International Journal of Engineering Research & Management Technology ISSN: 2348-4039

September- 2014 Volume 1, Issue-5

Email: editor@ijermt.org www.ijermt.org

Anomaly Based Detection of DDoS Attacks: A Review

Gulshan Kumar
Department of Computer Applications
Shaheed Bhagat Singh State Technical Campus
Ferozepur, Punjab, India

Jaswinder Singh
Department of Computer Engineering
Punjab Technical University
Jalandhar, Punjab, India

Monika Sachdeva , Krishan Kumar
Department of Computer Science and Engineering
Shaheed Bhagat Singh State Technical Campus
Ferozepur, Punjab, India

ABSTRACT:
Internet is widely spread in each corner of the world. With rapidly growing the use of computer resources and network over internet, it becomes the serious issue for network security. There are number of issues for network security like integrity, authentication, validity, non-repudiation, availability etc., but the availability of internet is very critical issue for the economic growth. One of the major security problems in the current Internet, is the denial-of-service (DoS) attack always attempts to stop the victim from serving legitimate users. Denial-of-service (DoS) and distributed-denial-of-service (DDoS) attacks cause a serious danger to Internet operation. An important method for stopping DDoS attacks is to detect attackers and masters (handlers). Detection of DDoS attacks is a challenging problem for network security. The proposed work aims at detecting DDoS attacks in the network using Entropy Based Anomaly Detection Algorithm. This paper presents the updated review of anomaly based detection methods using entropy and discuss the method for detection of DDoS attack using host based address entropy and change-point monitoring.

Keywords: DoS, DDoS, Availability, Entropy, Detection, Intrusions.

1. INTRODUCTION

Internet is largely used in government, military and commercial institutions. The new emerging protocols and new network architectures permit to share, consult, exchange and transfer information from any place all over the world to any other one situated in different country. Despite the above progress, the actual networks are becoming more complex and are designed with functionality while security is not considered as a main goal [30]. Internet security includes aspects such as confidentiality, authentication, integrity, non repudiation and availability. Traditional security solutions concentrate on protecting the network connection's confidentiality and integrity, protecting the server from break-in and protecting the client's private information from unintended disclosure. A lot of protocols and mechanisms have been developed that address these issues individually [15,16]. One area that has been neglected so far is service availability in the presence of denial of service (DoS) attacks, and their distributed variants (DDoS).

Security objectives are violated by set of activities is called intrusions. Thus secure information requires four phases that provide (1) protection: automatic protection from intrusions; (2) detection: automatic detection of intrusions; (3) reaction: automatic reaction or alarm when system is intruded; (4) recovery: repair or recovery of loss caused due to intrusion [28]. The perfect detection is very important among these phases of intrusion. Computers connected through internet are used for effective communication, transforming secure information, number of online transactions and other online facilities that becomes very important part in our daily life. Computers are exposed to diverse intrusions from World Wide Web. To protect the computers from these unauthorized attacks, effective intrusion detection system needed.Intrusion detection techniques of two types namely; Signature based detection and Anomaly based detection.

One of the major security problems in the current Internet, a denial-of-service (DoS) attack always attempts to stop the victim from serving legitimate users. Denial-of-service (DoS) and distributed-denial-of-service

(DDoS) attacks cause a serious danger to Internet operation. A distributed denial-of-service (DDoS) attack is a DoS attack which relies on multiple compromised hosts in the network to attack the victim [19]. There are mainly two types of DDoS attacks. The first type of DDoS attacks aim of attacking the victim to force it not to serve legitimate users by exploiting software and protocol vulnerabilities. The second type of DDoS attack is based on a massive volume of attack traffic, which is known as a flooding-based DDoS attack. A flooding-based DDoS attack attempts to congest the victim's network bandwidth with real-looking but unwanted data. As a result, legitimate packets cannot reach the victim due to a lack of bandwidth resource.

