International Journal of Scientific Engineering and Science
Volume 1, Issue 10, pp. 24-27, 2017. ISSN (Online): 2456-7361

Mobility Aware Route Selection and Packet Scheduling Using Dynamic Secure Path Identifier

T. Parameswaran[1], S. Vickma[2]
[1, 2]Department of Computer Science, Anna University Regional Campus, Coimbatore, Tamil Nadu, India-641046

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**—** *Inter domain routing, distributed denial of service attacks, 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, pathlet routing was proposed by Godfrey et al., through the 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 architecture known as CoLoR that also uses PIDs as inter-domain routing objects in order to enable the innovation and adoption of new routing architectures.

There are two different use cases of PIDs. In the first case, the PIDs are globally advertised. As a result, an end user knows the PID(s) toward any node in the network. Accordingly, attackers can launch DDoS attacks as they do in the current Internet. In the second case, conversely, PIDs are only known by the network and are secret to end users. In the latter case, the network adopts an information-centric approach where an end user (i.e., a content provider) knows the PID(s) toward a destination (i.e., a content consumer) only when the destination sends a content request message to the end user. After knowing the PID(s), the end user sends packets of the content to the destination by encapsulating the PID(s) into the packet headers. Routers in the network then forward the packets to the destination based on the PIDs.

It seems that keeping PIDs secret to the end users makes difficult for attackers to launch flooding attacks since they do not know the PIDs in the network. However, keeping PIDs secret to end users is not enough for preventing DDoS flooding attacks if PIDs are static. To address this issue, the design, implementation and evaluation of a dynamic PID (D-PID) mechanism are used. In D-PID, two adjacent domains periodically update the PIDs between them and install the new PIDs into the data plane for packet forwarding. Even if the attacker obtains the PIDs to its target and sends the malicious packets successfully, these PIDs will become invalid after a certain period.

II. LITERATURE SURVEY

A. 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, 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.

B. Capabillity 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, but only updated hosts will enjoy the benefits of it. The routers simply discard the packet when it is not accepted by an end host.

C. 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.

D. 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.

E. 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.

F. 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 by means of various locations; Here the detection usually occurs at intermediate network and destination, and response usually occurs at the sources & upstream routers near the sources.

G. 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. Here the route can be determined without holdup. This paper is focused on different types of DOS attacks like Warmhole attack, blackhole attack, Grayhole attack.

H. 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. It discovers the secure route of nodes and it is also

I. Intrusion Detection System

The Intrusion Detection System (IDS) is used to discover the intrusion from the network packet data or system audit data. The major problem is packet data are overwhelming. So, there was a necessary to reduce the size of the data. In order to perform this markov layer discovery and genetic algorithm were proposed in this paper. The intrusion Detection System is distributed in nature. So, each node of a MANET are equipped with an IDs.

J. DOS Attack on Vanet

VANET is a life saving factor which has more attention on automotive industries and researchers. The paper is based on survey of attack on network availability and its security environment. Here the nodes are represented as self organizing and self managing information. The Working is based on combining the equipped devices along with computer equipment, sensor and wireless communication. Therefore the vehicle nodes on the roads can know the speed of the neighbor vehicle. So, the vehicle could send the warning messages to its neighbor to predict the speed in order to avoid the chance of accidents on the road. DOS attack on VANET has no fixed access point.

TABLE I. Various Techniques, Features, Advantages, Drawbacks.

Technique	Description	Features	Advantages	Drawbacks
Off by default [1]	Two hosts are not permitted to communicate by default.	IP-Prefix granularity	unwanted communication is eliminated.	This technique cause significant routing dynamics. The allowed IP-prefixes of an end hosts change often. The destinations need to re-send GET messages.
Capability-based designs [2]	Sender gets permission upon sending data packets	communications are initiated by receivers in D-PID	The routers simply discard the packets when it is not accepted by the end host.	capability-based approaches are vulnerable to "denial of capability" attacks,
COLOR [3]	It is based on coupling Service location and inter-domain routing while decoupling them from forwarding the packets	receiver-driven information centric network architecture	COLOR assigns every content a persistent and unique SID which is application-independent and location-independent	COLOR needs to choose the path identifiers if there are multiple path identifiers between two domains
D-PID [4]	Information-centric network architecture with dynamic PID	Content granularity. communications are initiated by receivers in D-PID	PIDs are kept secret and change dynamically in D-PID. D-PID effectively mitigates denial-of capability" attacks,	Routing scalability and multi-path routing issues arises Time for PID updation should be given.
Traceback [5]	Routers are need to work by exchanging its messages with their neighbor	Encodes the information and reconstruction process is done by mark recognition and recovery	To detect the unknown attack and trace the real source in very less time.	Little scalability to high attacker population. Poor performace in presence of router
Defense mechanism against DDOS [6]	Detection and response are deployed at various locations	Detection occurs at destination & intermediate nodes Response usually occurs at the sources & upstream routers.	Aims to detect and respond to attack traffic at the source and before it wastes lots of resources. More resources at various levels(eg. source, destination and network) are available to tackle DDOS attacks	Need trusted communications among various distributed components to collaborate/cooperate. High storage and processing overhead at the routers
DOS attacks in MANET [7]	Using a common neighbors acting as a watchdog to detect the attack and discover the new route if there is a blackhole present	Common neighbor listening and Route confirmation request reply	Route can be selected without any kind of holdup	Doesn't work if two consecutive nodes are malicious Routing control overhead Increase average end to end delay
MANET attacks [8]	Verifying the authenticity of the node by sending the reply packet and wait for reply packets from more than one node	Reply packet authenticity Last packet sequence number	Discovers secure route of nodes Trust based approach that uses passive acknowledgement	Longer time delay, The malicious nodes can listen to the channel and update the tables for the last packet sequence number
INTRUSION DETECTION SYSTEM [9]	IDS are distributed in nature, each node of a MANET are equipped with an IDs	Signature based intrusion detection Anomaly based intrusion detection	Doesn't require prior information of the node Reduce the limitation problem	If there is an attack and its signature is not in the IDS database then IDS cannot detect

III. 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 as they do in the current Internet. And the existing system generated DPID to overcome the DDOS attacks, but the security for 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.

