# DETECTION AND PREVENTION OF DISTRIBUTED FAULTY NODE ATTACKS USING DYNAMIC PATH IDENTIFIERS

**G. Ravindranath[1], M. Padma Priya Lahari[2], K. Sai Divya[3], K. Siva[4], K. Lakshmi Durga[5]**

*[1]Asst.Professor in Department of CSE, Lendi Institute of Engineering and Technology, Vizianagaram*
*[2, 3, 4, 5]Eighth Semester Students, Dept. of CSE, Lendi Institute of Engineering and Technology, Vizianagaram*

---------------------------------------------------------------------***---------------------------------------------------------------------

**Abstract -** *Now-a-days path identifiers (PIDs) are used as inter-domain routing objects. Nevertheless, the PIDs used in current methods are static, making it possible for attackers to conduct distributed denial of service (DDoS) flooding attacks. To address this issue, this project presents the design, implementation and evaluation of Dynamic Path Identifiers (D-PIDs), a framework that uses PIDs negotiated between adjacent domains as inter-domain routing objects. In D-PID, the PID of the inter-domain route linking the two domains is kept hidden and dynamically modified. We explain in depth how neighboring realms manage PIDs, how to retain continuing interactions as PIDs alter. We build a prototype and perform virtual simulation to test the feasibility, efficiency and cost of the D-PID.*

***Key Words***: **Inter-Domain Routing, Security, Distributed Denial-of-Service (DDoS) Attacks, Path Identifiers.**

## 1. INTRODUCTION

Security plays a key role in every aspect of the world today, such as banking, software, malls, e-commerce, schools, colleges and hospitals, etc. Although protection plays a very important position, many people often want to access information inappropriately and want to manipulate information during transmission. The process of converting the regular flow to an abnormal state and creating a disturbance is known as an attack. There are several ways to create attacks during data transmission, such as physical attacks or non-physical attacks. Physical attacks are ones that arise as a consequence of an attacker and the contents may be disrupted or changed or destroyed during transmission from the chosen source node to the correct destination. Such threats inflict physical harm to the data that has been transferred. But non-physical threats fall under a hazard paradigm that does not affect the original material, but instead causes any pause during transmission. Some of the various forms of attacks is a forgery assault that may try to manipulate or alter the details of the sender and recipient through data transmission and may physically adjust the integrity of the data. As this attack may lead a physical change, in the content to be send this attack come under physical mode.

## 2. PREVIOUS WORK

In the current method, the key explanation for a DDoS flood assault is that a node will submit any amount of data packets to any destination, irrespective of whether or not the destination needs packets. Many methods have been suggested to fix this problem in the current framework. In the current method, the key explanation for a DDoS flood assault is that a node will submit any amount of data packets to any destination, irrespective of whether or not the destination needs packets. Many methods have been suggested to fix this problem in the current framework. Throughout the traditional methods, two hosts are not able to connect by traditional. There will then be a predefined route for transmitting data from a legitimate source to a target node that allows the intruder to transform the nodes to a flawed state. Also, in the existing system, if there is a node that becomes defective, the data needs to be transferred again from the start to the destination node and therefore the delay-tolerant network is very time-consuming. There is also no proper mechanism for identifying the alternate path from the Point of Attack (POI) in the existing system.

## 3. PROPOSED WORK

In the proposed system, the system proposes a fully distributed and easy-to-use approach that allows each DTN node to quickly identify whether its sensors produce faulty data. The dynamic behavior of the proposed algorithm is approximated by some continuous-time state equations, where each node is defined on the basis of its location. The dynamic behavior of the proposed algorithm is approximated by certain continuous-time state equations, where each node is described on the basis of its position.

## 4. ALGORITHM

**Algorithm** RANDOMIZEDSELECTOR (source, destination, packet)

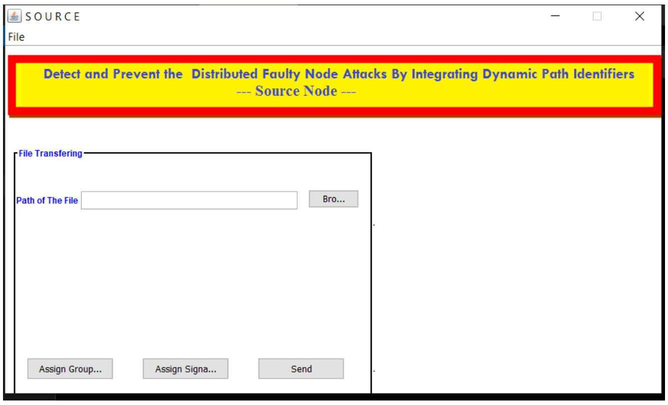
```
Let $h_s$ be the used next hop for the previous packet delivery for the source node s.
if $h_s \in C_t^{Nt}$ then
    if $|C_t^{Nt}| > 1$ then
        Randomly choose a node x from { $C_t^{Nt}$ - $h_s$} as a next hop, and send the packet to the next node x
        $h_s$ = x, and update the routing table of $N_i$.
    else
        Send the packet to $h_s$.
    end if
else
    Randomly choose a node y from $C_t^{Nt}$ as a next hop and send the packet to the node y.
    $h_s$ = y, and update the routing table of $N_i$.
end if
```

## 5. IMPLEMENTATION

The proposed system is implementing 5 modules using Java and AWT. The modules contain code for a Source window which has all the options to send data to a destination window which is designed by a module. An attacker module to create attacks on the network and a Network manager module to handle the attacks and send the data through another route in the network. To select an alternate node this system uses an algorithm to generate random node which has connection to destination node. AWT is used to create the User Interface.

