International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

A Survey on Preventing distributed denial of service attacks and data security

Korrai Vamsi Krishna1, K.Narayana Rao2
1 Pg Scholar Department Of Cs,Au College Of Engineering ,Andhra University,Visakhapathnam,Andhra Pradesh 530003.
2 Reasearch Scholar Department Of Cs&Se, Au College Of Engineering ,Andhra University,Visakhapathnam,Andhra Pradesh 530003.

Abstract:
Amid my exploration for this postulation ,In a DDoS assault, the assault utilizes generally dispersed zombies to send a lot of activity to the objective framework, subsequently keeping real clients from getting to organize assets. In the meantime, as of late here are expanding interests in utilizing way identifiers PIDs that distinguish ways between system elements as between area directing items, since doing this not just aides tending to the steering versatility and multi-way steering issues yet in addition can encourage the and reception of various steering structures. For example, Godfrey et al. proposed path let steering ,which systems publicize the PIDs of path throughout the Internet and a sender in the system develops its select path lets into a conclusion to-end source course.

I.INTRODUCTION

Distributed Denial of Service (DDoS) is the organized endeavor to bargain the accessibility of system resources or servers as appeared in figure 1. These attacks make money related misfortunes by hindering true blue access servers and online administrations. To moderate the effect of these attacks solid safeguard components are required that can identify and prevent progressing attacks. Numerous resistance instruments have been proposed and sent at different areas in current web. The viability of these systems relies upon the execution exchange offs and cost acquired in deployment.

DDoS recognition systems recognize the deviation of movement from typical conduct. This activity is named attack movement and afterward obstructed by proper resistance instrument. For exactness the recognition system should bring about low false positive and false negative rate. At the same time, in recent years there are increasing interests in using path identifiers PIDs that identify paths between network entities as inter-domain routing objects, since doing this not only helps addressing the routing scalability and multi-path routing issues [21], but also can facilitate the innovation and adoption of different routing architectures [22]. For instance, Godfrey et al. proposed pathlet routing [21], 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. Koponen et al. further argued in their insightful architectural paper that using pathlets for inter-domain routing can allow networks to deploy different routing architectures, thus encouraging the innovation and adoption of novel routing architectures [22]. Jokela et al. proposed in LIPSIN 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 into a zFilter (i.e., a PID), which is then encapsulated into the packet header and used by routers to forward packets. Luo et al. proposed an information-centric internet architecture called CoLoR [24] that also uses PIDs as inter-domain routing objects in order to enable the innovation and adoption of new routing architectures, as in [22].

There are two different use cases of PIDs in the afore-mentioned approaches. In the first case, the PIDs are globally advertised (as in pathlet routing [21] and [22]). As a result, 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. In the second case, conversely, PIDs are only known by the network and are secret to end users (as in LIPSIN [23] and CoLoR [24]). In the latter case, the network adopts an information-centric approach [25] - [27] 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 end users (as in [23], [24]) makes it difficult for attackers to launch DDoS 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. For example, Antikainen et al. argued that an adversary can construct novel zFilters (i.e., PIDs) based on existing ones and even obtain the link identifiers through reverse-engineering, thus launching DDoS flooding attacks [28]. Moreover, as it is shown in Sec. II-B, attackers can launch DDoS flooding attacks by learning PIDs if they are static.

To address this issue, in this paper, we present the design, implementation and evaluation of a dynamic PID (D-PID) mechanism. 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 and the subsequent attacking packets will be discarded by the network. Moreover, if the attacker tries to obtain the new PIDs and keep a DDoS flooding attack going, it not only significantly increases the attacking cost but also makes it easy to detect the attacker In particular, our main contributions are two fold.

On one hand, we propose the D-PID design by addressing the following challenges. First, how and how often should PIDs change while respecting local policies of autonomous systems (ASes)? To address this challenge, D-PID lets neigh-boring domains negotiate the PIDs for their inter-domain paths based on their local policies (Sec. III-B). In particular, two neighboring domains negotiate a PID-prefix (as an IP-prefix) and a PID update period for every inter-domain path connecting them. At the end of a PID update

period for an inter-domain path, the two domains negotiate a different PID (among the PID-prefix assigned to the path) to be used in the next PID update period. In addition, the new PID of an inter-domain path is still kept secret by the two neighboring domains connected by the path.