DDoS attacks are comprised of packet streams from disparate sources. These attacks engage the power of a vast number of coordinated Internet hosts to consume some critical resource at the target and deny the service to legitimate clients. The traffic is usually difficult to distinguish legitimate packets from attack packets. The attack volume can be larger than the system can handle. A DDoS victim can suffer from damages ranging from system shutdown and file corruption, to total or partial loss of services [6]. There are no apparent characteristics of DDoS streams that could be directly used for their detection and filtering. The attacks achieve their desired effect by the sheer volume of attack packets.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are specific attacks that targets the availability of networks. They access networks, servers, services or other resources in order to prevent legitimate users An important method for controlling DDoS attacks is to detect attackers and masters (handlers). Attack detection techniques aims to detect DDoS attack in process of an attack and characterise to discriminate attack traffic from legitimate traffic [14,15].
The responsibility of Anomaly based Attack detection technique is identify various types of attacks like DDoS attacks or attack packets. The False Positive Ratio (FPR) and False Negative Ratio (FNR) can quantitatively measure the effectiveness of attack detection. False Positive Ratio is given by the number of packets classified as attack packets (positive) by a detection system that are confirmed to be normal (negative), divided by the total number of confirmed normal packets. The False Negative Ratio, on the other hand, is given by the number of packets classified as normal (negative) by a detection system that are confirmed to be attack packets (positive), divided by total number of confirmed attack packets [26].

The main aim of Attack detection techniques is to detect DDoS attacks by analyzing host or network ‘s behavior. They analyse the behavior of system and network under normal conditions and generate profiles for normal usage. When they detect an abnormal behavior, they invoke some prevention methods.

According to [7] in order to meet the increasing need for detection and response, researchers face following major issues, like a) A router routes the attack path and automatically recognizes the attack in network and also adjust its flow of traffic . b)The response and detection techniques should be adaptable to a wide range of network environments. c) The accuracy of detection of attacks should be as much as possible. False positives (fp) can lead to inappropriate responses that cause denial of service to legitimate users. False positives are the amount of attack detected when it is actually normal, called as false alarm.False negatives (fn) result in attacks going unnoticed. False negatives means the amount of normal detected when it is actually attack, namely the attack which can be detected by IDS. d). Attack response should employ intelligent packet discard mechanisms to reduce the downstream impact of the flood while preserving and routing the non-attack packets. e). The detection method should be effective because of availability of variety of attack tools today and also the detection method should be robust against future attempts by attackers to prevaricate detection.

2.LITERATURE REVIEW

The first well-publicized DDoS attack in the public press was in February 2000. On February 7, *Yahoo!* was the victim of a DDoS during which its Internet portal was inaccessible for three hours. On February 8, Amazon, Buy.com, CNN, and eBay were all hit by DDoS attacks that caused them to either stop functioning completely or slowed them down significantly. And, on February 9, E*Trade and ZDNet both suffered DDoS attacks. Analysts estimated that during the three hours Yahoo was down, it suffered a loss of e-commerce and advertising revenue that amounted to about $500,000. According to book seller Amazon.com, its widely

publicized attack resulted in a loss of $600,000 during the 10 hours it was down. During their DDoS attacks, Buy.com went from 100% availability to 9.4%, while CNN.com's users went down to below 5% of normal volume and Zdnet.com and E*Trade.com were virtually unreachable [34].
(Jain, 2011) [1] proposed a scheme to find out the source of the attack with the help of entropy variation in dynamic by calculating the packet size, which shows the variation between normal and DDOS attack traffic, which is fundamentally different from commonly used packet marking techniques. (Feinstein, et al., 2003) [7] developed methods to identify DDoS attacks by computing entropy and frequency-sorted distributions of selected packet attributes. (Gupta et al.,2008) [9] proposed a novel framework that deals with the detection of variety of DDoS attacks by monitoring propagation of abrupt traffic changes inside ISP Domain and then characterizes flows that carry attack traffic. Two statistical metrics namely, Volume and Flow are used as parameters to detect DDoS attacks.

