# Design and Analysis of a Novel Architecture for Network Intrusion Detection and Prevention by Using Dynamic Path Identifier Approach (DPID)

**SHANKAR KOPANATI [#1], J.SANTOSHI KUMARI [#2] ,**

**RAMARAO VANGAPANDU [#3], DUMMU APARNA[#4]**

[#1] Associate Professor, Department of Computer Science and Engineering, Nadimpalli Satyanarayana Raju Institute of Technology (NSRIT), Sontyam, Pendurthi-Anandapuram Highway, Visakhapatnam, India-531173.

[#2, #4] Assistant Professor, Department of Computer Science and Engineering, Nadimpalli Satyanarayana Raju Institute of Technology (NSRIT), Sontyam, Pendurthi-Anandapuram Highway, Visakhapatnam, India-531173.

[#3] Assistant Professor, Department of Computer Science and Engineering, Rajiv Gandhi University of Knowledge and Technology, Nuzvid- Andhra Pradesh, India-521202.

## ABSTRACT

In current days PIDs act as inter-domain routing objects to avoid distributed denial-of-service (DDoS) attacks. These are mainly used in order to identify the best path from the source node to destination node in order to transfer the information. As we all know that path identifier is designed earlier, those are static in nature and hence it is very easy for the attackers to create any attack on a fixed path. This paper is mainly designed in order to identify the several threats that are arise due to network intrusion detection. Hence we try to design a new model like network intrusion detection and prevention systems (NIDPSs) in which there is prevention of such intruder attacks during data transfer. In this present application, we try to design and implement novel path identifiers for data communication like dynamic D-PID, a framework that is not at all implemented in any DTNs till today. In this current D-PID method, the PID of an inter-domain path connecting two domains is kept secret and changes dynamically, so there is no chance for an attacker to identify which path the data is traveling and he can't able to convert nodes into intruder state. We simulated our application using socket programming language along with java network package to verify the effectiveness and cost. The results from both simulations and experiments show that the dynamic nature of identifying network intruders and providing alternate paths for data transfer can effectively prevent DDoS attacks.

**Key Words:** Denial of Service Attacks, Attackers, Network Intrusion Detection, Path Identifiers, Socket Programming.

# 1. INTRODUCTION

Now a day's security plays an important role in each and every aspect like banking, software, Malls, E-commerce and Hospitals etc. As security plays a very important role, still a lot of users try to access the contents illegally and they want to misuse the content during transmission. The process of converting the regular flow into abnormal state and create a disturbance is known as attack. There are several ways of creating attacks during data transmission like physical attack or non-physical attack. Physical attacks are those which are occurred due to an intruder and the content will be damaged or modified or lost during the transmission from a selected source node to valid destination. These attacks create physical damage for the data which is been transferred. But non-physical attacks come under a threat model which willn't damage the original content but just creates some delay while transmission. One among the several types of attacks is forgery attack which will try to do some modification or change in the content of sender and receiver during the data transfer and it will physically change the data content. As this attack may lead a physical change in the content to be send, this attack come under physical mode[1].

