JES
Journal of Engineering Sciences
Vol 10, Issue 12, Dec /2019
ISSN NO:0377-9254

Preclude handling DDoS Attacks using Effective Routing schema

Sz.PARVEEN, J SUNIL
Annamacharya Institute of Technology & Science,Kadapa

Abstract: Distributed Denial of Service (DDoS) attacks is the most difficult issues for network security. The attacker utilizes vast number of traded off hosts to dispatch attack on victim. Finding the most likely path satisfying a requested additive Quality-of-Service (QoS) value such as delay. This paper designs two independent architectures for HTTP and FTP which uses an extended hidden semi-Markov model is proposed to describe the browsing habits of web searchers. we propose to advance the state of the art by using a novel distributed divide-and-conquer approach in designing a new data dissemination architecture that efficiently tracks attack sources. This dissertation presents a Distributed denial-ofservice Adaptive ResponsE (DARE) system, capable of executing appropriate detection and mitigation responses automatically and adaptively according to the attacks. introducing randomness and anonymity into the forwarding architecture, making it difficult for an attacker to target nodes along the path to a specific SOSprotected destination. The first to propose a transform-based approach for the QoS routing problem of finding the most likely path to thousands of high-bandwidth flows simultaneously, and conclude that we can truly achieve single packet trace back guarantees with minimal overhead and high efficiency.

Index Terms: Defense, deployment, Types of DDoS Attack. Denial of Service (DOS), FTP and HTTP. Adaptive Response System. SOS-secure overlay service.

1. INTRODUCTION

Distributed Denial of Service (DDoS) is the organized endeavor to bargain the accessibility of system resources or servers . These attacks make money related misfortunes by hindering true blue access servers and online administrations [1]. Routing algorithms that must satisfy a set of constraints, such as maximum bandwidth and/or minimum delay, are often described as QoS Routing algorithms [2]. QoS routing is a difficult problem due to the network dynamics, traffic volatilities and aggregation techniques that make it almost impossible to have an accurate picture of the underlying network state information [3]. To circumvent detection, they attack the victim Web servers by HTTP GET requests and pulling large image files from the victim server in overwhelming numbers. In another case, attackers run a massive number of queries through the victim search engine data base query to bring the server down [4]. Such attacks are called application-layer DDoS (App-DDoS) attacks. The ideal strategy of deploying ingress filters at each subnet connected to the Internet is also impractical, given the limited support that current networks offer [5]. An optimal filtering strategy would thus place the few available filters at appropriate locations in the entire network, exploiting the attack traffic convergence characteristics evident in the frequency-weighted tree [6]. Traffic Redirection Attack Protection System designed for the IPv6 networks. We show how TRAPS is able to provide server protection against DDoS attacks through virtual relocation using the existing Mobile IPv6 protocol [7]. Therefore, no change is required to the end-hosts which are potentially all the Internet nodes [8]. Once inside the overlay, the traffic is tunneled securely for several hops along the overlay to the approved locations, which can then forward the validated traffic through the filtering routers to the target [9].

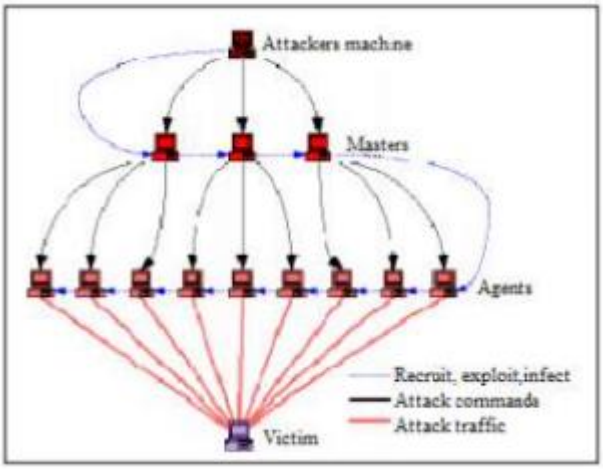

Fig. 1: DDoS attack model.

