International Journal of Computing, Programming and Database Management

E-ISSN: 2707-6644
P-ISSN: 2707-6636
IJCPDM 2020; 1(1): 30-34
Received: 15-11-2019
Accepted: 20-12-2019

Appakondappagari Jayakrishna
Department of Computer Science, Sri Venkateswara University, Tirupati, Andhra Pradesh, India

Corresponding Author:
Appakondappagari Jayakrishna
Department of Computer Science, Sri Venkateswara University, Tirupati, Andhra Pradesh, India

A survey on preventing distributed denial of service attacks and data security

Appakondappagari Jayakrishna

DOI: https://doi.org/10.33545/27076636.2020.v1.i1a.7

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 it select path lets into a conclusion to-end source course.

Keywords: preventing, DDoS assault and PIDs

1. Introduction

Conveyed Denial of Service (DDoS) is the sorted-out undertaking to deal the availability of framework assets or servers as showed up in figure 1. These assaults bring in cash related disasters by ruining good 'ol fashioned access servers and online organizations. To direct the impact of these assaults strong defend segments are required that can distinguish and forestall advancing assaults. Various opposition instruments have been proposed and sent at various territories in current web. The practicality of these frameworks depends upon the execution tradeoffs and cost gained in arrangement.

DDoS acknowledgment frameworks perceive the deviation of development from normal lead. This action is named assault development and thereafter blocked by legitimate opposition instrument. For precision the acknowledgment framework ought to achieve low bogus positive and bogus negative rate. Simultaneously, as of late there are expanding interests in utilizing way identifiers PIDs that distinguish ways between organize substances as between area steering objects, since doing this not just aides tending to the directing adaptability and multi-way steering issues [21], yet additionally can encourage the advancement and selection of various steering structures [22]. For example, Godfrey *et al*. proposed pathlet steering [21], in which systems promote the PIDs of pathlets all through the Internet and a sender in the system builds its chose pathlets into a start to finish source course. Koponen *et al*. further contended in their canny structural paper that utilizing pathlets for between space directing can permit systems to send distinctive steering designs, along these lines empowering the advancement and selection of novel directing models [22]. Jokela *et al*. proposed in LIPSIN to appoint identifiers to joins in a system and to encode the connection identifiers along the way from a substance supplier to a substance buyer into a zFilter (i.e., a PID), which is then epitomized into the parcel header and utilized by switches to advance bundles. Luo *et al*. proposed a data driven web engineering called CoLoR [24] that additionally utilizes PIDs as between area directing items so as to empower the advancement and selection of new steering structures, as in [22].

There are two diverse use instances of PIDs in the up to referenced methodologies. In the main case, the PIDs are universally publicized (as in pathlet directing [21] and [22]). Thus, an end client knows the PID (s) toward any hub in the system. Likewise, assailants can dispatch DDoS flooding assaults as they do in the present Internet. In the subsequent case, then again, PIDs are just known by the system and are mystery to end clients (as in LIPSIN [23] and CoLoR [24]). In the last case, the system receives a data driven methodology [25, 27] where an end client (i.e., a substance supplier) knows the PID(s) toward a goal (i.e., a substance purchaser) just when the goal sends a substance demand message to the end client. In the wake of knowing the PID(s), the end client sends parcels of the substance to the goal by embodying the PID(s) into the bundle headers. Switches in the system at that point forward the bundles to the goal dependent on the PIDs.

It appears that keeping PIDs mystery to end clients (as in [23, 24]) makes it hard for aggressors to dispatch DDoS flooding assaults since they don't have the foggiest idea about the PIDs in the system. Nonetheless, keeping PIDs mystery to end clients isn't sufficient for forestalling DDoS flooding assaults if PIDs are static. For instance, Antikainen *et al*. contended that an enemy can build novel zFilters (i.e., PIDs) in view of existing ones and even acquire the connection identifiers through figuring out, in this way propelling DDoS flooding assaults [28]. Besides, as it is appeared in Sec. II-B, aggressors can dispatch DDoS flooding assaults by learning PIDs in the event that they are static.

To address this issue, right now, present the structure, execution and assessment of a unique PID (D-PID) system. In D-PID, two neighboring spaces occasionally update the PIDs among them and introduce the new PIDs into the information plane for bundle sending. Regardless of whether the assailant acquires the PIDs to its objective and sends the malevolent parcels effectively, these PIDs will get invalid after a specific period and the ensuing assaulting bundles will be disposed of by the system. In addition, if the assailant attempts to acquire the new PIDs and keep a DDoS flooding assault going, it essentially expands the assaulting cost as well as makes it simple to distinguish the aggressor specifically, our primary commitments are two overlap.

