ISSN: 0976-3104
SPECIAL ISSUE: Emerging Technologies in Networking and Security (ETNS)

ARTICLE OPEN ACCESS

CHASED APPROACH TO DETECT DDOS

Sathya Priya[1*], Rajagopalan[2], Ramakrishnan[3]
[1]Dept.of CSE, Anna University, Chennai, INDIA
[2]Dept.of CSE, GKM Engineering College, Chennai, INDIA
[3]Dept.of IT, Madurai Kamraj University, Chennai, INDIA

ABSTRACT

Distributed Denial of Service (DDoS) poses severe threat to the network. DDoS seems to be more severe than all the other attacks, as there is no need to do complex cryptographic techniques to enter the network and corrupt data. This paper focuses on detecting DDoS attack at an early stage using cryptographic hashing technique. The use of SHA-1 implementation in place of normal hashing or non-cryptographic hash function prevents attackers from degrading network performance by finding hash collisions. Moreover for attack free communication between the sender and receiver, a pre-shared key authentication mechanism is followed. This paper proposed Cryptographic Hash based Edge router Deployment (CHASED) approach to detect DDoS attacks and prevent IP spoofing by avoiding hash collisions.

Published on: 10th– August-2016

KEY WORDS

DDoS, Pre-shared key, SHA-1, Hash Collision.

INTRODUCTION

DDoS is one of the challenging network attacks which exploit the network resources [1]. In DDoS attacks, most of the websites were made virtually unreachable to the internet users, hence results in heavy financial loss, fall in reputation of the organization, many unsatisfied customers and so on [2]. Denial of Service (Dos) or DDoS attacks have become a serious threat and great nuisance that destabilizes the internet. DDoS attacks have become one of the major research issues in the field of network security. DDoS attacks are handled by zombies knowingly or unknowingly and attacks the victim [3]. It is best to divide DDoS attacks as local and remote (network based) in order to gain actual knowledge about it. In local attacks, a form of malicious software resides in the computer system affects the other system in the network.

Remote based attacks also called as a network based DDoS attack, which disturbs the client accessing the server from the remote means. Examples of remote based attacks are syn flood attacks, Smurf attacks and so on. DDoS can be implemented by compromising any one of the system in the network, and through that compromise other nodes called zombies and send unwanted or exhausted packets to the server to make it as a victim.

For Example, to introduce attack on the popular website, the attacker can send false HTTP requests over the same network [4]. This type of request is same as that of one made by the intend user. Thus the attacker bypasses the network through any security mechanisms [5]. This paper explores the idea of detecting DDoS using cryptographic hash technique. Cryptographic algorithms are developed using computational hardness, ensuring such algorithms are very hard to break by the adversaries. It can be breakable by theoretical concepts, but it is infeasible for the practical means so these techniques are termed as computationally secured one [6]. This paper focuses on SHA-1 cryptographic hashing technique to detect the DDoS attack in early stage. The below **[Figure - 1]** shows how a DDoS attack takes place.

