DETECTING, DETERMINING AND LOCALIZING MULTIPLE ATTACKS IN WIRELESS SENSOR NETWORK - MALICIOUS NODE DETECTION AND FAULT NODE RECOVERY SYSTEM

Rajalakshmi[1], Umamaheswari[2] and A.Vijayaraj[3]
[1]Department of Computer Applications, Dhanalakshmi College of Engineering, Chennai, India
[2]Department of Computer Science and Engineering, RRASE Engineering College, Chennai, India
[3]Department of Information Technology, Saveetha Engineering College, Chennai, India

ABSTRACT

In wireless and sensor network are deployed, they will increase malicious attacks. Faking approaches are represent in the form identify compromise and can provide a variety of traffic injection approach a reducing the performance of network. To avoid faking approach to detect the presents of various type of attacks and eliminate them from the network. To handle these attack to apply cryptography authentication, RSS, cluster based mechanism and support vector machines rule requires additional infrastructure overhead and achieve ninety percentage hit ratio. In this paper, I take a different method by using physical property associate wireless transmission to detect Sybil and worm hole attacks, results achieve over ninety six percent hit ratio and Precision when defining the sybil, worm and black hole attacks, Internet Protocol address faking approach and distributed algorithm measures and localizing this medium access control address faking approach. Our approach proposed blast efficiently and separately. Another proposed local monitoring algorithm monitors the neighbour node locally, based on the malicious information from neighbour nodes the attacker form its surroundings is detected and localized. This kind of monitoring process works on overall network. After localization malicious nodes are eliminated from the network.

Keywords: wireless network security (WNS), sybil, worm and black hole attacks, internet protocol, medium access control address faking approach.

1. INTRODUCTION

Security in WSN might be as important in military and security applications (e.g. intruder detection). Attackers may attempt to block traffic in networks (i.e. perform a denial of service blast) or compromise data by adding some spoofed sensed data to network (i.e. aggregating blast). Attackers from the inside (corrupted node is placed into WSN) can commit routing attacks by leading data flow to spoofed sinkholes. Defences against blasts depend on the particular blast type. For example, to suppress denial of service blasts, rerouting technique may be used (avoiding affected region). Another prevention technique lies in usage of error-detection codes which produce redundant information about message to assure the integrity of message. Network encryption and sensor node authentication are great approaches to secure WSN. However, sensor nodes need to be equipped with physical resources in order to compute cryptographic algorithms which may lead to more expensive sensor nodes. Moreover, computation of such algorithms negatively influences network's energy consumption. The base station also needs to be aware of security arrangement of WSN in order to be able to communicate with protected WSN and therefore a base station software developer must understand such arrangements of the related WSN.

Wireless multiple approaches like sybil, worm hole and black hole attacks, Internet Protocol and Medium Access Control address faking approaches are easy to launch and can significantly impact the performance of networks. Although the identity and security of a node can be verified through various security mechanisms are not always suitable to improve the wireless network performance and fault node cannot be easily recover from the attacks. I propose to use distributed detection algorithm to efficiently measure the performance of networks and handle those blasts in accurate and separate manner. In extension to distributed detection algorithm a three separate intrusion detection system is proposed to detect these types of blasts efficiently with good accuracy. Local monitoring algorithm is proposed to detect the multiple blasts

2. SCOPE OF THE PAPER

The scope of this paper is to detecting various blasts, determining the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple adversaries in wireless sensor networks. The transmitted data from server is send to client in secure manner. If an intruder comes during transaction server discover and localize that specific system. These optimizations will ultimately enhance the WSN lifetime and reduce sensor node replacement cost. The algorithm can result in fewer replacements of sensor nodes and more reused routing paths.

3. LITERATURE SURVEY

An authentication framework for Ad Hoc Sensor Networks, this Research paper describes energy efficient distributed scheme to multi-cast messages from impersonating a middle-tier node. This research result show that the energy efficient scheme for Ad hoc sensor networks.

