Intrusion Detection System against Blackhole Attack in Wireless Network

Vishnu Priya .P
School of Information Technology and
Engineering,
VIT University,
Vellore – 632 014
India.

Thanapal.P
Assistant Professor Senior,
School of Information Technology and
Engineering,
VIT University,
Vellore - 632 014.
India.

ABSTRACT:

Security is an essential requirement in wireless network to provide secure communication or to transfer data between nodes. Due to unique characteristics of wireless network, it creates number of challenges in its security design. To overcome this, we need to build a security solution (i.e) Intrusion Detection System for protection and efficient network performance. Intrusion Detection is defined as a mechanism for wireless networks to detect the existence of incorrect or anomalous attackers or intruders. In this paper , we consider this issue according to heterogenous wireless network models. Since it is wireless network, it is vulnerable to several attacks, Black Hole is one of the possible attack which drops the data packets that has been send from the server.

KEYWORDS: Intrusion Detection System, Blackhole Attack, Heterogenous Network.

INTRODUCTION:

Wireless Network is an Infrastructure less network that is not connected by cables of any kind. It's a method used to avoid costly process of introducing cables as a connection between various locations. The implementation takes place at physical layer of the OSI network architecture. It consists of sensor nodes which is responsible for communicating or to transfer data. Here, one node acts as a server and other nodes acts as clients. It does not have access point to transfer data so it's not secure for communicating nodes or to transfer data between nodes. Since it's not secure and due to node mobility, network topology changes frequently so data delivery is not guaranteed and possible for many types of attacks. Wireless Network is of various types based on the network topologies been used are:

Wireless Local Area Network is used to connect two or more devices within a short distance. It's often used in cities to connect network in two or more buildings without wired cables. It mostly provides an access point for internet access.

Wireless Mesh Network :

Wireless Mesh Network is a type of network which consists of radio nodes. Each node forwards data or information on behalf of other nodes. It automatically re-routes among the nodes that has lost power.

Wireless MAN (WMAN) :

Wireless Metropolitan Area Network is a network which is used to connect several Wireless LANs together.

Wireless WAN (WWAN) :

Wireless Wide Area Network is a network that typically covers large areas fro one city to another. It's mostly used for business purpose like to connect branch offices of the organization or as public internet access system.

1) Wireless PAN (WPAN) :

Wireless Personal Area Network is used to interconnect devices within particular range. There are so many devices which uses WPAN nowadays for ex, Bluetooth radio, invisible infrared light uses this technology to interconnect devices. To make communication between nodes, trust between nodes is necessary. Due to the flexibility of this network it introduces many security issues. To overcome this, a security system (Intrusion Detection System) has been introduced. A Intrusion Detection System (IDS) is a technology which is an essential part of security system and also overcome the challenges in Wireless network which is used to identify an unauthorized access or to find the malicious activities in the Wireless network. The malicious activities include various types of attacks in Wireless networks. Blackhole is one the prominent type of attack which drops the data or information between nodes sent from the server.

This paper discusses about an unauthorized access in the Wireless network and Intrusion Detection System been used to identify the unauthorized access and also the Blackhole attack to drop the data. The rest of the paper organized as follows : Literature Review in section 2, Detailed Problem Definition in section 3, Frame work in section 4, Experimental Results in section 5 and Conclusion in section 6.

2) LITERATURE REVIEW:

In the literature, trust has been used to enhance the security factors from source to destination in attempt to solve issues of information security based on[1]-[3]. The author[4] proposed a scheme called Certification Management Node Scheme to improve the security in ad-hoc network as ad-hoc is vulnerable to various attacks. This method is used to select certificate management node in ad hoc network. This node collects and distributes certificates to other nodes in the network. To select a node to be Certificate Management Node in ad hoc network, the selection process is based on the value at each node that was proposed in OLSR protocol which specifies how a node is willing to be forwarding traffic on behalf of other nodes. If a node has highest value, which may be set to any integer value from 0 to 7, then this node is eligible to be Certificate Management Node in ad hoc network.

Humaira Ehsan, Farrukh Aslam Khan[5] in their work, proposed a solution for the severity level of MANETs against some attacks such as blackhole attack, sinkhole attack, selfish node behaviour, RREQ flood, hello flood and wormhole attack has been investigated. packet efficiency, routing overhead and throughput are the performance metrics for AODV protocol.