Second, since inter-domain packet forwarding is based on PIDs that change dynamically, it is necessary to maintain legitimate communications while preventing illegal commu-nications when the PIDs change. To address this challenge, D-PID lets every domain distribute its PIDs to the routers in the domain (Sec. III-C). For every inter-domain path, the routers in a domain forward data packets based on the PID of the previous PID update period and that of the current PID update period. In addition, D-PID uses a mechanism similar to the one that the current Internet collects the minimum MTU (maximum transmission unit) of networks so that a content consumer knows the minimum update period of PIDs along the path from a content provider to it Based on this period, the content consumer periodically re-sends a content request message to the network in order to renew the PIDs along the path.

Third, the overheads incurred by changing PIDs should be kept as small as possible. This includes not only the overhead in negotiating PIDs by neighboring domains, but also the overhead for a domain to distribute the updated PIDs to routers in the domain, and that for transmitting content request messages resent by content consumers. To address this challenge, the PID prefix assigned to an inter-domain path is unique among the PID prefixes assigned by the two domains connected by the inter-domain path.

2.LITERATURE SURVEY:

We discourse the problematic of DDoS attacks and extant the theoretical foundation, arc hitecture, and algorithms of FireCol. The core of FireCol is collected of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. We recommend the StackPi design, a new packet marking scheme based on Pi , and new sieving mechanisms. The StackPi marking structure involves of two new marking methods that noticeably rally Pi's incremental deployment performance: Stack-based marking and write-ahead marking. Our outline almost fully eliminates the outcome of a few bequest routers on a path, and performs 2-4 times improved than the original Pi scheme in a thin deployment of Pi-enabled routers.

3.PROBLEM DEFINTION:

D-PID is based on information-centric system building and works at the happy granularity. The IP-prefixes that a conclusion hor de wants to accept packets from are broadcasted during the Internet in the “off by default” line, which may origin substantial routing undercurrents if the acceptable IP-prefixes of end hosts change commonly. On the other hand, the PIDs are kept undisclosed and change enthusiastically in D-PID. While this acquires cost then destinations need to re-send GET messages,

4.PROPOSED APPROACH:

- The arrangement recommends the D-PID plan by talking the following challenges. First,

how and how often should PIDs change while in respect of local policies of autonomous systems? To discourse this challenge, D-PID let's next domains convert the PIDs for their inter-domain paths based on their local guidelines.

