Analysis of Countermeasures for DDoS Attacks and Evaluation of Entropy based Detection Mechanism using NS2

Raghav Vadehra1, Manjit Singh2, Nitika Chowdhary3

[1,2]ECE Dept., GNDU, RC, Jalandhar

[3]CSE Dept., GNDU, RC, Jalandhar

E-mail: [1]raghav.vadehra12@gmail.com, [2]manu_kml@yahoo.co.in, [3]nitu.expert@gmail.com

Abstract. An attack which deprives legitimate users of the services rendered by a server is termed as a DDoS Attack. Since, attacks like these have already proved to be detrimental for the standard functionalities of the World Wide Web so there crops up an exigency for making our systems proactively smart and cautious in order to counteract such situations. In the view of the past records of the DDoS attacks, sincere researches have been made in this area and several new techniques and methods have been devised as well. However, this does not deter attackers from taking a step back; they are also equally earnest in finding new ways of attacking to outsmart these countermeasures. The paper covers the architecture of Botnet for the basic understanding of DDoS attacks and the need to combat the same. Along with botnet taxonomy, it discusses the methodologies that have been developed and implemented so far. It also talks about the upcoming techniques like Entropy based detection mechanism that are on the radar of development and testing to counterattack the ever growing new nefarious designs of the attackers.

Keywords: Distributed Denial of Service Attacks (DDoS), botnet, throttle, entropy, honeypot, agents, handlers, C&C (Command and Control)

1. Introduction

Internet today is no more a luxury anymore but a necessity which itself triggers out the importance of keeping the World Wide Web absolutely safe. People across the globe use internet for running their businesses worth millions of dollars. A slight leverage on this front can not only result in major loss on the financial grounds but also loss of highly confidential data as well. DDoS is an attack when the legitimate users are rendered paralysed to use the victim system ad access its services [1]. The attack is activated with the help of a network of computers called the Botnet, so before we actually delve into the countermeasures, it becomes mandatory to understand the basic nature and the real motive of these attacks.

The paper gradually unfolds the background of the attacks and explains Botnet lifecycle in Section 2.Section 3 talks about the related works of our research so far. It also explains different ways to counteract these attacks with their associated pros and cons. Section 4 explains the simulation methodology to study entropy based detection mechanism for DDoS attacks. Section 5 discusses the results based on the simulation done in the previous section. Finally the paper culminates with Section 6, which includes the concluding remarks on the DDoS Attacks.

2. Background

The history of these attacks dates back to 1987, when the first attack of its kind called the Morris Worm hit the headlines of every daily journal [2]. Following the trend in 1994 and 1995 were the password sniffing and the IP spoofing attacks respectively. These attacks deprived the authorized users the right of the network security. The world rolled back once again in 2000, when an attack was made on a larger scale where popular websites like Copyright.com, BMI.com went completely offline [3]. The major weapon that makes the DDoS attacks possible is the botnet. Botnet is defined to be a network of similar communicating machines in order to complete a repetitive task and objective [4].The botnet theory revolves around a large pool of compromised machines which are used to disrupt, gather sensitive data or increase army (zombies). In a bandwidth depletion attack these zombies prevent the processing of legitimate requests by congesting the network bandwidth with the unwanted traffic [5].

Table 1. Classification of Botnets based on network [6]

1.	IRC Oriented	The master takes over the control over all the infected computers connected to the IRC master server where in they wait for the commands to be issued by the master
2.	Web oriented	A newly developed classification type wherein the bot is connected to a predefined server on the world wide web and waits for a signal .Example : HTTP botnet

3. Related Work

Looking at the variety of DDoS attacks, it becomes really important to devise such techniques that could themselves act as a shield and help maintain the sustainability of the system against such attacks. This section describes various centralised and decentralised defensive techniques have been developed in order to control the DDoS attacks. Researches done by Monika Sachdeva et al. [7] amplify the differences between centralised and decentralised techniques of defence. In the centralised system, the three modules: Traffic Analysis, Traffic Monitoring ,Traffic Filtering are all executed at a single point i.e. only one router or system is used for all the three purposes. The advantage of such a system is it does not involve a heavy cost in terms of infrastructure or installation. However, the major drawback is that if the system fails that controls the entire unit, then the entire mechanism is rendered paralysed[8, 9].Hence this system is quite vulnerable to attacks since the attackers will have to take down a single unit in order to disrupt the entire defence mechanism. In decentralised system, all the three modules are managed by different devices at different points in the entire network. There are multiple set ups that lead to a successful transmission of the legitimate data even if one of the routers is under attack. Moreover, cracking down this system is not an easy activity for the attackers, although it involves a heavy cost on installation and maintenance [10].

