DDoS Traffic Verification Algorithm for Legitimate Clients Identification in Distributed Denial of Service (DDoS) Attacks

S. K. Lavanya
Department of Computer Science
Sona College of Technology
Salem, TamilNadu, India

R. B. Vinothkumar
Department of Computer Science
Sona College of Technology
Salem, TamilNadu, India

ABSTRACT
Distributed Denial of Service (DDoS) attacks have become a major threat to the stability of the internet and there is no satisfactory solution yet. These attacks are familiar threats to internet users for more than 10 years. Such attacks are carried out by a "bot-net", an army of zombie hosts spread around the internet, that overwhelm the bandwidth toward their victim web server, by sending traffic upon command. This paper introduces traffic verification algorithm is especially designed to protect the victim server from the harm attacks and legitimate clients are identified in an effective manner. The legitimate clients are maintained in a separate list called "whitelist" and it will be refreshed frequently. So the attacker can't spoof the legitimate client addresses. The simulation result shows that the legitimate clients are maintained in an effective manner.

Keywords
Distributed Denial of Service (DDoS), botnet, zombie.

1. INTRODUCTION
Current Denial-of-Service (DoS) attacks are directed towards a specific victim over the past decades, the internet has become of critical importance for social, business and government activities. The DoS attack, especially the Distributed Denial of Service (DDoS) attack, has become one of the major threats to the internet. Generally, attackers launch DDoS attacks by directing a massive number of attacks sources to send useless traffic to the victim. the victim's services are disrupted when its host or network resources are occupied by the attack traffic. The threat of DDoS attacks has become even more severe as attackers can compromise a huge number of computers by spreading a computer victim using vulnerabilities in popular operating system.

The internet was initially designed for openness and scalability. On the internet, anyone can send any packet to anyone without being authenticated, while the receiver has to process any packet that arrives to a provided service. The lack of authentication means that attackers can create a fake identity, and send malicious traffic with impunity. DoS attacks can be launched in two forms. The first form is to exploit software vulnerabilities of a target by sending malformed packets and crash the system. The second form is to use massive volumes of useless traffic to occupy all the resources that could service legitimate traffic. While it is possible to protect the first form of attack by patching known vulnerabilities, the second form of attack cannot be so easily prevented. The target can be attacked simple because they are connected to the public internet.

The rest of the paper is organized as follows: section II provides a brief review of related work. Section III discusses the rationale and architecture of DDoS traffic verification algorithm. Section IV presents the experimental evaluation. Section V discusses several design issues and concludes this paper.

2. RELATED WORK
A Distributed Denial of Service (DDoS) attack is commonly characterized as an event in which a legitimate user or organization is stripped of certain services, like web, email or network connectivity, that they would normally expect to have [1]. DDoS attack is basically a resource overloading problem. The resource can be bandwidth, memory, CPU cycles, file descriptors, buffers etc. The attackers scare resources either by flood of packets or a single packet which can activate a series of processes to exhaust the limited resources [2].

Researchers have used the distribution of TTL values seen at servers to detect abnormal spikes due to DDoS traffic [3]. Several filtering solution which must execute on IP routers have been proposed to prevent spoofed IP packets from reaching intended victims. The most straightforward scheme is ingress filtering, which blocks spoofed packets at edge routers, where address ownership is relatively unambiguous, and traffic load is low [4]. Protection against DoS attacks highly depends on the model of the network and the type of attack. Several mechanisms have been proposed to solve the problem of DoS attacks. Research on DDoS attacks is primarily focused on attack detection and response mechanisms. Attack detection aims to detect an ongoing attack and to discriminate malicious traffic from legitimate traffic.

Several researchers have studied the frequency and nature of internet DoS attacks [5, 6, 7, 8, 9]. Ferguson and Senie propose to deploy network ingress filtering to limit spoofing of the source IP address [10]. SYN-cookies [11] are designed to prevent SYN floods from exhausting server connection state with half-open connections. They operate by using a cryptographically secure cookie in place of the ISN in the SYN|ACK from the server. Filter based approaches, such as Pushback [12] and AITF [13] require the identification and blocking of illegitimate traffic from within the network.

In Pushback, a router attempts to identify attack traffic by determining that it is in a congested state, finding an "aggregate" that describes the attack traffic, and pushing the "aggregate" upstream to be blocked close to the source. AITF is an optimization of Pushback that is based on the observation that a pure filter based approach requires too much state in core routers.