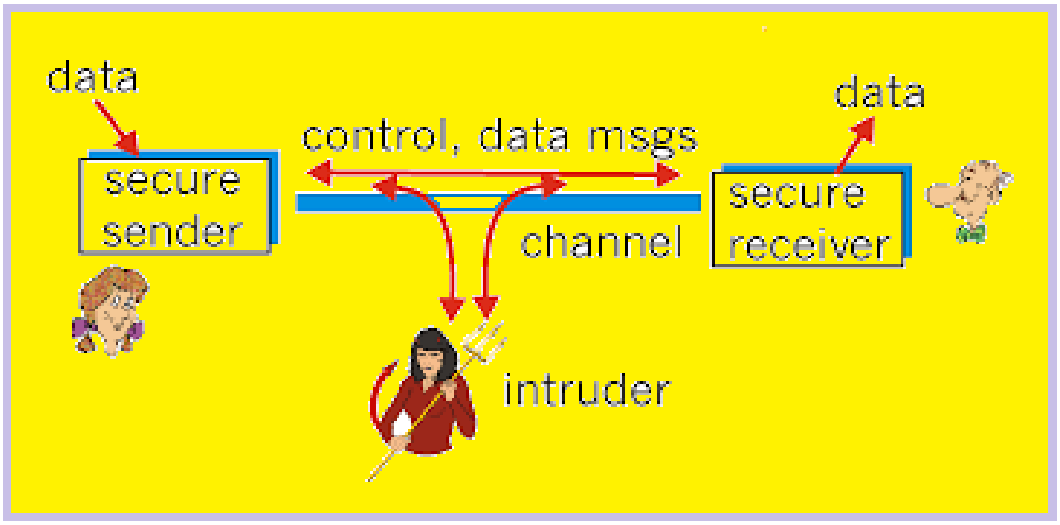



**Figure 1. Denotes the Intruder try to Create Attack during Data Transmission**

From the above figure 1, we can clearly identify an secure sender try to send his valuable or sensitive data to the secure receiver with the help of secure channel. The data will be transmitted in the form of packets and all the data will be reached to the destination packet wise. During the data transmission there may be some nodes who try to create attack on the sensitive

data. The intruder is one who illegally enters the network and try to inject fake data inside the channel and then try to re-direct the data to a wrong destination or sometimes try to delete the data within the network. In the area of data communication, a forgery/Impression attack is an attempt to turn the machine changed or altered to its intended users, such as to interrupt the data which is being transmitted for the end user and this will create some sort of attack on the data which is transmitted [2]- [5]. Generally a lot of criminals or intruders often target valuable sites like bank servers or credit card payment gateways or online shopping gateways and they try to make the process go with some modified values by changing the recipient account details or amount specified limit and then try to send those into their account, which in turn leads to attack.

## 2. BACKGROUND WORK

In this section we mainly try to discuss about the related literature work that is carried out in order to identify the intruder within the network during data transfer and try to prevent the data loss.

**Distributed Intruder Node Detection in Delay Tolerant Networks: Design and Analysis**
Authors: Wenjie Li and Francesca Bassi

The two well know authors try to propose the intrusion detection system as critical issue. In case of Delay Tolerant Networks (DTN) in particular, the rare meeting events require that nodes are efficient in propagating only correct information. For that purpose, mechanisms to rapidly identify possible intruder nodes should be developed. Distributed intruder node detection has been addressed in the literature in the context of sensor and vehicular networks, but already proposed solutions suffer from long delays in identifying and isolating nodes producing intruder data[6]. This is unsuitable to DTNs where nodes meet only rarely. This paper proposes a fully distributed and easily implementable approach to allow each DTN node to rapidly identify whether its sensors are producing intruder data. The dynamical behavior of the proposed algorithm is approximated by some continuous-time state equations, whose equilibrium is characterized. The presence of misbehaving nodes, trying to perturb the intruder node detection process, is also taken into account.

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

Authors: Hongbin Luo and Athanasios

The two well know authors try to propose that there are increasing interests in using path identifiers (*PIDs*) as inter- domain routing objects. However, the *PIDs* used in existing approaches are static, which makes it easy for attackers to launch distributed denial-of service (DDoS) flooding attacks. To address this issue, in this paper, we present the design, implementation, and evaluation of D-PID, a framework that uses *PIDs* negotiated between neighboring domains as inter-domain routing objects. In DPID, the *PID* of an inter-domain path connecting two domains is kept secret and changes dynamically. We describe in detail how neighboring domains negotiate *PIDs*, how to maintain ongoing communications when *PIDs* change. We build a 42-node prototype comprised by six domains to verify D-PID's feasibility and conduct extensive simulations to evaluate its effectiveness and cost. The results from both simulations and experiments show that D-PID can effectively prevent DDoS attacks[7].

**FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks**

Authors: Jérôme François and Raouf Boutaba

The two well know authors try to propose that ddos attacks remain a major security problem the mitigation of which is very hard especially when it comes to highly distributed botnetbased attacks. The early discovery of these attacks, although challenging, is necessary to protect end users as well as the expensive network infrastructure resources. In this paper, we address the problem of DDoS attacks and present the theoretical foundation, architecture and algorithms of FireCol. The core of FireCol is composed of Intrusion Prevention Systems (IPSs) located at the Internet Service Providers (ISPs) level. The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information. The evaluation of FireCol using extensive simulations and a real dataset is presented, showing FireCol effectiveness and low overhead, as well as its support for incremental deployment in real networks[8].