2. RELATED WORK

The first study for finding the path of highest probability to satisfy a given request from computer networking perspective focused on finding the impact of inaccuracy on the path selection process [10]. The authors analyzed the bandwidth and delay separately. For the bandwidth, a simple algorithm, called Most Reliable Path. For the delay, NP-hardness of the general case is given with some polynomial algorithms for some specific cases [11]. Client Puzzle Protocol (CPP) is an algorithm for use in Internet communication, whose goal is to make abuse of server resources infeasible. The idea of the CPP is to necessitate all clients connecting to a server to correctly solve a mathematical puzzle before establishing a connection, if the server is under attack

[12]. Stone proposed Center Track that automated this traditional input debugging mechanism for route-inference, by re-routing attack traffic over a specialized overlay network architecture [13]. Bellovin proposed iTrace, a low volume ICMP-based out-of-band messaging channel for the victim to detect packet audit trails. Different types of attacks requires different detection methods to increase true positives and achieve minimal false negatives, in particular when selecting the detection parameters thresholds and normal profiles for anomaly-based detection methods which have inherently lower reliability than signature-based ones [14]. The attackers can also know the IP addresses of the nodes that participate in the overlay and of the target that is to be protected, as well as the details of the operation of protocols used to perform the forwarding [15].

3. DARE ARCHITECTURE

We present the architecture overview of DARE which is based on the architecture of the EU Diadem Firewall project in which we were involved [16]. The Diadem Firewall project was an European Union funded project to develop an architecture that enables an Internet Service Provider (ISP) to protect its own networking environment as well as the connected hosts and servers of its customer against network attacks [17]. The Web Server attack detector builds normal user behavior models by monitoring service requests for the server objects. A change-point detection algorithm checks for changes in the browsing behavior of the users, to detect web server overloading attacks [18]. We built a new Adaptive System Manager (ASM) for coordinating the events from the detection modules and response triggering. The SM in Diadem was written in Java and it supports the alert and response event coordination between the existing modules in Diadem [19]. The XML Subscriber and Parser module is created in DARE as TOPAS only comes with a built-in XML Publisher to send out IDMEF alerts. IDMEF alerts received by TOPAS catered only for the Non-Intrusive IP Trace back through the use of a flag in a file to trigger the trace back process.

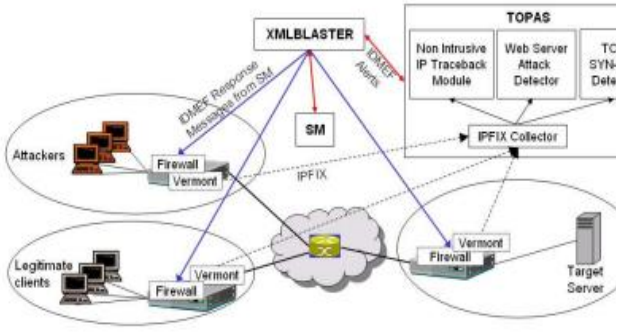

Fig. 2: Architecture Overview of Diadem

4. PROPOSED METHODOLOGY

The proposed system architecture with detailed explanation are discussed the proposed system architecture. These packets are sent to different server via client or hacker in sense of flooding. The Poisson distribution is used to control and manage the arrival rate of the packets over networks [20]. The exponential distribution is used to define the service time of the packets in the network. When packets arrived at server end the server checks the packet constantly for any viruses or malicious packets. It calculates the malicious packets via correlation analysis.

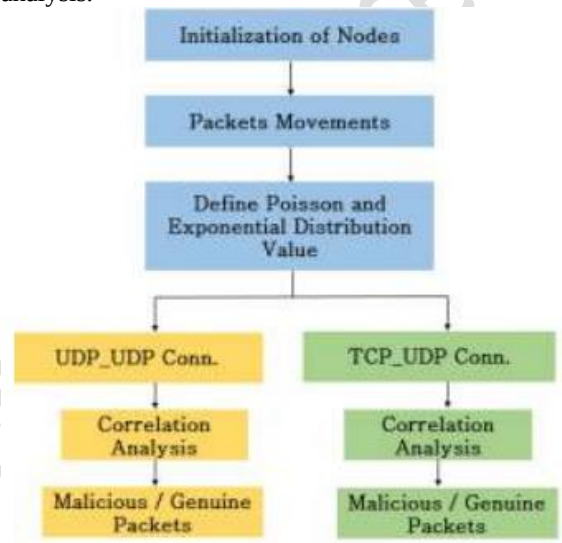

Fig. 3. Proposed system work flow

5. DDOS OVERVIEW

The operating systems and network protocols are developed without applying security engineering which results in providing hackers a lot of insecure machines on Internet. An attacker gradually implants attack programs on these insecure machines [21]. The resource can be bandwidth, memory, CPU cycles, file descriptors and buffers the attackers bombard the scarce resource by sheer flood of packets flood of packets is shown, which congests the link between ISP's edge router and border router of victim domain [22].