Number-Based medium access control address spoofing detection, this Research describes to detect spoofing by number-based Medium Access Control address. It can detect spoofing attack without changing the wireless station. This research result can detect only minimum spoofing frames.

Radar An in-Building system and RF based user location, this Research paper describes the radio frequency based system for tracking and locating various users inside the campus. The RADAR works by signal strength information to provide overlapping coverage in the infrastructure. This research's result find the location of user with accuracy.

A probabilistic approach to WLAN user location estimation, this research paper finds out user location based on radio signal strength. To find out the user location can be based on measurements collected at various geographical areas of location. This research paper show that the various field test for find out the various location of user.

A Practical Approach to Landmark Development for Indoor Localization, this research paper provides novel algorithm finds a pattern that minimizes the maximum localization error in landmark. The results of this research work show the improvement in the performance of localization through novel algorithm.

4. EXISTING METHOD

The existing system was implemented by received signal strength (RSS) inherited from wireless networks to detect the multiple blasts like sybil and Medium Access Control approaches. We then frame the problem of determining the number of spoofing attackers as a multiclass detection problem. To determine the number of attackers with the help of vector based rule. In addition, to identify and localize the positions of multiple blasters through cluster based rule and then improve the accuracy of detecting many attacks through support vector machines. The multiple faking blasts are identified and localized through IDOL an integrated system that can detect, determine many attackers and localize multiple adversaries.

We can't determine the number of attackers. Can't get accuracy result. Existing methods can achieve over 90 percent hit rate and precision when determining the number of attackers.

- The routing path may cause a break.
- The batteries of sensor nodes can be depleted, requiring more relay nodes.
- The inside nodes may have the largest data transmission loading, consuming energy at a faster rate.

5. PROPOSED METHOD

I propose to use distributed detection algorithm to efficiently measure the performance of networks and handle those blasts accurately and separately. In extension to distributed algorithm a three separate intrusion detection system is proposed to detect the types of attacks efficiently and high accuracy. Local monitoring algorithm is proposed to detect the various attacks like spoofing, sybil, worm hole and black hole. After detecting these attacks and attacker nodes are eliminated. The simulation results show better performance of our proposed system. Using the FNR algorithm can result in fewer replacements of sensor nodes and more reused routing paths. Thus, the algorithm is boon for the WSN lifetime but also reduces the cost of replacing the sensor nodes. The goal of replacing fewer sensor nodes that are inoperative or have depleted batteries, and use the same maximum number of routing paths again.

Advantages of proposed system

- Increases the WSN lifetime by changing some of the sensor nodes that are not functioning.
- Increases the WSN lifetime and decrease sensor node replacement cost.
- To increase the active nodes and decreasing the data losses.

6. PROPOSED METHODOLOGY

In this propose system to detecting and determining the following attacks efficiently with good accuracy such as

a) Worm hole

The malicious node enters into the network and affects one of the intermediate nodes by sending false packets. So the malicious nodes drain the energy of the intermediate node and lose its energy then intermediate node goes to the dead state.

b) Internet protocol address spoofing attack

This kind of blast is more dangerous for networks, a malicious node which communicate with other neighbor nodes in different Internet Protocol address. This kind of blasts can easily able to hack the data information from all other nodes, thus it leads to create a jammer in the network, which causes more vulnerable.

c) Medium access control address spoofing attack

The node in the network which drops the data packets received from the neighbor hop node is termed as black hole blast. This type of blast doesn't affect the other nodes, but it affects the network performance so it causes a failure in data delivery ratio.

d) Sybil

It is a computer hacker blast on a peer to peer network. In this attack, the blaster subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities and using them to gain a disproportionately large influence.