**A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks**

Authors: James Joshi and David Tipper

The two well know authors try to propose that flooding attacks are one of the biggest concerns for security professionals. DDoS flooding attacks are typically explicit attempts to disrupt legitimate users' access to services. Attackers usually gain access to a large number of computers by exploiting their vulnerabilities to set up attack armies (i.e., Botnets). Once an attack army has been set up, an attacker can invoke a coordinated, large-scale attack against one or more targets. Developing a comprehensive defense mechanism against identified and anticipated DDoS flooding attacks is a desired goal of the intrusion detection and prevention research community. However, the development of such a mechanism requires a comprehensive understanding of the problem and the techniques that have been used thus far in preventing, detecting, and responding to various DDoS flooding attacks[9].

**A New Method for Preventing Ddos Attack by Active Path Identifiers in Internet**
Authors: N.Brahma Naidu and E.Ramakrishna

The two well know authors try to propose the outline, usage and assessment of a dynamic PID (D-PID) system. In D-PID, two contiguous areas intermittently refresh the PIDs amongst them and introduce the new PIDs into the information plane for parcel sending. Regardless of whether the attacker acquires the PIDs to its objective and sends the malevolent parcels effectively, these PIDs will wind up invalid after a specific period and the consequent attacking packets will be disposed of by the system. In addition, if the aggressor tries to acquire the new PIDs and keep a DDoS flooding attack going, it significantly builds the attacking cost, as well as makes it simple to identify the attacker[10].

## 3. PROPOSED DYNAMIC PATH IDENTIFIERS TO AUTOMATIC DETECTION AND PREVENTION OF INTRUDERS IN A DISTRIBUTED NETWORK

In this section we will find out the proposed dynamic path identifiers to automatic detection and prevention of intruder nodes in a distributed network.

### Scope

In the proposed system, the system proposes 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 let's neighboring domains negotiates the PIDs [8] for their inter-domain paths based on their local policies. Here the two neighbors try to choose a unique ID which shouldn't be effected with flooding attacks or DOS attack.

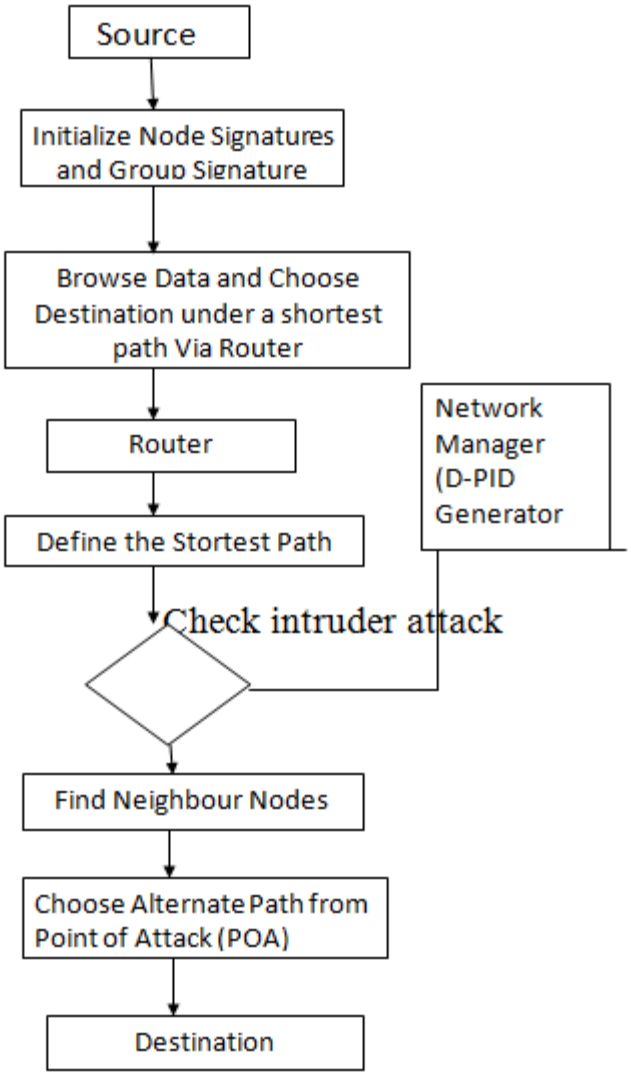



**Figure 2. Represents Proposed Architecture of DPID Approach**

The following are the advantages of using the DPID in a distributed network.