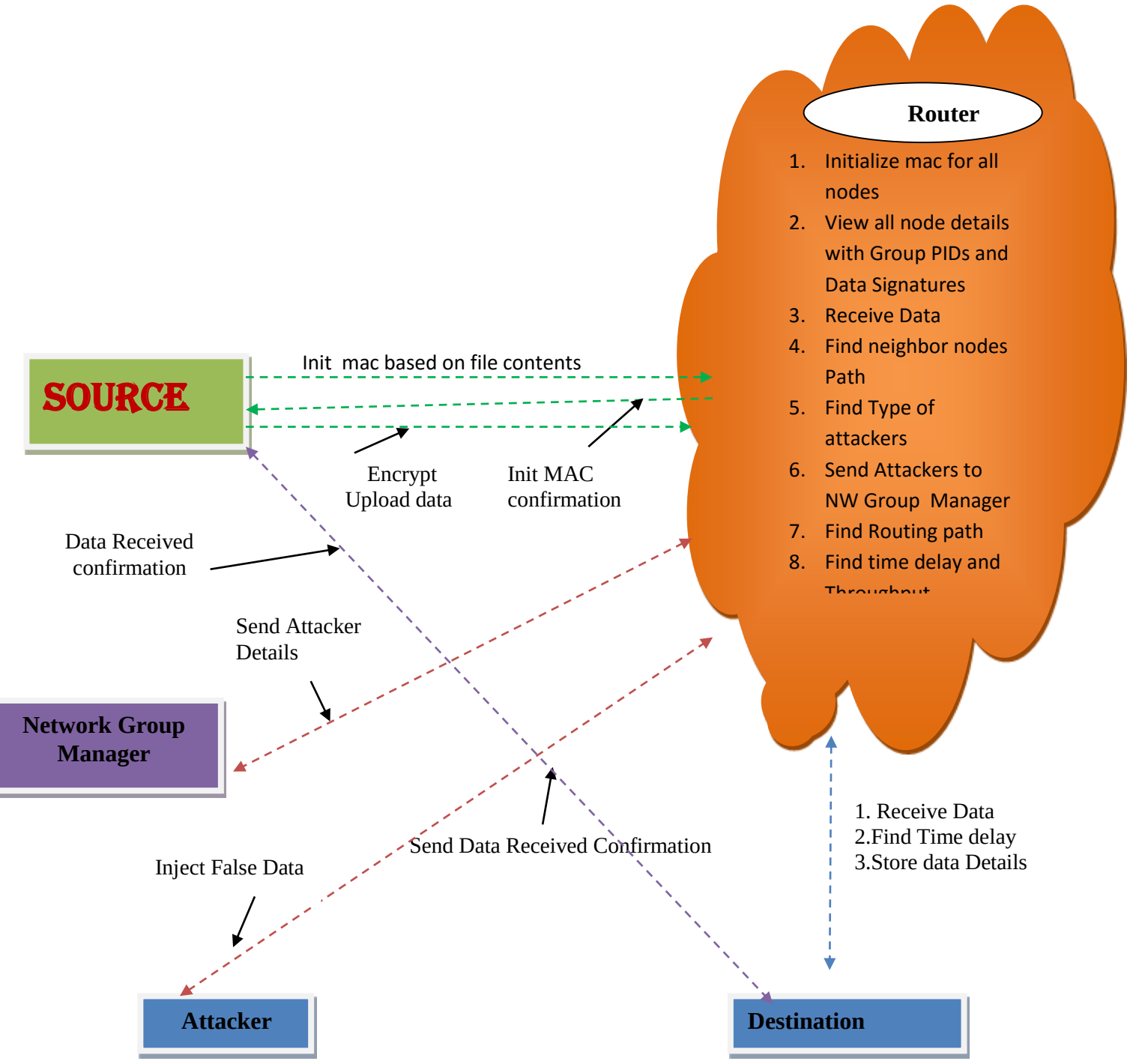
- **Source**

In this module, the Source will browse an file, assign signature to all nodes, assign group PIDs to all groups (group1, group2 and group3) and then send to particular user (A, B, C, D and F). After receiving the file he will get response from the receiver. The Source can have capable of manipulating the data file and initializing keys / PIDs to all nodes before sending data to touter.

- **Router**

The Router manages a multiple Groups (Group1, Group2, Group3, and Group4) to provide data storage service. In Group n-number of nodes (n1, n2, n3, n4…) are present, and in a Router will check all PIDs and it will select the Neighbor node path. The router also will perform the following operations such as Initialize mac for all nodes, View all node details with Group PIDs and Data Signatures, Receive Data, Find neighbor nodes Path ,Find Type of attackers, Send Attackers to NW Group Manager, Find Routing path, Find time delay and Throughput.

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018



- **Group Manager**

In this module, the group manager can distribute key for each and every group (Group1, Group2 and Group3) and a group each node has a pair of group public/private keys issued by the group manager. Group signature scheme can provide authentications without disturbing the anonymity. Every member in a group may have a pair of group public and private keys issued by the group trust authority (Group Manager). Only the group trust authority (Group Manager) can trace the signer's identity and revoke the group keys. If any attacker will found in a node then the group manager will identify and then send to the particular users.

