International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

Optimizing a Wireless Sensor Network through Wormhole Detection

Mohit Malik1; Shabnam Sangwan[2] & Suryakiran[3]
[1] M. Tech Scholar, Sat kabir institute of Technology and Managment
[2]Assistant Professor, Sat kabir institute of Technology and Management
[3]Assistant Professor, Sat kabir institute of Technology and Management

ABSTRACT –

Collaborative work between sensors requires an intelligent organization to transmit information from the sensing field to the base station in order to save energy re-sources of the network. Because of the insignificant computational capability and the lack of energy sources, the Flooding algorithms are not a proper solution for routing of WSN application. The flooding algorithms broadcast the data to all overlapped nodes to the extent that cause an implosion and some nodes redundantly receive multiple copies of the same message. Wireless sensor networks are widely used. Here in the proposed work we will detect the wormhole routing and try to optimize the entire system. We will start with taking 50 nodes at random. We will code and work to find out nodes with their neighbor. Different color nodes are represented and hence wormhole is also detected,

Keywords – Wireless sensor network; routing; wormhole; nodes

CHAPTER 1

INTRODUCTION

Wireless sensor networks

One of the main design aims of WSNs is to transfer data communication while trying to extend the lifetime of the network and avoid connectivity degradation by employing aggressive energy management techniques. Due to the limited range of communication, ensuring the direct connection between a sensor and the base station may make the nodes transmit their messages with such a high power that their resources could be quickly depleted. Thus, the collaboration of nodes ensures the communication between distant nodes and base station. In this method, intermediate nodes transmit messages so that a path with multiple links or hops to the base station is established. Collaborative work between sensors requires an intelligent organization to transmit information from the sensing field to the base station in order to save energy re-sources of the network. Because of the insignificant computational capability and the lack of energy sources, the Flooding algorithms are not a proper solution for routing of WSN application. The flooding algorithms broadcast the data to all overlapped nodes to the extent that cause an implosion and some nodes redundantly receive multiple copies of the same message. Gossiping algorithm comes with a better performance, avoiding implosion as the sensor and sending the message to a selected neighbor instead of informing all of its neighbors. However, it is still not the proper solution[1]

An ad-hoc network is a dynamic network formed on demand by a group of nodes without any pre-existing network infrastructure. Wireless ad-hoc network may be classified in two types, Mobile Ad-hoc Network (MANET) and Stationary Ad-hoc Network (SANET). Self- configurability and easy deployment feature of the Mo- bile Ad-hoc network (MANET) resulted in numerous applications in modern era. Community network, military and emergency rescue are some application of ad- hoc network where infrastructure is unavailable or difficult to install. Directional antenna offers the great benefits for wireless ad-hoc networks, with directional trans- mission and reception. With increasing application of ad-hoc wireless network, the need for supporting quality of service (QoS) is becoming essential. However, Distributed Coordination Function (DCF) [1] MAC (Medium Access Control) of IEEE 802.11, which is the most widely used MAC protocol in MANETs, does not support the QoS in MANETs due to its inherent problems [4]

Types of WSN

In general, the network structure or architecture in WSNs can be divided into homogenous and heterogenous WSN.

- Homogenous WSN Architecture

In homogeneous WSN architecture, the SNs have identical capabilities and functionality with respect to the various aspects of sensing, communication and resource constraints.

- Heterogenous WSN Architecture

In heterogeneous WSN architecture, each node may have different capabilities and execute different functions in terms of energy heterogeneity, link heterogeneity and computational heterogeneity [5].

1.1 Application of WSN

- Area monitoring: Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines.
- Health care monitoring: The medical applications can be of two types: wearable and implanted. Wearable devices are used on the body surface of a human or just at close proximity of the user. The implantable medical devices are those that are inserted inside human body. There are many other applications too e.g. body position measurement and location of the person, overall monitoring of ill patients in hospitals and at homes. Body-area networks can collect information about an individual's health, fitness, and energy expenditure.
- Environmental/Earth sensing: There are many applications in monitoring environmental parameters, examples of which are given below. They share the extra challenges of harsh environments and reduced power supply.
- Air pollution monitoring: Wireless sensor networks have been deployed in several cities (Stockholm, London and Brisbane) to monitor the concentration of dangerous gases for citizens. These can take advantage of the ad hoc wireless links rather than wired installations, which also make them more mobile for testing readings in different areas.
- Forest fire detection: A network of Sensor Nodes can be installed in a forest to detect when a fire has started. The nodes can be equipped with sensors to measure temperature, humidity and gases which are produced by fire in the trees or vegetation. The early detection is crucial for a successful action of the firefighters; thanks to Wireless Sensor Networks, the fire brigade will be able to know when a fire is started and how it is spreading.
- Landslide detection: A landslide detection system makes use of a wireless sensor network to detect the slight movements of soil and changes in various parameters that may occur before or during a landslide. Through the data gathered it may be possible to know the occurrence of landslides long before it actually happens.
- Water quality monitoring: Water quality monitoring involves analyzing water properties in dams, rivers, lakes & oceans, as well as underground water reserves. The use of many wireless distributed sensors enables the creation of a more accurate map of the water status, and allows the permanent deployment of monitoring stations in locations of difficult access, without the need of manual data retrieval.

- Natural disaster prevention: Wireless sensor networks can effectively act to prevent the consequences of natural disasters, like floods. Wireless nodes have successfully been deployed in rivers where changes of the water levels have to be monitored in real time.
- Chemical agent detection: The U.S. Department of Homeland Security has sponsored the integration of chemical agent sensor systems into city infrastructures as part of its counterterrorism efforts. In addition, DHS is supporting the development of crowdsourced sensing systems that will draw upon chemical agent detectors embedded in mobile phones.
- Machine health monitoring: Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionality.Wireless sensors can be placed in locations difficult or impossible to reach with a wired system, such as rotating machinery and untethered vehicles.
- Data logging: Wireless sensor networks are also used for the collection of data for monitoring of environmental information, this can be as simple as the monitoring of the temperature in a fridge to the level of water in overflow tanks in nuclear power plants. The statistical information can then be used to show how systems have been working. The advantage of WSNs over conventional loggers is the "live" data feed that is possible.
- Water/Waste water monitoring: Monitoring the quality and level of water includes many activities such as checking the quality of underground or surface water and ensuring a country’s water infrastructure for the benefit of both human and animal.It may be used to protect the wastage of water.
- Structural Health Monitoring: Wireless sensor networks can be used to monitor the condition of civil infrastructure and related geo-physical processes close to real time, and over long periods through data logging, using appropriately interfaced sensors.

