Mac Based Security from Malicious Nodes For Cluster Based Wireless Sensor Network

[1]Rameshwarayya, [2]Ramesh Patil

[1] M.Tech Student, Electronics and Communication, Guru Nanak Dev Engineering College Bidar, Karnataka, India.
[2]HOD, Computer Science, Guru Nanak Dev Engineering College Bidar, Karnataka, India.

Abstract: **WSN is composed of network of devices, denoted as nodes, that can provide low cost solution to variety of real-world problems. Sensors are low cost tiny devices with limited storage, computational capability and power. They can be deployed in large scale for performing both military and civilian tasks. Security will be one of the main concerned when they will be deployed in large scale In wireless network however one cannot make assumption that wireless users are trusted. Malicious individuals could easily disrupt the network & is critical to protect a sensor network from such malicious attacks, which presents a demand for providing security mechanisms in the network. In this project, we propose a new approach of Security Solution for Cluster Based Wireless Sensor Networks. In the proposed methodology, an efficient MAC address based intruder tracking system has been developed for early intruder detection and its prevention.**

Keywords: **Wireless Sensor Networks (WSNs), Cluster Head (CH), Base Station (BS), Intrusion Detection System (IDS).**

I. INTRODUCTION

Recent advances in wireless communications and electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untethered in short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks. Sensor networks represent a significant improvement over traditional sensors.

Security is becoming a major concern for protocol designers of WSN because of the broad security-critical applications of wireless sensor networks (WSNs). To protect a network, there are usually several security requirements, which should be considered in the design of a security solution, including confidentiality, integrity, and authenticity. An effective security solution should provide services to meet these requirements. In many cases, no matter how carefully we design a security infrastructure for a network, attackers may stil find a way to break into it and launch attacks from the inside of the network. If they just keep quiet to eavesdrop on traffic flows, they can stay safe without being detected. If they behave more actively to disrupt the network communications, there will be some anomalies, indicating the existence of malicious intrusion or attacks. An intrusion can be defined as a set of actions that can lead to an unauthorized access or alteration of the wireless network system. Intrusion detection mechanisms can detect malicious intruders based on those anomalies. Intrusion detection system (IDS) attempts to monitor computer networks and systems, detecting possible intrusions in the network, and alerting users after intrusions had been detected, reconfiguring the network if this is possible [1], [2]. Usually, the neighbors of a malicious node are the first entities learning those abnormal behaviors. Therefore, it is convenient to let each node monitor its neighbors such that intrusion detection mechanisms can be triggered as soon as possible.

In case of cluster-based hierarchical routing wireless sensor network, network topology depend on communication range of the nodes, location information, distance between the nodes and remaining battery power [3], [4], [5], [6], [7]. An intruder can manipulate these parameters to mount spoofed, altered, or replayed routing information attack and attract the network towards it to create a sinkhole. This sink hole may turn into black hole if it absorbs the data completely. These protocols transmit data in multi-hop so intermediate nodes take the responsibility of data aggregation/fusion and forward data to upper level. An adversary who joins the network in setup phase can selectively forward data to upper level and change the data to lead data integrity attack. Attacker can mount adversary nodes with same id in different place of the network and actively join the network. These nodes generate the false data and disrupt the data communication. Also, in multi-hop hierarchical routing, whenever a node sends data to another node, it expects an acknowledgement from the receiving node. Adversary nodes may take the benefit of this and send false acknowledgement for weak and dead nodes to convince the network as alive [8].

II. SECURITY SOLUTIONS FOR CLUSTER BASED WIRELESS SENSOR NETWORKS

A. Related work:

Continuous monitoring may be energy consuming, which is not desirable in WSNs. Therefore, a cluster-based detection approach is developed for WSNs in Ref. [12]. In this approach, a network is divided into clusters. Each cluster head monitors its cluster members. All the members in a cluster are further divided into groups and the groups take turns to monitor the cluster head. Not all the sensor nodes keep monitoring, thus reducing the overall network energy cost. The security protocol proposed in Ref. [10] uses local monitoring, in which a neighbor of both a sender and a receiver can oversee the communication behaviors of the receiver. If the receiver has any abnormal behavior on the received packets, it may be detected. If the number of abnormal behaviors is larger than a threshold, the neighbors of the detected malicious node refuse to receive packets from and send packets to it so that the malicious node is isolated from the network. In Ref. [11], a reputation-based framework is established, in which each node holds reputations for other nodes. Based on the observations of whether other nodes are cooperative or not, those reputations are updated through an iterative procedure and are used as criteria to decide whether a node is malicious or not.

