REVIEW ON DDOS ATTACKS AND VARIOUS DETECTION MECHANISMS

Lovepreet Kaur[1] (M. Tech), Abhinav Bhandari[2] (Asst. Prof)
Department of Computer Engineering
Punjabi University, Patiala
Punjab, India.

Abstract: DDoS attack is a coordinated attack on massive scale and it is a major threat in current computer networks. It is not easy to detect the attack , The seriousness of the DDoS problem and the increased frequency of DDoS attacks have led to the advent of numerous DDoS defense mechanisms. Detection mechanism is the first step to avoid the DDoS attack. Some of these mechanisms address a specific kind of DDoS attack such as attacks on Web servers or authentication servers. The defense system taxonomy is illustrated using only the currently known approaches. The goal of this paper is to impose the comprehensive survey of DDoS attacks, architecture of DDoS, detection mechanism of DDoS attack, detection classification, various detection approaches of DDoS and issues and challenges have been presented.

Keywords: DDoS, chi- square, Intrusion Detection System, and Destination port no.

I. INTRODUCTION

With the rapid development of the internet it becomes more complicated and there are so many areas which are not completely secure [1]. The threat of DDoS attacks is the major issue of security in the internet [1].The distributed denial of service is the critical problem which is not solved yet. There is no complete solution existing of the DDoS attacks. The DOS means the attacker launches the large tragic to victim and make it so busy to respond the traffic and it rejects the requests of the legitimate user also. When many attackers launch this kind of attack then it is called distributed denial of service. [2].The first large scale DDOS attack took place on February 7, 2000 on Yahoo! And the internet portal was inaccessible for three hours. DDoS attack network follow two types of architectures: the internet relay chat and the agent handler architecture [3]. The agent handler architecture for DDOS attacks is comprised of clients, handlers and agents. The attacker communicates with the rest of the DDoS attack system at the client system. In the IRC based used channels to connect the client to the agents. IRC ports are used for sending commands to the agent. A recent attacking tool based on the IRC IS Low Orbit Ion cannon (LOIC) [4].It includes three primary attacks for UDP, TCP, and HTTP. If the size of the compromised hosts is bigger than the attack is more powerful.[6]Along with the evolution of DDoS attack tools there are many detection mechanisms are also launched. Detection approaches include statistical, soft-computing, clustering, knowledge based and classifiers [9].In the section 2 architecture of the DDoS attacks are expl-ained, In section 3 the different techniques are preset which are used to detect the DDoS attacks and in section 4 and 5 datasets and issues and challenges are explained respectively.

II. DDoS ATTACK ARCHITECTURE

As stated in [3], A DDoS attack can be defined as an attack which uses a large no. of computers to launch a coordinated dos attack against a single machine or multiple victim machines. A DDoS attack is composed of several elements like attackers, victim, zombies and reflectors. The DDoS attacks of two types are direct DDoS attacks and indirect DDoS attacks. Generally, DDOS attacks can also be grouped in three types- service overloading, message flooding and clogging. Service overloading occurs when floods of request are made to a server process. Message flooding occurs when a user slows down a system on the network; it prevents the system from processing its normal workload. Clogging is the type of attack that rejects the three way handshaking in the TCP. It leads to exhaustion of the system resources [6]. DDoS attacks mainly take advantage of the architecture of the Internet and this is what makes them powerful. While designing the Internet, the prime concern was to provide for functionality, not security.[6] Internet security is highly interdependent. No matter how secure a victim's system may be, whether or not this system will be a DDoS victim depends on the rest of the global Internet [15, 16]. Internet resources are limited. Every Internet host has limited resources that sooner or later can be exhausted by a sufficiently large number of users.

