IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 30-34

Prevention Of Distributed Denial Of Service Flooding Attacks Using Dynamic Random And Secure Path Identifiers

M.Newlin Rajkumar,Vickma. S, Susithra. D, Preetha Rexlin. P.L
(Master Of Engineering in Computer Science, Anna University Regional Campus, Coimbatore, Tamil Nadu, India)

***Abstract**: There are increasing interests in using path identifiers as inter domain routing objects. However, the static path identifiers will easily makes the attackers to launch the distributed denial of service (DDoS) flooding attacks .To overcome this effect, for every transmission of packets the path identifiers is kept secret and will get updated dynamically. But there is a possibility that the attacking node will compromise the other nodes to take the overall control towards it. To prevent this issue, Dynamic random and secure path identifiers are used (DSPID). This paper analyses the network ingress filtering, IP trace back techniques to verify and guarantee that the incoming packets are really come from the legitimate networks. This work proposes the concept of providing the anonymous unique path identifiers to every nodes.*

***Keywords:** Distributed Denial of Service attacks, Inter domain routing, Ingress Filtering, IP trace back.*

I. Introduction

The fast and excellent growth of internet is sometimes interrupted by many types of security threats. Distributed Denial of Service (DDOS) flooding attacks are the top most harmful issue in the internet. Here, the attacker creates congestion, traffic to the target host with the use of distributed zombies, so that the attacker will spread large amount of traffic to the legitimate user host, this will restrict the legitimate users from accessing to the network services. At the time of DDoS attacks, an online service can be brought down by overwhelming it with traffic from multiple sources. Many incidents with DDOS attacks exist recently, which affected the network for a period of time. So, in order to protect network from the DDOS flooding attacks several techniques were proposed. The DDOS flooding attacks can be prevented by using network ingress filtering, IP traceback techniques. The Ingress filtering technique is used to guarantee that the incoming packets are really come from the legitimate networks. In the IP traceback approach, the packet source of malicious traffic can be identified.

Recently there are increasing interests in using path identifiers PIDs that identify paths between network entities as inter-domain routing objects, this not only helps addressing the routing scalability and multi-path routing issues , but also can facilitate the innovation and adoption of different routing architectures . For instance, Godfrey et al. proposed pathlet routing, in which networks advertise the PIDs of pathlets throughout the Internet and a sender in the network constructs its selected pathlets into an end-to-end source route. Jokela et al. proposed to assign identifiers to links in a network and to encode the link identifiers along the path from a content provider to a content consumer. Luo et al. proposed an information-centric internet architecture called CoLoR that also uses PIDs as inter-domain routing objects in order to enable the innovation and adoption of new routing architectures.

II. Literature Survey

2.1 Off By Default

Capabilities based networks presented a fundamental shift in the security design of network architectures. This capabilities based protocol performs verification on every hop in the network. Instead of permitting the transmission of packets from any source to any destination, the routers deny forwarding of packets by default. For a successful transmission of packets need to positively identify themselves and their permissions to the router. A major challenge is an efficient design of the credentials that are carried in the packet and the verification procedure on the router. A capabilities based system that uses packet credentials is based on Bloom filters. The credentials are of fixed length and can be verified by routers with a few simple operations. By this high-performance design of capabilities, the traffic is verified on every router in the network and limits the unauthorized traffic with only a small per-packet overhead.

2.2 Capability Based Designs

One of the fundamental limitations of the Internet is the inability of packet flow recipient to halt disruptive flows before they consume the recipient's network link resources. By using SIFF, a Stateless Internet Flow Filter, allows an end-host to selectively stop individual flows from reaching its network. By dividing all network traffic into two classes, privileged (prioritized packets subject to recipient control) and unprivileged

(legacy traffic)Privileged channels are established through a capability exchange handshake. Capabilities are verified statelessly by the routers in the network, and can be revoked by quenching update messages to an offending host. SIFF is transparent to legacy clients and servers.

2.3 Color

An information-centric Internet architecture called CoLoR couples the service location and inter-domain routing while decoupling them from forwarding.