### 5.1 Source Window

This window has all the fields to capture data from the user like to select path of the file to be sent, buttons to Assign Groups, Signatures and Send. This also has fields to select a destination folder.



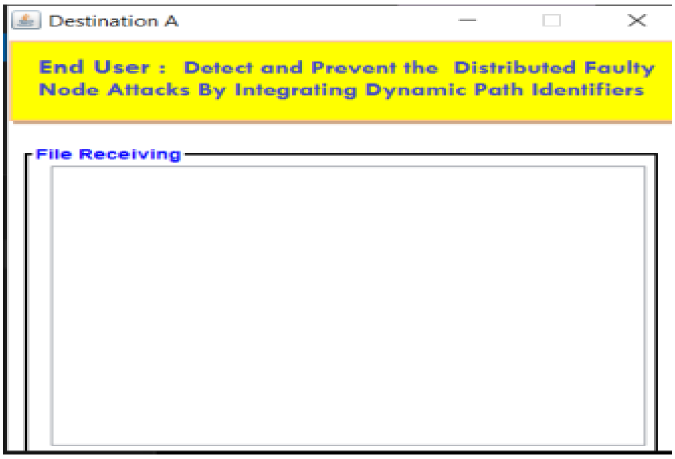
SOURCE

Detect and Prevent the Distributed Faulty Node Attacks By Integrating Dynamic Path Identifiers
--- Source Node ---

**Fig – 1:** Source Window

### 5.2 Destination Window

This window displays all the content that is sent from the source.



Destination A

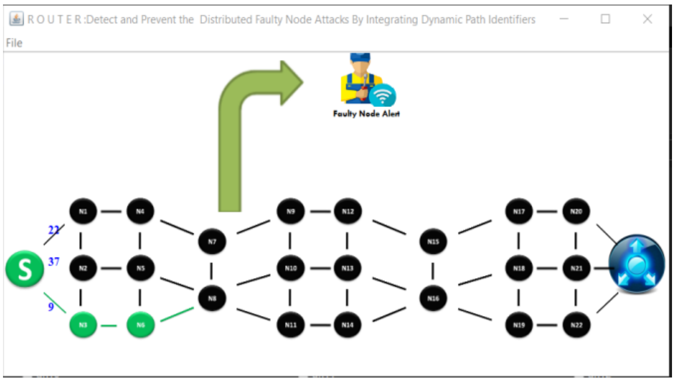
End User : Detect and Prevent the Distributed Faulty Node Attacks By Integrating Dynamic Path Identifiers

File Receiving

**Fig -2**: Destination Window

### 5.3 Network Manager Window

This window shows how the data is being passed from one hop to another, how nodes are randomly selected and also displays node in red color when it is attacked.



ROUTER :Detect and Prevent the Distributed Faulty Node Attacks By Integrating Dynamic Path Identifiers

**Fig – 3**: Network Manager Window

## 6. CONCLUSION

This proposed research addresses the architecture and implementation of DPID, a system that dynamically modifies path identifiers (PIDs) of inter-domain paths in order to recognize the flawed nodes that are present within the network during data transmission. In DPID, the PID of the inter-domain route between the two domains is held hidden and dynamically modified, and there is no possibility for an intruder to know the direction the data moves so he cannot transform the nodes to a defective state. We simulated our application using a socket programming language along with a Java network package to check productivity and expense. The findings of both simulations and studies demonstrate that the complex complexity of the detection of defective nodes and the availability of alternative pathways for data transmission will effectively eliminate defective nodes inside the distributed network. There are also comparative reports for the delay and throughput.

## 7. FUTURE SCOPE

This thesis is a theoretical approach to detecting attacks using DPIDs on a network. This can be simulated using simulators such as OPNET, etc. Various encryption techniques, such as AES and other advanced encryption techniques, can be used to encrypt data.