B. Problem formulation:

The problem of the work can be stated as malicious node detection for WSN, based on the concept of MAC address. This is comprehensively stated as “Security Solution for Cluster-Based Wireless Sensor Networks”.

The problem demonstration involves browsing the information, selection of port numbers, packetizing and sending over the network, further developed IDS which detects the intruder and presents an alarm message to user.

C. Proposed system:

1. Intrusion detection in heterogeneous WSNs by characterizing intrusion detection with respect to the network parameters

2. Two detection models are: Single-sensing detection and Multiple-sensing detection models

These are two detection models. We are detecting the intruder both single sensor and multiple sensor wireless sensor network..

Advantages:

- Through sensing the network we able to find possible node in the wireless Sensor network.
- By finding the intruders we can send our information in a secured manner.

Disadvantages:

- The sensed information provided by a single sensor might be inadequate for recognizing the intruder.
- So that there is no guarantee for our information has been sent securely

D. System design.

In the present developed system the two networks are deployed one for Multiple Sensor Network and the other for Single Sensor Network.

The Multiple Sensor Network is composed of source nodes, sink nodes and detector nodes.

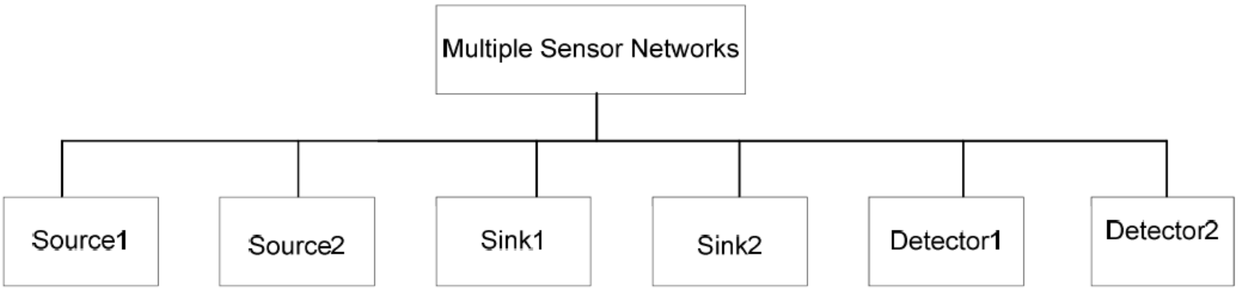


Figure : Multiple Sensor Networks

The Single Sensor Network is composed of source node, sink node and receiver nodes.

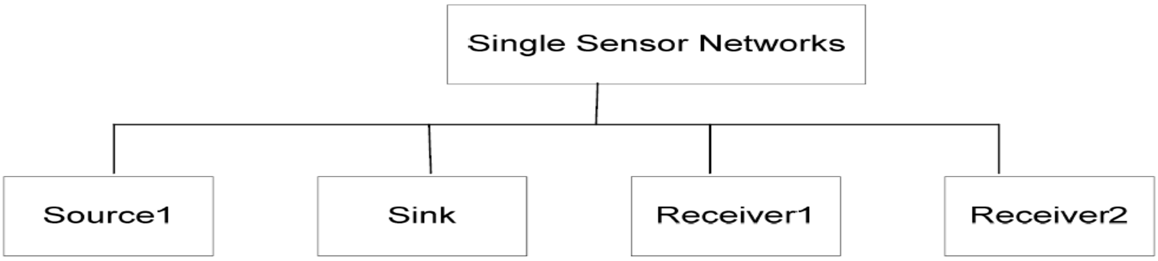


Figure : Single Sensor Networks

IDS flow diagram

The flow chart is a graphical representation of the flow of control through the system.

The figure in this section discusses the flow chart of data transfer and intrusion detection.