1. Distributed denial-of-service (DDoS) attacks to avoid attackers
2. More security due to path identifiers are dynamic in nature (D-PIDs).
3. IT is dynamic in nature so there is no scope of data loss if any doS attacks occur during transmission

4. In this proposed approach we can achieve high level of accuracy in sending the packets to the destination node[11].
5. It is efficient and practical method for packet delivery.

From the above figure 2 ,we can clearly able to identify the architecture flow of our proposed approach D-PID in order to eliminate the intruder nodes inside the distributed networks.We can clearly find out the process of finding the intruder nodes [11] in a distributed network for a certain node includes the following fields like

1) The node ID,

2) An Acknowledgement of the last seen packet flow.

The Ack for the packets can be generated in several ways to serve this purpose. In our solution, a node ni creates a vertex vi for every jth packet it generates/forwards[12]. The vertex $ID_{vidi}$ is generated as follows:

$$\begin{aligned} vid_i &= generateVID\,(\,n_i,\, seq[j],\, pSeq_i\,) \\ &= E_{K_i}(\,seq[j] \,\|\, pSeq_i\,), \end{aligned}$$

Where the fields like **pSeqi** is the knowledge of ni (i.e. Data transfer Update) about the sequence number of the previous packet in the flow[13].

**ni** is defined as the updates of the data transfer for the packet by inserting vidi into the iBF.

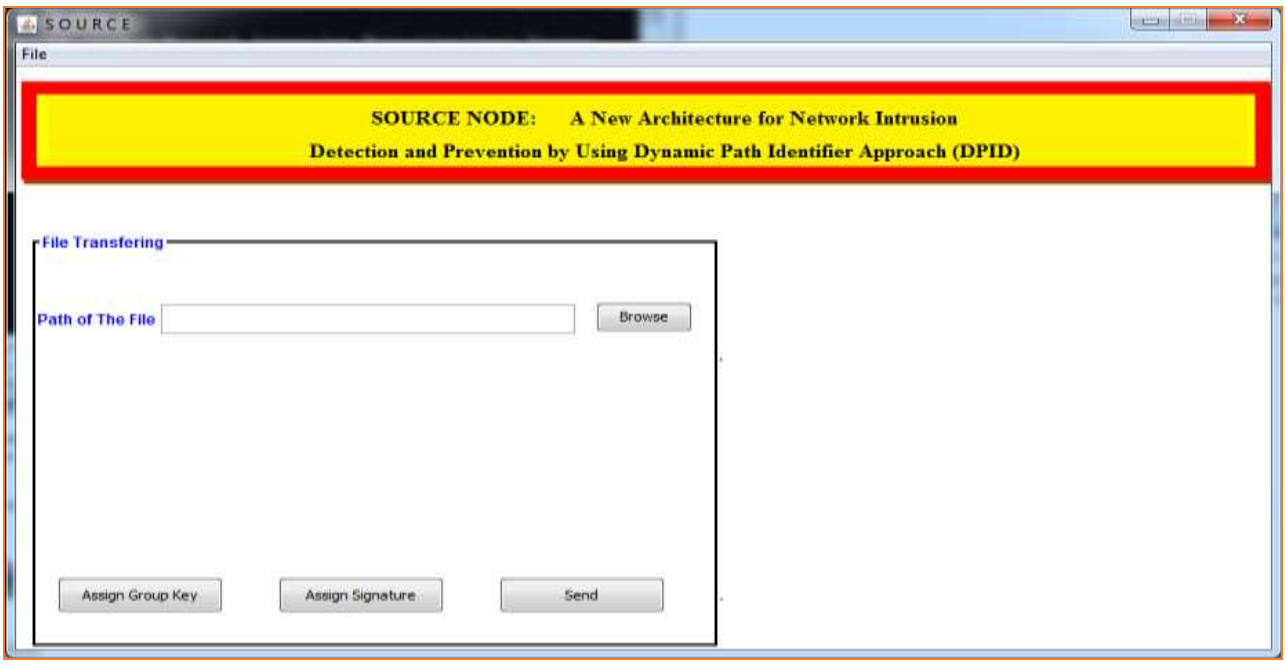
From the above equation we can able to identify those nodes which are not in normal state like how it is initiated earlier and we try to find out the state of that node. If the node is in abnormal state due to any of its modified parameters, we try to identify that appropriate node as intruder attack node and we try to provide a prevention mechanism from that point of attack (POA) node. In this proposed application as we are using DPID approach, the router will immediately choose an alternate path from that point of attack node and try to send the data under new path to the valid destination node. Here the packets are identified based on the