7. PROPOSED MECHANISIM

a) Distributed algorithm

A distributed algorithm is implementing to run on computer hardware constructed from interconnected processors and localizing various attacks efficiently and separately.

b) Node configuration setting

The wireless nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

c) Data routing

The two nodes such as source and destination transmits the data packets are placed at larger distance through the intermediate hop nodes using UDP user data gram protocol, link state routing like PLGP act as an ad hoc routing protocol.

d) Local monitoring algorithm

This is a proposed intrusion detection system which monitors the neighbor nodes locally, based on the malicious information from neighbor nodes the attacker from its surroundings is detected and localized. This kind of monitoring process works on overall network. After localization malicious nodes are eliminated from network

e) Graph examination

The existing method of work and proposed method of work is examined through graphical analysis.

8. RELATED WORKS

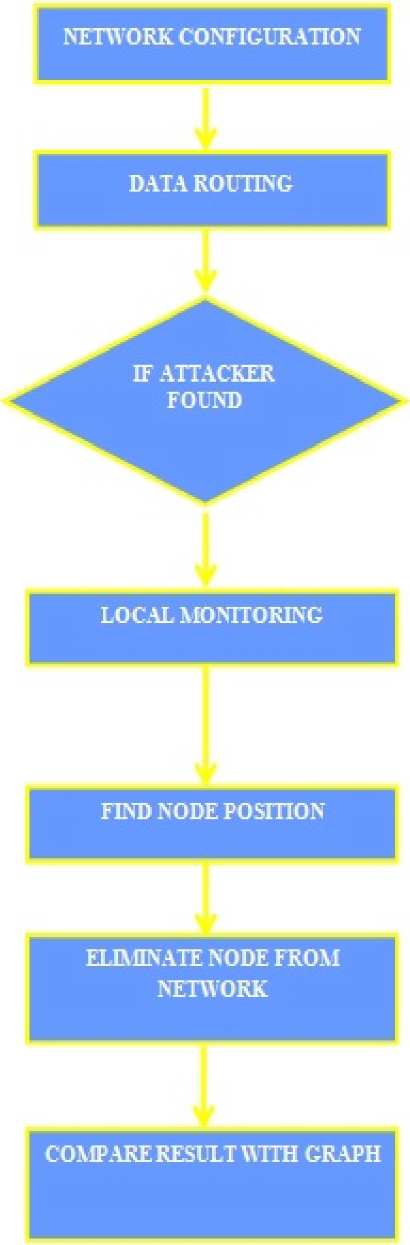


Figure-1. Process flow diagram.

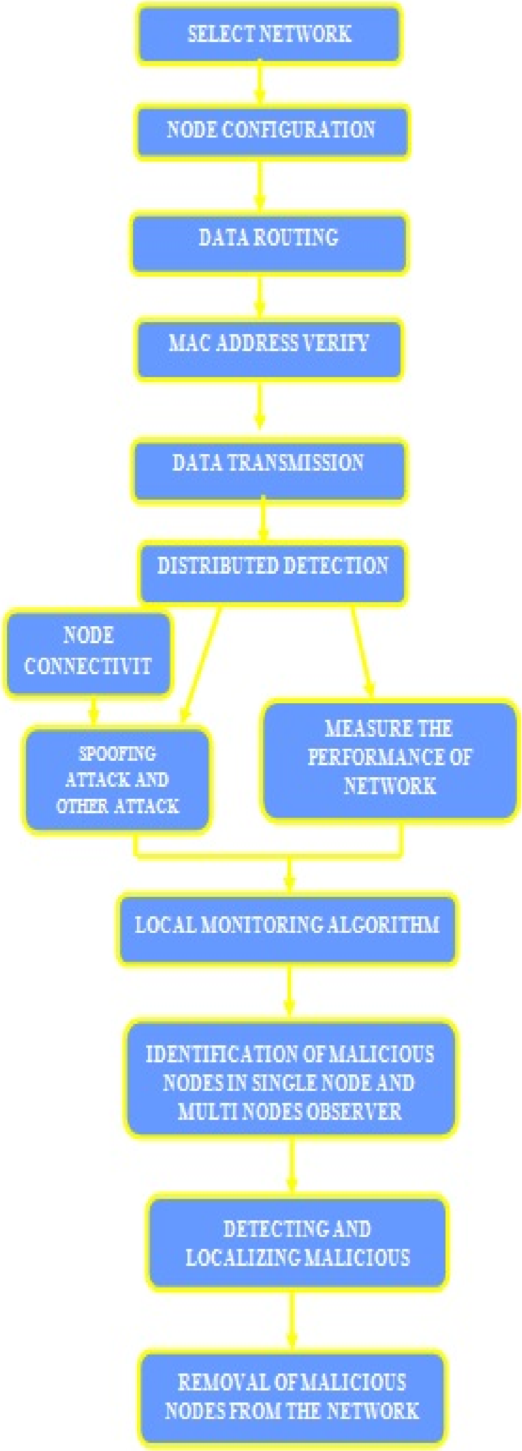
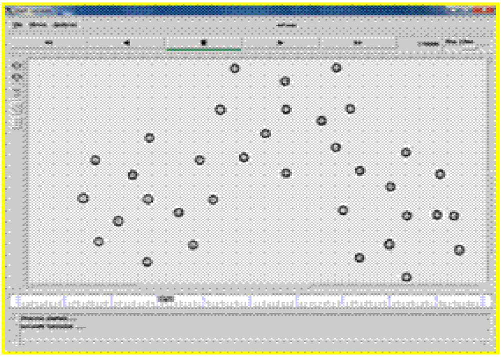