Music Technology: Wireless sensor networks are also used in music technology, for example to sense live performers, and transmit the sensor data to a central computer which then plays back sound or visuals in sync with the music. One example of such an application are the audio cubes, smart objects which form a star network and which can sense each other's location, orientation and relative distance, as well as distance to the user of the network (i.e. the performer) [6].

CHAPTER - 2

LITERATURE REVIEW

Guikai Liu et. Al., in Subarea Tree Routing (STR) in Multi-hop Wireless Ad hoc Networks proposed a Multi-hop wireless ad hoc network, also called multi-hop wireless self-organizing network, does not rely on a fixed infrastructure and the network structure changes dynamically due to member mobility. Wireless ad hoc networks are very attractive for tactical communication in military and also expected to play an important role in many fields without the presence or use of a fixed infrastructure such as disaster search-and-rescue operations, data acquisition in remote areas, conference and convention centers etc. Each node in this network not only as a host but also as a router discovers and maintains routes to other nodes that may not be within direct wireless transmission range. To provide communications throughout the network, a sequence of neighbor nodes from a source to a destination form a multi-hop path and intermediate hosts relay

packets in a store-and-forward mode. The major challenges for multi-hop routing in wireless ad hoc networks are continuously changing network topology, low transmission power, and low available band Multi-hop wireless ad hoc network, also called multi-hop wireless self-organizing network, does not rely on a fixed infrastructure and the network structure changes dynamically due to member mobility. Wireless ad hoc networks are very attractive for tactical communication in military and also expected to play an important role in many fields without the presence or use of a fixed infrastructure such as disaster search-and-rescue operations, data acquisition in remote areas, conference and convention centers etc. Each node in this network not only as a host but also as a router discovers and maintains routes to other nodes that may not be within direct wireless transmission range. To provide communications throughout the network, a sequence of neighbor nodes from a source to a destination form a multi-hop path and intermediate hosts relay packets in a store-and-forward mode. The major challenges for multi-hop routing in wireless ad hoc networks are continuously changing network topology, low transmission power, and low available bandwidth. In order to support multi-hop routing, much work has been done in this area and many protocols have been proposed. There are different standards to categorize these routing protocols: proactive routing versus on demand routing, or flat routing versus hierarchical routing

Minghui Li et. Al., in Accurate Angle-of-Arrival Measurement Using Particle Swarm Optimization proposed A chief goal of wireless communication research has long been to enhance the network capacity, data rate and communication performance. In comparison with solutions of increasing spectrum usage, smart antenna technology provides a more practical and cost-efficient solution. The benefits of using smart antennas are that the sender can focus the transmission energy towards the desired user while minimizing the effect of interference, and the receiver can form a directed beam towards the sender while simultaneously placing nulls in the directions of the other transmitters. This spatial filtering capability leads to increased user capacity, reduced power consumption, lower bit error rates (BER), and larger range coverage. A key component that aids the array to be ‘smart’ and adaptive to the environment is AOA estimation of the desired signals and co-channel interferers. To fully exploit the AOA capability in mobile communications, various Medium Access Control (MAC) protocols have been developed. In recent years, AOA estimation has received considerable attention from radar and communication communities, and several high resolution algorithms have been proposed based on the white Gaussian noise model, such as multiple signal classification (MUSIC), maxi-mum likelihood (ML) , and others. However, in many circumstances, the emitters reside in a “radio hostile” environment and the noise fields tend to be correlated along the array due to the dominant ambient noise. Furthermore, the systems are often forced to work under unfavorable conditions involving low signal-to- noise ratio (SNR), highly correlated signals, and small array with few elements due to the cost, energy and size constraints. The standard AOA techniques become in-competent in such scenarios. In this paper, proposed an algorithm for accurate AOA measurement in colored noise fields and harsh application scenarios. By modeling the unknown noise co-variance as a linear combination of known weighting matrices, a maximum likelihood criterion is derived with respect to AOA and unknown noise parameters. ML criteria may yield superior statistical performance, but the cost function is multimodal, nonlinear and high-dimensional. To tackle it efficiently, we propose to use the particle swarm optimization (PSO) paradigm as a robust and fast global search tool. PSO is a recent addition to evolutionary algorithms. Most of the applications demonstrated that PSO could give competitive or even better results in a much faster and cheaper way, compared to other heuristic methods such as genetic algorithms (GA).

Ka Lun Lam et. Al., in A Study of Address Shortage in a Tree Based ZigBee Network for Mobile Health Applications proposed The ZigBee protocol was originally defined for non-mo- bile applications and has gained increasingly importance recently. Pilot works on ZigBee did not discuss the de-sign of large scale system which demands mobility. There are increasingly more applications which demand mobility within a large ZigBee fixed network, say for patient monitoring application in hospitals and aged- person caring centers. Up to present, there has been no study on enabling mobility in a fixed ZigBee network. It will soon be explained that such mobility enabling is different from the traditional ZigBee ad hoc networks in terms of topology and addressing requirement. Aging tends to be a serious worldwide problem in coming 20 years. Health care for aged persons will be a very alarming issue. It is insightful to understand the pragmatic application of ZigBee by studying the de mands of future health care for inpatients and outpatients within hospitals. Let us envisage the required environ-ment in hospitals in the future as follows. In the hospital, mobile sensors e.g. blood pressure monitor, pulse oximeter and blood glucose meter will be carried by patients. The health status from these sensors will be regularly collected and sent to the centralized patient monitoring server. Under such a circumstance, the server and routers typically needs to communicate with a pool of mobile devices to ensure a robust communication between mo-bile sensors and the centralized server. The application scenario just described is referred as mobile health. There is no doubt that mobile health for patient monitoring will be deployed in the future to help relieving the burden of hospitals and thus rendering the application important.

