ENHANCING NETWORK SECURITY BY MODIFIED SECURE DYNAMIC PATH IDENTIFIERS

AlbyAlphonsa Joseph[1], Chinju K[2], Dr. Vinodh P Vijayan[3]

[1]M.Tech Student, Department of Computer Science & Engineering, M G University, Kerala, India
[2] Assistant Professor, Department of Computer Science & Engineering, M G University, Kerala, India
[3] Associate Professor & Head of the Dept, Department of Computer Science & Engineering, Mangalam College of Engineering, Kerala, India

---***---

ABSTRACT - *A Distributed Denial of Service Flooding attack is the most highlighted and important attacks of today's cyber world. It is characterized by an explicit attempt by an attacker to prevent legitimate users from using resources. An attacker may attempt to flood a network and thus reduce a legitimate user's bandwidth, prevent access to a service, or disrupt service to a specific system or a user. Very few users are interests in using path identifiers to mitigate the DDoS flooding attacks in the network. Existing PIDs are static and also insecure. To address the above issue , in this paper we developed the design, implementation, and evaluation of secure dynamic path identifiers, a framework that uses dynamic secure PIDs (MDSPID) verified with every packet to avoid the DDoS flooding attacks. The experiments and results shows the proposed system achieved better result in terms of several QoS parameters.*

Keywords:- DDoSFlooding , Secure Dynamic Path Identifiers, End to End Delay, Level Checking, Packet Delivery Ratio

1. INTRODUCTION

Internet is confronted with serious security threats and it is very hard to defense against them due to the open environment of the Internet. Distributed-Denial-of-Service (DDoS) attacks pose a grave danger to Internet operation. They are resource overloading attacks. The aim of the attacker is to tie up a chosen key resource at the victim, usually by sending a high volume of legitimate traffic requesting some service from the victim. The overconsumption of the resource leads to degradation or denial of the victim's service to its legitimate clients. In the absence of effective defense mechanisms, the denial of service effect lasts for the entire duration of the attack and vanishes quickly once the attack is aborted. Various techniques and algorithmic protocols are designed and proposed by various authors for preventing from distributed denial of service attacks.

Many related works have been introduced in order to protect flooding attacks, containing color, lipsin, capability based designs, and ingress filtering. Several path based routing architectures have been proposed. In [3], the authors proposed pathlet routing, and define pathlets as fragments of paths that are constructed by sequences of virtual nodes. It tries to address the challenges of scalability and multipath routing for Internet routing, and the results show that the number of forwarding plane entries of pathlet routing is much smaller than that of the current BGP routing. LIPSIN [4] is a novel forwarding fabric based on the publish/subscribe architecture. It uses Link Ids and in-packet zFilters to forward packets and benefits from its simple forwarding decisions and small forwarding tables, so such system can scale up to metropolitan WAN sizes. However, both the two frameworks announce the path identifiers globally. Such feature makes the network risky for malicious attacks because of two reasons. First : it is easy for an attacker to directly send malicious packets to the target since the path identifiers are known globally .Second : it is difficult to dynamically change the path identifiers for enhanced security, due to the foreseeably vast overheads that will be caused by the notification messages. Disadvantages of existing system are easy to launch attacks if path identifiers arestatic, high complexity, less performance, more loss occur and high overhead. Existing path identifiers are static and also insecure. To overcome this problem we developed the design, implementation and evaluation of MDSPID. Modified secure dynamic path identifier is a framework that uses modified secure path identifiers verified with each packet to destory the DDoS flooding and spoofing attacks.

2. SYSTEM DESIGN

The MDSPID has several steps, where PID generation is the initial step. The main idea of generating PID is to dynamically change for inter-domain path. It also hides the node id in the selected path. For example if the selected path is A->B->C, then there will be a unique PID generated and assigned. In DPID, it doesn't include the update period. After each transaction the path identifiers will be updated. So there is a unique PID for each path after every transaction. This significantly reduces cost by eliminating time based PID updating. When the PID of the path changes to new PID based on the time, the ongoing communications may be interrupted. But this issue is destroyed in the proposed system. We propose a timestamp (Ts) mechanism method. The PID generation time is indexed with the Ts value. Based on these Ts, the content consumer can authenticate the received GET message to the network. If the Ts values are verified and transaction is completed, then a new MDSPIDs will be generated along the path.

2.1 MDSPID Generation

Each path from the origin to the destination has a PID and each node in the path has its unique anonymous node id ($AN_{ID)}$. A path is uniquely identified for every transaction by the MDSPID. The MDSPID is generated per-transaction based on the packet sequence number (seq) and the AN_{ID} .Use a modified Chaskey algorithm to produce this unique MDSPID and AN_{ID} in a secure manner. Thus for a given data packet for selected path, the MDSPID of a path representing the node AN_{ID} is computed as,

MDSPIDi= generateMDSPID(AN_{IDi}, seq)= C AN_{IDi}(seq) where C is the Chaskey block chipper function.