SELECT NETWORK
NODE CONFIGURATION
DATA ROUTING
MAC ADDRESS VERIFY
DATA TRANSMISSION
DISTRIBUTED DETECTION
NODE CONNECTIVIT
SPOOFING ATTACK AND OTHER ATTACK
MEASURE THE PERFORMANCE OF NETWORK
LOCAL MONITORING ALGORITHM
IDENTIFICATION OF MALICIOUS NODES IN SINGLE NODE AND MULTI NODES OBSERVER
DETECTING AND LOCALIZING MALICIOUS
REMOVAL OF MALICIOUS NODES FROM THE NETWORK

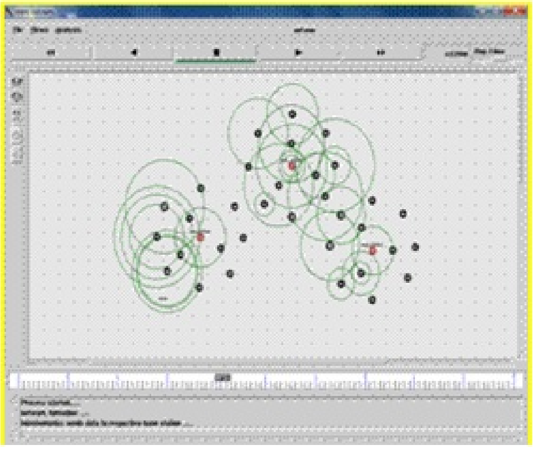
Figure-2. System flow diagram.