(Nychis et al., 2008) [11] proposed that the time series of entropy values of the address and port distributions are strongly correlated with each other and provide very similar anomaly detection capabilities.(Yu and Zhou, 2008) [37] presents and proved the effectiveness of their method in theory to discriminate the DDoS attacks from legitimate accessing by using information theory parameter, entropy rate. (Yuan and Mills, 2005) [12] proposed a method for early attack detection. Using only a few observation points, proposed method can monitor the macroscopic effect of DDoS flooding attacks. (Peng, 2003) [18] prpposed a practical scheme to defend against Distributed Denial of Service (DDoS) attacks based on IP source address filtering, in which the edge router keep tracks a history of all the legitimate IP addresses those are already appeared in the network. History decides whether to admit or block an incoming IP packet due to overloading of router.. Unlike other proposals to defend against DDoS attacks, thescheme works well during highly-distributed DDoS attacks, i.e., from a large number of sources. They present several heuristic methods to make the IP address database accurate and robust, and presents results that demonstrate the effectiveness to defend against distributed DDoS attacks.

3.METHODOLOGY

3.1. Techniques for Intrusion Detection

Each malicious activity or attack has a specific pattern. The patterns of only some of the attacks are known whereas the other attacks only show some deviation from the normal patterns. Therefore, the techniques used for detecting intrusions are based on whether the patterns of the attacks are known or unknown. The two main techniques used are:

A. Anomaly Based Detection System: It is based on the assumption that intrusions always reflect some deviations from normal patterns. Anomaly detection may be divided into static and dynamic anomaly detection. A static anomaly detection is based on the fact that when there is a portion of system which is monitored by anomaly detection that does not change. Actually the code that is the static part of system and the correct functionality of system depends upon constant portion of the data, is also code of system.
Dynamic anomaly detection mainly operates on audit records or on monitored network traffic data. Audit records of operating system that records only event of interest rather than record all events[33].
The normal state of the network, traffic load, breakdown, protocol and packet size are defined by the system administrator in advance. Thus, anomaly detector compares the current state of the network to the normal behavior and looks for malicious behavior. It can detect both known and unknown attacks.[29]
Detects the abnormal behaviours of host or network. It stores the features of user's usual behaviours hooked on database, and then it compares user's present behaviour with database. The deviation of the monitored traffic from the normal profile is measured [31] [32].

B. Misuse Detection System: It is based on the previous knowledge of known patterns of previous attacks and system vulnerabilities. Misuse detection continuously compares current activity to known intrusion patterns to ensure that any attacker is not attempting to exploit known vulnerabilities. To accomplish this task, it is required to describe each intrusion pattern in detail [29].

Table 1: Merits/demerits of Detection Systems

Detection System	Advantages	Disadvantages
Anomaly Based	• Can detect unknown attacks. • Can also detect variation to common attacks. • Can detect novel attacks against software systems and deviation of normal usage of programs. • Resource consuming is low. • Avoids to slow down the throughput.	• It raises high false alarm. • Limited by training data.
Misuse Based	• Raises fewer false alarms. • Integrate the human knowledge • Rules are pre-defined	• Unable to detect unknown attacks. • Requires much resources

3.2. Where to do Intrusion Detection According to the monitored system, the source of input information can be on a host or network or host and network. Thus IDS is further classified into three categories as follows :

i) Network-based intrusion detection system (NIDS) It examines or checks the data exchanged between different computers on the network.It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems gain access to network traffic by connecting to a network hub, network switch configured for port mirroring, or network tap.

In this plateform, Network IP-address based entropy is used to detect the presence of attacks. According to the class of network, network based entropy is categorized according to the class of network like 8-bit entropy is used as performance metric to detect attacks in class-A networks where 16-bit entropy and 24-bit entropy are used for class-B and class-C networks respectively.

ii) Host-based intrusion detection system (HIDS) It examines or checks the data that is held on individual computer or host.The network architecture of host based intrusion detection system is agent based, means that a software agent resides on each of host that will be controlled by the system [33]. In other words, It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host activities and state. In a HIDS, sensors usually consist of a software agent.In this 32-bit entropy is used as performance evaluation metric to identify attacks in networks.This entropy value is based on IP address of individual host in the network, so called host based or source based entropy.

iii) Hybrid Intrusion detection system (Hybrid IDS) It is the combined technique that is used to complements the drawbacks of each. It is able to monitor the network traffic for a specific host to complements HIDS system.; it is different from the NIDS that monitors all network traffic . In computer security, a Network Intrusion Detection System (NIDS) is an intrusion detection system that analyses the network traffic on computer network for indication of malicious activity in order to attempts to discover unauthorized access to a computer network [29].