- **Destination**

In this module, there are an n-numbers of receivers are present (A, B, C, D and F). All the receivers can receive the data file from the service provider. The service provider will send data file to router and router will connect to all groups and send to the particular receiver, without changing any file contents. The user can only access the data file. For the user level, all the privileges are given by the NGM authority and the Data users are controlled by the NGM Authority only. Users may try to access data files within the router.

- **Attacker**

In this module, the attacker can attack the node in three ways Passive attack, DOS attack and Impression attack. Dos attack means he will inject fake Group to the particular node, Passive attack means he will change the IP address of the particular node and Impression attack means he will inject malicious data to the particular node.

5.RESULTS & DISCUSSION

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

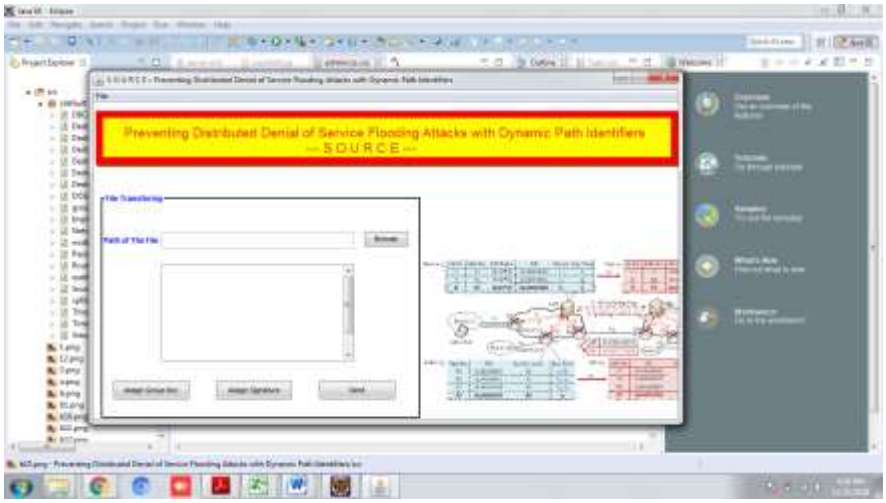


Fig 5.1 Source Screen

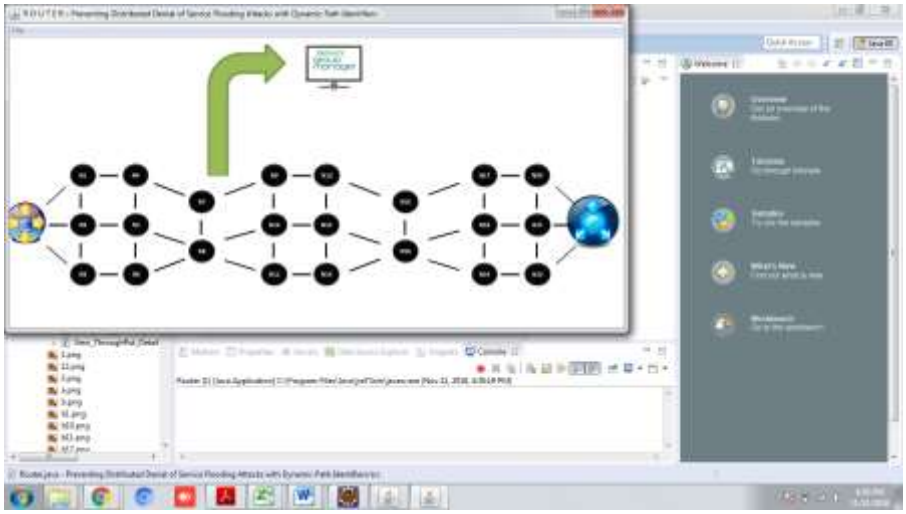


Fig 5.2 Router Screen

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

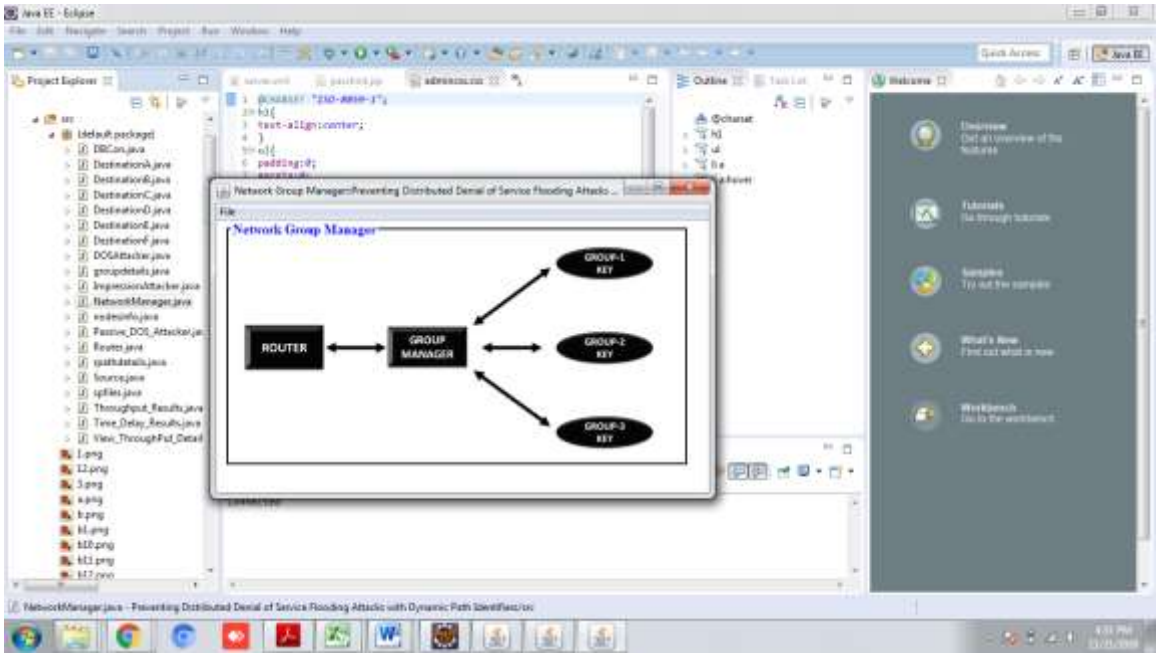


Fig 5.3 Network Manager screen

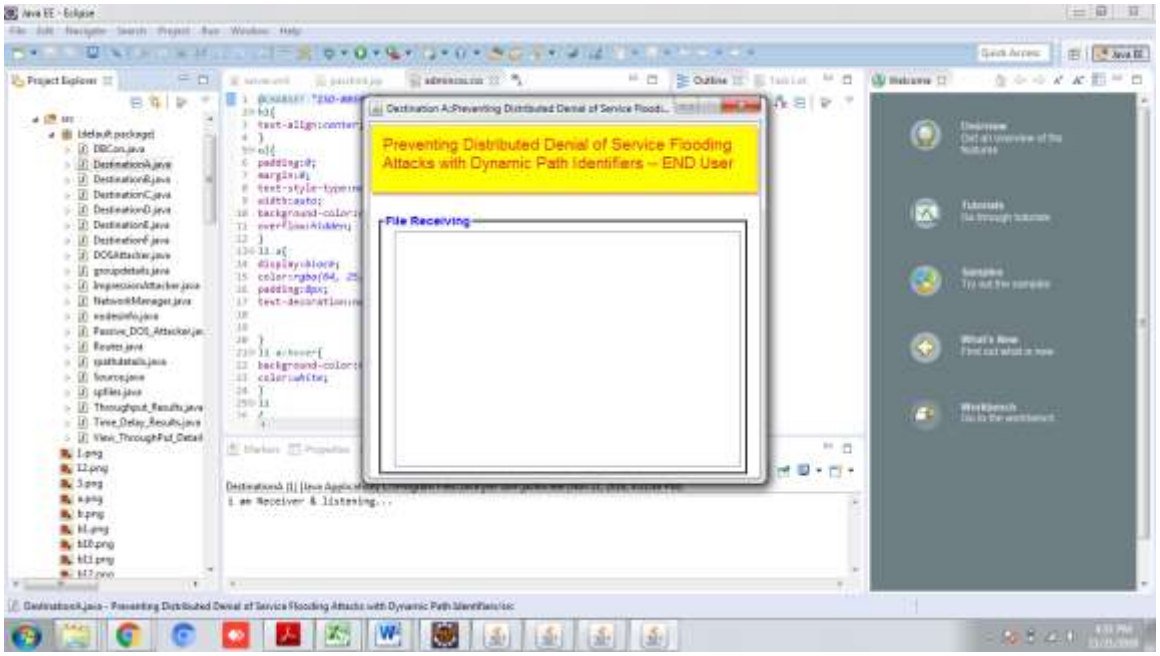


Fig 5.4 Destination Screen

6. CONCLUSION