3.1 Some of the existing DDoS Defence Techniques

High bandwidth aggregates are major contributors to the 'congestion based rate limiting criteria’. Pushback technique enables routers to identify such high bandwidth aggregate. If the congested router cannot control the aggregate itself, it requests its upstream neighbour to help in rate limiting[11]. Pushback certainly cannot work in a non contiguous deployment and thus cannot detect attacks that do not congest the core routers. However, attacks are more accurately detected using traffic distribution. Shingang Chen et al. [12] described the parameters based mechanism for the internet service provider (ISP). It also provides anti-DDoS services to customers that completely rely on edge routers filtering traffic and not involving outside routers to avoid stress on the ISP core routers.

Very well on the same grounds Tupakula et al. [13] proposes a controller agent model to counteract the DDoS attacks within the same ISP model. In this model agents represent edge routers and the controller is the trusted entity owned by the ISP. It uses a marking scheme to determine the source of attack. Once the target detects an attack, it sends a request to the controller asking all the agents to mark all the packets to the target. The edge router responsible for the attack can be detected easily based on the markings .The target then sends information to the source to filter out the packets based on the attack signatures and send only the legitimate traffic. This is how zombies are ruled out of the ISP network.

3.2 DDoS Countermeasures

Different defence techniques have evolved to combat DDoS attacks. Some of the countermeasures and challenges associated with their implementation have been discussed below:

Table 2. Countermeasures of DDoS Attacks

Countermeasures	Technique	Pros	Cons
1. Detect or Prevent Potential attacks using Firewalls	Egress filtering i.e. filters is installed on the sub networks of the potential secondary victims [14].	DDoS attacks majorly use a spoofed IP address. This IP can be easily traced by scanning of IP packet headers using a firewall for the packet leaving a network. If the packet meets the base criteria, it is routed outside the sub-network otherwise discarded.	Firewalls lead to increase in cost to help in protecting against DDoS attacks.
	Management Information Base [15]	Router MIB data contains various attributes that indicate different packet and routing statistics. It focuses on developing pattern statistical pattern to identify ICMP, UDP TCP attacks.	It is cumbersome to adjust the network parameters in order to compensate for traffic from illegitimate sources.
2. Mitigating the effects of DDoS Attacks	Load balancing [7]	Network providers can prevent the attack situation by increasing bandwidth in case there is huge inflow of traffic on critical connections.	It is a bit costly method to combat attacks.
	Throttling [16]	In this method, routers are used to regulate incoming traffic to the safer levels. This can prevent flooding based DDoS attacks.	It is very difficult to decipher legitimate traffic from malicious traffic for routers
	IP Traceback technique [17]	The concept involves tracing back the internet traffic back to its source. Thereby, helps to identify the attacker if it uses a spoofed IP address.	High precision is required for tracing the traffic back to its source. It involves a big cost to keep an eye on the entire network

3.3 Most Efficient DDoS Detection Technique

Deterministic Packet Mining (DPM), Probabilistic Packet Marking (PPM) has been suggested to identify the attackers by B.M Patil et al. [18]. However, on further investigations it has been determined that only these two approaches are not enough because these require introducing marks into the individual packets to identify the attackers. Moreover, these are not even scalable enough to be deployed in a real network scenario. In order to overcome these drawbacks, a method based on Entropy variation is used which measures "changes in uncertainty of flows" at a router for a given period of time [19]. If the entropy of the network attribute like Source Address or Flow Id is lesser than the threshold than we can classify it as DDoS attack situation. However, this scheme suffers from a serious drawback of increased false positive rate due to flash events. Krishan Kumar et al. [20] suggested Traffic cluster entropy as another detection method that not only detects DDoS attack but also helps to distinguish DDoS attack from Flash Events.