3.3 Evaluation Metric

In order to detect DDoS or Novel attack in a network, a performance metric can be used as anomaly detection based parameter, is called entopy. Entropy can be defined as measurement of the randomness based on host IP addresses on a web server. Entropy can be calculated as:

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

Where p_i is the probability value that defines rate of recurrence of unique symbol by total number of all symbols.

Host IP address based entropy can be calculated for anomaly base attack detection. Source IP address based entropy or Host IP address based entropy is also called 32-bit entropy [34].

4. CONCLUSION

This paper presents a review on detection system for DDoS attacks or worms, these detection techniques are based on locally findings of anomalies.Discovery and distinctiveness facilitates of attack type provides association of distributed detection systems in heterogeneous environments and may simplify countermeasures that can facilitates by other tasks. The entropy of flows at a router, router entropy can be calculated, if the router entropy is less than a given threshold, then a attack alarm is raised; If the entropy rates are more than a given value, then there is is a pour of legitimate accessing, otherwise we can confirm that there is an attack. Once the DDoS or Dos attacks recognized among the network then entropy value vary in wide range. In order to ensure flexibility and extensibility to future requirements and detection methods, both processing control and identification build on a generalized modeling of the entities participating in attack detection. The proposed anomaly-based attack identification consists of a rule-based mechanism and a subsequent demanddriven geometric classifier. The simulative evaluation showed that the identification is able to return accurate results but to a certain degree depends on the correctness and accuracy of the preceding anomaly detection.

REFERENCES

1. J. Anusha, "Entropy Based Detection of DDOS Attacks", International Journal of Soft Computing and Engineering (IJSCE), Vol. 1, pp. 564-567, 2011.
2. G. Carl, G. Kesidis, R. R. Brooks and S. Rai, "Denial-of-Service Attack- Detection Techniques", Published by the IEEE Computer Society, pp.82-89, 2006.
3. DDoS History In Brief, Available at: "http://www.anml.iu.edu/ddos/history.html". [last accessed October, 2014]
4. C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art", ELSEVIER Journal of Computer Networks, vol.44 no.5, pp. 643-666, 2004.
5. L. Feinstein, D. Schnackenberg, R. Balupari and D. Kindred, "Statistical Approaches to DDoS Attack Detection and Response", Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03), Washington, DC, USA, Vol. 1, pp. 303-314, 2003
6. G. M. Fernandez, J. E. Dıaz-Verdejo, and P. Garcia-Teodoro, "Evaluation of a low-rate DoS attack against application servers", Computers & Security, Vol. 27, ISSN: 0167-4048, pp. 335-354, 2008.
7. B. B. Gupta, M. Misra, and R. C. Joshi, "An ISP Level Solution to Combat DDoS Attacks using Combined Statistical Based Approach", Journal of Information Assurance and Security 2, pp.102-110, 2008.
8. G. Koutepas, , F. Stamatelopoulos, and B. Maglaris, "Distributed Management Architecture for Cooperative Detection and Reaction to DDOS Attacks", Journal of Network and Systems Management, Volume 12, Issue 1, pp.73 - 94 , 2004.
9. G. Nychis, , V. Sekar, D. G.Andersen, H. Kim, and H. ZhangS, "An Empirical Evaluation of Entropy-based Traffic Anomaly Detection", Proceedings of the 8th ACM SIGCOMM conference on Internet measurement,pp. 151-156, 2008.
10. J. Yuan, and K.. Mills, "Monitoring the Macroscopic Effect of DDoS Flooding Attacks", IEEE Transactions on Dependable and Secure Computing, Vol.2, No.4,pp.277-288, 2005.
11. Y. You, "A Defense Framework for Flooding-based DDoS Attacks", Master's Thesis, Queen's University Kingston, Ontario, Canada, 2007.
12. F. Wang, H. Wang, X. Wang, and J. Su, "A new multistage approach to detect subtle DDoS attacks", Journal Mathematical and Computer Modelling, Volume 55, Issues 1–2, pp. 198-213, 2012.
13. M. Sachdeva, G. Singh, K. Kumar, and K. Singh, "Measuring Impact of DDOS Attacks on Web Services", Journal of Information Assurance and Security 5, pp. 392-400, 2010.
14. N. Sidhu, K. Kumar, S.S. Sra, J.S. Sidhu, "An Analysis of DDoS Attacks Impact on Web Services using Real Time Traces", CiiT International Journal of Digital Image Processing Volume 2, No. 10, pp. 422-426, 2010.
15. M. Sachdeva, G. Singh, and K. Kumar, "Deployment of Distributed Defense against DDoS Attacks in ISP Domain", International Journal of Computer Applications (IJCA), Vol. 15, No .2, pp. 25-31, 2011.
16. J. Singh, K. Kumar, M. Sachdeva, and N. Sidhu, "DDoS Attack's Simulation Using Legitimate and Attack Real Data Sets", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, pp. 1-5, 2012.
17. T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems", ACM Computing Surveys, Vol. 39, No. 1, Article 3. pp. 553-557, 2007.