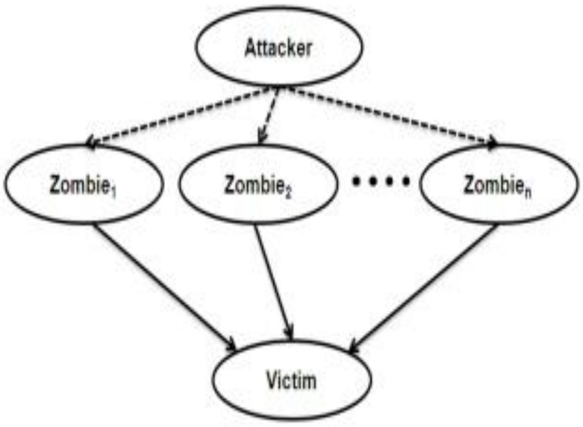

Fig. 1: Direct DDoS Attack [4]

Many against a few: If the resources of the attackers are greater than the resources of the victims, the success of the attack is always definite.

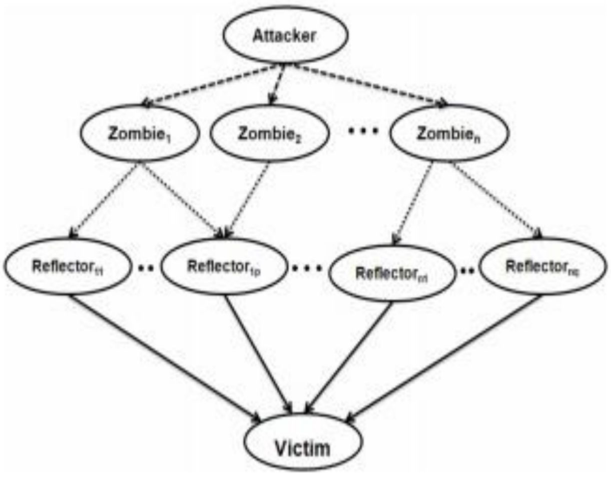

Fig. 2: Indirect DDoS Attack [4]

III. OVERVIEW OF DDOS ATTACK DETECTION

The seriousness of the DDoS problem and the increased frequency of DDoS attacks have led to the advent of numerous DDoS defense mechanisms. Some of these mechanisms address a specific kind of DDoS attack such as attacks on Web servers or authentication servers. Other approaches attempt to solve the entire generic DDoS problem. Most of the proposed approaches require certain features to achieve their peak performance, and will perform quite differently if deployed in an environment where these requirements are not met. As is frequently pointed out, there is no “silver bullet" against DDoS attacks. Therefore we need to understand not only each existing DDoS defense approach, but also how those approaches might be combined together to effectively and completely solve the problem. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature based systems which can only detect attacks for which a signature has previously been created. In order to determine what attack traffic is, the system must be taught to recognize normal system activity. This can be accomplished in several ways, most often with artificial intelligence type techniques and second is signature based works as by reading the files of computer and cross referencing their contents with the ‘code signatures, belonging to the known viruses. A library code signature is updated and refreshed constantly by the antivirus software vendor. If a virtual signature is detected the software acts to protect the user system from damage [18].

IV. CLASSIFICATION OF DETECTION

Reactive mechanisms strive to alleviate the impact of an attack on the victim. In order to attain this goal they need to detect the attack and respond to it. The goal of attack detection is to detect every attempted DDoS attack as early as possible and to have a low degree of false positives. Upon attack detection, steps can be taken to characterize the packets belonging to the attack stream and provide this characterization to the response mechanism. We classify reactive mechanisms based on the attack detection strategy into mechanisms that deploy pattern detection, anomaly detection, hybrid detection, and third-party detection.[18]

A. Mechanism with Pattern Attack Detection

Mechanisms that deploy pattern detection store the signatures of known attacks in a database. Each communication is monitored and compared with database entries to discover occurrences of DDoS attacks. Occasionally, the database is updated with new attack signatures. The obvious drawback of this detection mechanism is that it can only detect known attacks, and it is usually helpless against new attacks or even slight variations of old attacks that cannot be matched to the stored signature. On the other hand, known attacks are easily and reliably detected, and no false positives are encountered. [18]

B. Mechanism with Anomaly Detection

Mechanisms that deploy anomaly detection have a model of normal system behavior, such as a model of normal traffic dynamics or expected system performance. The current state of the system is periodically compared with the models to detect anomalies. The advantage of anomaly detection over pattern detection is that unknown attacks can be discovered.