4. Simulation and Methodology

This section deals with Entropy based mechanism in order to detect Flooding based DDoS attack. NS-2 simulator is used to describe the simulation scenarios. NS-2 is an open source tool used for wireless or wired event based applications. It supports network traffic sources like CBR, FTP and protocols such as UDP, HTTP. Simulation methodology to study Entropy based detection technique is explained with the help of flow diagram as illustrated in Figure 2.

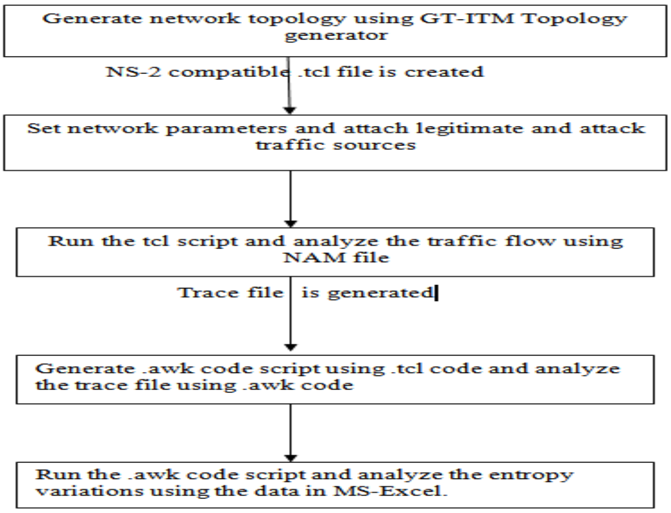
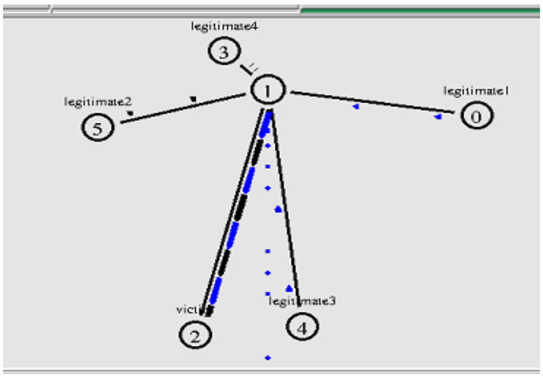

Generate network topology using GT-ITM Topology generator
NS-2 compatible .tcl file is created
Set network parameters and attach legitimate and attack traffic sources
Run the tcl script and analyze the traffic flow using NAM file
Trace file is generated
Generate .awk code script using .tcl code and analyze the trace file using .awk code
Run the .awk code script and analyze the entropy variations using the data in MS-Excel.

Fig. 1 Simulation Methodology

First and foremost network topology is generated using GT-ITM topology generator. Legitimate and illegitimate traffic sources are attached in the network and various network parameters are adjusted. Run the tcl script and monitor the traffic using NAM file. Next phase involves analyzing the trace file using .awk script. And last step involves analysing the entropy variations of Flow Id in case of DDoS attack and comparing the results with the normal scenario.

5. Results and discussion

Detection of DDoS attacks using Entropy method is explained graphically with the help of different scenarios. In subsequent subsection we simulate different topologies with or without the presence of attackers. Figure 2 and 3, illustrate the two scenarios. One is having four legitimate nodes sending traffic to the destination server and other in which the victim server is hit by DDoS attack.