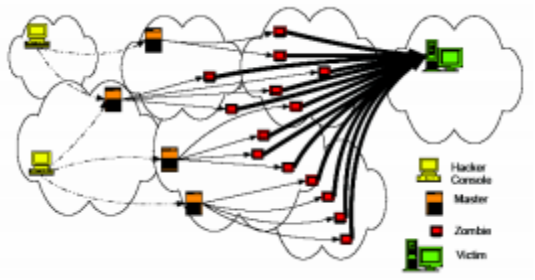

Fig 4. Attack modus operandi.

1) **System memory resources:**

An attack targeting system memory resources typically aims to crash its network handling software rather than consuming bandwidth with large volume of traffic. Specific packets are sent to confuse the operating system or other resources of the victim's machine.

2) **System CPU resources:**

An attack targeting system's CPU resources typically aims to employ a sequence of queries to execute complex commands and then overwhelmed the CPU. The Internet key Exchange protocol (IKE) is the current IETF standard for key establishment and SA parameter negotiation of IPsec.

1. ATTACK PATH FREQUENCY DETECTION

During a highly disruptive distributed DoS attack, it is probably easy to weed out persistent high volume attackers. However, DDoS attacks employing large botnets with a low median traffic volume per source, often make it difficult to classify packet sources as legitimate or those with malicious intent [23].

1. **Frequency Measurement**:

Simple path frequency detection using active measurement requires just one counter per path in the attack tree, an increment being triggered on receipt of a packet associated with that path. Hence, frequency detection on a per-packet granularity can easily be achieved at the victim, as guaranteed by unique packet to path association.

2. **Frequency Inference**:

The attack tree we have obtained thus far using out-of-band packet marking, is essentially an attack path tree, embedding only the router connectivity information. We propose to overload this attack path tree to also embed path frequency information, to construct a novel attack path frequency tree. Along similar lines of the proposed distributed divide-and-conquer tree construction mechanism.

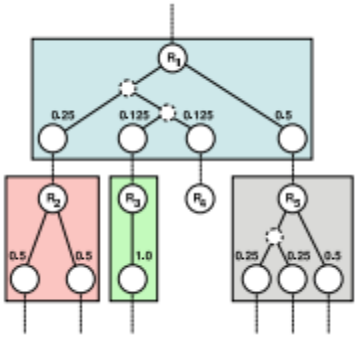

Figure 5. Modular Path Frequency Tree

2. SECURE SERVICE OVERLAY (SOS) MODEL

The goal of the SOS architecture is to allow communication between a confirmed user and a target. The model proposes a proactive approach to prevent DoS attacks. A target is protected by removing all incoming packets from unapproved sources [24]. A network of selected nodes form an overlay which protect a specific target. Packets are validated at entry points of the overlay and once inside are tunneled securely to secretly designated nodes. Once validated, all traffic is forwarded to the target through the overlay [25].

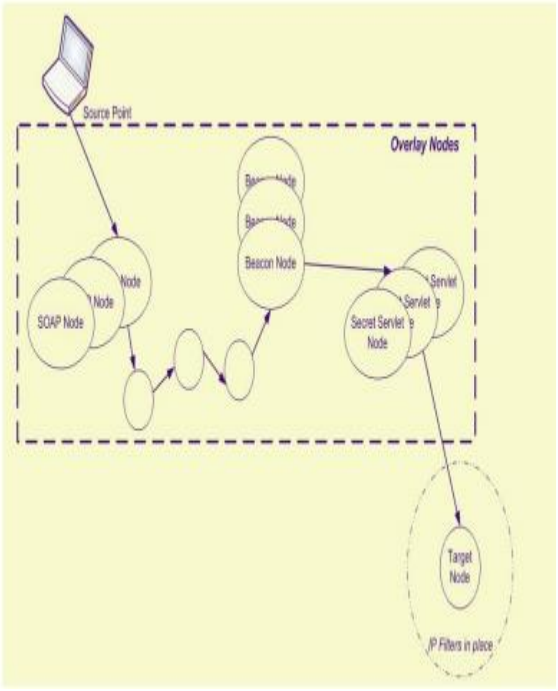

Fig.6. SOS Architecture

A.SOAP - Secure Overlay Access Point : o The start point in for all traffic that will communicate with the target. o Handles authentication of users and traffic.