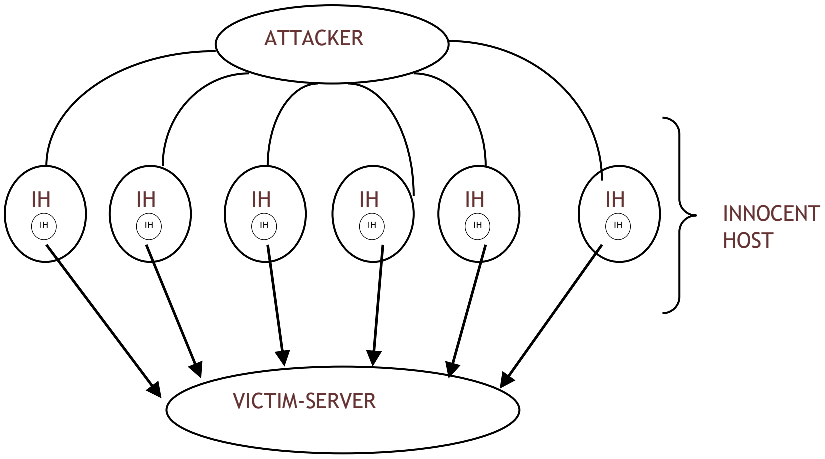


Fig: 1. DDoS Attack

The **[Figure - 1]** also shows how multiple attackers can attack simultaneously and the existence of multiple attack paths. It is not necessary, that attack can take place only at ingress edge, the attacker can also attack through intermediate routers in the network [7]. Because of the non-stable characteristics of the internet and anonymous behavior, there is no evidence of record of the transmission path of the packet. This paper focuses to detect DDoS attack from the identification of first non-matching packet itself and to break the path in which flooding takes place. For the best results, it is expected each router participating in the network must work in coordinating manner to identify the attacker's path.

RELATED WORK

Bin Xiao et al, [8] proposed a system to consist of a client detector and a server detector. The client detector is implemented on the side of the innocent clients and utilizes Bloom filter-based detection strategy for generating precise detection outcomes yet utilizes least amount of storage as well as computation resources. Sever detectors may actively monitor and control the warning process by sending requests to innocent hosts. A counter is implemented to calculate the SYN and SYN-FIN handshake signals. When only the SYN handshake signal reaches a threshold value, the client detector generates an alarm to inform the server detector. The server detector drops the packets on receiving the alarm. The throughput of this paper in detecting DDoS attack is good but results in hash collision.

Wang H et al., [9], instead of monitoring the ongoing traffic at the front end (like firewall or proxy) or a victim server itself, this detection mechanism detects the SYN flooding attacks at leaf routers that connect end hosts to the Internet. The detection mechanism is based on the protocol behavior of TCP SYN–FIN (RST) pairs. To make the detection mechanism insensitive to site and access pattern, a non-parametric Cumulative Sum (CUSUM) method is applied. From this paper, the idea of implementing the algorithm in the intermediate routers instead of ingress and engress router was proved to defend the DDoS attack and cause less effect on the server in the network. Then a scheme for filtering spoofed packets (DDOS attack) which is a combination of path identification (Pi) and client puzzle (CP) concepts was implemented. In ingress router, client puzzle for the client is placed. In this each IP packet, a unique Pi is added and router marks forwarding packets to generate unique identifiers corresponding to different paths. With this Pi, hop count value is also added. Thus the victim can use the <Pi, HC> tuple to identify and discard malicious packets from the attacker.

Praveena V et al, [10], gave the idea of including hop count in the cryptographic hash table to provide a better way to secure the server from attack. DDoS defense systems are deployed in the network to detect DDoS attacks independently. A communication mechanism is used to exchange information about network assaults among the independent detection nodes for aggregating data regarding overall network assaults noted. We assume that the Internet is composed of a set of Autonomous Systems (AS). The system is implemented with the overlay network to share the attack information using a gossip protocol based on epidemic algorithm over the Internet. Using the aggregated information, the individual defense nodes have approximate information about global network attacks and can stop them more effectively and accurately. Guangsen Zhang et al, [11] derived the concept of adding more information for the routers to detect the DDoS attack.

Keromytis A et al, [12] gave the concept of intense filtering. An architecture called Secure Overlay Services (SOS) proactively prevents DoS attacks. Here reduced the probability of successful attacks by (i) performing intensive filtering near protected network edges, and (ii) introduction of arbitrariness as well as anonymity in forwarding path to a specific SOS-protected destination.

Almost all recent DDoS assault detection as well as prevention strategies are employed either on victim servers (assault source) or between the two [13]. The spoofed packets could be distinguished from normal ones by the Hop- Count deviation [14].

Source side mechanisms to detect as well as prevent DDoS assaults may be challenging to deploy. Source-end implemented methods works better but are difficult to deploy. After attacks are identified, attack sources can be discovered through traceback [15] as well as pushback technique. Most traceback schemes are implemented by either marking some packets in their routing paths or by sending special packets. By tracking these special marks, it is easy to reconstruct the real routing path reconstructed and locate the true source IP [16].