The attacks such as RREQ flood and hello flood can increase the amount of routing overhead and attacks such as sinkhole and blackhole affect the packet efficiency and decrease the throughput level leads the AODV protocol a malicious[5]. Misbehaving nodes can be a significant problem i.e.) nodes that agree to forward packets but failed to do so.

To mitigate this problem the author in [6], used watchdog and pathrater techniques to detect and avoid those misbehaving nodes. Watchdog technique identifies misbehaving nodes and pathrater helps routing protocols to avoid these nodes. When both these techniques used together increases throughput by 17% and during extreme mobility, it increases throughput by 27%. Pramod Kumar Singh, Govind Sharma [7] proposed a solution to blackhole attack in MANET based on one of the prominent routing algorithm called ad hoc on demand distance vector (AODV) routing.

The proposed method uses promisc mode(it is a mode used in wired or wireless network that causes controller to pass all traffic it receives to one particular node) to detect malicious node and propagate information to all other nodes. The result of this method shown as throughput does not getting worse in presence of blackholes.

L. Prema Rajeswari, R. Arockia Xavier Annie, A. Kannan [8] also proposed an enhancement for Intrusion Detection Systems in ad hoc network that uses intrusion detection techniques to detect active attacks.

The enhancement of intrusion detection system for ad hoc network does not make any changes to the underlying protocol and acts an intermediate between network traffic and the underlying routing protocol. This system was developed to operate in ad hoc network on AODV enabled routing. It also detect packet dropping and fabrication attacks in wireless network.

3) DETAILED PROBLEM DEFINITION :

In this approach, we consider the Wireless network to transfer data or to communicate between nodes. Depending on the several security issues of Wireless network, an Intrusion Detection System has been introduced to find the unauthorized access in the Wireless environment. Here one node acts as an server and other nodes acts as clients. The data will be send from server to all its clients. Before sending data it has been converted into number of packets to travel via Wireless network. The packets can then be forward to client nodes.

The IDS acts as an security system between nodes so it'll check whether all the data packets are from reliable path by checking its authorized port number. Once if the port number is authorized then IDS will forward the data packets to the sink to display else if the data packets are from unauthorized port then it'll forward all the data packets to Inter Domain Filter. Here the Blackhole acts as an Inter Domain Filter and it'll drop the unauthorized packets rather sending it to the sink. This approach is implemented using Java Technology.

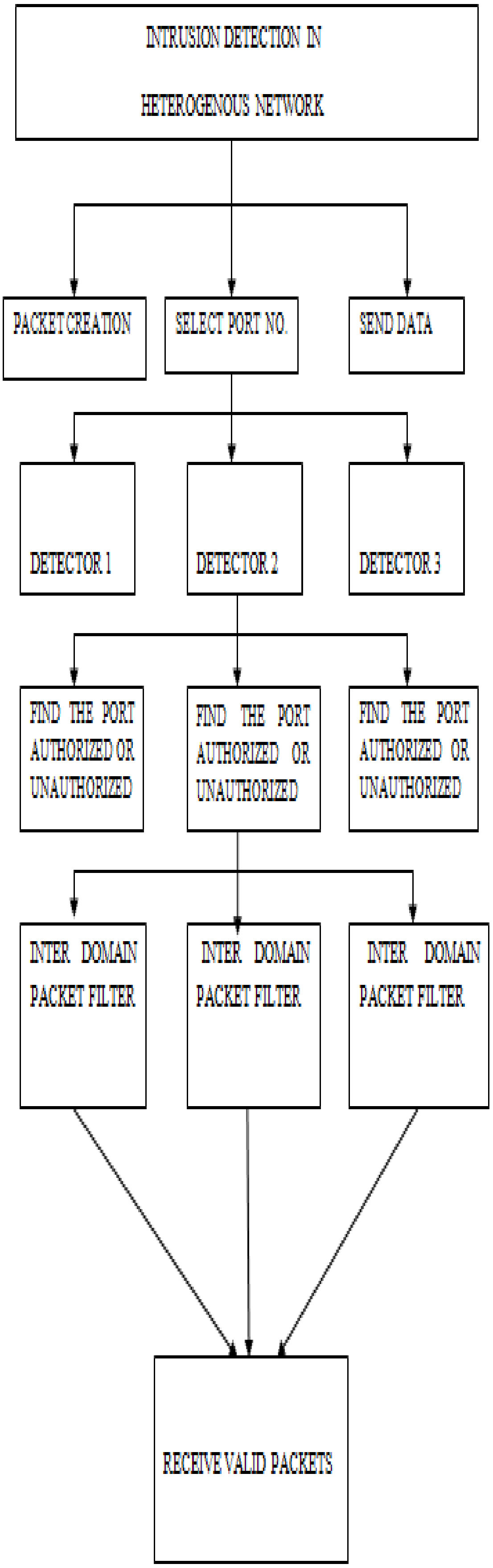
Java Swing is a technology, it can be used here to implement this concept. Here the systems we are connecting through LAN cable acts as no. of nodes. Initially the IP address and Port numbers of the nodes connected are being stored.