B. Target : o The nodes or set of nodes that will be filtered to only allow overlay traffic

C. Beacon : o The end-point in a chord ring. o Beacon forwards traffic to the Secret Servlet.

D. Secret Servlet : o The node that will communicate with a specific target or group of targets.

E. To mitigate attacks : o No unauthenticated traffic is allowed in the overlay. o Filtering of non-overlay traffic near the target can be done at linespeed. o The vulnerability of the target is offloaded onto the overlay. o The overlay is recoverable.

F. Design Rationale : Fundamentally, the goal of the SOS infrastructure is to distinguish between authorized and unauthorized traffic [26].

6. PERFORMANCE EVALUATION

We have used ns2 and Internet topology generator BRITE with both the Waxman and Barabasi-Albert models . The link metric values are generated by using the Normal, Exponential, Gamma, Weibull and

Lognormal distributions. PDF parameters are generated randomly using the uniform distribution. Then, based on these parameters, link metric values corresponding the probability distributions. Once the network state information becomes stale their performance will degrade. Statistical techniques, such as our transform algorithm, may not provide the best performance when perfect and up-to-date state information is available to the network nodes. We have assumed, in this estimation, that an intermediate router has an equal probability of being present at any of the different tree depths, when viewed globally for all the potential attack victims in the Internet. Although this assumption might seem inaccurate, it helps us realistically estimate different benchmarks for any router in today's Internet.

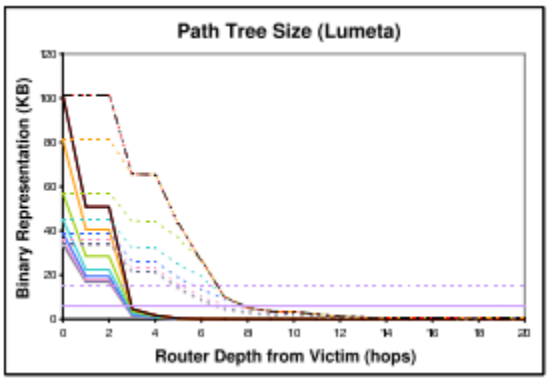

Figure 7. Freq. Measure

7. CONCLUSION AND FUTURE WORK

Our analysis of the DDoS attack tools provided a useful resource for understanding how the code was structured and what design decisions. We also looked into the protection of next generation IPv6 networks from DDoS attacks. We proposed TRAPS which can be easily deployed, utilizing the built-in Mobile IPv6 feature to verify the authenticity of the source by performing virtual relocations of the server. We call this architecture Secure Overlay Services, or SOS the resistance of a SOS network against DoS attacks increases greatly with the number of nodes that participate in the overlay. We have presented the transform-based approach for the problem of finding a path subject to an additive QoS metric represented by means of independent random variables. An interesting extension of our work is to study when the link pdfs are not independent. Future work we are planning to pursue we would like to study adaptive numerical integration techniques, such as the Gauss-Kronrod, that has built-in error estimation in order to report them to the decision makers as well as possibly adjusting the algorithm based on the magnitude of the errors.

8. **REFERENCES**

[1] J. Francois, I. Aib, and R. Boutaba, "FireCol: A collaborative protection network for the detection of flooding DDoS attacks," IEEE/ACM Trans. Netw., vol. 20, no. 6, pp. 1828–1841, Dec. 2012.

[2] V. A. Foroushani, A. N. Zincir-Heywood, "TDFA: Trace back based Defense against DDoS Flooding Attacks", IEEE 28th International Conference on Advanced Information Networking and Applications, pp. 597-604, May 2014.

[3] B. Liu, J. Bi, A. V. Vasilakos, "Toward Incentivizing Anti Spoofing Deployment", IEEE Transactions on Information Forensics and Security, vol. 9, no. 3, pp. 436-450, March 2014.

[4] A. Compagno, M. Conti, P. Gasti, G. Tsudik, "Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking", IEEE 38th Conference on Local Computer Networks, pp. 630-638, Oct. 2013.