2.2 Timestamp Formation

Timestamp mechanism helps to detect the actual MDSPID generation and AN_{ID} generation time of each node in the network. Using the timestamp for MDSPID and data transmission that no can able to modify or make forgery, so the path identifiers can never be spoofed.

Step: 1. create two prime numbers (A) and (B)
Step: 2. selects a random number(r) as private key
Step: 3. C=B ^{x}modA
Step: 4. send [A,B,C] to each nodes Ni
Step: 5. send key C to each node Ni
Step: 6. Append T with C where T is the timestamp
Step: 7. selects a random value (K), and calculates two new values (x and y):
a. x=BKmodA
b. y=CKDmodA
Step: 8. Verification process
D(verify)=y/(X^x)modA where D is the data content.

3. ARCHITECTURE

The node 1 sends a request message to node 2. The node 2 will check the identity and the timestamp of its key value from the detector nodes. The decider and detector nodes are the centralized domain authority, which will provide the MDSPID for the requested transaction. The corresponding nodes will receive the MDSPID, here the MDSPID is a sequence binary number which has been created from the nodes anonymous id AN_{ID}, so, for every request, the validation will be performed and the respective GET message is transmitted to the requestor node. At the time of next requesting from node 1, the GET message appends the AN_{ID} details in the packet header. The node 2 will receive the GET message and validates the MDSPID and previous request id in the MDSPID index table. So the two levels of verification allow the node to detect and prevent the DDoS flooding attacks in the network.

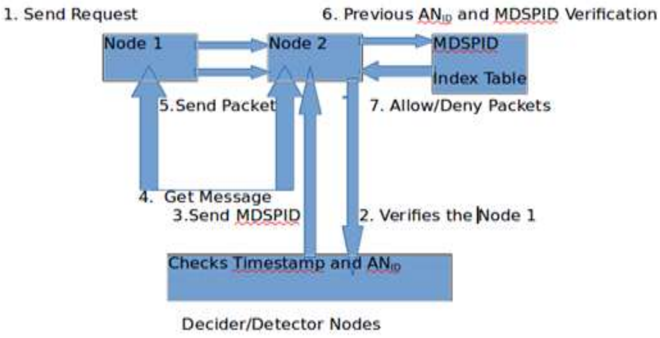

Fig -1: Process Flow Architecture

The MDSPID system is well suitable for the high mobility and scalable network infrastructure. In case multiple requests from multiple clients, the requesters are segregated into high and low priority nodes. This priority has been given based on the GET message. This is based on the probability of the attacks from the network, which the node made requests from.

4. EXPERIMENTAL IMPLEMENTATION

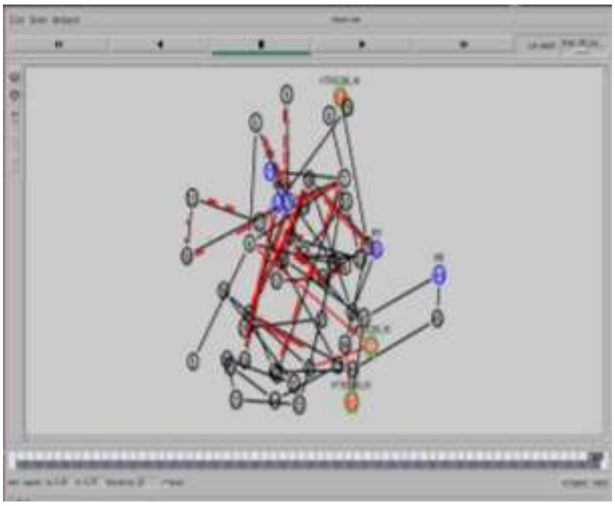

Fig -2: Two Level Checking to resolve DDoS Flooding Attack

This section evaluate the experimental setup and real time formation of the DDoS flooding attack in the wireless network. The prevention and detection technique of flooding attack is carried out in NS2 simulator with 50 mobile nodes. An efficient technique MDSPID is proposed to defend against DDoS flooding attack. This new scheme involves a two level checking of the client's request. These are, path-level and timestamping. The existing solutions to defend against TCP SYN flood and DDoS attacks involves checking only the client's availability, to confirm that the incoming packet is from a legitimate source. But, this does not ensure the security feature of non- repudiation. In the MDSPID scheme, the introduction of time stamping in the packet will provide security feature of nonrepudiation, which is not available in the existing schemes. To defend against the DDoS, new proposed solution of two levels checking process performed very efficiently .Each domain maintains a resource manager (RM) used to spread the reachability information of service identifiers. The blue color circle indicates resource manager at each domain. The red color indicates packet flows and acknowledgments of each domain. And also red line indicates no packet flow between nodes.Thehexagon green color indicates lure where the attacker locates. There are several ways for the attacker to obtains a subgraph of the whole Internet, and it can freely send packets within the range of this subgraph. After each transaction, the MDSPID should be updated. The effectiveness of the proposed scheme can be evaluated by checking the AN_{ID} and its previous identity at the destination with the PID, if the node id found in the MDSPID and it is similar to the timestamp value and table value, then it is a legitimate packet. If the timestamp value and node identity differs it can be spoofed packet. Two level checking allow the nodes to detect and prevent DDoS flooding attack in the network.