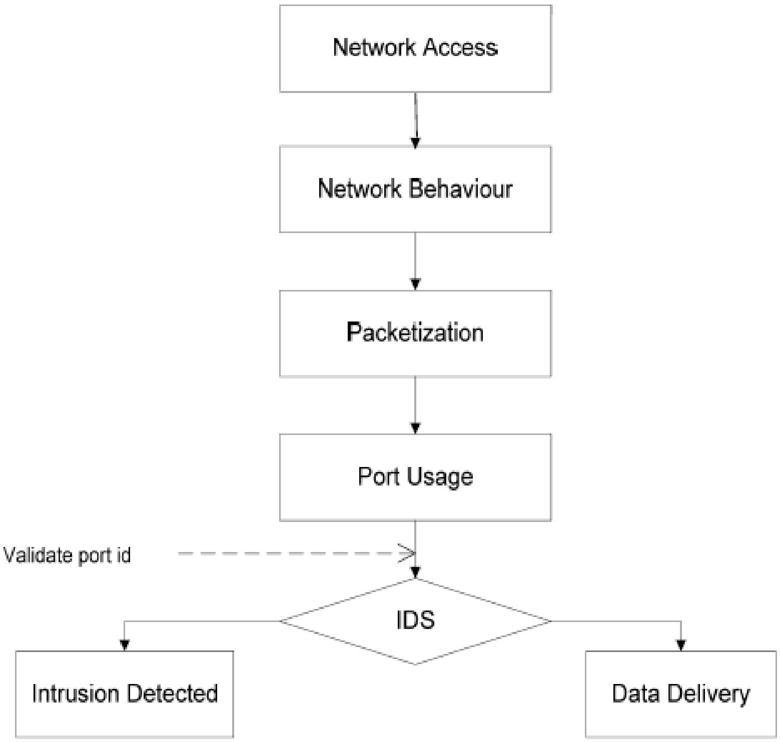


Figure : IDS Flow Diagram

Steps:

Step1: Deployment of the network and each node is connected to neighbor node.

Step2: Behavior of the network is analyzed.

Step3: Selected data is converted into fixed size packets.

Step4: Port number authorization.

Step5: Detector and Sink participate in transfer of packets and detection of intrusion

Step6: Using pid the packets are validated by IDS.

Step7: Intruder detected packets are discarded and the genuine packets are delivered.

E. Case Diagram:

A use case diagram is a type of behavioral diagram defined by and created from a Use case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The Figure shows the use case of the system. Case diagram for proposed system:

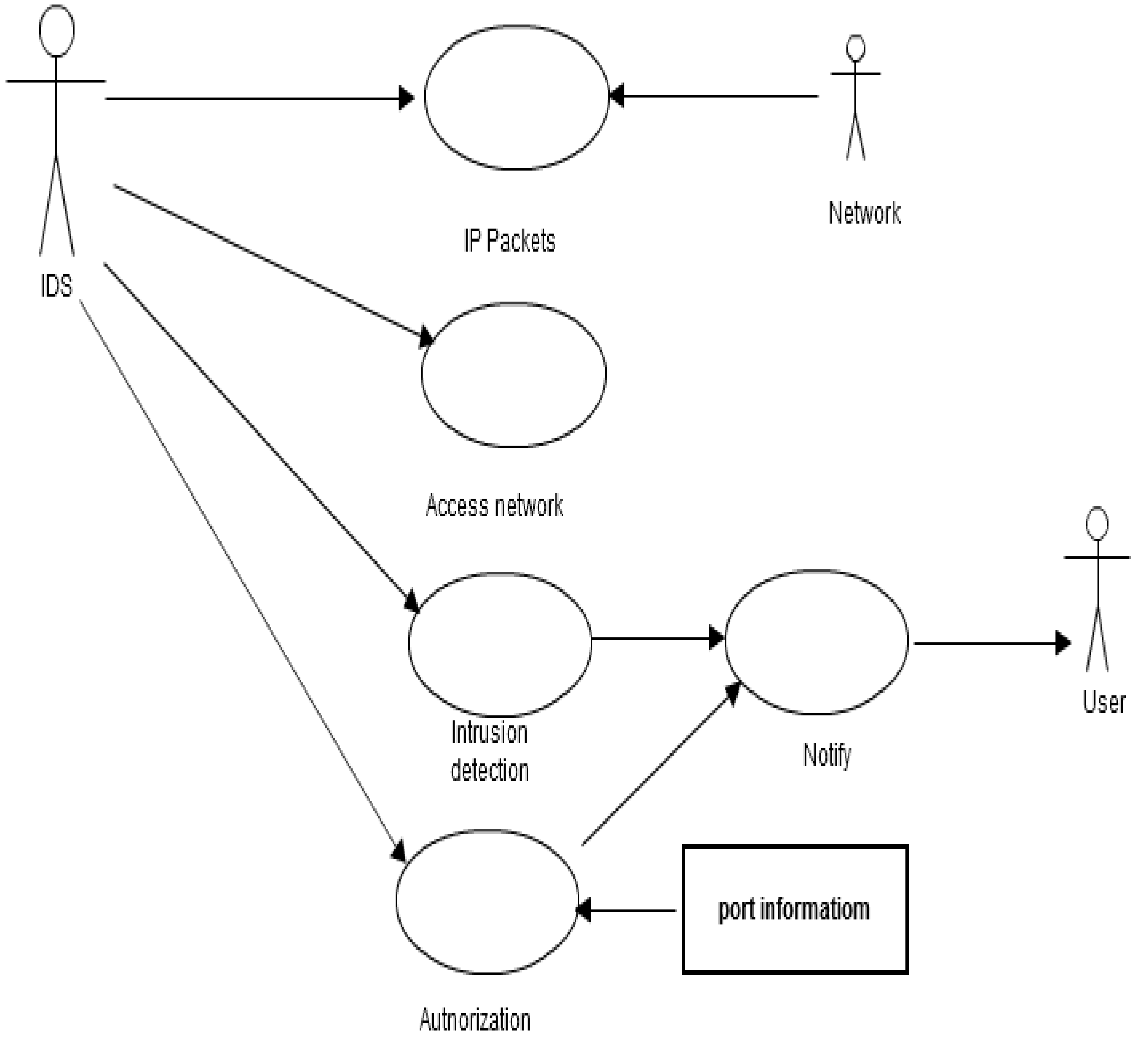
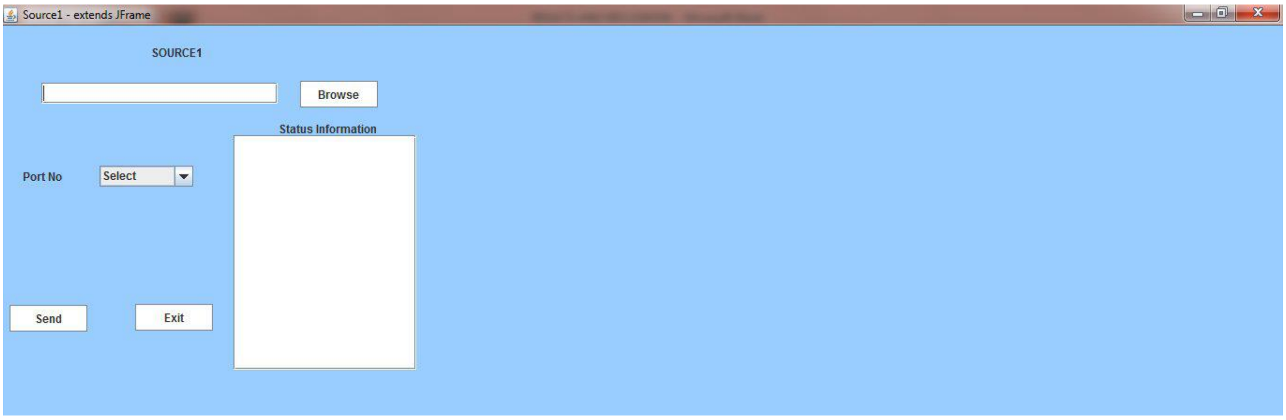