CHAPTER – 3

OBJECTIVES AND METHODOLOGY USED IN THE PAPER

1. TO DESIGN A WIRELESS ENVIOURMENT SUITABLE FOR OPTIMIZATION
2. TO STUDY AND BUILD A WIRELESS STRUCTURE OF 50 NODES.
3. TO REPRESENT DIFFERENT KINDS OF NODES WITH CHANGING COLOR.
4. TO DETETCT WORMHOLE NODES AMONG THE ENTIRE CLUSTURE.

Assumptions

The following assumptions are taken in order to design the proposed algorithm:

1. A node interacts with its 1-hop neighbors or 2-hop neighbors.
2. Every node has a unique id in the network, which is assigned to a new node by existing nodes.
3. The wormhole is closed i.e both the two wormhole nodes participate in the attack process.
4. The wormhole is Byzantine attack.
5. Each node does not need to know other nodes' specific locations.

Detection of Malicious Behavior

In AODV routing protocol a malicious nodes can easily disrupt the communication. A malicious node that is not part of any route may launch Denial of Service (DoS) Attack.

Also once a route is formed, any node in the route may turn malicious and may cease forwarding packets, alter them before forwarding or may even forward to an incorrect intermediate node. Such malicious performance by a misbehaving node cannot be detected for in pure AODV protocol [33].

During the judgment process the neighbors send their conclusion about a node. When the node collects all conclusions of neighbors, it decides about honesty behaviour of reply's sender node. The decision is based on the following cases which are used to judge about honesty of a node.

Steps to judge an honesty node

CASE 1: If a node delivers many data packets to destinations, it is supposed as an honest node.

CASE 2: If a node receives many packets but do not sent same data packets, it is probable that the current node is a misbehavior node.

CASE 3: When the case 2 is correct about a node, if the current node has sent any Route REPLY packets; therefore surely the current node is misbehavior node.

CASE 4: When the case 2 is correct about a node, if the current node has not sent any Route REPLY packets; therefore the current node is a failed node.

In this dissertation, a proactive scheme is proposed to detect the above-mentioned malicious activities. A malicious node flooding the network with fake control packets, such as RREQs (Route Requests) causes congestion in the network. The processing of RREQ by the nodes in the network leads to further degradation in performance of the network. This abnormal behavior is handled in our scheme by checking the local neighborhood information to decide whether the network topology is true or faked. In our model, every node has a current list of its s-neighbor i.e same neighbor. If two neighbor nodes have at least one same neighbor; we say the two neighbor nodes have the same neighbor. And the same neighbor is called *s-neighbor*. Finally, each node can know one-hop neighbor information and two-hop neighbors as well. After a node starts the wormhole detection process, the node first broadcasts message including a packet to notify its neighbors, which will increase the transmission range. After sending the message the transmission range of node A is increased to 2r. If the neighbors of node B are still neighbors of node A then no wormhole attack. If any one of the neighbor of node B is not a neighbor of A, a wormhole will be detected. By comparing its current neighbor list with previous list, a test node can find the existence of false topology that does not exist in a normal network. Then the wormhole is detected.

Algorithm to Isolate Malicious Node

```
Given: Network N with node radius r, wormhole number c=0
While check every node m in N do
Expand radius of m to R = 2r
For each node n in N (m) do
If there exists once d ϵ N (n) and d Ɇ N (m)
Then c+1
End for
End while
```