Once real routes of spoofed packets are detected, pushback method performs advanced filtering and works at the last few routers before the malicious traffic reaches the target victim [17]. Hence, it is not easy to detect abnormal deviations until the DDoS attack is at the final traffic-bursting stage [18].

Existing solutions can fail to raise accurate alarms when DDoS occurs and results in false positives and also using simple hash techniques results in large number of collisions [19]. So, cryptographic hash function is used in place of normal hash function to prevent collision attacks and to reduce false positive at high level.

METHODOLOGY

The proposed work mainly based on cryptographic hashing technique over the edge routers. Unlike the previous research works on different type of hashing techniques, cryptographic puzzle, special cryptographic masking and so on, the explored work shows better results, as it is collision resistant.

The proposed work is implemented by considering the following assumptions in order to make the approach more effective and practical.

- Edge routers were implemented with cryptographic hashing technique.
- Routers are stable enough to perform hashing computation, which is collision free.
- Threshold value is set to identify normal user from abnormal user.
- Pre shared key authentication mechanism is used to avoid other nodes does not interfere the intend path for packet transmission.
- Multiple attackers can attack at the same or different time, hence multiple attack paths exist.
- It is assumed all routers should work in a coordinated manner, in order to produce good results.
- Each router is implemented with the alarm, in order to raise the alarm whenever it faces DDoS attack. In our simulation, it intimates by changing its color.
- Attackers can generate any volume of attacks and hence tries to flood or crash the server.

Methodology of Proposed Work

From the previous work [21], it is observed that the hash based technique is comparatively good for identification of DDoS attack. Even though hash based technique has the limitation of collision attacks.

So, in this paper we implemented the DDOS detection approach in Cryptographic Hashing technique, which is highly collision resistant. . As the work simulated in IPV4, the SHA1 is applicable to be used than the SHA3 or other Cryptographic Hashing technique. In this, the IP address of the authorized users in the network is implemented with cryptographic hashing. So for the packets sent/received in a network, the identity should be unique in each router hash table. Hence, it is difficult for the attacker to break or even trying to make collision attacks in cryptographic based hashing technique

The work considers the following factors:-

- Packets sent / received must meet the threshold value which is already set.
- Pre-shared key authentication mechanism.
- Cryptographic hashed IP address traversed through each router.

Pre Shared Key authentication mechanism:

The main concern of pre shared key authentication mechanism is to overcome IP spoofed packets.

Sender Node(S_N) sends request using TCP/SYN Hashed (H) with pre shared key(PS) given by routers to Ingress routers (IG). Ingress router checks authentication by Dehash (H') TCP/SYN using pre shared key and sends acknowledgement to sender node. Now, communication starts between the sender node to the destination node (D_N).

$$\text{S\_N} \xrightarrow{\text{H(TCP/SYN, PS)}} \text{H(TCP/SYN,PS) IG}$$

$$\text{IG} \xrightarrow[\text{ack}]{\text{H'(TCP/SYN, PS)}} \text{H'(TCP/SYN,PS) S\_N}$$

$$\text{S\_N} \xrightarrow{\text{Forwards packet}} \text{forwards packets D\_N}$$

Cryptographic Hash function:-

In Ingress router cryptographic hash function (SHA1) is implemented. Once authentication mechanism starts between sender node to the destination node, then Ingress router cryptographically hash the IP address coming through it and forwards the packet to the next router in the network. SHA 1 cryptographic hash function hashes the IP address of the nodes and generates a unique value. [20]. Cryptographic hash function helps to prevent IP spoofing.