9. IMPLEMENTATION WORK

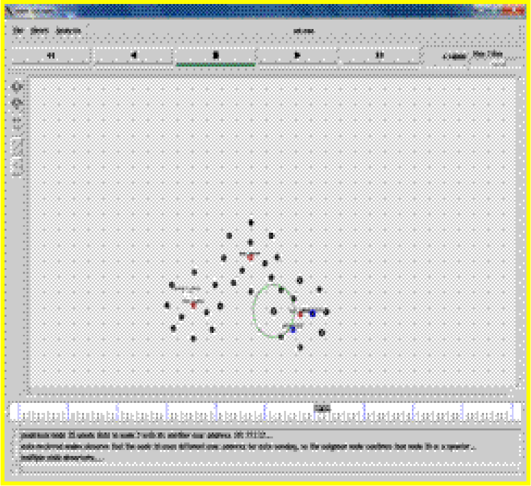
9.1 Network formation



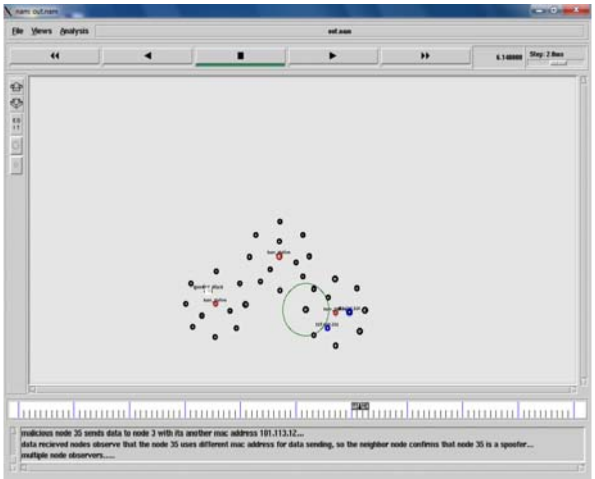
9.2 Data transmission



9.3 Identification of malicious node in multiple node observers

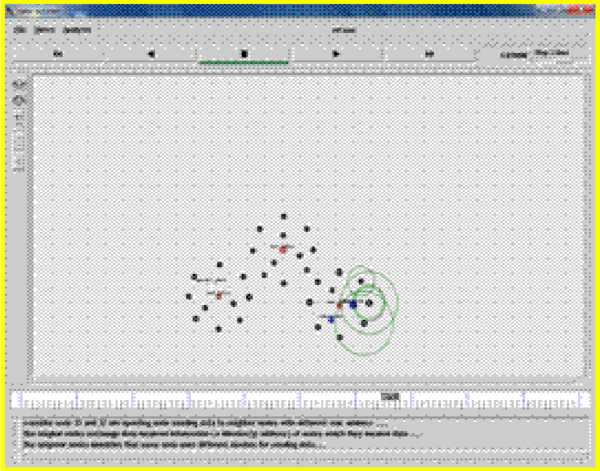


9.4 Identification of malicious node in multiple node observers



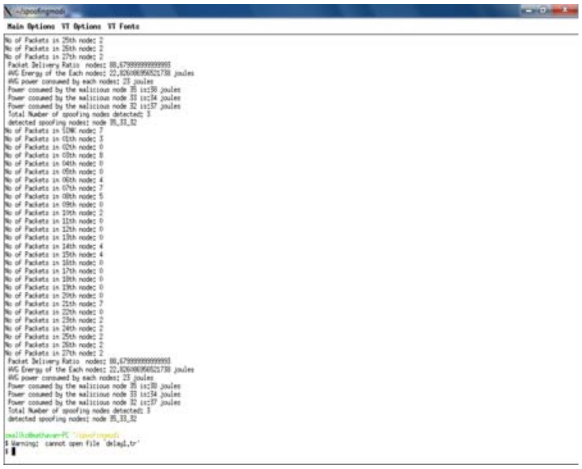
```
malicious node 35 sends data to node 3 with its another mac address 101.113.12...
data recieved nodes observe that the node 35 uses different mac address for data sending, so the neighbor node confirms that node 35 is a spoofer...
multiple node observers.....
```

9.5 Catch malicious node



```
malicious node 35 and 32 are spoofing and sending data to neighbor nodes with different mac address ....
the neighbor nodes exchange their received information [illegible] ....
the neighbor nodes identifies that same node uses different ids for sending data....
```

