10, issue 5, ver. 1.0, pp. 23-27 (2010).

[12] Rui Zhong, Guangxue yue, "DDoS Detection System Based on Data Mining," ISBN 978-952-5726-09-1(Print) Proceeding of The Second International Symposium on Networking and Network Securities (ISNNS '10) Jinggangshan, P. R .China, pp. 062-065(2010).

[13] Sumit dua, Xian Du, "Data mining an Machine Learning in Cyber Security," Auerbach Publications, International Standard Book No-13; 978-4398-39430 (2011).

[14] Y. Xiang, Li, K., and Zhou, W., "Low –rate DDoS attacks detection and traceback by using new information metrics," IEEE T Inf. Foren. Sec., 6, pp. 426-437 (2011).

[15] Kanwal Garag, Rshma Chawla, "Detection of DDoS attack using Data Mining," International Journal of Computing and Business research(IJCBR), pp. 2229-6166 (2011).

[16] Yu, S., Zhou, W., Doss, R., and Jia, W., "Traceback of DDoS Attacks Using Entropy Variations," IEEE Transactions on Parall. Distr., 22: pp. 412-425 (2011).

[17] K. Kumar, A.L. Sangal and A. Bhandari, "Traceback Techniques Against DDoS Attacks: A Comprehensive Review" Proceedings of IEEE 2nd International Conference on Computer and Communicational Technology (ICCCT), pp. 491-498 (2011).

[18] Baskar. M, Gnanasekaran. T, Saravanan. S, "Adaptive IP Traceback Mechanism for Detecting Low Rate DDoS Attacks" IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN), pp. 373-377 (2013)

[19] Jignesh Vania, Arvind Meniya and Hari Krishna Jethva, "Association Rule Based Data Mining Approach to HTTP Botnet Detection," IJAIEM, vol. 2, Issue 4 ISSN, pp 2319-4847 (2013)