In this paper, we've got presented the design, implementation and analysis of D-PID, a framework that dynamically changes path identifiers (PIDs) of inter-domain methods so as to stop DDoS flooding attacks, once PIDs area unit used as inter-domain routing objects. we've got represented the look details of D-PID and enforced it in a very 42-node paradigm to verify its practicableness and effectiveness. we've got bestowed numerical results from running experiments on the paradigm. The results show that the time spent in negotiating and distributing PIDs area unit quite little (in the order of ms) and D-PID is effective in preventing DDoS attacks. we've got conjointly conducted in depth simulations to judge the value in launching DDoS

REFERENCES

[1]. S. Yu, Y. Tian, S. Guo, D. Wu, "Can We Beat DDoS Attacks in Clouds", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2245-2254, Sept. 2014.

[2]. V. A. Foroushani, A. N. Zincir-Heywood, "TDFA: Trace back based Defense against DDoS Flooding Attacks", IEEE 28th International Conference on Advanced Information Networking and Applications, pp. 597-604, May 2014.

[3]. B. Liu, J. Bi, A. V. Vasilakos, "Toward Incentivizing Anti Spoofing Deployment", IEEE Transactions on Information Forensics and Security, vol. 9, no. 3, pp. 436-450, March 2014.

[4]. A. Compagno, M. Conti, P. Gasti, G. Tsudik, "Poseidon:Mitigating Interest Flooding DDoS Attacks in Named Data Networking", IEEE 38th Conference on Local Computer Networks, pp. 630-638, Oct. 2013.

[5]. C. Chung, P. Khatkar, T. Xing, J. Lee, D. Huang, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems", IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 198-211, July/Aug. 2013.