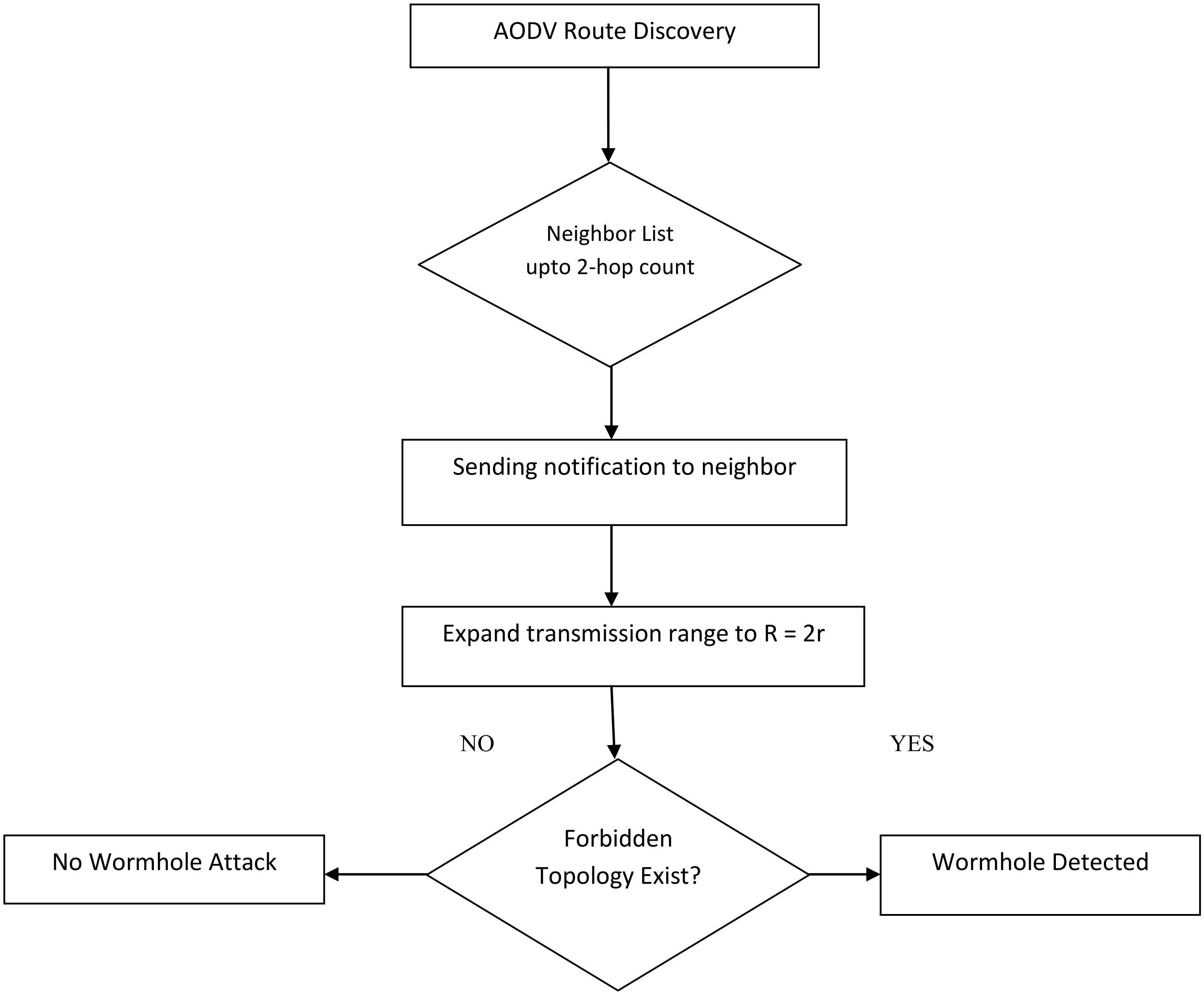
Explanation of Algorithm

Step 1: Source node sends the RREQ to the next neighbor node. If the route is found sends a RREP to the source node.

Step 2: If the route is established then source node sends data packet to the next node.

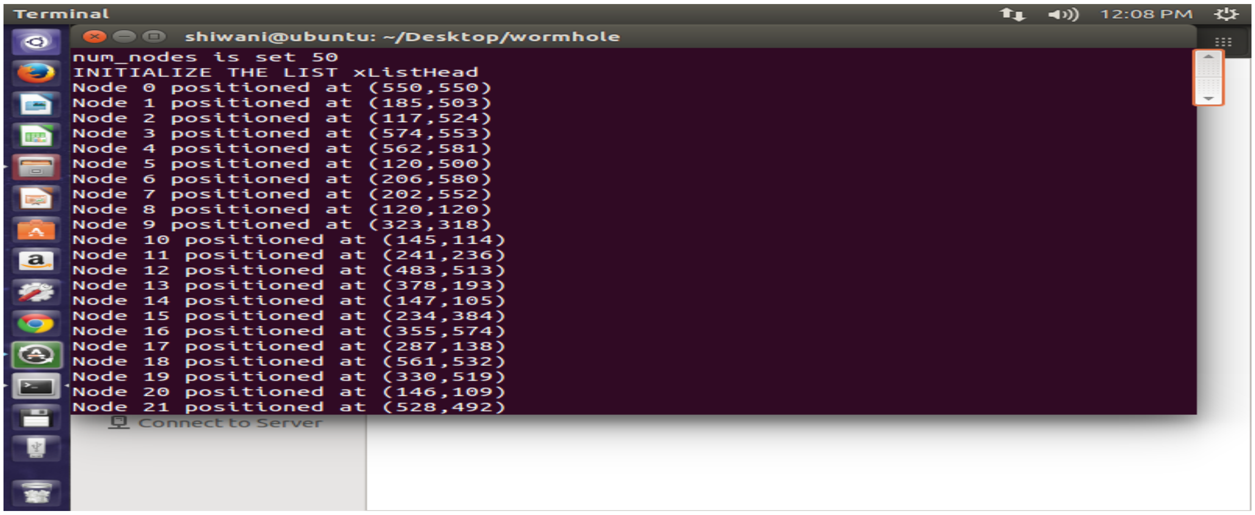
Step 3: If the intermediate node is a malicious node it will drop the packets which it receives from the neighbor node.

Step 4: The malicious node may send the fake RREQ to other nodes. So stop fake route request by ignoring the RREQ from the malicious node.


AODV Route Discovery
Neighbor List
upto 2-hop count
Sending notification to neighbor
Expand transmission range to R = 2r
NO
YES
Forbidden
Topology Exist?
No Wormhole Attack
Wormhole Detected