18. T. Peng, C. Leckie and K. Ramamohanarao, "Protection from Distributed Denial of Service Attacks Using History-Based IP filtering", In Proceedings of ICC2003, USA, pp. 482-486, 2003.
19. N. Sidhu, K. Kumar, S. Singh, M. Sachdeva and J. Singh, "Measuring DDoS Attack's Impact on Web Services using Real Time Traces", International Conference on Computer Engineering & Technology,2010 (ICCET'10)" , pp. G174-G179, 2010.
20. J. Mirkovic, E. Arikan, S. Wei, S. Fahmy, R. Thomas, and P. Reiher, "Benchmarks for DDoS Defense Evaluation," Proceedings of the IEEE AFCEA MILCOM, pp. 1-10, 2006.
21. J. Mirkovic, G. Prier, P. Reiher, "Attacking DDoS at the source", Proceedings of ICNP -2002, Paris, France, pp. 312-321, 2002.
22. C. M. Cheng, H. T. Kung, and K. S. Tan, "Use of spectral analysis in defense against DoS attacks", Proceedings of IEEE GLOBECOM 2002, Taipei, Taiwan, pp. 2143-2148, 2002.
23. S. Akbar, K. N. Rao, and J. A. Chandulal, "Intrusion Detection System Methodologies based on Data Analysis", International Journal of Computer Application, Volume 5, No. 2, pp.10 - 20 , 2010.
24. R. Singh and D. Singh , "A Review of Network Intrusion Detection System Based on KDD Dataset", International Journal of Engineering and Technical Science, Volume 5,No. 1,pp. 10-15,2014.
25. M. Gyanchandani, J. L. Rana, and R. N. Yadav, "Taxonomy of Anomaly Based Intrusion Detection System: A Review ", International Journal of Scientific and Research Publication, Volume 2, Issue 12, 2012.
26. R. Gaidhane, C. Vaidya, and M. Raghuwanshi, "Survey: Learning Techniques for Intrusion detection System", International Journal of Advance Foundation and Research in Computer, Volume 1, Issue 2, 2014.
27. M. Aggarwal and Amrita, "Performance Analysis of Different Feature Selection Methods in Intrusion Detection", International Journal of Scientific and Technology Research, Volume 2, Issue 6, 2013.
28. G. Kumar and K. Kumar, "The Use of Artificial-Intelligence-Based Ensemble for Intrusion Detection: A Review", Hindawi Publishing Corporation, Applied Computational Intelligence and Soft Computing,Volume 2012, Article ID 850160,20 pages,2012.
29. R. S. Landge and A. P. Wadhe, "Review of Various Detection Techniques based on data Mining Approach", International Journal of Engineering Research and Application, Volume 3, Issue 3, pp.-430-435, 2013.
30. A. Araar and R. Bouslama, "A Comparative Study of Classification Models for Detection in IP Networks Intrusions", Journal of Theoretical and Applied Information Technology, Volume 64, No. 1,pp- 107-114, 2014.
31. A. A. Raj, "A Study on Data Mining Based Intrusion Detection System", International Journal of Innovative Research in Advanced Engineering, Volume 1, Issue 1, 2014
32. R. Venkatesan, R. Ganeshan, A. A. L Selvakumar, "A Survey on Intrusion Detecion using Data Mining Techniques", International Journal of Computers and Distributed System, 2012.
33. R. Patel, A. Thakkar, and A. Ganatra, "A Survey and Comparative Analysis of Data Mining Techniques for Network Intrusion Detection Systems", International Journal of Soft Computing and Engineering, Volume 2, Issue 1, 2012.
34. J. Singh, M. Sachdeva and K. Kumar, "Detection of DDoS Attacks using Source IP Based Entropy", International Journal of Computer Science Engineering and Information Technology Research, Volume 3, Issue 1,pp. 201-210, 2013.
35. H. Wang, D. Zhang, K.G. Shine, " Change-Point Monitoring for Detection of DDoS Attacks", IEEE Transactions on Dependable and Secure Computing, Volume 1, No. 4, pp. 193-208, 2004.
36. T. Gamer, "Anomaly based Identification of Large Scale Attacks", Institute of telematics, University of Karlsruhe,Germany.
37. Yu, Shui and Zhou,"Entropy based collaborative detection of DDoS Attacks on Community Networks", in proceedings of the 6th Annual IEEE International Conference on pervasive computing and communications, IEEE, Piscataway,N. J.,pp. 566-571, 2008.