Implementation and analysis shows that CoLoR is promising since it satisfies many requirements of the future Internet, including being information-centric, encouraging innovations, and providing efficient support for mobility, multicast, multi-homing, and middleboxes.

2.4 Dynamic Path Identifier

By using the static path identifier makes the attackers to launch the distributed denial of service attack. To overcome this path identifiers are kept secret during every transmission of packets and then updated dynamically. The communications are initiated by means of receivers in dynamic path identifier. It is based on content granularity and it can easily mitigates the DDOS attacks.

2.5 Traceback Mechanism

Nowadays collaborative applications are feasible and more popular due to internet working advancement. This is based on the applications which includes space research, military application, e governance, e-health care system. In these applications, computing resources for particular organization spread and communication is achieved through the internet. Therefore the resources must be protected against the security attacks. A survey on the Arbor network reveals that approximately 1200DDOS attacks occur. To counter these attacks in a collaborative environment, all the routers need to work by exchanging its caveat messages with their neighbor.

2.6 Defense Mechanism Against Ddos

This paper is focused on the scope of the DDOS flooding attack problem and attempts to combat it. The main primary intension of this work is to stimulate the research community on developing creative, efficient, effective, prevention, detection and response mechanism that addresses the DDOS flooding problem before, during and after the actual attack. In distribution, detection and response are deployed at various locations; Here the detection usually occurs at destinations and intermediate networks, and response usually occurs at the sources & upstream routers near the sources.

2.7 Dos Attacks In Manet

Mobile Ad hoc Networks includes dynamic topology, wireless radio medium, limited resources and lack of centralized administration; so as a result there is a higher chance of affecting the MANET by different types of attacks in different layers. Here each node are capable of acting as a router, the routing has various security concerns. This paper is focused on different types of DOS attacks like Warmhole attack , blackhole attack, Grayhole attack.

2.8 Manet Attacks

Compared to the wired network, due to the lack of a trusted centralized authority MANETs are more vulnerable to security attack. Here in a MANET, nodes within each other wireless transmission ranges can communicate directly; however, nodes outside each other range relied on some other nodes to relay messages. This shows how routing protocol encapsulates an essential set of security mechanism. These mechanism prevent, detect and respond to a security attack.

2.9 Proposed System

The problem definition is that the PIDs are globally advertised. So, an end user knows the PID(s) toward any node in the network. Accordingly, attackers can launch DDoS flooding attacks.And the existing system generated DPID is still not properly performed. When the source node request for the DPID to the other node before transmitting the packets, there is a possibility that the attackers can take overall control of the end user by responding them with same DPID and also there is a chance that the attacking node will compromise all the other nodes to launch the flooding attack.

In the proposed work, DDOS flooding attack, PID forgery and spoofing attacks are concentrated. So, a new prototype named as Dynamic secure path identifiers (DSPID) is proposed. It set Anonymous unique ID and timestamp to all the nodes that cannot be identified by the attacking nodes .Whenever the content provider request for the path identifier, the respective content consumer will respond the provider with its anonymous id and corresponding timestamp.

This work effectively mitigates and resolves DDoS flooding attacks with enhanced random anonymous secure path identifiers. To avoid PID forgery and PID spoofing, a newly improved Timestamp calculation and verification schemes were used. For secure dynamic PID generation a new MAC algorithm is used, which is based on the Chaskey algorithm.