Each and every time before the datas are being send between nodes, the IP address and Port numbers which we are stored already been checked to find whether it is available or not i.e) to find authorized or unauthorized path. Only if the IP address and port number which has been stored matches with the client node, the data transfer from the server.

Before transferring, the data is converted into no. of packets to transfer via network. By using Binary Tree Traversal, the data is converted into packets.

If the IP address and Port number of any client node does not match then it has been considered as unauthorized path. So the detector will not transfer the data to destination rather it will drop the packets. Finally, all the valid data packets will reach the destination through Intrusion Detector.

4) PROPOSED ARCHITECTURE:


INTRUSION DETECTION IN HETEROGENOUS NETWORK
PACKET CREATION
SELECT PORT NO.
SEND DATA
DETECTOR 1
DETECTOR 2
DETECTOR 3
FIND THE PORT AUTHORIZED OR UNAUTHORIZED
FIND THE PORT AUTHORIZED OR UNAUTHORIZED
FIND THE PORT AUTHORIZED OR UNAUTHORIZED
INTER DOMAIN PACKET FILTER
INTER DOMAIN PACKET FILTER
INTER DOMAIN PACKET FILTER
RECEIVE VALID PACKETS

This is the framework which explains how the data transferring between nodes and how the Intrusion Detector works and how the Inter Domain Filter drops the data packets. Here this framework has been splitted into 4 modules for program independence and easy maintenance.

4.1) NODE REGISTRATION AND CONNECTION:

In this module, all the nodes are connected together to connect to the network for transferring data between them and also all the nodes to be registered for validation and connection confirmation. Initially all the nodes to be registered i.e) stored in a database for the user to select the source and its neighbor node to transfer the data and a connection must be provided between the nodes for secure data transfer.

4.2) NODE FRAME CREATION:

In this module, the node frame to be created to select and send the data to the destination node and also to forward data to Intrusion Detection System to check it is valid. Every node has its node frame which has authorized port number of its own for transferring data or to communicate between them. The datas send from the source frame will reach the destination frame only if the port number is authorized. Before that the datas will be forwarded to Intrusion Detection System.

4.3) INTRUSION DETECTION SYSTEM:

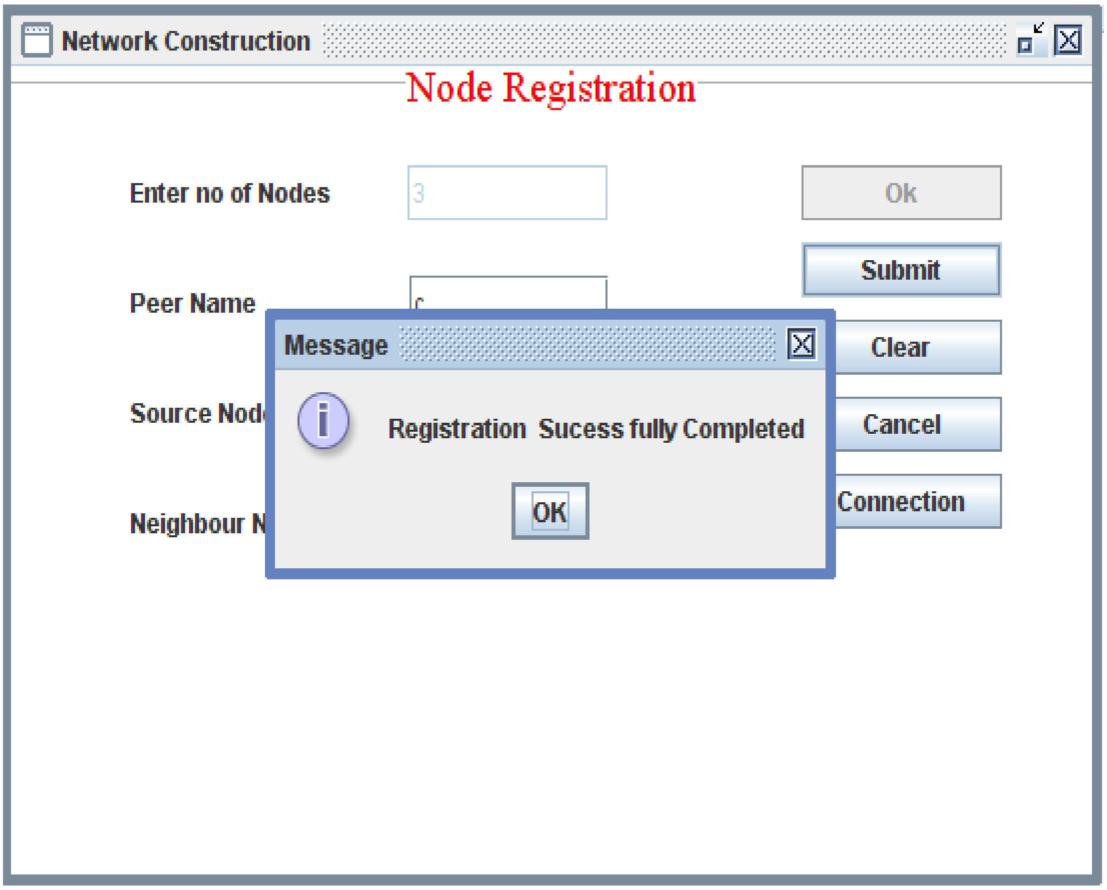
In this module, the Intrusion Detection System will check whether the data is from authorized path or unauthorized path.If the datas from authorized path it will be forwarded to valid destination and the datas from unauthorized path will get dropped. Also the datas are converted into packets to transfer via protocol.

4.4) BLACK HOLE GUARD:

In this module, it will display the normal user who sending data to valid destination and also attackers who trying to deny the service of particular node. Here the normal user is the one who are sending the data from the valid port number and the IP address and the attacker is the one who is trying to get the service of normal user so the datas will not reach the destination and it'll get dropped by Intrusion Detection System itself.

5)RESULT AND ANALYSIS:

This section will provide the basic idea about the data transferring between nodes and an IDS to detect the data. First we need to register the nodes are being connected together for data transfer and also to assign connection between source and destination node.