AUTHORS

Dr. Gulshan Kumar has received his MCA degree from Guru Nanak Dev University Amritsar (Punjab)India in 2001, and M.Tech. degree in computer science & engineering from JRN Rajasthan Vidyapeeth Deemed University, Udaipur (Rajasthan)-India, in 2009. He got his Ph.D. from Punjab Technical University, Jalandhar (Punjab)-India. He has 12 year of teaching experience. He has 30 international and national publications to his name. Currently, he is working as Assistant Professor in Computer Applications department at Shaheed Bhagat Singh State Technical Campus, Ferozepur (Punjab)-India. He has supervised 03 M. Tech. students for their final thesis. His current research interests in- volve Artificial Intelligence, Network Security, Machine Learning and Databases.

Er. Jaswinder Singh has done B.Tech. omputer Science & Engineering from Punjab Technical University Jalandhar, Punjab, India in year 2006. He had completed M.Tech. in Computer Science & Engineering from Punjab Technical University, Jalandhar, Punjab, India in 2012. Currently he is a research scholar at Punjab Technical University, Jalandhar, Punjab, India. His research interests include Network Security, DDoS attacks, Intrusion Detection, Data Mining and Artificial Intelligence.

Dr. Monika Sachdeva has done B.Tech. Computer Science and Engineering from National Institute of Technology NIT, Jalandhar in 1997. She finished her MS software systems from BITS Pilani in 2002. In, she finished her Ph.D. from Department of Computer Engineering, Guru Nanak Dev University, Amritsar, Punjab, India. Currently She is an Associate Professor, Department of Computer Science & Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur (Punjab)-India. Her research interests include Web Services, Distributed Denial-of-Service, and Design and Analysis of algorithms.

Dr. Krishan Kumar has done B.Tech. Computer Science and Engineering from National Institute of Technology NIT, Hamirpur in 1995. He finished his MS Software Systems from BITS Pilani in 2001. In Feb. 2008, he finished his Ph. D. from Department of Electronic and Computer Engineering at Indian Institute of Technology, Roorkee, India. Currently, He is a Professor at Department of Computer Science & Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur (Punjab)-India. His general research interests are in the areas of Information Security and Computer Networks. Specific research interests include Intrusion Detection, Protection from Internet Attacks, Web performance and Network architecture/protocols.