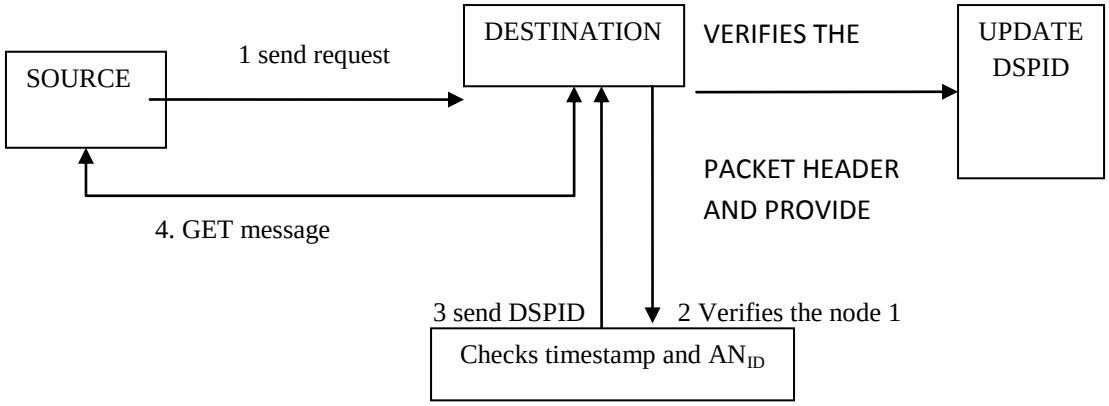

Fig-1: Architecture Diagram

III. Algorithm Proposed

There are three algorithms have been proposed to mitigate DDoS attack in wireless network.

3.1 Node Unique ID Generation and Timestamp Embedding:

Every node in the network receives a unique node id, which is created for anonymous the transaction to avoid the selective flooding attack in the network. The generation process of the node id is given below.

AN_{ID} Generation Process:

Notations: Gt- timestamp value, Node Ni, D-data content

Step: 1. create a prime number (A) and a number (B)
Step: 2. selects a random number(R) as private key
Step: 3. $C=B^{\times} \text{mod} A$
Step: 4. send ([A,B,C] to every nodes Ni
Step: 5. send key C to every node Ni respectively
Step: 6. Join Gt with the C.
Step: 7. selects a random value (T), and calculates two new values (x and y):
  a. where T is a random number (Ex: T= 80)
  b. x=BTmodA
Step: 8. y=CTDmodA
Step: 9. Verification process
  - $D(\text{verfiy})=y/(x^{x})\text{mod}A$

The algorithm represents the overall key generation and verification of the proposed work. This performs key generation, management and key verification process on the requested data.

3.2 Chaskey:

With data D, it is proven secure up to $T = 2^{128}/D$ evaluations of π.
Best data/time tradeoff: $D = T = 2^{64}$.
In case |m| = 0. It also takes a 128-bit key K, which must be chosen independently and uniformly at random from the entire key space. From K, two 128-bit subkeys K1 and K2 are derived, each by means of a 128- bit shift and a 128-bit conditional XOR.

The NID is generated per-node based on the top-k packet sequence number (seq) and the secret key Ki of the query responsor node.

IV. System Implementation

4.1 Module Description

4.1.1 Network construction and route discovery

The first module is initial network construction with 50 mobile nodes. The system simulated the proposed scheme by using the ns-2 network simulator. In the simulation, 35 mobile nodes are placed within a square area of 1800 m × *18*00 m. this use Random Mobility model to determine movements of mobile sensor nodes. In the Random mobility model, each node moves to a randomly chosen location with a randomly selected speed between a predefined minimum and maximum speed. After reaching that location, it stays there for a predefined pause time. It then randomly chooses another location after that pause time and moves to that location. This

random movement process is repeated during a simulation time. The proposed DSPID framework provide a proactive way to protect the data from DDoS attacks.

4.1.2 Route discovery

RREQ: DSPID-AODV routing protocol is based upon distance vector and uses destination numbers to determine the node failure prediction of routes along with the rebuild constraints. DSPID -AODV is capable of failure less routing. DSPID -AODV requires hosts to maintain only active routes, for example the route used to forward at least one packet within the past active timeout period. When a host needs to reach to destination and does not have an active route, it broadcasts a route request (RREQ) packet, which is disseminated in the network.

RREP: A (RREP) route reply is replied back to the source of RREQ to establish the route in the network. It uses HELLO message to determine the connectivity among the neighbors. Along with the RREP, the receiver authentication key will be updated.

4.1.3 Attacker Model

There are many scenarios are taken to determine the correctness in the attacker model. In the first scenario, the legitimate user tries to access the PID for the first time, and tries to do DDoS flooding. In the second scenario, the attacker who acts like a legitimate node with spoofed node ID and tries to access the PID for the first time sends an illegitimate request to the source to obtain the GET message. In the third scenario, the attacker spoofs the source IP address of a legitimate node, when the client is not connected to the network or not involved with the transaction. At every scenario, the defense scheme should work well. Due to DDoS flooding, many packets can be dropped. This unexpected behavior from a compromised node should also be tracked. When an attacker interrupts the transaction by spoofing or with the forgery ID, this can be identified by verifying the timestamp value.