5. PERFORMANCE ANALYSIS AND RESULT

Xgraph allows to make graphs and used with ns2 .It collect statistical data synchronized. The system performance and its effects are analyzed and compared when a DDoSflooding attack is launched. The performance evaluation performed includes the packet delivery ratio, packet lost and end to end delay.

5.1 Packet Delivery Ratio

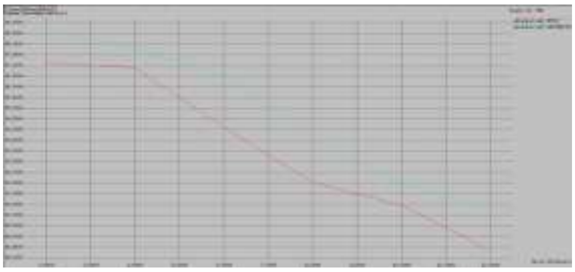

Fig -3: Graph for Packet Delivery Ratio

Packet delivery ratio is the ratio of number of packets delivered to the destination.
Packet delivery ratio = ∑ Number of packet receive /∑ Number of packet send
The greater value of packet delivery ratio means the better performance of the system.From the graph in Fig-3, it can be seen that in presence of DDoS attack, the packet delivery ratio of network drops significantly. Also, if more than one malicious node is present in the network, packet delivery ratio further decreases in any security attack. ModifiedSecurePID provides greater value of packet delivery ratio compared than DPID.

5.2 Packet Loss

It is the number of packets dropped or lost per unit time during simulation.
(∑ No. of packets sent - ∑ No. of packets received) / (Stop Time – Start Time)
Low value of packet loss corresponds to the better performance of the system.The figure 3 shows the number of packets dropped during simulation either because of malicious node or because of wireless nature of the network. As the number of malicious nodes increases, the effect of these nodes further increases. Instead of providing threshold for PID generation, the proposed system performs the PID generation and distribution at the end of the transaction. This distributes the PID only to the participated nodes in the transaction.

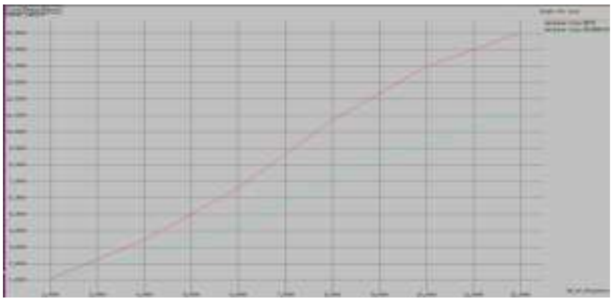

Fig -4: Graph for Packet Loss

5.3 End-to-End Delay

It is the average time taken by a data packet to arrive at destination from the source. It includes the delay caused by routing process and the queue in data transmission process.
End to End Delay = (Arrive time – send time) / ∑ Number of connections
Low value of End-to-End delay corresponds to the better performance of the protocol. The graph in Fig- 4 shows average end to end delay present in the transmission of packet. The results of the simulation show that the end to end delay keeps on increasing as the number of attacker nodes are increased in the network. The attacker nodes present in the network drop the packets and hence a retransmission is required.

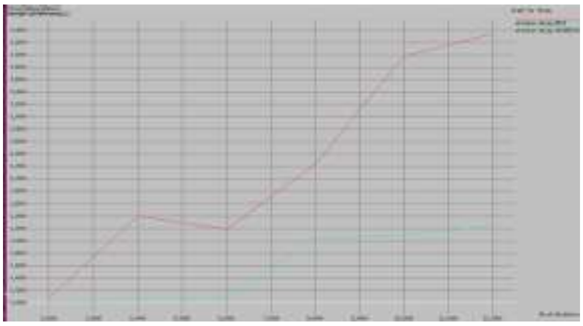

Fig -5: Graph for End-to-End Delay

5.5 Detection Ratio

The detection approaches depends on the nature of data that is available either from the end-users (source or victim) or the network.