Network Construction

Node Registration

Enter no of Nodes 3

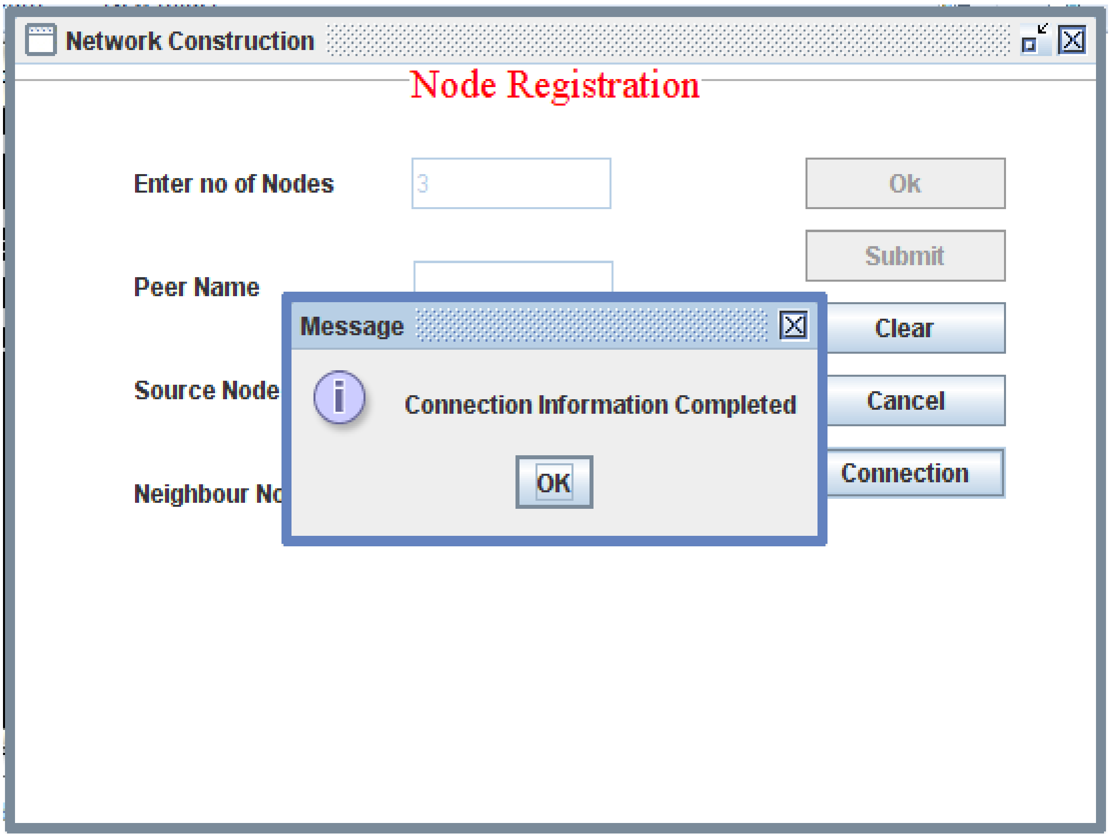
Peer Name c

Source Nod

Neighbour N

Message

Registration Sucess fully Completed



Network Construction

Node Registration

Enter no of Nodes 3

Peer Name

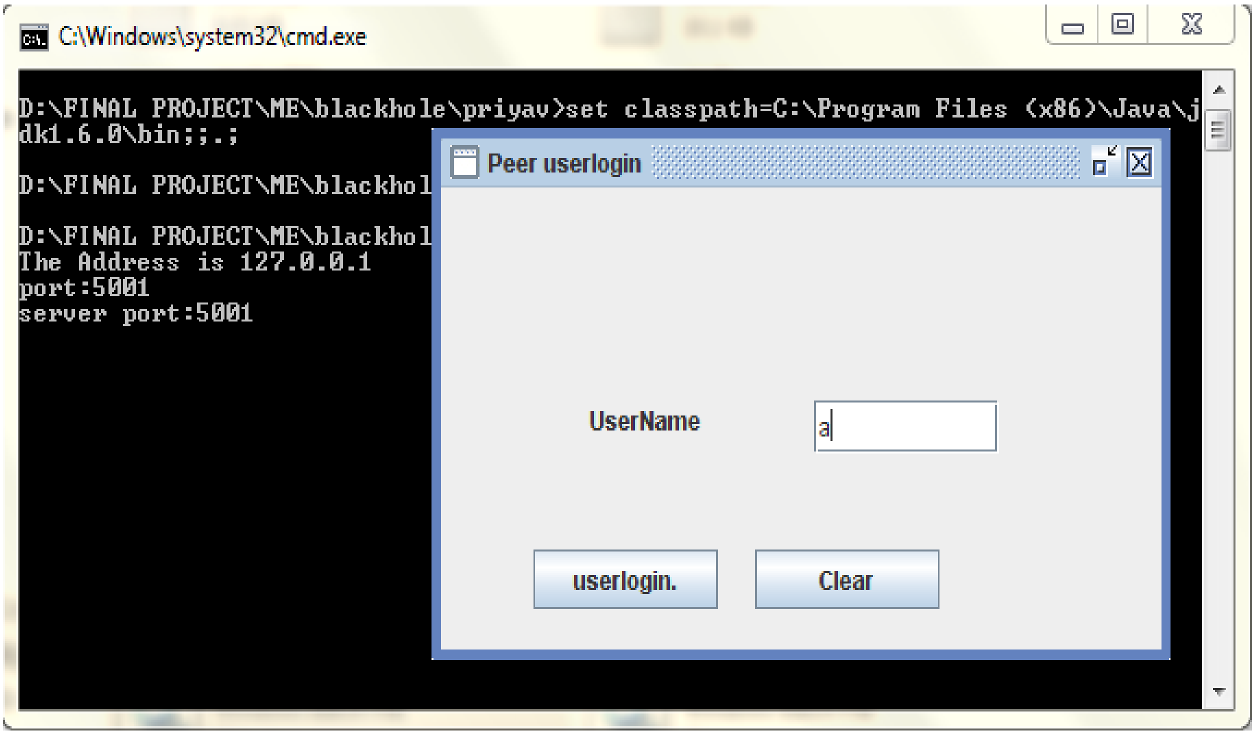
Source Node

Neighbour No

Message

Connection Information Completed

After creating connection between source and destination node, the node frame to be created for each and every node to select and transfer the data from the server port to client via Intrusion Detection System.