4.1.4 DSPID Generation:

For a data packet transmission, DSPID refers to generating the vertices in the PID graph and inserting them into the Chaskey encode table (CET). 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 DSPID. The DSPID is generated per-transaction based on the packet sequence number (seq) and the AN_{ID}. We use a Chaskey algorithm to produce this unique *DSPID* and AN_{ID} in a secure manner.

4.1.5 Timestamp Generation:

This helps to detect the exact DSPID generation and AN_{ID} generation time of every in the network. This **Time stamping** is used to hold the PID without keeping track of the creation and modification time of an ID and its updating. Using the timestamp mechanism for DSPID and data transmission process that no can able to modify or make forgery, so the PID can never be spoofed.

V. Result

The proposed work performs effectively and resolves flooding Attacks with random anonymous secure path identifiers. The existing PID is replaced with dynamic generation feature and then improved as D-PID; similarly D-PID is improved with additional features and named as improved dynamic and random secure PID (DSPID) for fast and secure routing.

Here the source node request the destination node to provide its PID.The provider is responded with anonymous unique ID and timestamp values.The content provider verifies and transmit the packets to the node. Most importantly DSPID gets updated dynamically.

VI. Conclusion

Dynamic and random secure path identifier is an eminent way to detect and prevent the distributed denial of service attack. The detect information includes the need if anonymous secure unique identifiers and timestamp value. The proposed scheme posess many advantage to avoid spoofing attack, PID forgery. The idea can be implemented in large scale to facilitate better safety to the internet in the future work.

Acknowledgement

I would like to express my gratitude to my guide Dr.M.NEWLIN RAJKUMAR.,M.E.,Ph.D, for guiding me properly in my project work and for helping to solve the project work difficulties. I would also like to thanks all the staff members of computer science and engineering department for supporting me and guiding me in my project work whenever required.

References

1. H. Ballani, Y. Chawathe, S. Ratnasamy, T. Roscoe, S. Shenker, "Off by default!," In Proc. HotNets-*IV*, Nov. 2005, College Park, MD, USA
2. A. Yaar, A. Perrig, and D. Song, "SIFF: a stateless internet flow filter to mitigate DDoS flooding attacks," In *Proc*. IEEE Symposium on Security and Privacy, May 2004, Oakland, CA, USA.
3. 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.
4. Luo, Hongbin, Zhe Chen, Jiawei Li, and Athanasios V. Vasilakos. "Preventing Distributed Denial-of-Service Flooding Attacks With Dynamic Path Identifiers.
5. P.Arun Raj Kumar, S.Selvakumar " Distributed denial of service DDOS Threat in Collaborative Environment – A Survey on DDOS attack tools and traceback mechanisms" 2009 IEEE International Advance Computing Conference
6. Saman Taghavi Zargar, Member, IEEE, James Joshi, Member, IEEE and David Tipper, Senior Member, IEEE – "A survey of Defense Mechanisms Against Distributed Denial of Service (DDOS) flooding attacks"
7. Rutvij H. Jhaveri, Sankita S. Patel, Devesh C. Jinwala "DOS attacks in Mobile Ad-hoc Networks" 2012 second International conference on Advanced Computing & communication techniques.
8. Pradip M. Jawandhiya "A Survey of Mobile Ad hoc Network Attack" International journal of Engineering Science and technology vol.2(9), 2010, 4060-4071
9. Nshunguye Justin, Nitin R. Gavai "A Survey On Intrusion Detection System for DDOS Attack in MANET" In IJARCCE: International Journal of Advanced Research in computer and communication Engineering Vol. 5, Issue 4, April 2016
10. Varsha Raghuwanshi, Simmi Jain "Denial of Service Attack On VANET: " International Journal of Engineering Trends and Technology (IJETT) – Volume 28 November1-october 2015