On one hand, we propose the D-PID configuration by tending to the accompanying difficulties. To begin with, how and how regularly should PIDs change while regarding nearby strategies of self-ruling frameworks (ASes)? To address this test, D-PID lets neigh-exhausting spaces arrange the PIDs for them between area ways dependent on their neighborhood approaches (Sec. III-B). Specifically, two neighboring spaces arrange a PID-prefix (as an IP-prefix) and a PID update period for each between area way associating them. Toward the finish of a PID update period for a between space way, the two areas arrange an alternate PID (among the PID-prefix allotted to the way) to be utilized in the following PID update period. Also, the new PID of a between area way is as yet stayed discreet by the two neighboring areas associated by the way.

Second, since between area bundles sending depends on PIDs that change powerfully, it is important to keep up genuine correspondences while forestalling unlawful communications when the PIDs change. To address this test, D-PID lets each space convey its PIDs to the switches in the area (Sec. III-C). For each between area way, the switches in a space forward information bundles dependent on the PID of the past PID update period and that of the present PID update period. Also, D-PID utilizes an instrument like the one that the present Internet gathers the base MTU (most extreme transmission unit) of systems with the goal that a substance shopper knows the base update time of PIDs along the way from a substance supplier to it Based on this period, the substance purchaser occasionally re-sends a substance demand message to the system so as to recharge the PIDs along the way.

Third, the overheads brought about by changing PIDs ought to be kept as little as could reasonably be expected. This incorporates not just the overhead in arranging PIDs by neighboring spaces, yet in addition the overhead for an area to circulate the refreshed PIDs to switches in the area, and that for transmitting content solicitation messages disdain by content customers. To address this test, the PID prefix doled out to a between area way is special among the PID prefixes allocated by the two spaces associated by the between space way.

2. Literature Survey

We discourse the problematic of DDoS attacks and extant the theoretical foundation, arc hitecture, and algorithms of Fire Col. The core of Fire Col is collected of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. We recommend the Stack Pi design, a new packet marking scheme based on Pi, and new sieving mechanisms. The Stack Pi 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 Definition

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 a 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 router.
- **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.
- **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 be 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