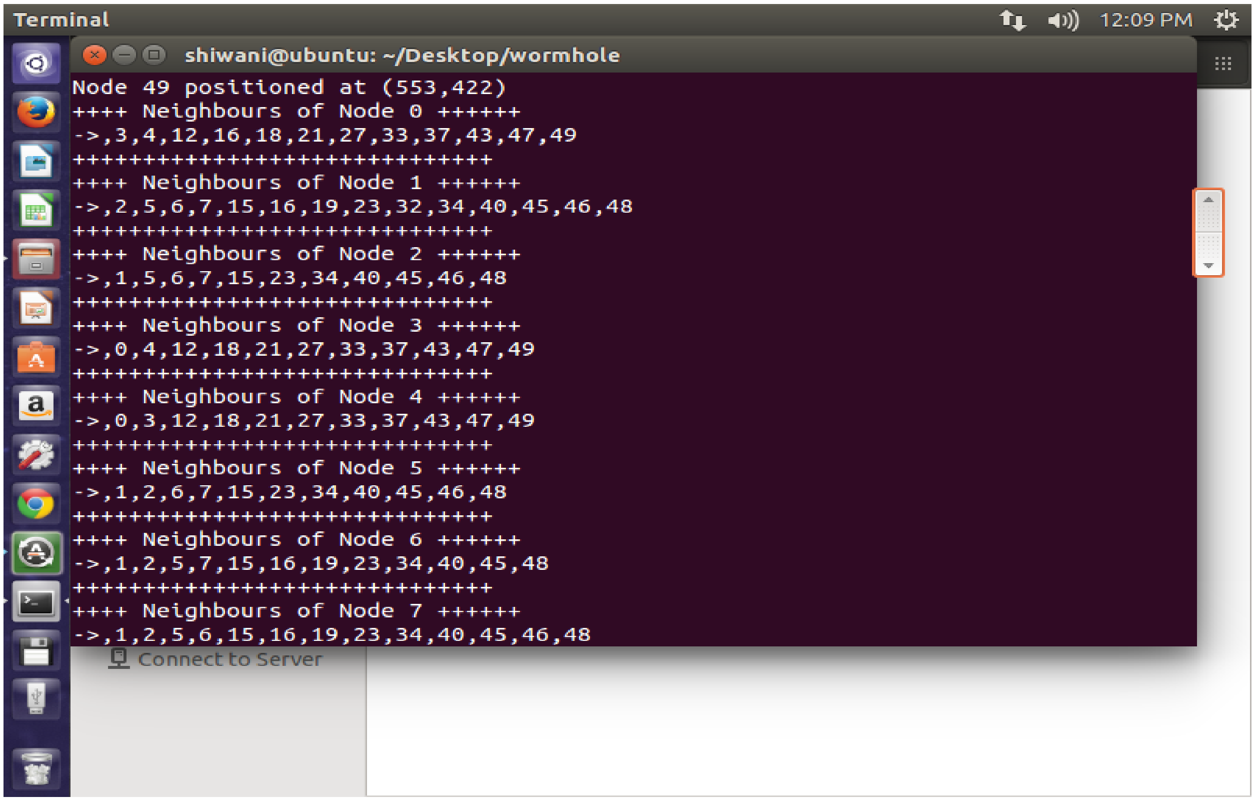
CHAPTER – 4

RESULT AND CONCLUSION



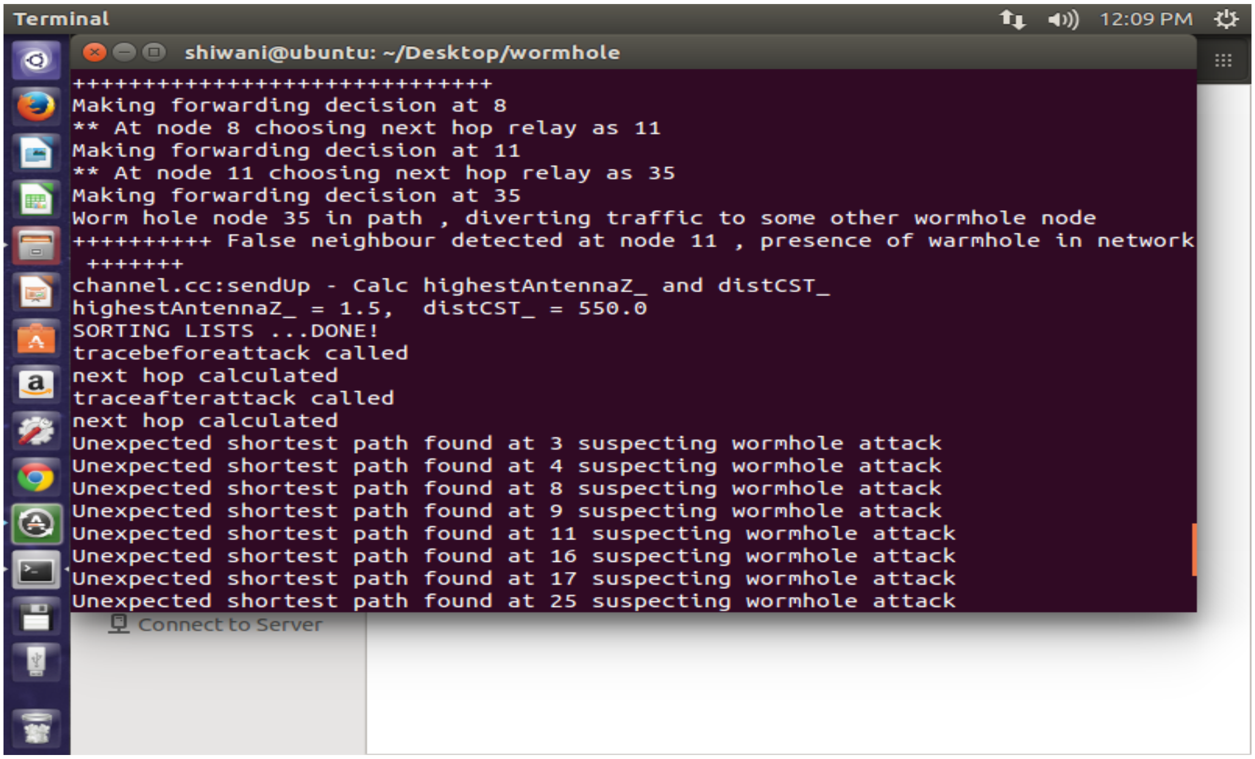
```
shiwani@ubuntu: ~/Desktop/wormhole
num_nodes is set 50
INITIALIZE THE LIST xListHead
Node 0 positioned at (550,550)
Node 1 positioned at (185,503)
Node 2 positioned at (117,524)
Node 3 positioned at (574,553)
Node 4 positioned at (562,581)
Node 5 positioned at (120,500)
Node 6 positioned at (206,580)
Node 7 positioned at (202,552)
Node 8 positioned at (120,120)
Node 9 positioned at (323,318)
Node 10 positioned at (145,114)
Node 11 positioned at (241,236)
Node 12 positioned at (483,513)
Node 13 positioned at (378,193)
Node 14 positioned at (147,105)
Node 15 positioned at (234,384)
Node 16 positioned at (355,574)
Node 17 positioned at (287,138)
Node 18 positioned at (561,532)
Node 19 positioned at (330,519)
Node 20 positioned at (146,109)
Node 21 positioned at (528,492)
```

Snapshot 1- Describes the intial position of nodes. We have taken 50 nodes(0-49). And they are placed randomly initially.