C. Threshold setting

Anomalies are detected when the current system state differs from the model by a certain threshold. The setting of a low threshold leads to many false positives, while a high threshold reduces the sensitivity of the detection mechanism. [18]

D. Model update

Systems and communication patterns evolve with time, and models need to be updated to reflect this change. Anomaly based systems usually perform automatic model update using statistics gathered at a time when no attack was detected. This approach makes the detection mechanism vulnerable to increasing rate attacks that can mistrain models and delay or even avoid attack detection. [18]

E. Mechanism with Hybrid Attack Detection

Mechanisms that deploy hybrid detection combine the pattern-based and anomaly-based detection, using data about attacks discovered through an anomaly detection mechanism to devise new attack signatures and update the database. Many intrusion detection systems use hybrid detection. If these systems are fully automated, properly extracting a signature from a detected attack can be challenging. The system must be careful not to permit attackers to fool it into detecting normal behavior as an attack signature, or the system itself becomes a denial-of-service tool [18].

F. Mechanism with Third Party Attack

Mechanisms that deploy third-party detection do not handle the detection process themselves, but rely on an external message that signals the occurrence of the attack and provides attack characterization. Examples of mechanisms that use third-party detection are easily found among trace back mechanisms. The goal of the attack response is to relieve the impact of the attack on the victim, while imposing minimal collateral damage to legitimate clients of the victim.[18]

V. RELATED WORK

A. Statistical approach to detect the DDoS attacks

The statistical approach is used to identify the DDoS attacks by computing entropy and frequency – sorted distributions of selected packet attributes. The detection accuracy and performance are analyzed using live traffics traces from a variety of network environments ranging from point in the core of the internet to those inside an edge network [5].Statistical properties of normal and attack patterns can be exploited for detection of DDoS attacks. Generally a statistical model for normal traffic is fitted and then a statistical inference test is applied. [4]

B. Information Entropy

Entropy is a concept identified by Shanon in 1948. Entropy is a quantity, a measure of the uncertainty of a random variable [7]. Let an information source have an independent symbol each with probability of choices p_i [5]. Then, the entropy H is defined as,

$$H = -\sum_{i=1}^{N} p_i \log_2 p_i \quad (1)$$

Hence, entropy can be computed on a sample of consecutive packets [5]. As stated in [7] the two types of entropy based computation approaches are used: Compression entropy using a data compression and modified entropy estimator; called fast entropy. The function of the basic properties of entropy is defined as a concave function of the distribution. The entropy value equals 0 when p = 0 or 1.Similarly, the entropy is maximum when p=1/2 .This property easily can be used in network traffic monitoring. If network traffic changes from normal to abnormal status such as when the DDoS attacker sends a bulk of packets with the same port no., the entropy of this port number will be decreased .By contrast, under normal conditions, the entropy of the port number will be increased. This phenomenon can be applied to various network information such as source IP address, destination IP address, source port, total number of packets, and even in the data clustering schemes. It is observed through experimentation that while a network is not under attack, the entropy values for various header fields each fail in a narrow range. While the network is under attack with current attack tools, these entropy values exceed these ranges in a detectable manner. The algorithm is used to compute the entropy based on the computation of packets entropy of a source will be calculated through a sliding window of fixed width, W. The probability ability value in the algorithm is actually the frequency of occurrence of each unique symbol is divided by the total number of symbols in the sample. The following steps are used to calculate the value of entropy: Compute the entropy of the first W packets with reference to the specific header parameters. Isolate the term in the summation corresponding to the first probability of symbol in the window and also the value for the corresponding probability. Slide the window so the new first term and the next w-1 consecutive terms are contained in the window. Isolate the term in the summation corresponding to the probability of the symbol acquired from shifting the window and subtracts off the terms isolated in steps in 2nd and 4th from the value computed in the first step and after that recomputed the affected probabilities for the current window of data. Using the values computed in the last step and add the two missing terms in the from the entropy summation back in and compare this new entropy value to the previous entropy computations. After that repeat all the steps to determine entropy values. The Window size, W is a tunable parameter that controls how much smoothing of short term fluctuations the detector will do. Increasing .It will reduce the rate of false positive resulting from brief and presumably insignificant anomalies and we should be kept small enough the attacks are detected quickly [1].