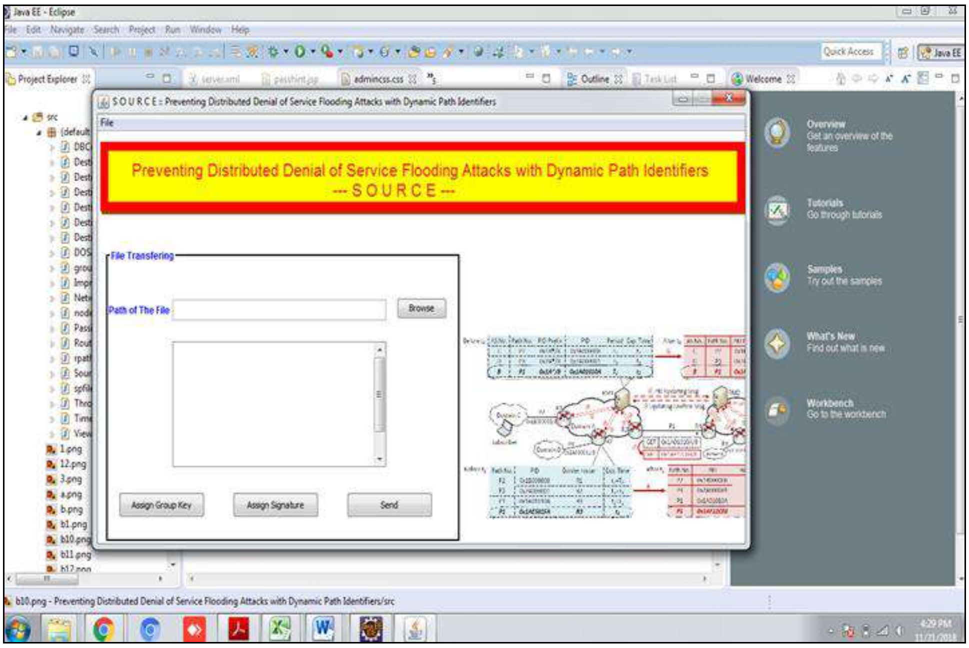
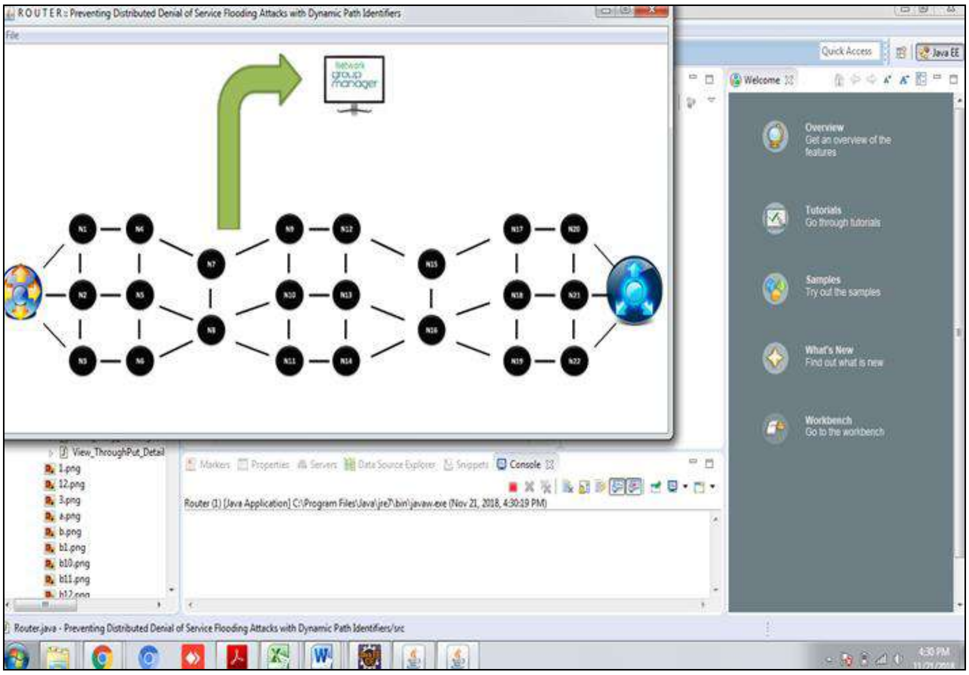
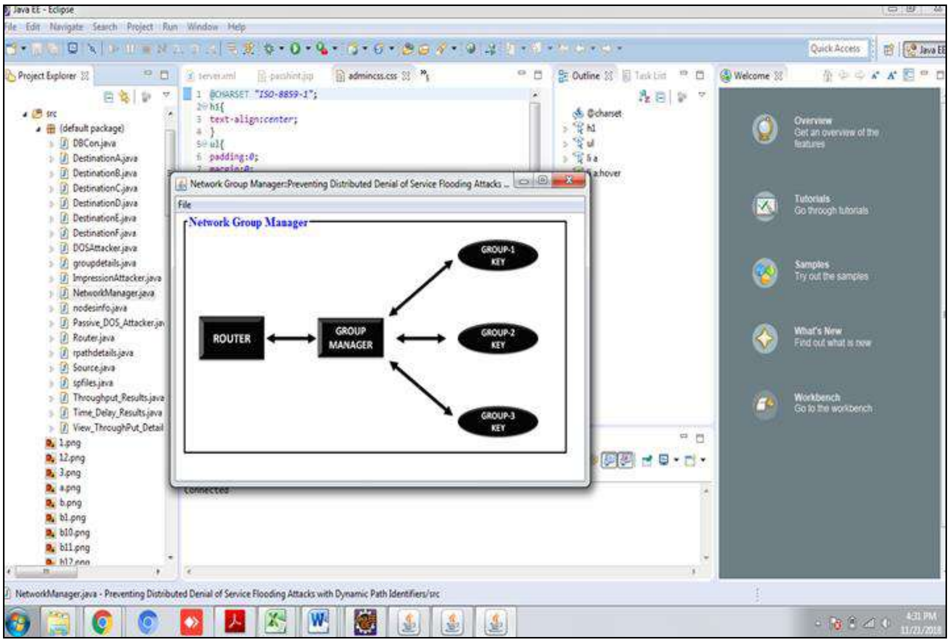