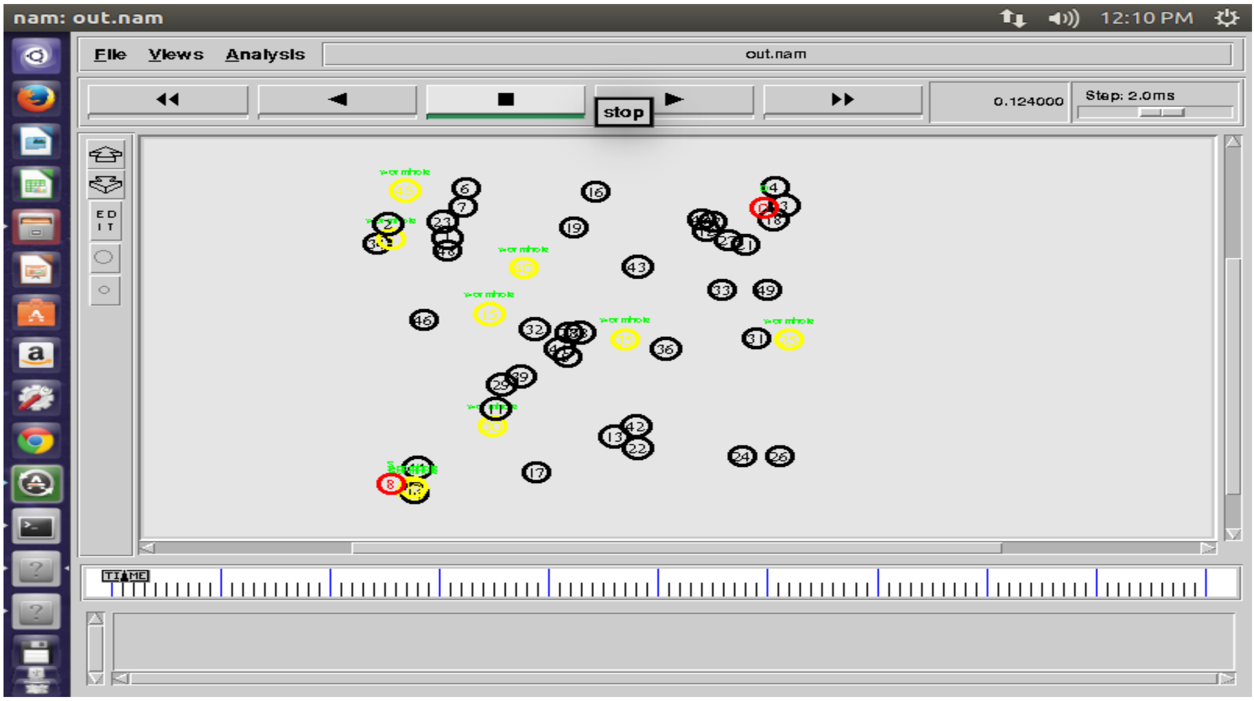
```
shiwani@ubuntu: ~/Desktop/wormhole
Node 49 positioned at (553,422)
++++ Neighbours of Node 0 ++++++
->,3,4,12,16,18,21,27,33,37,43,47,49
++++++++++++++++++++++++++++++
++++ Neighbours of Node 1 ++++++
->,2,5,6,7,15,16,19,23,32,34,40,45,46,48
++++++++++++++++++++++++++++++
++++ Neighbours of Node 2 ++++++
->,1,5,6,7,15,23,34,40,45,46,48
++++++++++++++++++++++++++++++
++++ Neighbours of Node 3 ++++++
->,0,4,12,18,21,27,33,37,43,47,49
++++++++++++++++++++++++++++++
++++ Neighbours of Node 4 ++++++
->,0,3,12,18,21,27,33,37,43,47,49
++++++++++++++++++++++++++++++
++++ Neighbours of Node 5 ++++++
->,1,2,6,7,15,23,34,40,45,46,48
++++++++++++++++++++++++++++++
++++ Neighbours of Node 6 ++++++
->,1,2,5,7,15,16,19,23,34,40,45,48
++++++++++++++++++++++++++++++
++++ Neighbours of Node 7 ++++++
->,1,2,5,6,15,16,19,23,34,40,45,46,48
```

Snapshot 2- Describes each node has calculated their 2-hop neighbor.