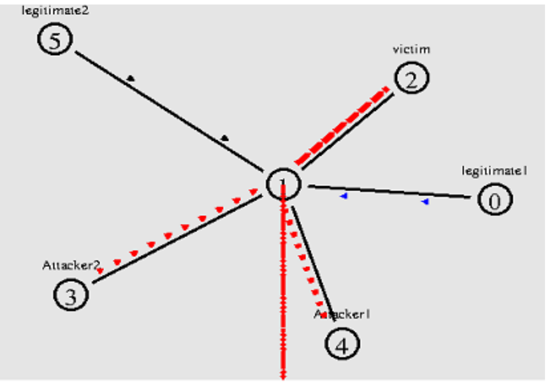
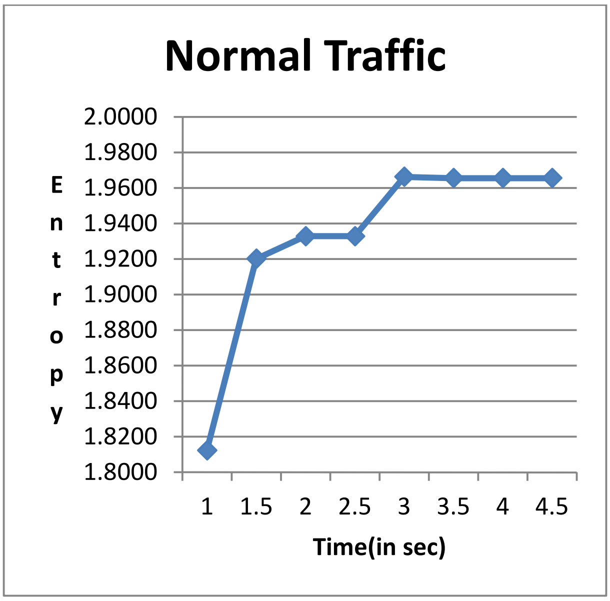


Fig. 2 Network with legitimate users

Fig. 3 Network hit by DDoS attack



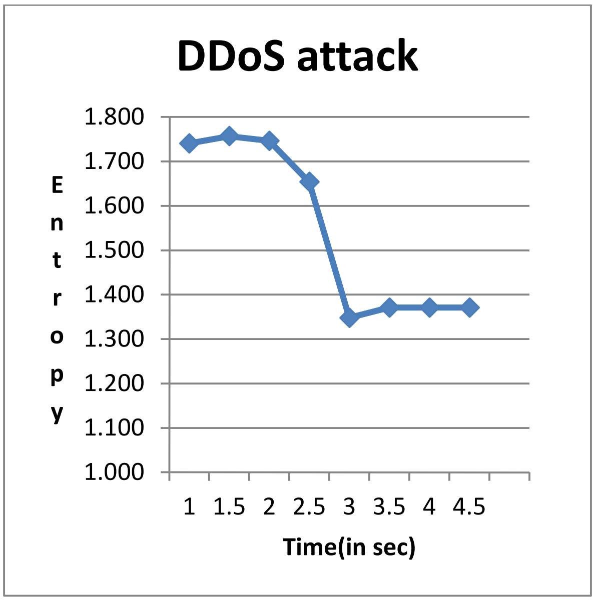


Fig. 4 Graph of entropy obtained after simulation for traffic from legitimate users

Fig. 5 Graph of entropy obtained when network is hit by DDoS attack

From Fig. 4, it is evident that entropy increases as the distribution of traffic is uniform among the four nodes. Since all the nodes are sending packets with nearly same probability and there is no attacker sending traffic at the higher rate. Hence, it is a normal scenario in which the traffic is legitimate. In contrast, from Fig. 5, it is clear that there is a decrease in entropy due to attack as attacker nodes as sending packets at higher rate as compared to legitimate nodes in order to block the resources of the victim server. Hence, entropy of different flows from legitimate nodes increases or remains constant in normal mode whereas it decreases in case of DDoS attacks.

6. Conclusion

This paper gives us provides the deep insight of the defence mechanisms to nullify DDoS attacks. The paper classifies botnets based communication network. It reviews different countermeasures to detect and mitigate these attacks. Moreover, it also implements the generic case of entropy based detection mechanism for the attacks. DDoS attacks pose a serious threat to the present network systems and can lead to critical economic and data losses. Thus, it is very important to develop, verify and implement more comprehensive solutions to tackle these attacks