Fig 1: Source Screen



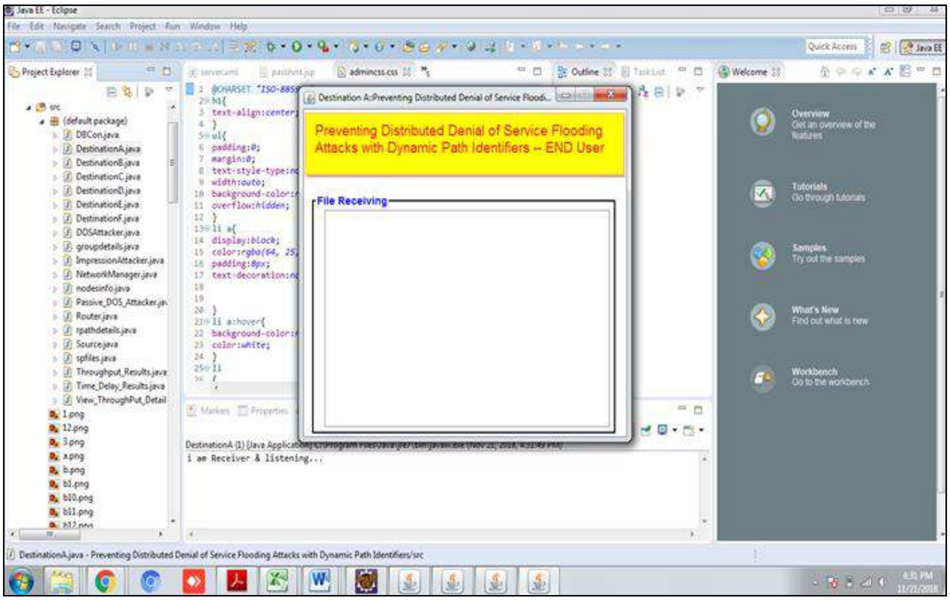
```
Router (1) [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Nov 21, 2018, 4:30:19 PM)
```

Fig 2: Router Screen


Network Group Manager:Preventing Distributed Denial of Service Flooding Attacks ...

NetworkManager.java - Preventing Distributed Denial of Service Flooding Attacks with Dynamic Path Identifiers/src

Fig 3: Network Manager Screen


Destination A:Preventing Distributed Denial of Service Flood...

Preventing Distributed Denial of Service Flooding Attacks with Dynamic Path Identifiers -- END User

File Receiving

```
I am Receiver & listening...
```

DestinationA.java - Preventing Distributed Denial of Service Flooding Attacks with Dynamic Path Identifiers/src

Fig 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. Yu S, Tian Y, Guo S, Wu D. "Can We Beat DDoS Attacks in Clouds", IEEE Transactions on Parallel and Distributed Systems. 2014; 25(9):2245-2254.
2. Foroushani VA, Zincir-Heywood AN. "TDFA: Trace back based Defense against DDoS Flooding Attacks", IEEE 28th International Conference on Advanced Information Networking and Applications, 2014, 597-604.
3. Liu B, Bi J, Vasilakos AV. "Toward Incentivizing Anti Spoofing Deployment", IEEE Transactions on Information Forensics and Security. 2014; 9(3):436-450.
4. Compagno M, Conti P, Gasti G, Tsudik. "Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking", IEEE 38th Conference on Local Computer Networks, 2013, 630-638.
5. 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. 2013; 10(4):198-211.

6. Rastegari S, Hingston P, Lam C, Brand M. "Testing A Distributed Denial of Service defense Mechanism Using Red Teaming", IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 2013, 23-29.
7. Jingna L. "An Analysis on DOS Attack and Defense Technology", IEEE 7th International Conference on Computer Science & Education (ICCSE), 2012, 1102-1105.
8. Yu S, Zhou W, Jia W, Guo S, Xiang Y, Tang F. "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient", IEEE Transactions on Parallel and Distributed Systems. 2012; 23(6):1073-1080.
9. Devi BSK, Preetha G, Shalinie SM. "DDoS Detection using Host-Network based Metrics and Mitigation in Experimental Testbed", IEEE International Conference on Recent Trends In Information Technology (ICRTIT), 2012, 423-427.
10. Mishra BB, Gupta RC, Joshi. "A Comparative study of Distributed Denial of Service Attacks, Intrusion Tolerance and mitigation Techniques", European Intelligence and Security Informatics Conference (EISIC), 2011, 286-289.
11. Chao-Yang Z. "DOS attack analysis and study of new measures to prevent", IEEE International Conference on Intelligence Science and Information Engineering, 2011, 426-429.
12. Mirkovic J, Kissel E. "Comparative Evaluation of Spoofing Defenses", IEEE Transactions on Dependable and Secure Computing. 2011; 8(2):218-232.
13. Bi X, Zheng Q. "Study on Network Safety Strategy against DDoS Attack", IEEE International Conference on Advanced Management Science (ICAMS), 2010, 623-627.