sequence numbers and the packet which is stopped at the intruder node will be identified uniquely and this will be passed to the destination node in very quick interval.

## 4. EXPERIMENTAL RESULT

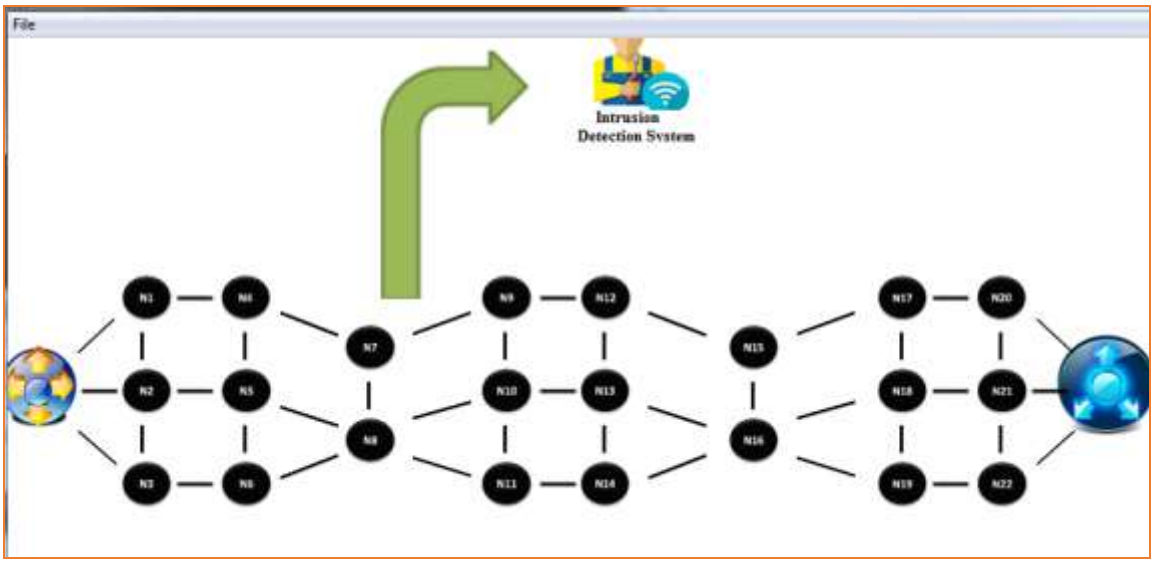
We have implemented the proposed application on Java programming language with JSE as the chosen language in order to show the performance this proposed model. The front end of the application takes AWT,SWINGS and NETWORKING PACKAGE and as a Back-End Data base we used My-SQL Server for maintaining all the details about data communication and attack details. In order to prove the performance of our proposed application, we examined multiple data selections from valid source to multiple destinations and observed the accuracy of our proposed application in automatic detection and prevention of faulty nodes during data transfer inside a network.