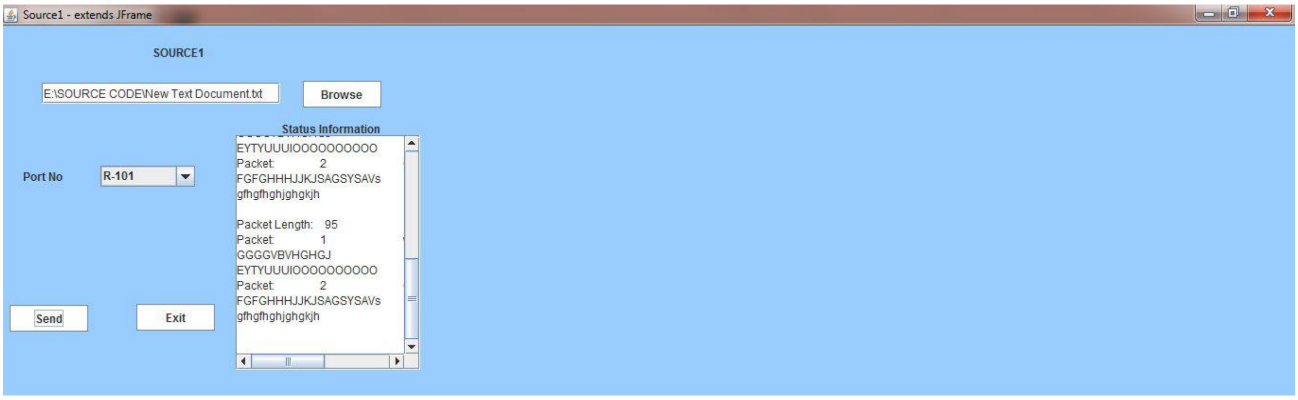
Figure : Use Case diagram

F. Results and discussion:

Source:



User is provided with an GUI where he has to choose a data file to send it across the network, by using port.