Example for SHA-1 algorithm:
Source IP Address: 198.162.1.4
Hashed Source IP Address:
0xe138a664841494de5a5154981f5a499095e3c18b7
The hashed IP address is 160 bit value. It is in hexadecimal format

An attacker compromises few innocent hosts to perform DDoS attack by making the innocent host create traffic in the network. The innocent host starts creating traffic in the network by passing numerous amounts of packets to the routers that is to be passed to the server. [Figure-3] depicts the following

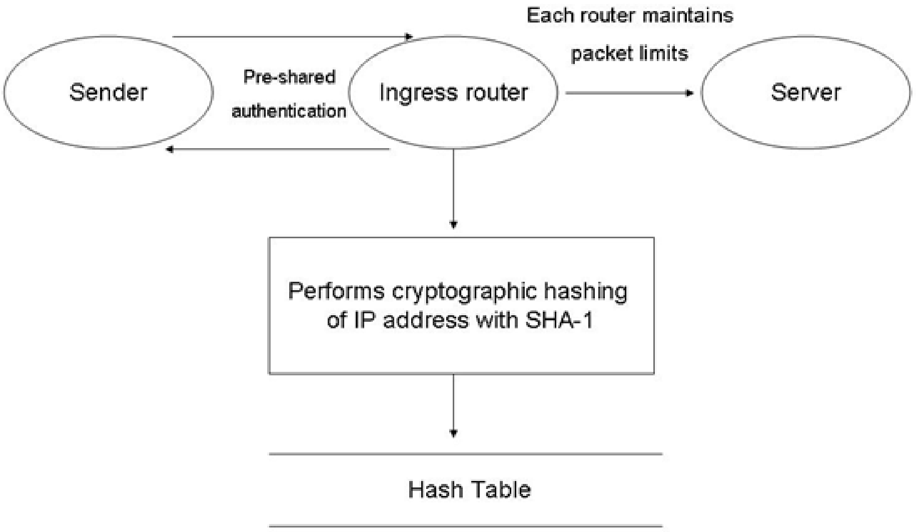
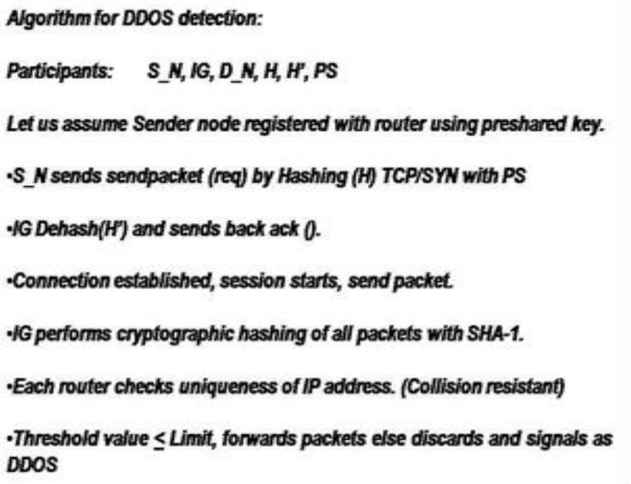


Figure 3: Proposed System Architecture

- Before transmitting the packet it performs pre shared key authentication
- When the packet reaches the ingress router, the router analyses the packets and hashes the source address using the hashing algorithm.
- The router checks the hashed source address with the source address in the hash table. If it matches, the router forwards the packet.
- Each router maintains the limit of packet in can hold. When the threshold value exceeds a certain value, the router starts dropping the packets which prevents exploitation of resources in the victim server.



Algorithm for DDOS detection:

Participants: ***S_N, IG, D_N, H, H', PS***

Let us assume Sender node registered with router using preshared key.

•S_N sends sendpacket (req) by Hashing (H) TCP/SYN with PS

•IG Dehash(H') and sends back ack ().

•Connection established, session starts, send packet.

•IG performs cryptographic hashing of all packets with SHA-1.

•Each router checks uniqueness of IP address. (Collision resistant)

•Threshold value ≤ Limit, forwards packets else discards and signals as DDOS

Router-Hash table Implementation

A router performs ‘traffic direction’ function on the Internet. Data packets are normally transmitted from one router to the next over networks which comprise the internetwork till they reach destination nodes [22].