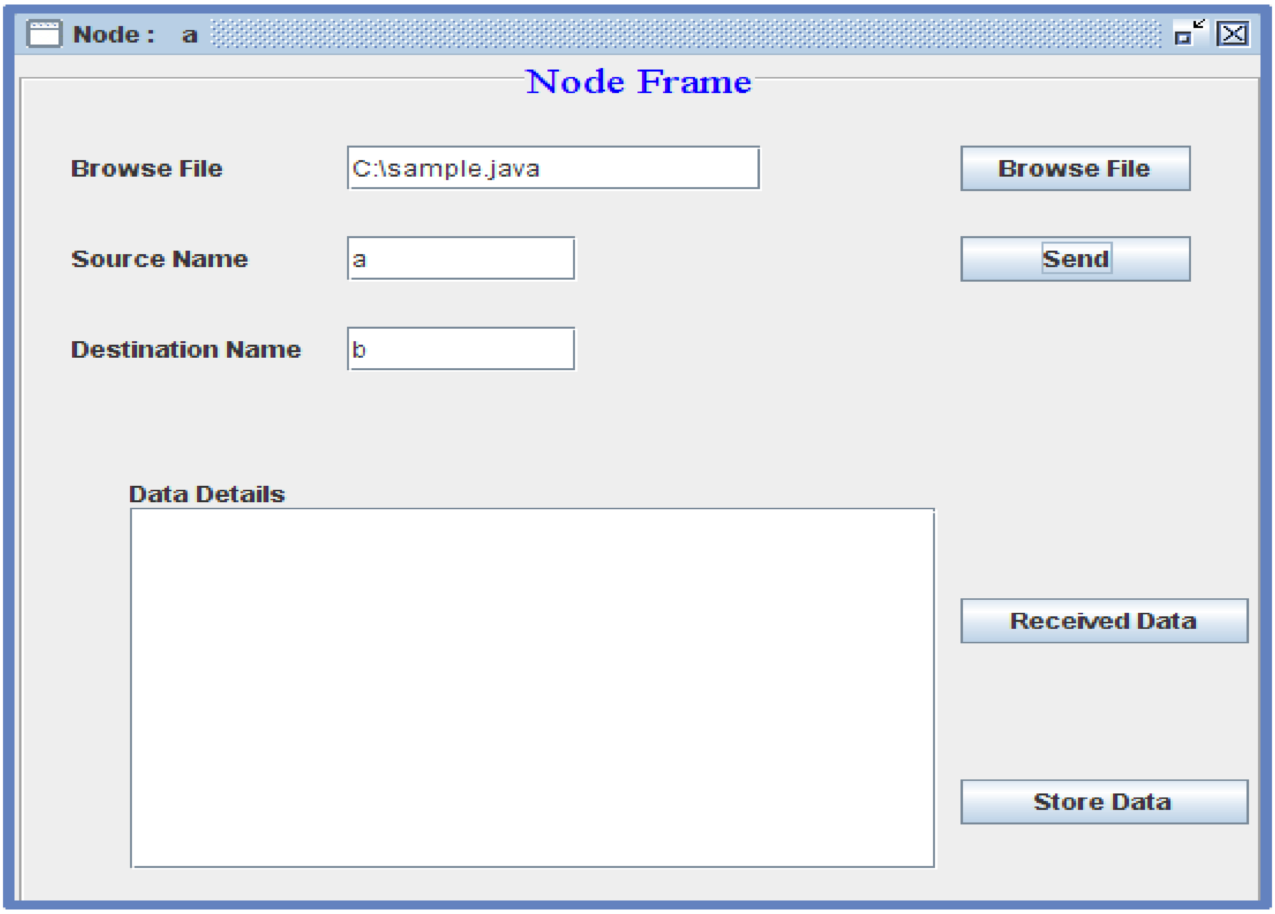


```
D:\FINAL PROJECT\ME\blackhole\priyav>set classpath=C:\Program Files (x86)\Java\j
dk1.6.0\bin;;.;

D:\FINAL PROJECT\ME\blackhol

D:\FINAL PROJECT\ME\blackhol
The Address is 127.0.0.1
port:5001
server port:5001
```