E:\SOURCE CODE\New Text Document.txt

Port No: R-101

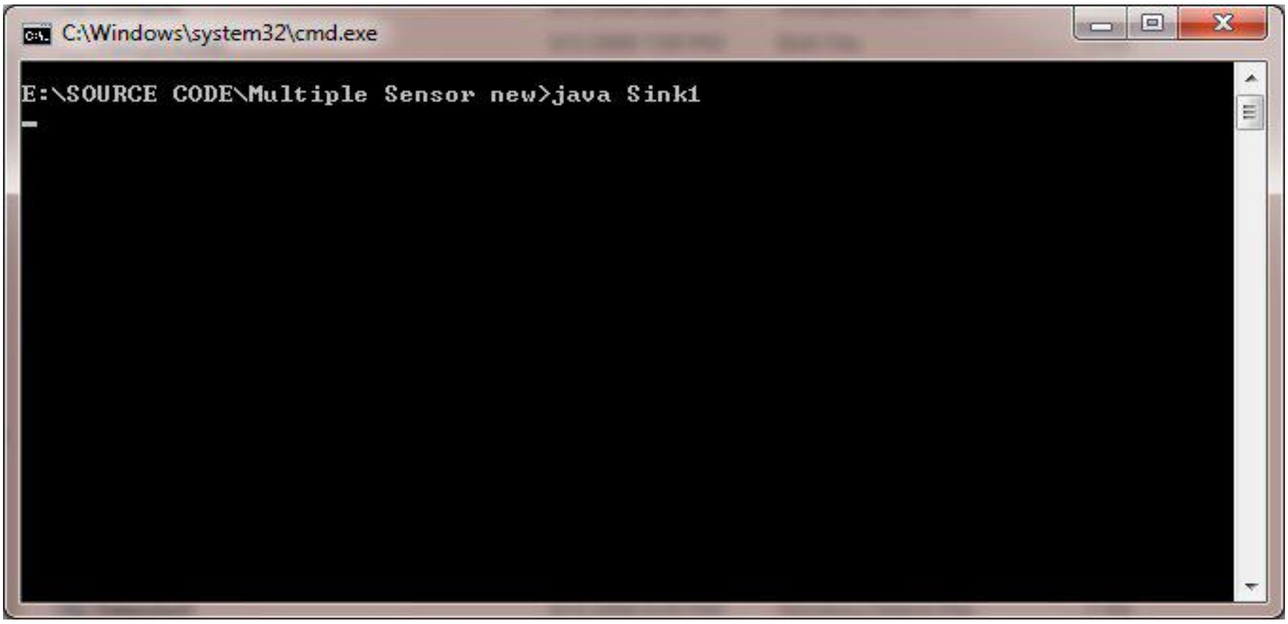
```
EYTYUUUIOOOOOOOOOOO
Packet:          2
FGFGHHHJJKJSAGSYSAVs
gfhgfhghjghgkjh

Packet Length:   95
Packet:          1
GGGGVBVHGHGJ
EYTYUUUIOOOOOOOOOOO
Packet:          2
FGFGHHHJJKJSAGSYSAVs
gfhgfhghjghgkjh
```

The above result shows the details after browsing, selected port number, status information associated with the data and packet detail packet length.

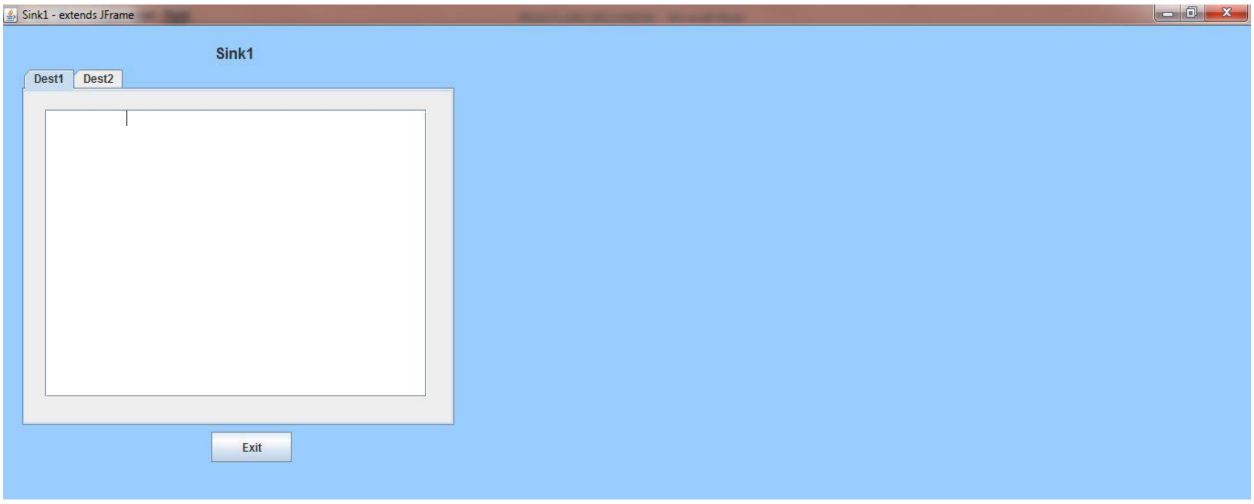
Sink:

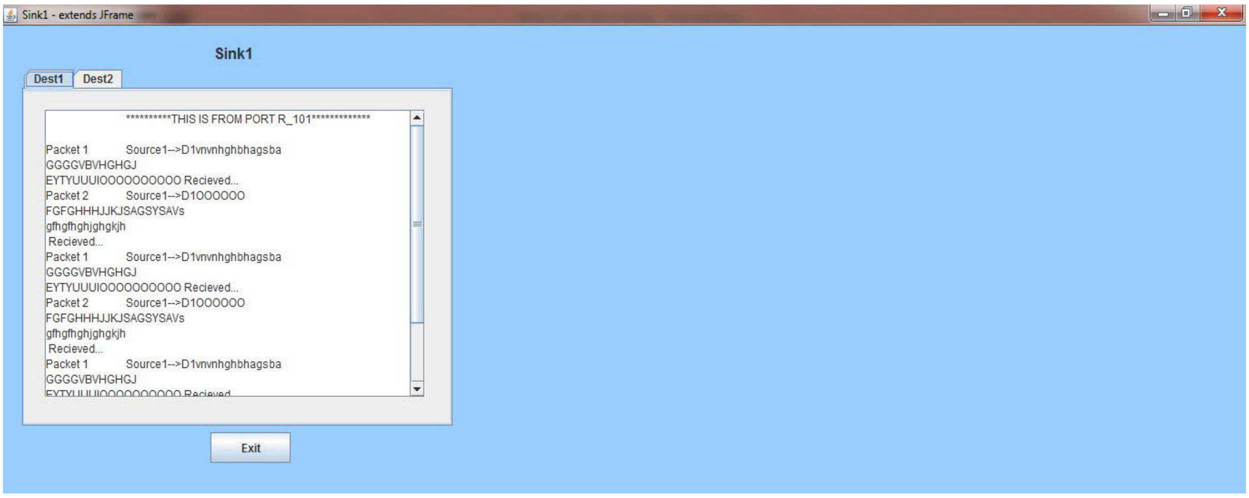
In this interface all data is collected for further transmission and detection process is logged/displayed.



```
E:\SOURCE CODE\Multiple Sensor new>java Sink1
_
```

After running Sink1 below user interface will be displayed



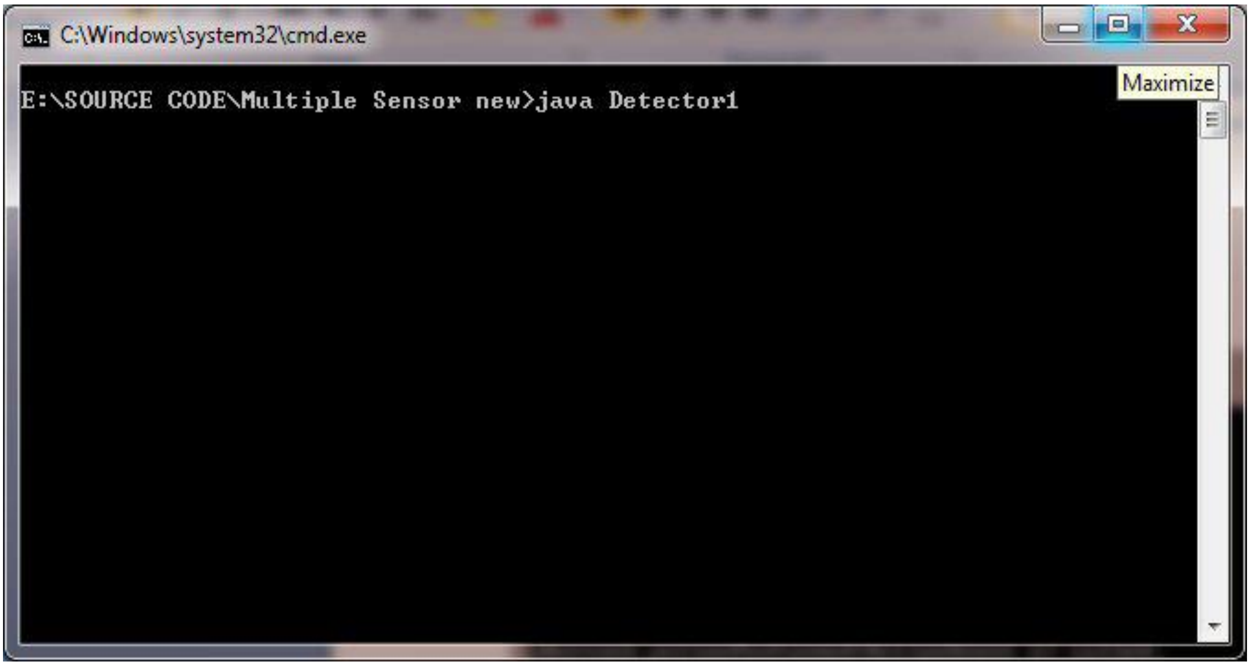


```
          **********THIS IS FROM PORT R_101*************

Packet 1        Source1-->D1vnvnhghbhagsba
GGGGVBVHGHGJ
EYTYUUUIOOOOOOOOOO Recieved...
Packet 2        Source1-->D1OOOOOO
FGFGHHHJJKJSAGSYSAVs
gfhgfhghjghgkjh
 Recieved...
Packet 1        Source1-->D1vnvnhghbhagsba
GGGGVBVHGHGJ
EYTYUUUIOOOOOOOOOO Recieved...
Packet 2        Source1-->D1OOOOOO
FGFGHHHJJKJSAGSYSAVs
gfhgfhghjghgkjh
 Recieved...
Packet 1        Source1-->D1vnvnhghbhagsba
GGGGVBVHGHGJ
EYTYUUUIOOOOOOOOOO Recieved
```