In this paper, we propose a new mitigation algorithm called traffic verification algorithm, for identifying the legitimate clients effectively. It is an analytical approach based on the mathematical equation which will be used to find the number of packets being malicious under legitimate data packets. This salgorithm will be used to mitigate the malicious packets which are coming along with the legitimate data and improve the effectiveness of network performance.

3. PROPOSED WORK – DDoS TRAFFIC VERIFICATION ALGORITHM

The DDoS traffic verification algorithm mitigates DDoS attacks by identifying the legitimate packets from the malicious attack packets. In this algorithm, to verify the DDoS traffic, puzzle generator, puzzle verifier and puzzle resolver are used.

3.1 Identify attack and victim system

The first challenge in solving the DDoS attack problem is to determine if there is any DDoS victim being attacked by the traffic passing through the router. When a victim is in under attack, we need to determine how much of traffic volume flow to the target victim. These are identified by using puzzle generator, verifier and resolver. The puzzle identifier/generator is deployed at the user machines. The victim is recognized, when a DDoS attack is detected. After detecting DDoS attack, the generator produces a puzzle and a unique puzzle identifier (UPI). The victim machine sends them to the routers and the generator will keep producing new UPIs and sending them to routers periodically.

3.2 Classification of legitimate and attack traffic

Once an attack victim is discovered, puzzle generator produces a puzzle and UPI and sending them to routers continuously. Puzzle verifiers are deployed in the intermediary routers. When an initiation of new connection to the victim is received, the router will not forward this request to the victim immediately. Instead, the verifier generates a new ID for the client and sends it along with the puzzle and UPI to the client. Then the router validates the client's responses. Only if the client solved the puzzle correctly the router will forward the connection initialization request to the victim. Otherwise, any packet sent by the client to the victim will be dropped.

3.3 DDoS Traffic Verification Algorithm

Once the attack traffic is classified, defense actions should be automatically taken place to mitigate the impact of the attack. By discarding the attack packets, there is a puzzle resolver at the client side. This enables the client to receive packets from the router, which contains a puzzle, a UPI, and an ID. Upon receiving such a packet, the resolver will figure out a puzzle solution and transmit the result to the appropriate router. Then the remaining legitimate clients are maintained as a "whitelist".

In this algorithm, once the victim server is identified, it generates the puzzle and Unique Puzzle Identifier (UPI). After generating puzzle and UPI, these are distributed to routers and meanwhile puzzle and UPI are updated by the victim server periodically. Client and routers are involved in the puzzle generation and verification. The victim server connections are initiated by the clients. The router sends puzzle, UPI and puzzle ID to the clients.

The client returns solution to the routers. Then the routers verify the solutions which are received from the clients. If the client results are matched with router solution then it will classify as legitimate clients otherwise the nodes are identified as attackers. The legitimate clients are maintained as a separate list called "whitelist". Whitelist contained all legitimate client IP addresses. It should be refreshed frequently with particular time intervals.