C. Chi-Square Method

Person's chi - square test is used to verify the difference between the measurement and expected distribution. For a sample of N packets, let B the no. of available bins. Define N_i as the no. of packets whose value falls in ith and n_i as the expected no. of packets and it can be defined as:

$$\chi^2 = \sum_{i=1}^{B} (N_i - n_i)^2 \div n_i \quad (2)$$

However, this can be achieved through "binning" that is a combining a set or range of possible values and treating them as one [5]. When the N_i and n_i values are large and the N measurements are independent and drawn from the expected distributions. This value follows the well-known chi –square distribution with B-1 degrees of freedom [5]. These assumptions do not typically hold for the packet field values even under normal conditions. Hence, comparison with the chi square distribution is of limited utility [5] .The robustness and the scalability of chi square mechanism over Canberra method for real time intrusion detection in large network [9]. They tested the method with different dataset containing both normal and intrusive activities and proved the good detection ratio. In high speed networks, the detection based on the packets can be expensive and while studying the chi – square to remove the expensiveness the use of chi – square techniques over flow data for network monitoring and anomaly detection are suggested. [10]

D. Knowledge based method

In this section .an expert system approach is proposed for the detection of DDoS attack. The defending system based on expert system is proposed to solve the problem of DDoS attacks completely. In order to detect and filter the garbage traffic produced by DDoS attacks, an expert system consisting four phases [1].

E. Knowledge construction phase
The prior knowledge such as detecting rules, state transition rules is explained in the knowledge construction phase [1].

F. Detecting phase
The system state is transformed from normal state to attacked state to attacked state by the event of attack.

G. Filtering phase
When the system state switched to attacked state, then the traffic will be selected for dropping adaptively in filtering phase [1]. In knowledge-based approaches, network events are checked against predefined rules or patterns of attack. In these approaches, general representations of known attacks are formulated to identify actual occurrences of attacks. Examples of knowledge-based approaches include expert systems, signature analysis, self-organizing maps, and state transition analysis. As in stated in [17], heuristic along with a data structure called MULTOPS (Multi-Level Tree for Online Packet Statistics), that monitor certain traffic characteristics which can be used by network devices such as routers to detect and eliminate DDoS attacks. MULTOPS is a tree of nodes that contains packet rate statistics for subnet prefixes at different aggregation levels. Expansion and contraction of the tree occurs within a pre-specified memory size. A network device using MULTOPS detects ongoing bandwidth attacks by the presence of a significant and disproportional difference between packet rates going to and coming from the victim or the attacker. Depending on their setup and their location on the network, MULTOPS equipped routers or network monitors may fail to detect a bandwidth attack that is mounted by attackers that randomizes IP source addresses on malicious packets. MULTOPS fails to detect attacks that deploy a large number of proportional flows to cripple a victim.