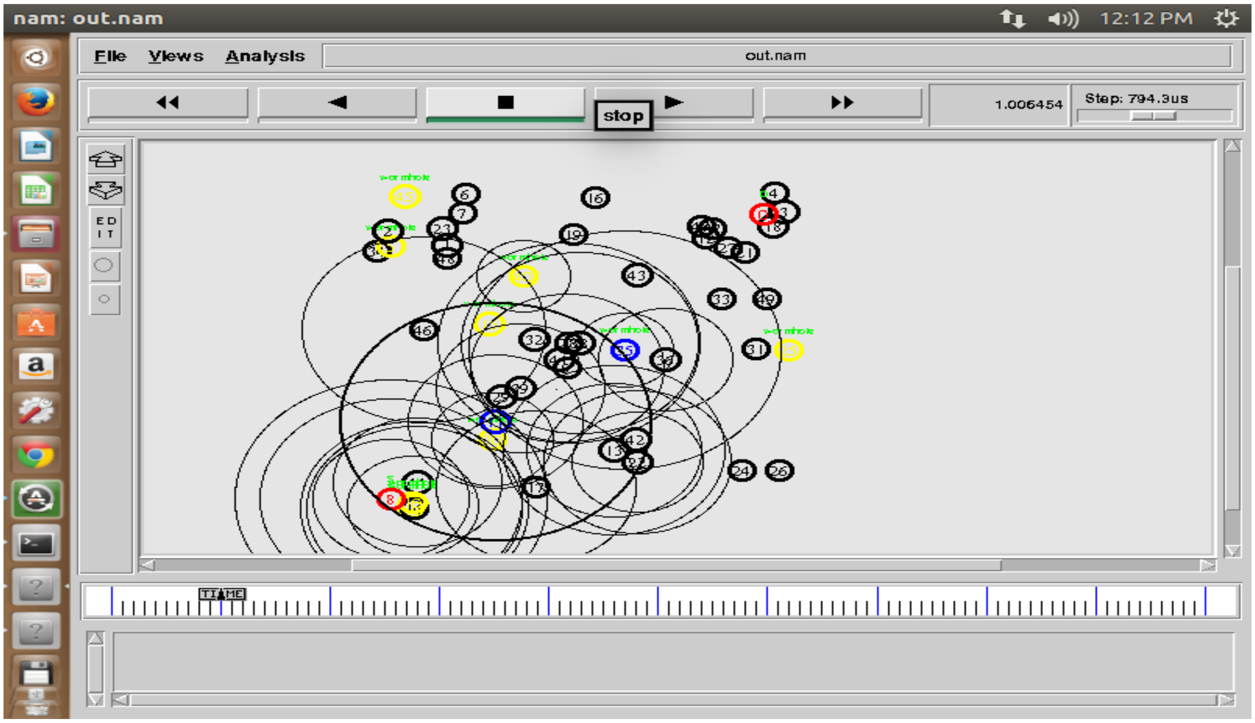


```
++++++++++++++++++++++++++++++
Making forwarding decision at 8
** At node 8 choosing next hop relay as 11
Making forwarding decision at 11
** At node 11 choosing next hop relay as 35
Making forwarding decision at 35
Worm hole node 35 in path , diverting traffic to some other wormhole node
++++++++++ False neighbour detected at node 11 , presence of warmhole in network
 +++++++
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
tracebeforeattack called
next hop calculated
traceafterattack called
next hop calculated
Unexpected shortest path found at 3 suspecting wormhole attack
Unexpected shortest path found at 4 suspecting wormhole attack
Unexpected shortest path found at 8 suspecting wormhole attack
Unexpected shortest path found at 9 suspecting wormhole attack
Unexpected shortest path found at 11 suspecting wormhole attack
Unexpected shortest path found at 16 suspecting wormhole attack
Unexpected shortest path found at 17 suspecting wormhole attack
Unexpected shortest path found at 25 suspecting wormhole attack
```

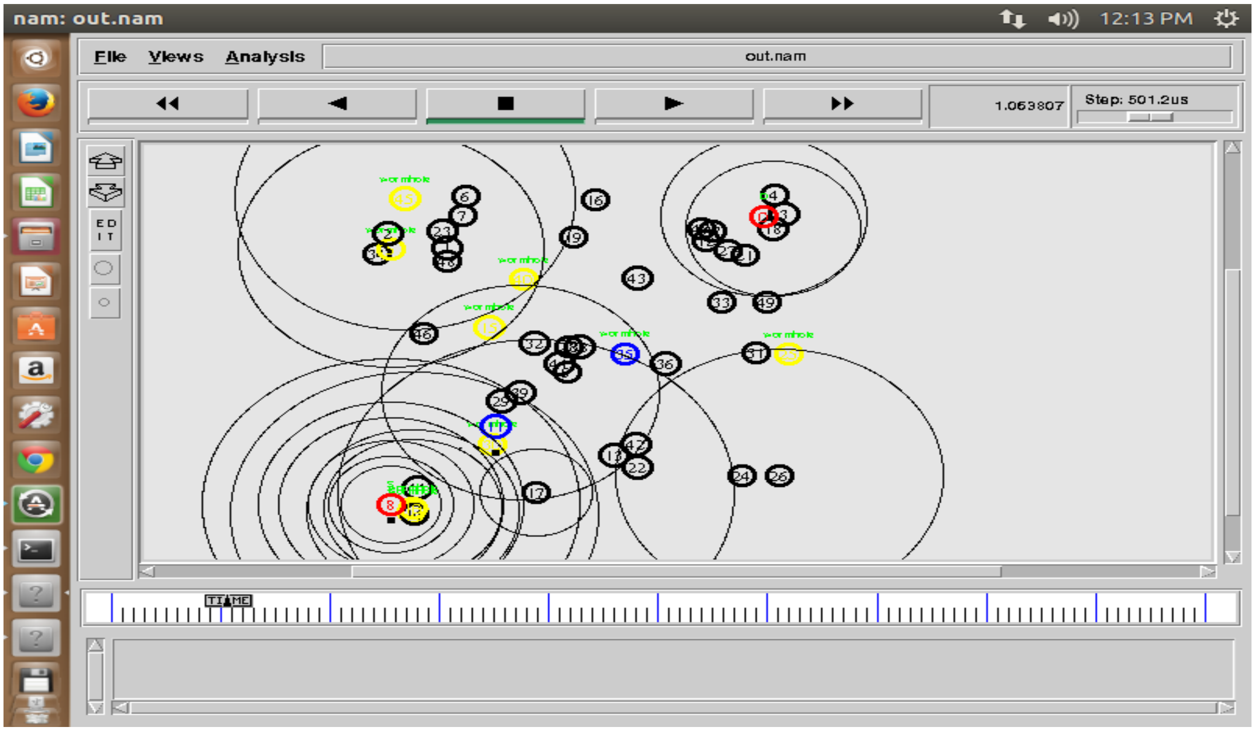
Snapshot 3- As the Source node and the destination node is declared intially i.e node 8 and node 0 respectively.