**SOURCE WINDOW**



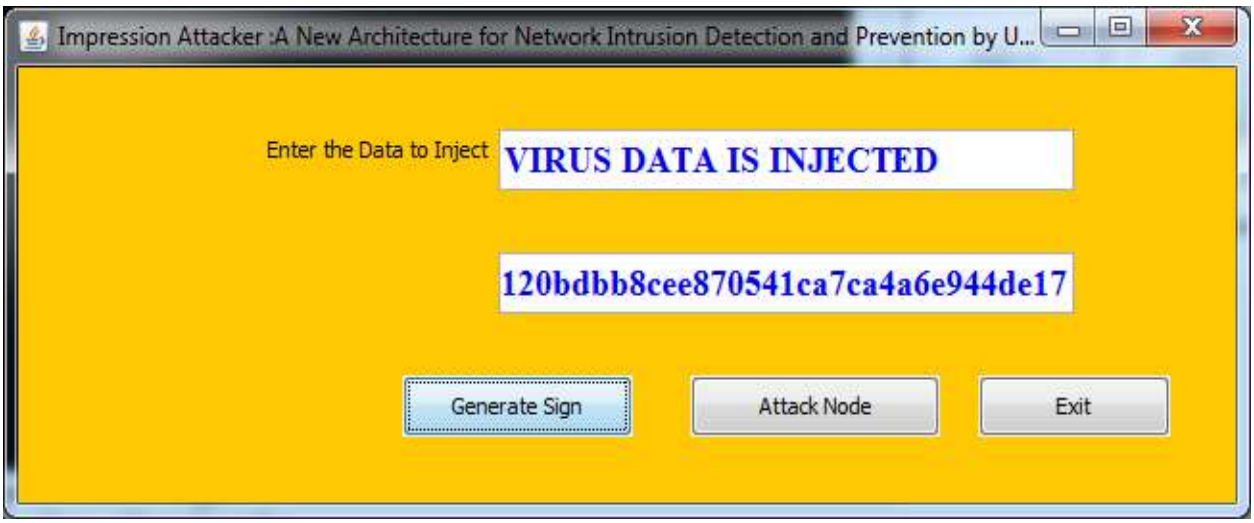

From the above window we can clearly identify that a source window is having a capability to browse the input file and choose destination to send that input file. Before it sends the data the source node will try to initialize assign signature and assign group key.

**ROUTER WINDOW**



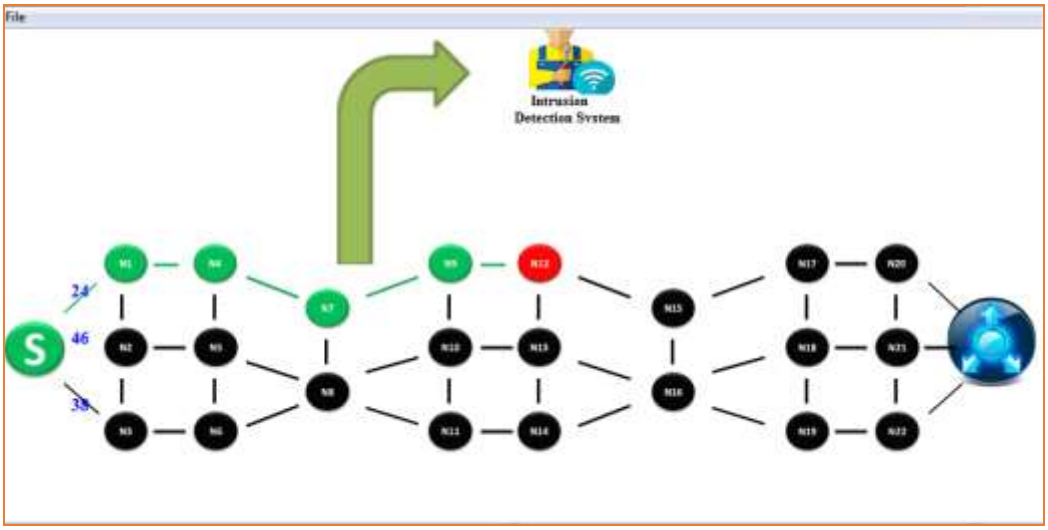

From the above window we can clearly identify that router is one which holds several intermediate nodes in a clustered manner. If the sender wants to send the data to the valid receiver nodes, then the router node will choose the best path for data transfer.