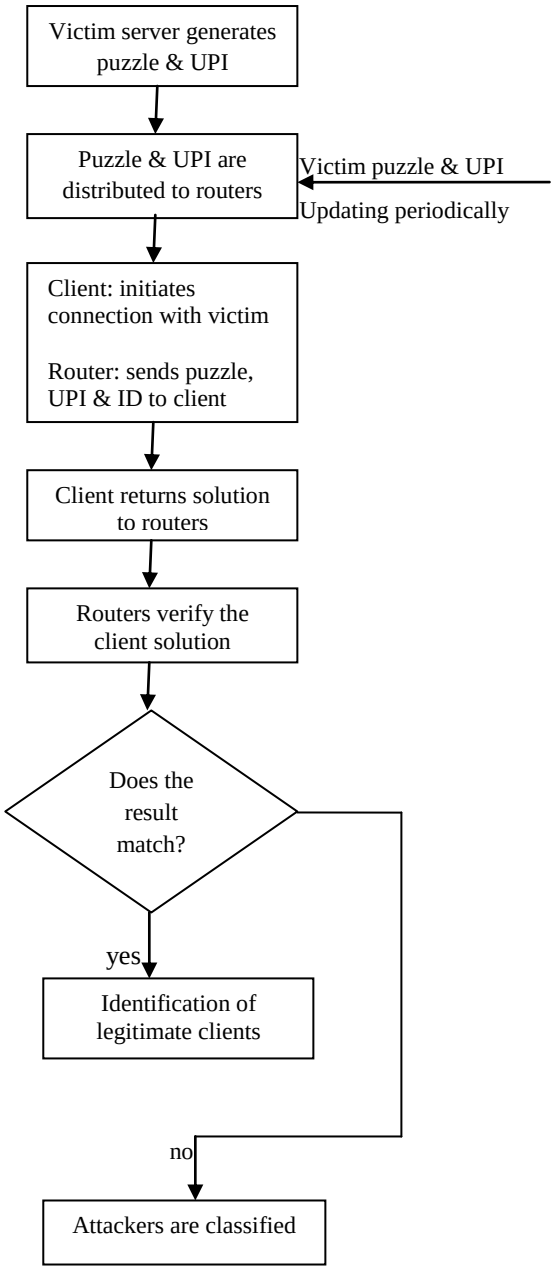

Fig. 1 architecture of DDoS traffic verification algorithm

DDoS traffic verification algorithm used to generate the time intervals for refreshing the whitelist. Instead of refreshing a user, this algorithm will refresh the entire whitelist frequently. So, the attacker cannot spoof the legitimate clients IP addresses. Whitelist can effectively maintain the legitimate clients. This algorithm not only prevents the bad packets from reaching the target victim but also automatically reduce the workload of routers that forward them and avoid wasting the network bandwidth in downstream network.

3.4 Mitigation using DDoS traffic verification algorithm

In DDoS attacks, the attacker sends large volume of malicious packets to the victim server. The attacker can prevent the resource access from the legitimate user. So, this algorithm is to find out number of packets being malicious in the legitimate request and mitigates the attack packets.

Let m= no. of malicious packets

n = no. of non-malicious packets

M=m+n= total no. of packets arrived with poisson's distribution 'λ'

Calculate each packet being malicious under legitimate packets using conditional probability is,

$$P(N_1 = m, N_2 = n) = P(m+n, n).P(m+n) \quad (1)$$

Binomial probability is,

$$P(m+n, m) = {}^{m+n}C_m p^m q^n$$

Poisson's distribution is,

$$P(m+n) = e^{-\lambda} \lambda^{m+n} / (m+n)!$$

Substitute binomial and poisson's distribution to the conditional probability (1)

$$P(m+n) = (m+n)!/m!n!.p^m q^n.e^{-\lambda} \lambda^{m+n} / (m+n)!$$

$$= p^m q^n.e^{-\lambda} \lambda^{m+n} / m!n!$$

$$= e^{-\lambda} (\lambda p)^m m!n!$$

By putting the value of this equation to (1), the value of poisson's distribution 'λ', we can find the number of malicious packets under the legitimate packets.

4. EXPERIMENTAL RESULTS

The experiment is conducted on the NS-2 to evaluate the performance of the algorithms. Fig. 2 shows that the number of nodes taken for simulates this algorithm. Fig. 3 shows that performance evaluation of the traffic verification algorithm. Fig. 4 shows that when the DDoS packet rate is increased, DDoS traffic verification algorithm increases the throughput of legitimate packets, packet delivery ratio and minimizes the packet delay.