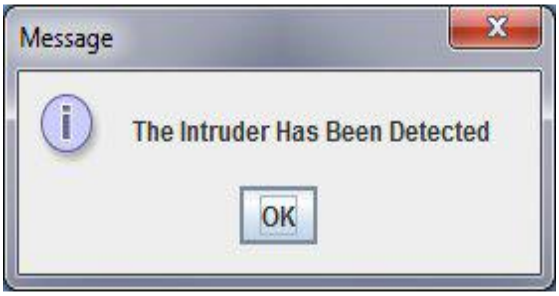
The above result shows the synchronized data ready to send for detection

Detector:

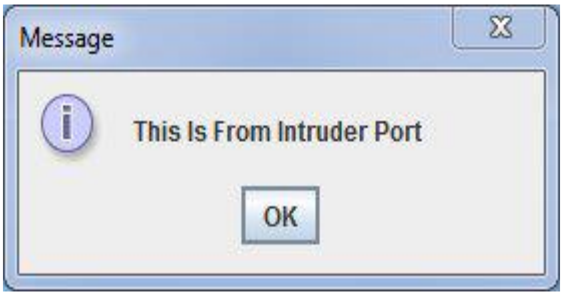


```
E:\SOURCE CODE\Multiple Sensor new>java Detector1
```

After running Detector1 below user interface will be displayed.