[6]. S. Rastegari, P. Hingston, C. Lam, M. Brand, "Testing A Distributed Denial of Service Defense Mechanism Using Red Teaming", IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), pp. 23-29, April 2013.

[7]. L. Jingna, "An Analysis on DOS Attack and Defense Technology", IEEE 7th International Conference on Computer Science & Education (ICCSE), pp. 1102-1105, July 2012.

[8]. S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient", IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 1073-1080, June 2012.

[9]. B. S. K. Devi, G. Preetha, S. M. Shalinie, "DDoS Detection using Host-Network based Metrics and Mitigation in Experimental Testbed", IEEE International Conference on Recent Trends In Information Technology (ICRTIT), pp. 423-427, April 2012.

[10]. A. Mishra, B. B. Gupta, R. C. Joshi, "A Comparative study of Distributed Denial of Service Attacks, Intrusion Tolerance and mitigation Techniques", European Intelligence and Security Informatics Conference (EISIC), pp. 286-289, Sept. 2011.

[11]. Z. Chao-yang, "DOS attack analysis and study of new measures to prevent", IEEE

International Conference on Intelligence Science and Information Engineering, pp. 426-429, Aug. 2011.

[12]. J. Mirkovic, E. Kissel, "Comparative Evaluation of Spoofing Defenses", IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 2, pp. 218-232, March-April 2011.

[13]. X. Bi, Q. Zheng, "Study on Network Safety Strategy against DDoS Attack", IEEE International Conference on Advanced Management Science (ICAMS), pp. 623-627, July 2010.