References

1. V.Buitron, J.Calahorrano, D.Chow, J.Marsh and M.Zogbaum, [Online] "Taxonomy of Botnets." Available at: http://www.cs.northwestern.edu/~ychen/classes/msit458-s09/Botnets_defense.ppt
2. M.Nassar. Denial of Service Attack.(PPT). Available at:http://www.powershow.com/view1/17bb9f-ZDc1Z/Arab_Academy_for_Banking_powerpoint_ppt_presentation
3. E.Alomari, S.Manickam, B.B Gupta, S.Karupayyah and R.Alfaris,Botnet based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art", IJCA, Vol. 49, No.7, pp. 24-32 ,July 2012.
4. A.Tyagi and G.Aghilla, "A Wide Scale Survey on Botnet", IJCA, Vol. 34, No.9, pp. 9-22 (Nov 2011)
5. S.A.Arunmozhi and Y.Venkataramani, "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks", IJNSA, Vol. 3, No.3, pp. 182-187 ,May 2011.
6. 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. 324-335 , Oct. –Dec. 2005.
7. M.Sachdeva, G.Singh, K.Kumar, and K.Singh, "A Comprehensive Survey of Distributed Defence Techniques against DDoS attacks", IJCSNS, Vol.9, No.12, pp. 7-15, Dec. 2009.
8. Papadopoulos, C., Lindell, R., J. Mehringer, Hussain, A. and Govindan,R, "CROSSACK: Coordinated Suppression of Simultaneous Attacks", Proceedings of DISCEX, pp. 2-13, 2003.
9. Keromytis, A. D., Misra, V. and Rubenstein, "D. SOS: An Architecture For Mitigating DDoS Attacks", IEEE Journal on Selected Areas in Communication, Vol. 22, No.1,pp. 176-188 , 2004.
10. Shi W., Xiang, Y., and Zhou, W., "Distributed Defense Against Distributed Denial-of-Service Attacks", Proceedings of ICA3PP 2005, LNCS 3719, pp. 357-362 , 2005.
11. J.Ioannidis and S. M. Bellovin, "Implementing Pushback: Router-Based DefenseAgainst DDoS Attacks", Proceedings of the Network and Distributed System Security Symposium (NDSS'02), pp. 6-8, Feb. 2002.
12. S.Chen,"Perimeter based Defense against High Bandwidth DDoS Attacks", IEEE Transactions on Parallel and Distributed Systems, Vol. 16, No.6, pp. 526-537, June 2005.
13. U.K.Tupakula. and V.Varadharajan "A Practical Method to Counteract Denial of Service Attacks", Proceedings of the 26th Australasian Computer Science Conference, Volume 16, pp. 275-284, Feb 2003.
14. Stephen M. Specht and Ruby B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures", Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, International Workshop on Security in Parallel and Distributed Systems, pp. 543-550, Sep. 2004.
15. Joao B. D. Cabrera, L.Lewis, Xinzhou Qin, Wenke Lee, Ravi K. Prasanth, B. Ravichandran, and Ramon K. Mehra, "Proactive Detection of Distributed Denial of Service Attacks Using MIB Traffic Variables – A Feasibility Study", Integrated Network Management Proceedings, pp. 609-622, 2001.

16. John C. S. Lui, David K. Y. Yau, Feng Liang and Yeung Yam, "Defending Against Distributed Denial-of-Service Attacks with Max-Min Fair Server-Centric Router Throttles", IEEE/ACM Transactions on Networking, Vol. 13, No.1, pp. 29-42, Feb. 2005.
17. A.John, T.Sivakumar, "DDoS: Survey of TracebackMethods",International Journal of Recent Trends in Engineering, Vol. 1, No.2, pp. 241-245, May 2009.
18. Poonam N. Jhadhav and B.M. Patil, "Low rate DDoS Detection method using Optimal Objective Entropy Method", IJCA, Volume 78, No.3, pp. 33-38, Sept. 2013.
19. A.S Syed Nawaz, V.Sangeetha and C.Prabhadevi, "Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud", IJCA, Volume 62, No.15, pp. 33-38, Jan. 2013.
20. M.Sachdeva and K.Kumar, "A Traffic Cluster based Entropy approach to Distinguish DDoS a attacks from Flash Events using DETER Method", ISRN Communications and Networking, Volume 2014, Article Id-259831, Hindawi Publishing Corporation, pp. 1-15, 2014.