Fig -6: Graph for Detection Ratio

The end-user information contains the data from TCP and UDP packets and it is specific to a particular user application. Various detection approaches are implemented on either source-end or victim-end. The graph in Fig- 6 shows that the detection ratio with respect to number of attackers .It also gives the overall resource utilization includes the GET message generation, verification and authentication. This graph compares the detection accuracy of the proposed MDSPID with timestamp scheme and the existing detection schemes such as the DPID.
In each trial, among the total number of packets, the number of legitimate and attack packets have equal weightage. As the proposed scheme is efficiently designed to detect and prevent the DDoS flooding attacks using system anomaly and traceback methods, when compared to the existing schemes, it shows improved detection accuracy. Though the number of packets increased, the proposed scheme shows 98.09%, 96.12% ,93.39% , 91.88 and 89.87 improvement in detection accuracy. This compares the results of detecting and preventing DDoS flooding attacks, spoofing and forgery attacks over the existing schemes. As the existing system do not follow the traceback detection scheme, their detection accuracy level is reduced over the proposed scheme. The results show the accuracy is increased when comparing with the earlier schemes.

6. CONCLUSION

Internet is confronted with serious security threats and it is very hard to defense against them due to the open environment of the Internet. In this paper, we have proposed a MDSPID mechanism to protect the network security. The attacker always aim to flood more packets and make DDoS attacks, this creates many issues like resource wastage, content delivery issues, malicious traffic etc. DDoS is the type of attack, which creates many issues which are difficult to solve. So there is a need to secure the network with optimal solution to thwart many attacks. To achieve this, the MDSPID system developed a new prototype which detects, mitigates and resolves the DDoS flooding, spoofing and PID forgery attacks. Path level and node level with timestamping allows two level verification of the requested data. This ensures authentication, anonymization and verification of the node and path identifiers. The results shows the proposed system achieved better result in terms of several quality of service parameters.

7. ACKNOWLEDGEMENT

It gives me great pleasure to deliver sincere thanks to my project guide Prof.Dr.Vinodh P Vijayan, Prof. Chinju K for their valuable guidance, constant encouragement and support. I appeal thanks to all the authors of the referenced papers as they help me and motivate me to work on this emerged area. Last but not least, I would like to deliver thanks to my family members, my colleague, and the people who directly or indirectly support me in this project work.

8. REFERENCES

[1] H. Luo, Z. Chen, J. Li, and A. V. Vasilakos, “Preventing distributed denial-of-service flooding attacks with dynamic path identifiers,” IEEE Transactions on Information Forensics and Security, vol. 12, issue 8, pp. 1801–1815, 2017.

[2] H. Luo, Z. Chen, J. Cui, H. Zhang, M. Zukerman, C. Qiao, “CoLoR: an information-centric internet architecture for innovations,” IEEE Network,vol. 28, no. 3, pp. 4 - 10, May 2014.

[3] P. B. Godfrey, I. Ganichev, S. Shenker, and I. Stoica, “Pathlet routing,” in Proc. SIGCOMM’09, Barcelona, Spain, pp. 111 – 122, Aug. 2009.

[4] Jokela, A. Zahemszky, C. E. Rothenberg, S. Arianfar, P. Nikander,“LIPSIN: Line Speed Publish/Subscribe Inter-networking,” in Proc.SIGCOMM’09, Barcelona, Spain, pp. 195 – 206, Aug. 2009.

[5] S. T. Zargar, J. Joshi, D. Tipper, “A Survey of DefenseMechanismsAgainst Distributed Denial of Service (DDoS) Flooding Attacks,” IEEE Commun. Surv. &Tut., vol. 15, no. 4, pp. 2046 - 2069, Nov. 2013.

[6] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Practical Network Support for IP Traceback,” In Proc. SIGCOMM’00, Stockholm, Sweden ,Aug. 2000 .

[7] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "DoS&DDoS in named-data networking," in Proc. IEEE ICCCN'13 , Nassau, Bahama, Aug. 2013.

[8] Z. Chen, H. Luo, M. Zhang, J. Li, "Improving network security by dynamically changing path identifiers in future Internet," in Proc. IEEE GLOBECOM'15, San Diego, CA, USA, Dec. 2015.

[9] N Mouha, BMennink, A Van Herrewege, D Watanabe, B Preneel, and I Verbauwhede. "Chaskey: an efficient MAC algorithm for 32-bit microcontrollers." In International Workshop on Selected Areas in Cryptography, pp. 306-323. Springer, Cham, 2014.

BIOGRAPHY

Alby Alphonsa Joseph. I have completed Bachelors in Computer Science & Engineering (BTech-CSE) from LMCST College, Kerala University and currently pursuing masters (MTech) in Computer Science & Engineering from School of Computer Sciences, Mahatma University. My research interests are Cloud computing, Database technologies, Network Security, Software Engineering.