The route consists of a table in which there are counters to count the number of packets of a particular source IP address. All counters are initialized to 0. When a key a (such as a source IP address) is inserted, the value of the counters are increased by 1 accordingly at the table addresses h1 (a), h2 (a), . . . ,hk (a). If an IP address b is stored in the hash table, the counters at the addresses h1 (b), h2 (b), . . . ,hk (b) in the table are all non-zero. This allows us to monitor the current statistic of control packets flowing through a router towards the server.

When the packet reaches the router, it analyzes the packet and gets the source IP address. When another packet reaches the router, it checks the hashed IP address in the hash table. If the packets are from the same IP address then the packet count is increased else the IP address is hashed and stored in the hash table.

The threshold value that is set can be differed according to various applications. In our proposed system, the threshold value is 200. So if any node sends packets that exceed 200 packets to the server, those packets of the node are dropped. Then the DDoS alarm has raised.

Securing the network

DDoS attacks impact great challenge for the availability of resources for Internet Service Provider (ISP). A virtual security ring is now implemented around the network. Now, each router is implemented with hash table that tracks the normal user from the abnormal user. Normally with Ingress and egress filtering the router capable of filtering all traffic coming from the normal user and IP Spoofers are identified. As this proposed paper works on predefined threshold value insecure cryptographic hashing environment once the number of packets is higher than that is expected from the normal user, then the server stops sending the CTS and quits the connection with that particular client. By this, attackers from outside the network could be minimized. Setting continuous monitoring with the hash table mapping, the network could reduce threats to the great extent.

RESULTS AND DISCUSSION

Our proposed system is compared with existing techniques to detect DDoS attack based on data delivery rate and data loss parameters. It shows reduced false positive. Implementing cryptographic hashing all over the network is cost effective but effective for the expected secure network. It is expected the approach extends its support to detect DDoS in effective manner with the collision resistant capability. **[Figure 5] [Figure 6]** below show the data loss for our proposed system produces better results with cryptographic hashing technique.

THE IIOAB JOURNAL
ISSN: 0976-3104

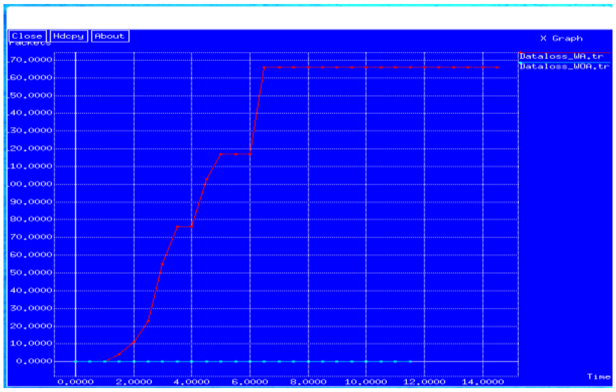


Fig: 5. Data Delivery Rate

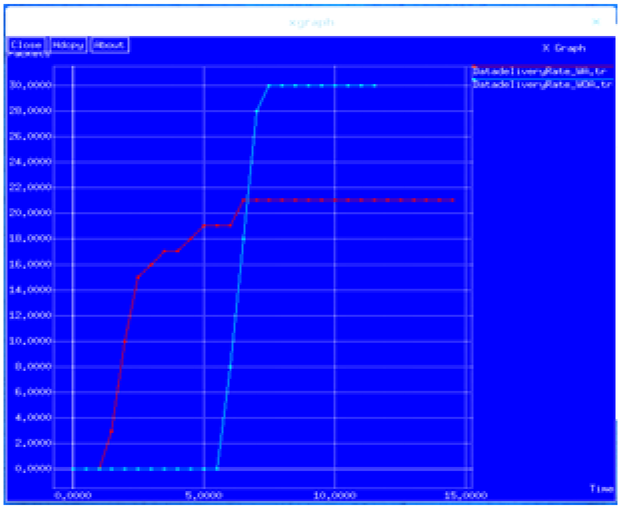


Fig:6. Data loss Rate

CONCLUSION AND FUTURE WORK

Our system makes use of cryptographic hash techniques that prevents server overloading. Collisions are minimized to a greater extent in the hash table. It also ensures that the information from the client reaches the server without any loss. Based on a particular application, the specified packet count can be deferred. The latency of our proposed system is high since there are various computations involved in the routers. The future work might involve reducing the latency of the system.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

The authors report no financial interests or potential conflicts of interest.