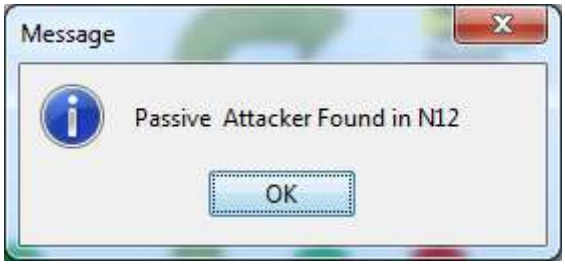
**ATTACKER/INTRUDER WINDOW**



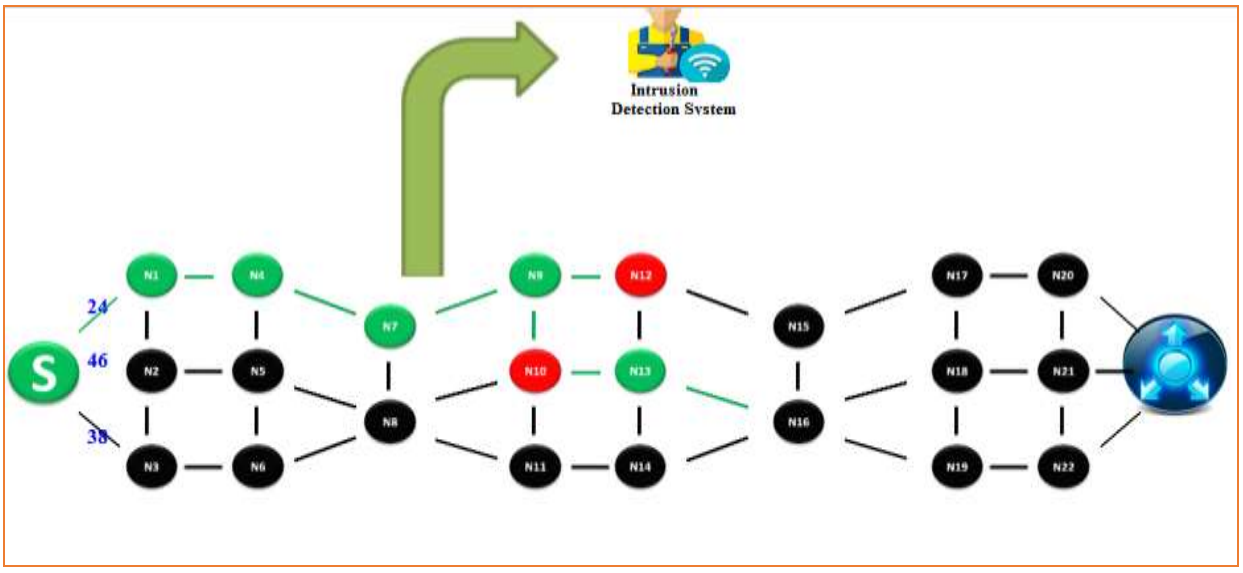

From the above window we can clearly identify the attacker is one who try to inject the virus data inside the network packets during data transfer and those type of injected packets are identified by the NIDPSs.This will be identified such a nodes and try to send the data in a alternate path which don't have any injected nodes.In this way our proposed mode NIDPS can able to generate a new dynamic path from the point of attack rather than sending the data from source node onwards till destination node.