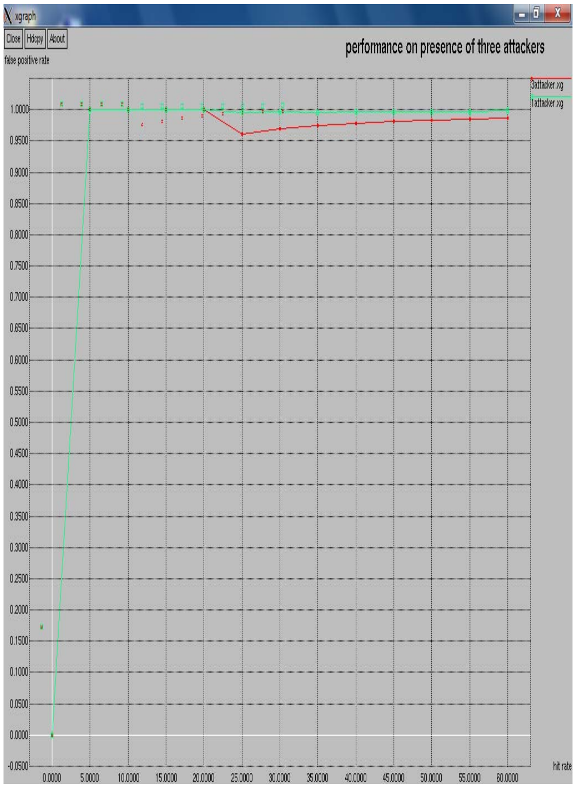
9.6 Detected faking nodes



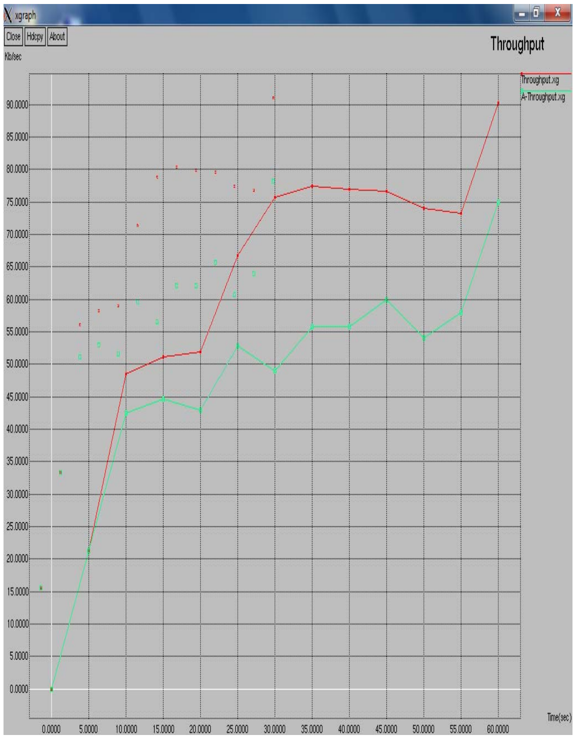
```
No of Packets in 25th node: 2
No of Packets in 26th node: 2
No of Packets in 27th node: 2
 Packet Delivery Ratio  nodes: 88.6799999999999
 AVG Energy of the Each nodes: 22.8260069560521738 joules
 AVG power consumed by each nodes: 23 joules
 Power cosumed by the malicious node 35 is:38 joules
 Power cosumed by the malicious node 33 is:34 joules
 Power cosumed by the malicious node 32 is:37 joules
 Total Number of spoofing nodes detected: 3
 detected spoofing nodes: node 35,33,32
No of Packets in SINK node: 7
No of Packets in 01th node: 3
No of Packets in 02th node: 0
No of Packets in 03th node: 8
No of Packets in 04th node: 0
No of Packets in 05th node: 0
No of Packets in 06th node: 4
No of Packets in 07th node: 7
No of Packets in 08th node: 5
No of Packets in 09th node: 0
No of Packets in 10th node: 2
No of Packets in 11th node: 0
No of Packets in 12th node: 0
No of Packets in 13th node: 0
No of Packets in 14th node: 4
No of Packets in 15th node: 4
No of Packets in 16th node: 0
No of Packets in 17th node: 0
No of Packets in 18th node: 0
No of Packets in 19th node: 0
No of Packets in 20th node: 0
No of Packets in 21th node: 7
No of Packets in 22th node: 0
No of Packets in 23th node: 2
No of Packets in 24th node: 2
No of Packets in 25th node: 2
No of Packets in 26th node: 2
No of Packets in 27th node: 2
 Packet Delivery Ratio  nodes: 88.6799999999999
 AVG Energy of the Each nodes: 22.8260069560521738 joules
 AVG power consumed by each nodes: 23 joules
 Power cosumed by the malicious node 35 is:38 joules
 Power cosumed by the malicious node 33 is:34 joules
 Power cosumed by the malicious node 32 is:37 joules
 Total Number of spoofing nodes detected: 3
 detected spoofing nodes: node 35,33,32

[illegible] ~/spoofingmodi
$ Warning:  cannot open file 'delay1.tr'
$ █
```