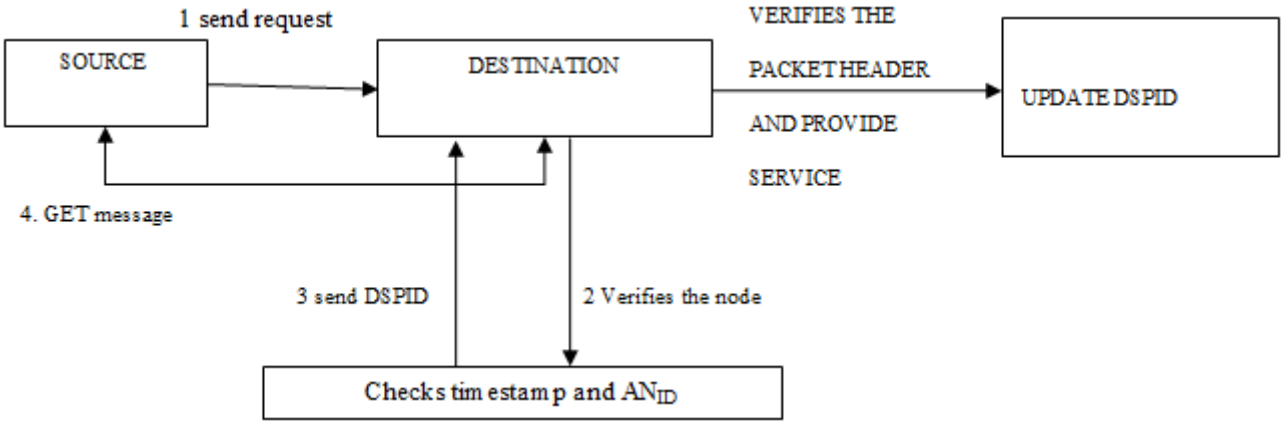

Fig. 1. Architecture diagram.

IV. 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.

V. 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.

Acknowledgment

I would like to express my sense of gratitude to my guide Dr. T. Parameswaran., 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, and 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, and M. Zukerman, C. Qiao, "CoLoR: An information-centric internet architecture for innovations," *IEEE Network*, vol. 28, no. 3, pp. 4-10, 2014.

[4] 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.

[5] P. Arun, R. Kumar, and S. Selvakumar, "Distributed denial of service DDOS threat in collaborative environment – A survey on DDOS attack tools and traceback mechanisms," *IEEE International Advance Computing Conference*, 2009.

[6] S. Taghavi Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," *IEEE Communications Surveys & Tutorials*, 2013.

[7] R. H. Jhaveri, S. S. Patel, and D. C. Jinwala, "DOS attacks in mobile ad-hoc networks- A survey," *Second International Conference on Advanced Computing & Communication Techniques*, 2012.

[8] P. M. Jawandhiya, "A survey of mobile ad hoc network attack," *International Journal of Engineering Science and Technology*, vol.2, issue 9, pp. 4060-4071, 2010.

[9] N. Justin and N. R. Gavai "A survey on intrusion detection system for DDOS attack in MANET," *International Journal of Advanced Research in computer and communication Engineering*, vol. 5, issue 4, pp. 1160-1163, 2016

[10] V. Raghuwanshi and S. Jain, "Denial of service attack on VANET: A survey," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 28, no. 1, pp. 15-20, 2015.

[11] J. Francois, I. Aib, and R. Boutaba, "Firecol: A collaborative protection network for the detection of flooding DDOS attacks," *IEEE/ACM Trans. on Netw.*, vol. 20, no. 6, pp. 1828-1841, 2012.

[12] OVH hosting suffers 1Tbps DDoS attack: largest Internet has ever seen. [Online] Available: https: //www.hackread.com/ovh-hosting- suffers-1tbps- ddos-attack/

[13] .602 Gbps! This May Have Been the Largest DDoS Attack in History. http://thehackernews.com/2016/01/biggest-ddos-attack.html.

[14] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surv. & Tut.*, vol. 15, no. 4, pp. 2046-2069, 2013.

[15] P. Ferguson and D. Senie, "Network ingress filtering: Defeating denial of service attacks that employ IP source address spoofing," *IETF Internet RFC 2827*, 2000.

[16] K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets," In *Proc. SIGCOMM'01*, San Diego, CA, USA, Aug. 2001.

[17] A. Yaar, A. Perrig, and D. Song, "StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense," *IEEE J. on Sel. Areas in Commun.*, vol. 24, no. 10, pp. 1853-1863, 2006.

[18] H. Wang, C. Jin, and K. G. Shin, "Defense against spoofed IP traffic using hop-count filtering," *IEEE/ACM Trans. on Netw.*, vol. 15, no. 1, pp. 40-53, 2007.

[19] Z. Duan, X. Yuan, and J. Chandrashekar, "Controlling IP spoofing through interdomain packet filters," *IEEE Trans. on Depend. and Secure Com- puting*, vol. 5, no. 1, pp. 22-36, 2008.

[20] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical net-work support for IP traceback," In *Proc. SIGCOMM'00*, Stockholm, Sweden, 2000.