**INTRUDER DETECTION AND PREVENTION WINDOW**



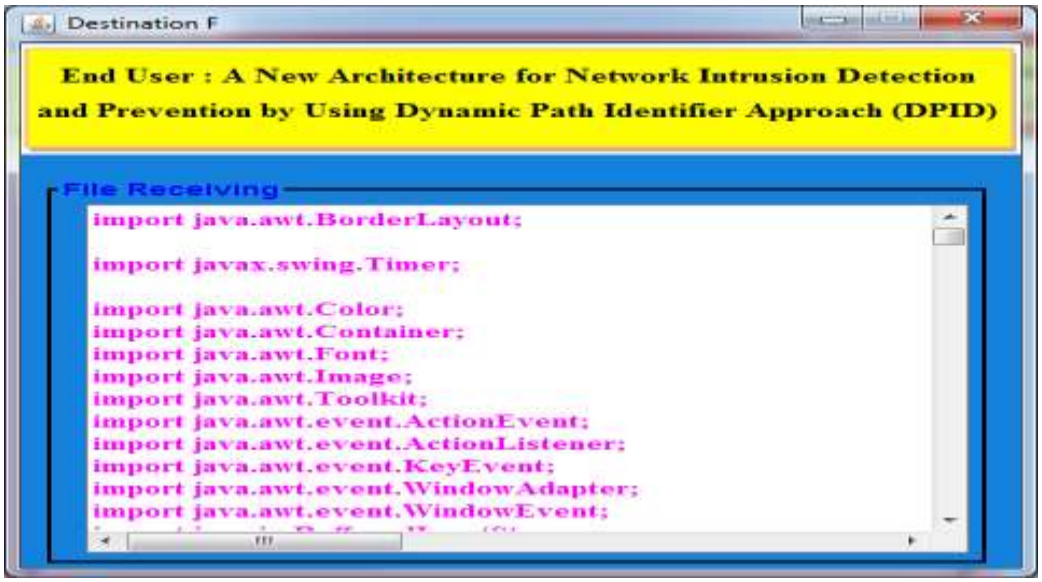




From the above window we can clearly identify there is one intrusion attack found in Node N12 and this is identified dynamically by the end user and the same router immediately try to regenerate a new path and send the data to the valid destination under a new dynamic path.This path will be choosed from the Node N12,but not from the starting N1 onwards.



From the above window we can clearly identify that N12 and N10 both are intruders inside the network,but the proposed NIDPS try to send the data from that attacked node to new alternate nodes which don't have any attacks and finally send the data to the valid destination nodes.

**DESTINATION WINDOW**




From the above window we can clearly identify that destination node will receive the data from the source node via router node and then finally it can be viewed and stored in its own location.

## 5. CONCLUSION

In this paper we finally designed a novel frame work for network intrusion detection and prevention using DPID approach, where the PID acts like an inter-domain path which connects two or more nodes for data communication by keeping the identity secret. Generally these PIDs are static in nature in which path is identified before and fixed throughout the data transfer. But in this proposed paper we try to design DPID in which the path identification is done dynamically and hence there is no chance for any attacker to identify which path the data is travelling and he can't able to convert nodes into attacked state. We simulated our application using socket programming language along with java network package to verify the effectiveness and cost. The results from both simulations and experiments show that dynamic nature of identifying intruder nodes and providing alternate path for data transfer can effectively prevent the intrusion attacks inside the distributed network.

## 6. REFERENCES

[1] Fed CIRC, "Defense Tactics for Distributed Denial of Service Attacks," Federal Computer Incident Response Center, Washington DC, 2000.

[2] 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.

[3] 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.

[4] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A Virtual Data System for Representing, Querying, and Automating Data Derivation," Proc. Conf. Scientific and Statistical Database Management,pp. 37-46, 2002.

[5] R. Guo, G. R. Chang, R. D. Hou, Y. H. Qin, B. J. Sun, A. Liu, Y. Jia and D. Peng, "Research on Counter Bandwidth Depletion DDoS Attacks Based on Genetic Algorithm.

[6] 602 Gbps! This May Have Been the Largest DDoS Attack in History. http://thehackernews.com/2016/01/biggest-ddos-attack.html.

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

[8] 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.

[9] 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.

[10] 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

[11] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-Aware Storage systems," Proc. USENIX Ann. Technical Conf., pp. 4-4, 2006.

[12] 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.

## 7. ABOUT THE AUTHORS

**SHANKAR KOPANATI** is currently working as an Associate Professor in the Department of Computer Science and Engineering at Nadimpalli Satyanarayana Raju Institute of Technology (NSRIT), Sontyam, Pendurthi- Anandapuram Highway, Visakhapatnam, India-531173.He has more than 17 years of teaching experience in various engineering colleges. His research interests include Computer Networks.

**J. SANTOSHI KUMARI** is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Nadimpalli Satyanarayana Raju Institute of Technology (NSRIT), Sontyam, Pendurthi- Anandapuram Highway, Visakhapatnam, India-531173.She has more than 10 years of teaching experience in various engineering colleges. Her research interests include Web Technologies and Computer Networks.

**RAMARAO VANGAPANDU** is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Rajiv Gandhi University of Knowledge and Technology, Nuzvid- Andhra Pradesh, India-521202.He has more than 5 years of teaching experience in various engineering colleges. His research interests include Networking and Computer Systems.

**DUMMU APARNA** is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Nadimpalli Satyanarayana Raju Institute of Technology (NSRIT), Sontyam, Pendurthi- Anandapuram Highway, Visakhapatnam, India-531173.She has more than 5 years of teaching experience in various engineering colleges. Her research interests include Image Processing.