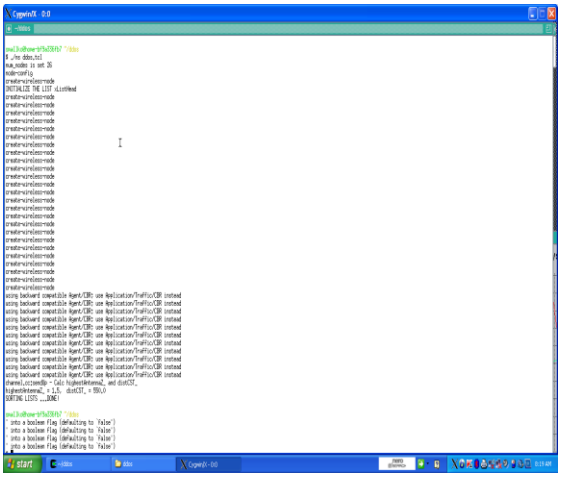

Fig. 2. simulation of nodes

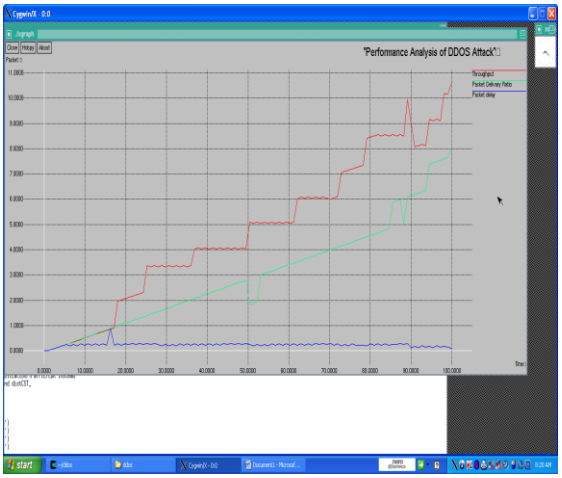

Fig. 3. successful connection rate

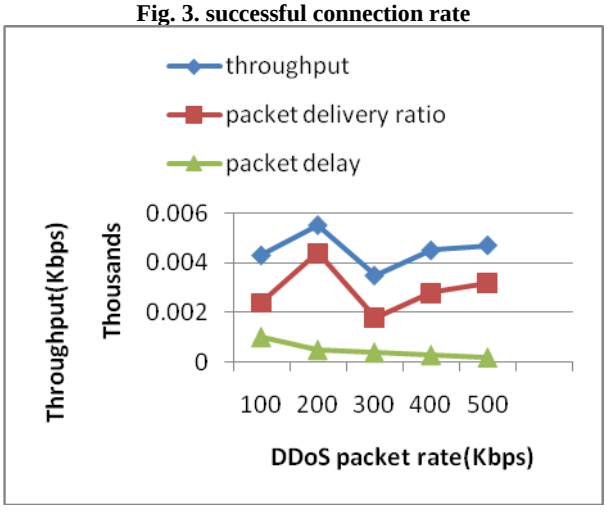

Fig. 4 throughput efficiency under DDoS traffic verification algorithm

5. CONCLUSION

In this paper, DDoS traffic verification algorithm is presented for detection and mitigation of DDoS attacks on a victim server. NS-2 simulation results shows that traffic verification Algorithm, the proposed algorithm shows that it not only effectively decreases the flow of malicious packets from DDoS attacks, but also provides smooth and constant flows sent by normal users and increase the throughput of the normal packets.

6. REFERENCES

[1] B.B. Gupta, R.C. Joshi and M. Misra, Distributed Denial of Service prevention techniques, in: International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April 2010, 1793-8163.

[2] K. Kumar, R.C. Joshi, K. Singh, An Integrated Approach for Defending against Distributed Denial of Service (DDoS) attacks, in: iriss, 2006, IIT Madras.

[3] Jin, C. Wang, H. Kang, G., Hop-Count filtering: An Effective Defense against spoofed traffic, in: IEEE transaction on Dependable & Secure Computing, 2004.

[4] Lipson, H.F., Tracking and Tracing Cyber attacks: Technical Challenges and Global policy issues, in: CMU/SEI-2002-SR-009, November 2002.

[5] L. Garber. Denial-of-service attacks rip the Internet. In *IEEE Computer*, volume 33, April 2000.

[6] G. Virgil. On denial of service in computer networks. In Proceedings *of International Conference on Data Engineering, pages* 608– 617, February 1986.

[7] J. Howard. *An Analysis of Security Incidents on the Internet*. PhD thesis, Carnegie Mellon University, August 1998.

[8] Jaeyeon Jung, Balachander Krishnamurthy, and Michael Rabinovich. Flash crowds and denial of service attacks: Characterization and Implications for CDNs and web sites. In *The Eleventh International World Wide Web Conference (WWW 11)*, May 2002.

[9] David Moore, Geoffrey Voelker, and Stefan Savage. Inferring Internet denial of service activity. In *Proceedings the 10th USENIX, Security Symposium*, Washington, D.C., August 2001. USENIX.

[10] P. Ferguson and D. Senie. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC 2267, January 1998.

[11] D. Bernstein. Syn cookies. http://cr.yp.to/syncookies.html, 1996.

[12] J. Ioannidis and S. M. Bellovin. Implementing pushback: Router-based defense against DDoS. In *Proceedings of Network and Distributed System Security Symposium*, 2002.

[13] K. Argyraki and D. R. Cheriton. Active internet traffic filtering: Real-time response to denial-of-service attacks. In *USENIX Annual Technical Conference*, 2005.

[14] S. M. Specht and R. B. Lee, Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures, *Proc. PDCS* 2004.

[15] Simpson, S., Lindsay, A.T., Hutchison, D.: Identifying Legitimate Clients under Distributed Denial-of-Service Attacks. In Network *and System Security (NSS).* IEEE, 2010.

[16] D. Garg, DDoS Mitigation Techniques-A Survey, *International Conference on Advanced Computing, Communication and Networks* 2011.

[17] L. Cook, W. G. Morein, A. D. Keromytis, V. Misra, and D. Rubenstein, "WebSOS: Protecting Web Servers from DDoS attacks," *Proceedings of the 11th IEEE International Conference on Networks (ICON 2003)*, September 2003, pp.455-460.