9.7 Graph examination



9.8 Throughputs



10. EXPERIMENTAL EVALUATION

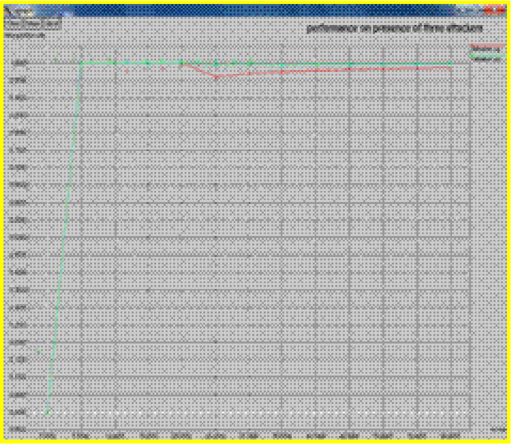


Figure-3. Performance on presence of three blasters.

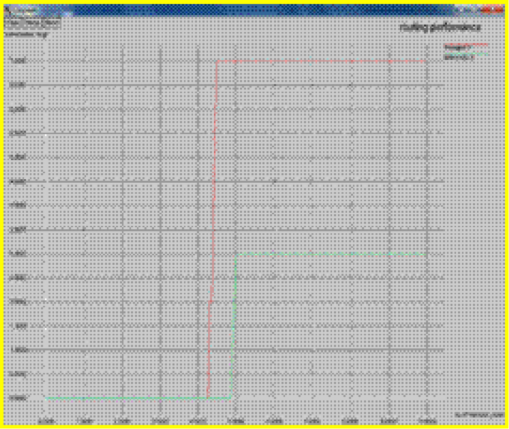


Figure-4. Routing performance.

11. CONCLUSIONS

In this work, distributed detection algorithm is used to efficiently measure the performance of networks and handle those blasts accurately and separately. In extension to distributed algorithm a three separate intrusion detection system is proposed to detect these types of blasts efficiently and high accuracy. Local monitoring algorithm is proposed to detect the various attacks like sybil, worm hole, black hole, Internet Protocol address and Medium Access Control address. After detecting these attacks and the attacker nodes are eliminated. The simulation result shows better performance of our proposed system. The techniques are evaluated through two test beds in two different networks. Our experimental results show that our proposed methods can achieve over ninety six percent hit Rate and Precision when determining the sybil, worm hole and black hole attacks, Internet Protocol address and Medium Access Control address faking approaches.

ACKNOWLEDGEMENTS

The research described in this paper is supported by the Inetz Techno Solutions Pvt Ltd by Wireless Sensor Network Program. The author thanks Dr. M. Umamaheswari for her support and encouragement.

REFERENCES

[1] Sarage and J. Bellardo. 2003. Real vulnerabilities and practical solutions.

[2] F. Ferreri, M. Bernaschi, L. Val Camanici. 2004. Access points vulnerabilities to dos attacks in 802.11 networks.

[3] J. Yang, Y.Chen, V. Trappe. 2000. Defecting spoofing attacks in mobile wireless environments.