REFERENCES

[1] Ben-Porat et al. [2013], Vulnerability of Network Mechanisms to Sophisticated DDoS attacks, *IEEE Transactions on Computers*, 62(5): 1031-1043.

[2] Bin Xiao et al.[2006] A Novel Approach to Detecting DDoS attacks at an Early Stage, *Super Comp* 36: 325-248.

[3] Houle K.J and Weaver GM. [2001] Trends in Denial of Service Attack Technology, CERT Coordination Center, pp 1-21.http://www.cert.org/archieve/pdf/Dos_trends.pdf.

[4] Mehdi and Angela. [2012] Review of SYN Flooding attack Detection Mechanism, *IJDPS*,3 (1)

[5] Changhua S et al.[2007] A Novel Router based scheme to Mitigate SYN flooding DDos attacks, *IEEE Infocom*.

[6] Dalip Kumar. [2013] Analysis of IP Spoofed DDoS Attack by Cryptocraphy, *IJCEM*,16(2).

[7] Belenky A et al.[2003]Tracing multiple attackers with deterministic packetmarking (DPM), *Proc IEEE PACRIM*'03, Victoria, BC, Canada,] 49–52.

[8] Bin Xiao et al.[2006] A Novel Approach to Detecting DDoS attacks at an Early Stage, *Super Comp* 36:325-248.

[9] Wang H et al.[2002] Detecting SYN Flooding Attacks

[10] Praveena V et al [2012], Mitigating Technique to Overcome DDOS Attack.

[11] Guangsen Zhang et al. [2005] Cooperative Defense against Network Attacks.

[12] Keromytis A et al, 2004,SOS: An architecture for mitigating DDoS attacks.

[13] Ferguson P and Senie D,[1998] RFC-2267-Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.

[14] Robert Beverly and Steven Bauer.[2005] The spoofer project: Inferring the extent of Source Address Filtering on the Intenet, USENIX SRUTI: *Steps to reducing unwanted traffic on the internet workshop*, (2):53-59.

[15] Song D.X and Perrig A.[2001] Advanced and Authenticated Marking schemes for IP Traceback, proceedings of the IEEE Infocom *IEEE Computer Society*, Los Alamitos, Calif

[16] uwari B and Govindarasu M. [2006] Novel hybrid schemes employing packet marking and logging for IP traceback, *IEEE Trans. Parallel Distributed Syst*, 17(5): 403–418.

[17] John Ioannidis et al. [2002] Implementing Pushback: Router based defense against DDoS Attack, Internet Society.

[18] Wei-Shen Lai et al. [2008] Using Adaptive bandwidth a location approach to defend DDoS attacks, *International Journal of Software Enginewering and Its Applications*,2(4): 61-72.

[19] Pyungkoo et al. [2012] A Pseudo State based Distributed DoS Detection Mechanism using Dynamic Hashing, *Springer* , 22-29.

[20] Zaihongzhou et al,[009] A Novel Distributed Scheme against DDoS attack, *Journal of Networks*.4(9).

[21] Santhanam et al.[2006] Taxonomy of IP Traceback, *Journal of Information Assurance and Security* 1:. 79-94

[22] Nashet D et al.[2008] Router based Detection for low rate DDoS attacks, *IntConf of HPS*, 177-182.

**DISCLAIMER: *This article is published as it is provided by author and approved by guest editor. Plagiarisms and references are not checked by IIOABJ.*