H. Other Data Mining and Machine learning methods
An effective defense system to protect network servers, network routers, and client hosts from becoming handlers, zombies, and victims of DDoS flood attacks is presented in [11]. The Net Shield system protects any IP-based public network on the Internet. It uses preventive and deterrent controls to remove system vulnerabilities on target machines. Adaptation techniques are used to launch protocol anomaly detection and provide corrective intrusion responses. The Net Shield system enforces dynamic security policies. Net Shield is especially tailored for protecting network resources against DDoS flood attacks. Chen et al. [12] present a comprehensive framework for DDoS attack detection known as DDoS container. It uses a network based detection method to overcome complex and evasive types of DDoS attacks. It works in inline mode to inspect and manipulate ongoing traffic in real time. By continuous monitoring of both DDoS attacks and legitimate applications, DDoS container covers stateful inspection on data streams and correlates events among different sessions. It proactively terminates the session when it detects an attack. Lee et al. [13] propose a method for proactive detection of DDoS attacks by exploiting an architecture consisting of a selection of handlers and agents that communicate compromise and attack. The method performs cluster analysis. The authors experiment with the DARPA 2000 Intrusion Detection Scenario specific Dataset to evaluate the method. There results show that each phase of the attack scenarios partitioned well and can detect precursors of a DDoS attack as well as the attack itself. There results show that each phase of the attack scenario is partitioned well and can detect precursors of a DDoS attack as well as the attack itself. Sekar et al. investigate the design space for in-network DDoS detection and propose a triggered, multi-stage approach that addresses both scalability and accuracy. Their contribution is the design and implementation of LADS (Large-scale Automated DDoS detection System). The system makes effective use of the data (such as Net Flow and SNMP feeds from routers) readily available to an ISP. Rahmani et al. [17] discuss a joint entropy analysis of multiple traffic distributions for DDoS attack detection. They observe that the time series of IP flow numbers and aggregate traffic sizes are strongly statistically dependent.

Table. 1: General Comparison of DDOS Attack Detection Methods

Technique Used	Objective	Remarks
Statistical Technique Laura Feinstein, Dan Schnackenberg, Ravinda Balupari, IIDarrell Kindred[5]	To identify DDoS attacks	In this statistical method is used to identify ddos attack by using entropy and frequency sorted distributions
Information Entopy theory Giseop No, Ilkyeun Ra[7]	Detection of DDoS attack	It is an entropy based intrusion detection approach and it uses the computation time for calculating information entropy.
Chi Square Method is Used under Statistical Approach Shunsuke Oshima, Arata Hirakawa, Takuo Nakashima, Toshinori Sueyoshi [8]	To defend DDoS attacks	Chi square method is used to analyses the amount of incoming packets basedon destination port no.
Secure Transport		It suggests a

Protocols based technique A. Z. Ghavidel, B. Issac [6]	Detection of DDoS attacks	symmetric key exchange and of secret codes by using UDP and TCP protocols.
Filtering Policy Guo-Yin Zhang ,Jian Li ,Guo –Chang Gu[1]	To defend DDoS attacks	It uses the filtering policy which is based on access control information and used to observe the behavior of DDoS attacks.
Flow based technique Muraleedharan N,Arun Parmar,Manish kumar[10]	Detection of DDoS attacks	Ip flow base system IP flow characteristics is used with chi square detection.

In this table, the various techniques for the detection of DDoS attacks like statistical method, entropy based technique, detect the DDoS attack by using the destination port no and by using the IP flow characteristics with chi –square detection mechanism.

VI. ISSUES AND CHALLENGES

Many methods for DDoS detection have been given in the literature, but only a few of them have been applied in a real network environment and work effectively because the implementation and designing is not easy in a real way. There are many challenges are available to detection system are following .In a DDoS attack, attackers try to make a service unavailable to its legitimate clients and launch the attack using a large number of zombies distributed in different networks. [6]. A DDoS defense mechanism cannot simply be judged based on its performance with a standard fixed dataset containing normal and a few attack packets. It must be scalable to real networks for actual deployment [6]. With the continuing progress in Internet technologies, attackers are developing and launching new attacks with greater sophistication day by day. [6]. the detection method should be dependent ona minimum number of input parameters if not independent of parameters and should also be based on a minimum number of traffic parameters or features [6]. In DDoS attacks with a large number of agents, attack behavior often conforms well to normal behavior. In such a situation, for a DDoS defense mechanism aiming to provide a near real time solution may have to be based on an incremental clustering algorithm to segregate the attack from normal traffic. This requires an appropriate proximity measure that works sensibly, quickly and reliably [6].

VII. CONCLUSION

In this paper, the overview of DDOS attacks and detection mechanism of DDoS attacks has been presented. The challenges and issues are also discussed. It is very difficult to provide security to internet from DDoS attacks because the implementation and designing of the detection system is very difficult but there are various techniques like entropy based technique , chi –square method, IP flow characteristics by using chi square method by using destination port no and secure transport protocols are available to detect the DDoS attacks.