## 8. RESULTS

### 8.1 Throughput Results Window

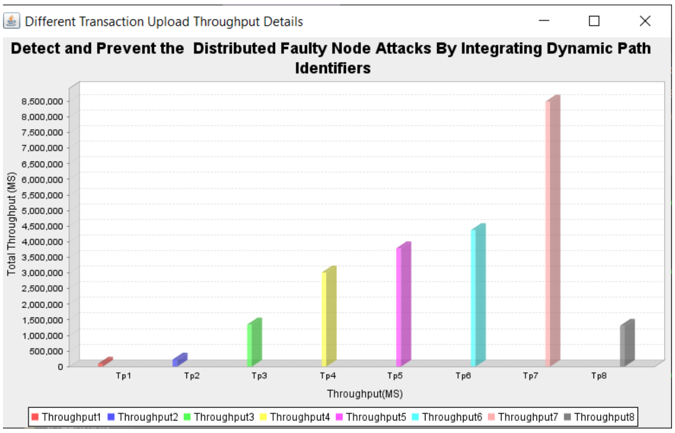


**Chart – 1:** Throughput Window

### 8.2 Delay Results Window

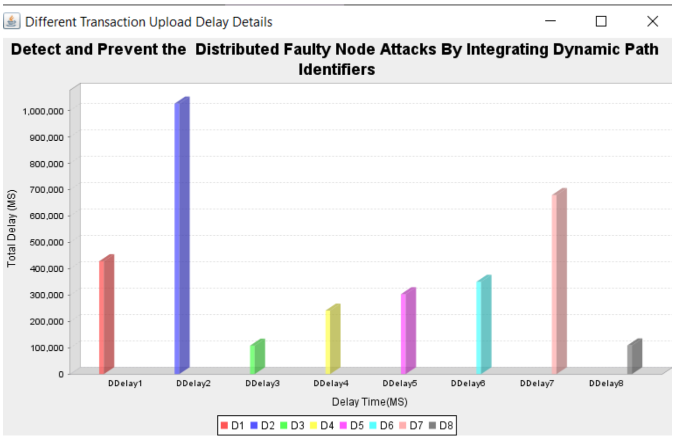


**Chart – 2:** Delay Window

## 9. REFERENCES

[1] 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, Dec. 2012, pp. 1828-1841.

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

[3] 602 Gbps! This May Have Been the Largest DDoS Attack in History. http://thehackernews.com/2016/01/biggest-ddos-attack.html.

[4] S. T. Zargar, J. Joshi, 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, Nov. 2013.

[5] P. Ferguson and D. Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks that Employ IP Source Address Spoofing,” *IETF Internet RFC 2827*, May 2000.

[6] 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*, Aug. 2001, San Diego, CA, USA.

[7] A. Yaar, A. Perrig, 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, Oct. 2006.

[8] H. Wang, C. Jin, K. G. Shin, “Defense Against Spoofed IP Traffic Using Hop-Count Filtering,” *IEEE/ACM Trans. on Netw.*, vol. 15, no. 1, pp. 40 - 53, Feb. 2007.

[9] Z. Duan, X. Yuan, J. Chandrashekar, “Controlling IP Spoofing through Interdomain Packet Filters,” *IEEE Trans. on Depend. and Secure Computing*, vol. 5, no. 1, pp. 22 - 36, Feb. 2008.

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

[11] A. C. Snoeren, C. Partridge, L. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer, “Hash-Based IP Traceback,” In *Proc. SIGCOMM’01*, Aug. 2001, San Diego, CA, USA.

[12] M. Sung, J. Xu, “IP traceback-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks,” *IEEE Trans. On Parall. and Distr. Sys.*, vol. 14, no. 9, pp. 861 - 872, Sep. 2003.

[13] M. Sung, J. Xu, J. Li, L. Li, “Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Information-Theoretic Foundation,” *IEEE/ACM Trans. on Netw.*, vol. 16, no. 6, pp. 1253 - 1266, Dec. 2008.

[14] Y. Xiang, K. Li, W. Zhou, “Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics,” *IEEE Trans. on Inf. Foren. and Sec.*, vol. 6, no. 2, pp. 426 - 437, May 2011.

[15] H. Ballani, Y. Chawathe, S. Ratnasamy, T. Roscoe, S. Shenker, “Off by default!,” In *Proc. HotNets-IV*, Nov. 2005, College Park, MD, USA.

[16] 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.

[17] B. Parno, D. Wendlandt, E. Shi, A. Perrig, B. Maggs, and Y. Hu, “Portcullis: Protecting connection setup from denial-of-capability attacks,” In *Proc. SIGCOMM’07*, Aug.2007, Kyoto, Japan.

[18] X. Yang, D. Wetherall, and T. Anderson, “TVA: A DoS-Limiting Network Architecture,” *IEEE/ACM Trans. on Netw.*, vol. 16, no. 3, pp. 1267 - 1280, Jun. 2008. IEEE Transactions on Information Forensics and Security,Volume:12,Issue:8,Issue Date:Aug.201715

[19] X. Liu, X. Yang, and Y. Lu, “To Filter or to Authorize: Network-Layer DoS Defense Against Multimillion-node Botnets,” In *Proc. SIGCOMM’ 08*, Aug. 2008, Seattle, WA, USA.

[20] D. G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon, and S. Shenker, “Accountable Internet Protocol (AIP),” In *Proc. SIGCOMM’ 08*, Aug. 2008, Seattle, WA, USA.