UserName a



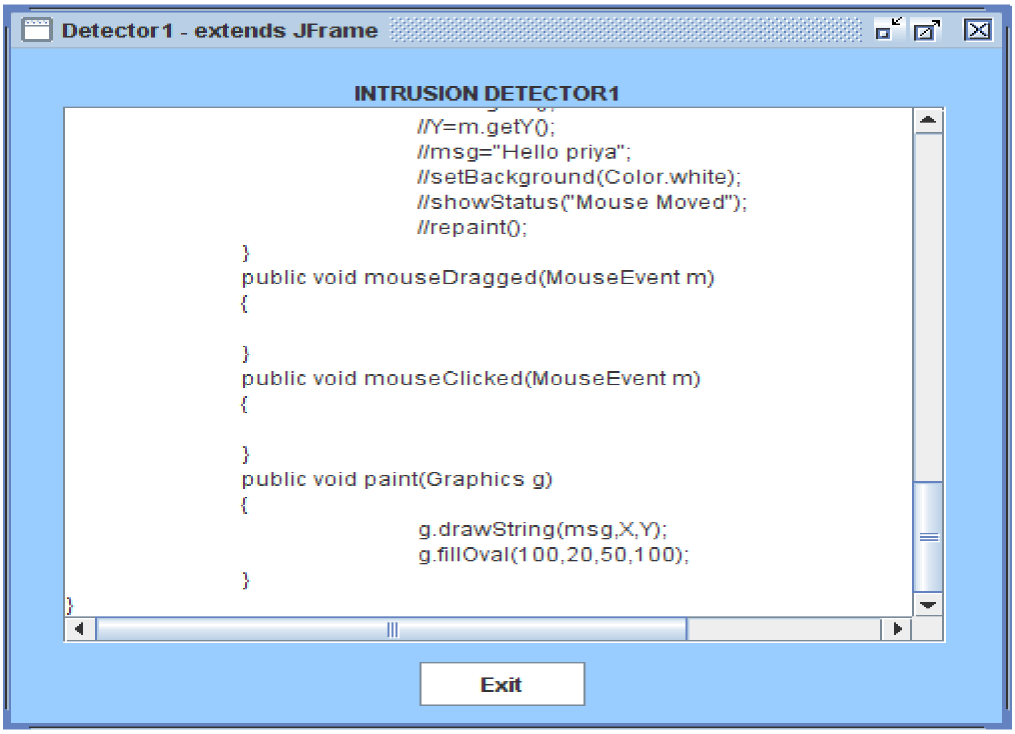
Browse File C:\sample.java

Source Name a

Destination Name b

Before sending data packets to destination, it has to be checked whether the data packets coming from authorized port by using a detector. Once the data packets coming from unauthorized port then detector will send the data packets to Inter Domain Filter(Blackhole) there the packets will gets dropped.

DETECTOR:



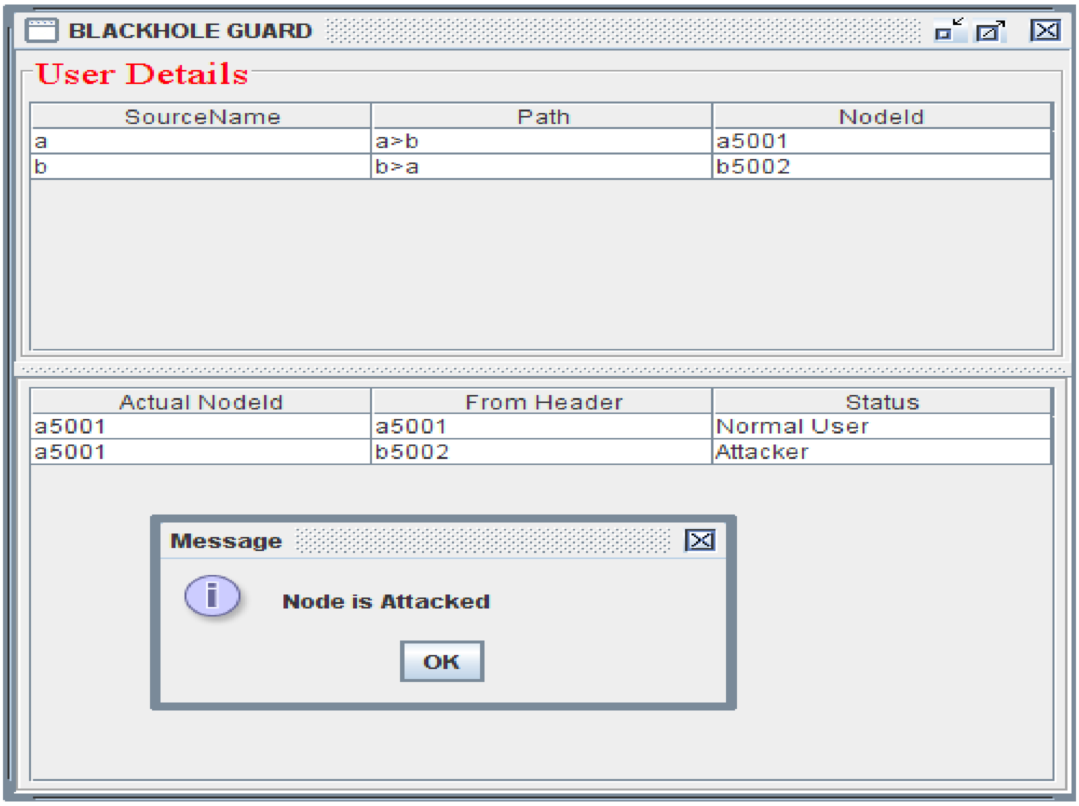
INTRUSION DETECTOR1

```
                    //Y=m.getY();
                    //msg="Hello priya";
                    //setBackground(Color.white);
                    //showStatus("Mouse Moved");
                    //repaint();
          }
          public void mouseDragged(MouseEvent m)
          {

          }
          public void mouseClicked(MouseEvent m)
          {

          }
          public void paint(Graphics g)
          {
                    g.drawString(msg,X,Y);
                    g.fillOval(100,20,50,100);
          }
}
```

After being checked all the data packets by the detector, the valid data packets will reach the destination. It is displayed via Blackhole guard whether the datas are coming from normal user or from attacker.



User Details

SourceName	Path	NodeId
a	a>b	a5001
b	b>a	b5002

Actual NodeId	From Header	Status
a5001	a5001	Normal User
a5001	b5002	Attacker

Message

Node is Attacked

6) CONCLUSION :

In this paper, an Intrusion Detection System(IDS) in wireless network is introduced. An IDS is used to detect the malicious behavior in wireless network and drops the unwanted packets using Inter Domain Filter in wireless network by identifying the best path to transfer data packets to valid destination. Analysis shows that the proposed IDS can detect the malicious node by means of Inter Domain Filter in wireless network.

REFERENCES:

[1] Niyati Shah, Sharada Valiveti , Intrusion Detection Systems for the Availability Attacks in Ad-Hoc Networks, International Journal of Electronics and Computer Science Engineering, pp.1850-1857.

[2] Wei Ou, Xiaofeng Wang, Wenbao Han, Yongjun Wang , Research on Trust Evaluation Model Based on TPM, International Conference on Frontier of Computer Science and Technology,2009, pp.593-598.

[3] Jimin Li, Junbao Li, Aiguo An, Zhenpeng Liu, Two-way Trust Evaluation Based on Feedback, IEEE transactions,2010, pp.1910-1915.

[4] Grzegorz Wierzowiecki and Adam Wierzbicki, Ph.D , Efficient and Correct Trust Propagation Using CloseLook, IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology,2010, pp.676-682.

[5] Yojiro takehana, Iichiro nishimura, Norihito yosaka, Tomoyuki nagase, and Yoshio yoshioka, Building Trust among Certificate Management Nodes in Mobile Ad-Hoc Network, 26th International Conference on Advanced Information Networking and Applications Workshops, 2012,pp.564-569.

[6] Humaira Ehsan, Farrukh Aslam Khan , Malicious AODV Implementation and Analysis of Routing Attacks in MANETs, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp.1181-1188.

[7] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, Mitigating Misbehaviour in Mobile Ad Hoc Networks, 2000 ACM, pp.255-266.

[8] Pramod Kumar Singh, Govind Sharma, An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications,2012, pp.902-907.

[9] L. Prema Rajeswari, R. Arockia Xavier Annie, A. Kannan, Enhanced intrusion detection techniques for mobile ad hoc networks, IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007), Dec. 20-22, 2007. pp.1008-1013.