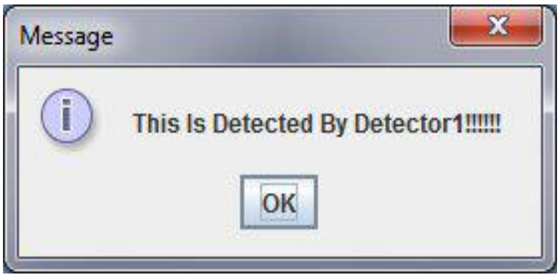
The Intruder Has Been Detected



This Is From Intruder Port

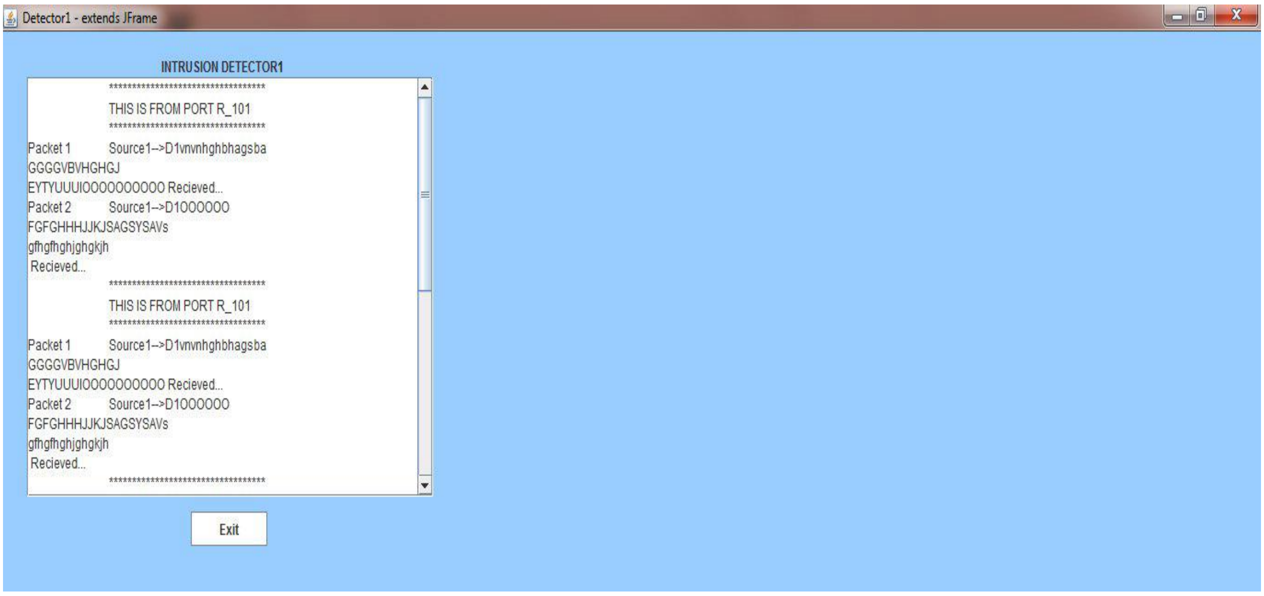
Alert message to user about the intruder port

Alert message to the user soon after the Intrusion detection by detector



This Is Detected By Detector1!!!!!!

Alert message to user showing the intrusion detected by the Detector1



```
                **********************************
                THIS IS FROM PORT R_101
                **********************************
Packet 1        Source1-->D1vnvnhghbhagsba
GGGGVBVHGHGJ
EYTYUUUIOOOOOOOOOO Recieved...
Packet 2        Source1-->D1OOOOOO
FGFGHHHJJKJSAGSYSAVs
gfhgfhghjghgkjh
 Recieved...
                **********************************
                THIS IS FROM PORT R_101
                **********************************
Packet 1        Source1-->D1vnvnhghbhagsba
GGGGVBVHGHGJ
EYTYUUUIOOOOOOOOOO Recieved...
Packet 2        Source1-->D1OOOOOO
FGFGHHHJJKJSAGSYSAVs
gfhgfhghjghgkjh
 Recieved...
                **********************************
```

III. CONCLUSION

In this paper a hop greedy routing protocol is introduced which finds the best possible path to destination in terms of both hop count and connectivity. A unicast request messages are forwarded to intended destination. For connectivity issues the concept of backbone node is introduced which tracks the movement of both source and destination and forwards the data in the changed direction by choosing a proper intermediate forwarding node to destination. The hop greedy routing also helps to reduce congestion, packet loss while broadcasting the message. The results of GPSR with BAHG in terms of packet delivery ratio and end to end delay are compared.

REFERENCES

[1] Jun Zheng and Abbas Jamalipour, “Wireless Sensor Networks: A Networking Perspective”, a book published by A John & Sons, Inc, and IEEEE, 2009.

[2] R. Bace,“Intrusion Detection”, MacMillan Technical Publishing, 2000.

[3] P. Mohanty, S. A. Panigrahi, N. Sarma, and S. S. Satapathy, “Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey” Journal of Theoretical and Applied Information Technology, 2010, pp. 14-27.

[4] Shio Kumar Singh, M.P. Singh, and D.K. Singh, “A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks”, International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.

[5] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energy-efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN), Aug. 2010, vol. 2, no. 3, pp. 49-61.

[6] Shio Kumar Singh, M.P. Singh, and D.K. Singh, “Applications, Classifications, and Selections of Routing Protocols for Wireless Sensor Networks” International Journal of Advanced Engineering Sciences and Technologies (IJAEST), November 2010, vol. 1, issue no. 2, pp. 85-95.

[7] Shio Kumar Singh, M.P. Singh, and D.K. Singh, “Routing Protocols in Wireless Sensor Networks – A Survey” International Journal of Computer Science and Engineering Survey (IJCSES), November 2011, Vol. 1, issue no. 2, pp. 63-83.

[8] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Performance Evaluation and Comparison of Energy efficient Routing Protocols for Wireless Sensor Network", Global Journal of Computer Application and Technology (GJCAT), Jan. 2011, vol. 1, no. 1, pp. 57-65.

[9] Kamal Kant, Nitin Gupta, “Application based Study on Wireless Sensor Network”, International Journal of Computer Applications (0975 – 8887) Volume 21– No.8, May 2011.

[10] I.F. Akyildiz, E.P. Stuntebeck, Wireless underground sensor networks: research challenges, Ad-Hoc Networks 4 (2006) 669–686