VIII. ACKNOWLEDGEMENT

The author is grateful to Mr. Abhinav Bhandari, Assistant Professor, Department of Computer Engineering, Punjabi University, Patiala for their support and guidance.

REFRENCES

[1] Guo-Yin Zhang, Jian Li, Guo-Chang Gu: Research on Defending DDoS Attack –An Expert System Approach .0-7803-8566-7/04© 2004 IEEE International Conference on Systems, Man and Cybernetics)

[2] Specht, S.M. and Lee, R.B. (2004) Distributed Denial of service: Taxonomies of attacks, tools and counter measures. Proceeding the ISCA 17thInternational Conference on Parallel and distributed computer systems, San Francisco, California, USA, 15-17 September ,pp. 543-550.ISCA

[3] Batishchev. A.M. (2004).LOIC. http://sourceforge .net/projects/loic/.

[4] Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharya, J. K. Kalita: Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions.

[5] Laura Feinstein Dan, Schnackenberg, Ravindra Balupari, Darrell Kindred: Statistical Approaches to DDOs attack Detection and Response. In Proceeding of the DARPA Information Survivability Conference and Exposition (DISCEX'03.

[6] A. Z. Ghavidel (Student),B .Issac, Member IEEE.1-4244-1470-9/07©2007 IEEE

[7] Giseop No, Ilkyeun Ra: An Efficient and Reliable DDoS Attack Detection using a Fast Entropy Computation Method. 978-1-4244-4522-6/09. ©2009 IEEE.

[8] Shunsuke Oshima, Arata Hirakawa, Takuo Nakashima, Toshinori Sueyoshi: DoS/DDoS Detection Scheme using Statistical Method based on the Destination Port Number.978-0-7695-3762-7/09©2009 IEEE.

[9] Sayed Masun Emran, Nang YE: robustness of chi-square and Canberra distance Metrics for computer Intrusion Detection, Quality and Reliability Engineering International, 2002.

[10] Muraleedharan N, Arun Parmar, Manish Kumar: A Flow Based Anomaly Detection using Chi-square technique.978-1-4244-4791-6/10©2010 IEEE.

[11] Hwang, K., Dave, P. and Tanachaiwiwat, S., (2003) Netshield: Protocol Anomaly Detection with data mining against DDoS attacks. Proceeding of the 6thInternational Symposiunon Recent Advances in IDS, Pittsburgh, PA, 8-10 September mpp.8-10.Springer-Verlag.

[12] Chen, Z., and Delis, A. (2007): An inline detection and Prevention Framework for distributed denial of service attacks.comp.,J.,50,7-40.

[13] Lee, K., Kim,J., Kwon ,K.H., Han .Y., and Kim s.(2008):DDoS attack detection method using cluster analysis. Expert Systems with Applications, 34, 1659-1665.

[14] Douligeris C. Mitrokosta, A. (2004) DDoS Attacks and Defense Mechanisms: Classification and State-of- the-Art. Computer Networks,44,643-666

[15] Houle, K. J. and Weaver, G. M. (2001) Trends in denial of service attack technology. Technical Report v1.0.CERT and CERT coordination center, Carnegie Mellon University, Pittsburgh, PA.

[16] Wong, T. Y., Law, K. T., Lui, J. C. S., and Wong, M.H. (2006) an efficient distributed algorithm to identify and trace back DDoS traffic. Comp. J., 49, 418–442

[17] Gil, T. M. and Poletto, M. (2001) MULTOPS: a data structure for bandwidth attack detection. Proceedings of the 10th conference on USENIX Security Symposium - Volume 10, Berkeley, CA, USA, 13-17 August 3. USENIX Association Berkeley

[18] A Taxonomy of DDoS attacks and DDoS Attack defense Mechanism Jelena Mirkovic, Janice Martin and Peter Reiher Computer Science Department University of California, Los Angeles Technical report #020018