[5] C. Chung, P. Khatkar, T. Xing, J. Lee, D. Huang, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems", IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 198- 211, July/Aug. 2013.

[6] R. Guerin and A. Orda, "QoS Routing in Networks with Inaccurate Information," IEEE INFOCOM Kobe, Japan, pp. 92–100, April 1997.

[7] S.Chen and K. Nahrstedt, "Distributed QoS Routing with Imprecise State Information," ICCCN, 1998.

[8] T. Korkmaz and M. Krunz, "Bandwidth-delay constrained path selection under inaccurate state information," IEEE/ACM ToN, vol. 11, no. 3, pp. 384–398, June 2003.

[9] A. Shaikh, J. Rexford, and K. G. Shin, "Evaluating the impact of stale link state on quality-of-service routing," IEEE/ACM Trans. Netw., vol. 9, no. 2, pp. 162–176, 2001.

[10] X. Yuan, W. Zheng, and S. Ding, "A comparative study of qos routing schemes that tolerate imprecise state information," in ICCCN, October 2002, pp. 230–235

[11] Mirkovic J. and Reiher P., "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," Computer Journal of ACM SIGCOMM, vol. 34, no. 2, pp. 39-53, 2004.

[12] A. M. G. Cooper, R. Tsui, and M. Wagner, Summary of Biosurveillance- Relevant Technologies. [Online]. Available: http://www.cs.cmu. edu/~awm/biosurvmethods.pdf

[13] W. Leland, M. Taqqu, W. Willinger, and D. Wilson, "On the selfsimilar nature of ethernet traffic (extended version)," IEEE/ACM Trans Networking, vol. 2, no. 1, pp. 1–15, Feb. 1994.

[14] Bai Y. and Kobayash H., "Intrusion Detection Systems: Technology and Development," in

Proceedings of the 17th International Conference on Advanced Information Networking and Applications, USA, pp. 710-715, 2003.
[15] D. Dean et.al., "An Algebraic Approach to IP Traceback", ACM TISSEC, 5(2), pp. 119-137, 2000.
[16] A. Yaar, A. Perrig, D. Song, "FIT: Fast Internet Traceback", IEEE INFOCOM, 2005. [
17] M. Goodrich, "Efficient Packet Marking for Large-Scale IP Traceback", ACM CCS, 2002.
[18] M. Adler, "Tradeoffs in Probabilistic Packet Marking for IP Traceback", STOC, pp. 407-418, 2002.
[19] M. Muthuprasanna, G. Manimaran, M. Alicherry, V. Kumar, "Coloring the Internet: IP Traceback", IEEE ICPADS, 2006.
[20] B. Al-Duwairi, G. Manimaran, "Novel Hybrid Schemes employing Packet Marking & Logging for Traceback", IEEE TPDS, vol. 17(5), 2005.
[21] V. L. L. Thing, M. Sloman, and N. Dulay, "A survey of bots used for distributed denial of service attacks," in 22nd IFIP International Information Security Conference (SEC), (Sandton, Gauteng, South Africa), May 2007.
[22] V. L. L. Thing, M. Sloman, and N. Dulay, "Non-intrusive IP traceback for DDoS attacks," in ACM Symposium on Information, Computer and Communications Security, (Singapore), Mar. 2007.
[23] V. L. L. Thing, M. Sloman, and N. Dulay, "Network domain entrypoint/path determination for DDoS attacks," in IEEE/IFIP Network Operations and Management Symposium (NOMS), (Salvador, Bahia, Brazil), Apr. 2008
[24] Angelos D. Keromytis_ Vishal Misra Dan Rubenstein Department of Computer Science Department of Electrical Engineering Columbia University New York, NY. "SOS: Secure Overlay Services".
[25] D. Andersen, H. Balakrishnan, F. Kaashoek, and R. Morris. Resilient Overlay Networks. In Proceedings of the 18th Symposium on Operating Systems Principles (SOSP), October 2001.
[26] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss. An Architecture for Differentiated Services. Technical report, IETF RFC 2475, December 1998

Author details:

[1]Sz.Parveen
Designation:Assistant Professor
Email:afreen.sal25@gmail.com
[2]J Sunil
sunil.jinkathoti06@gmail.com
Annamacharya Institute of Technology & Science,Kadapa