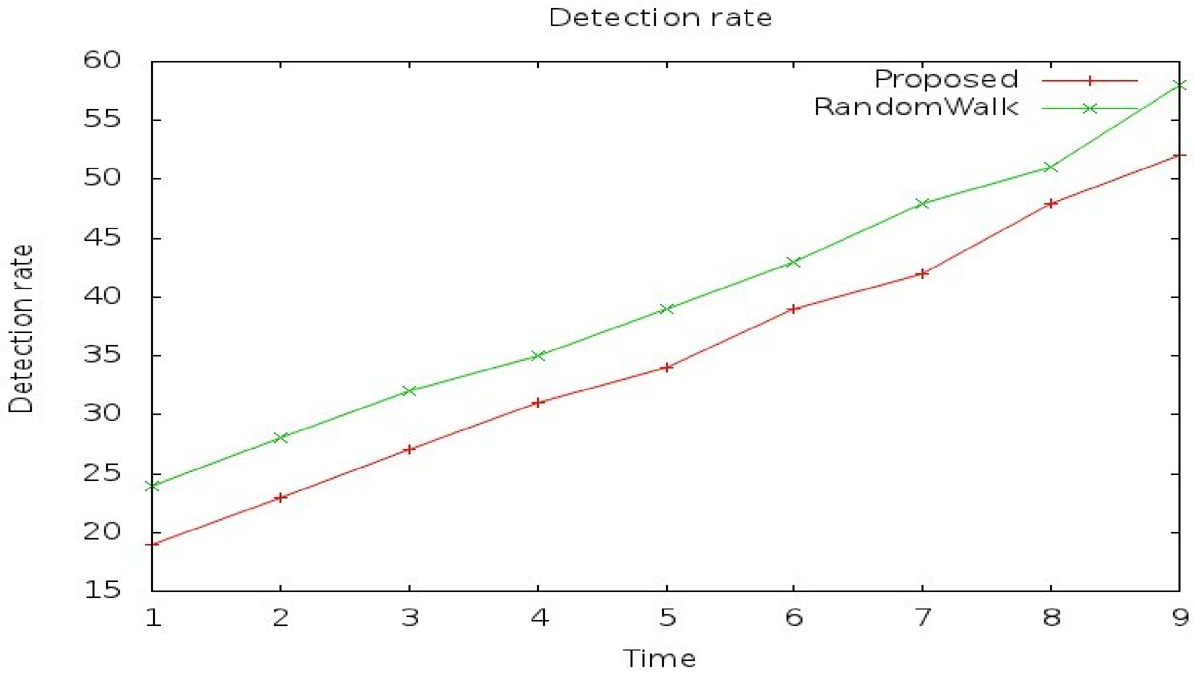
Snapshot 4- Red color node represent source and destination, Yellow color node represent Wormhole Node and Black color node represent normal node.



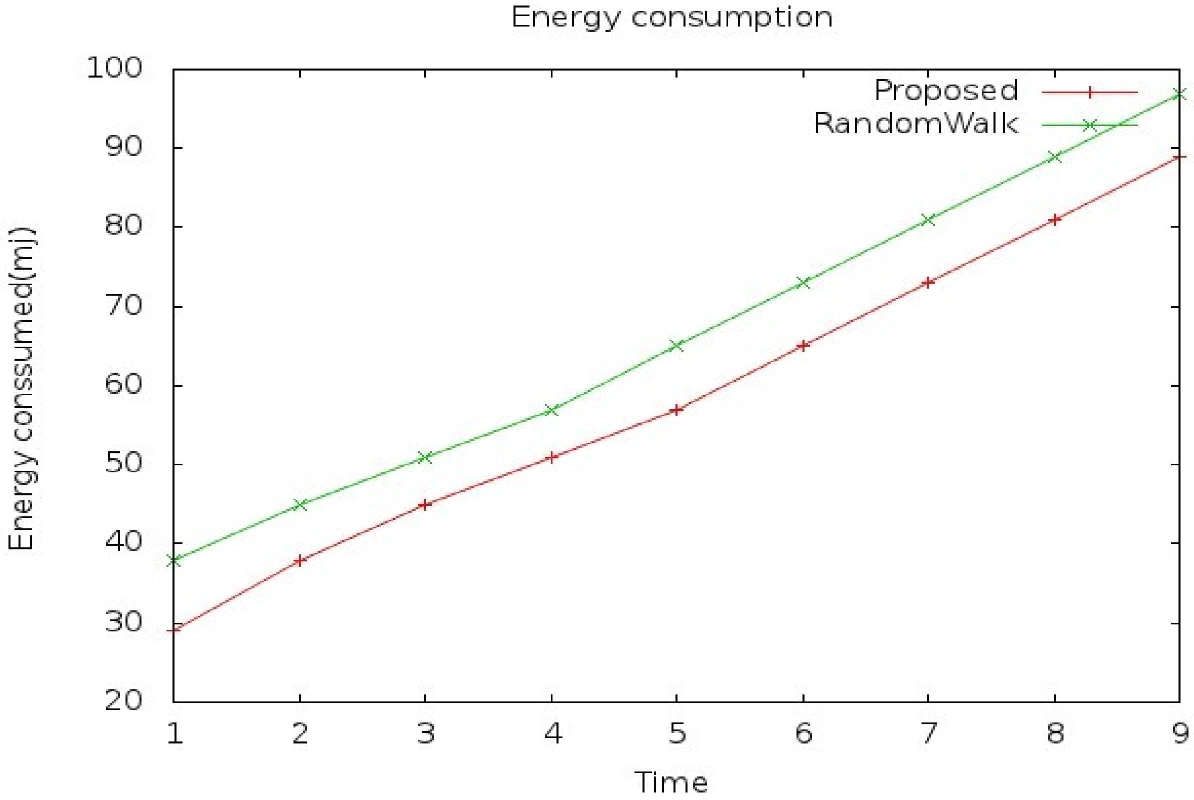
Snapshot 5- Blue color node represent the path through which data is passed using AODV protocol.



Snapshot 6- Packet loss occur due to the presence of wormhole node near the source and intermediate node ie. node 11.



Snapshot 7- Graph comparison of detection rate between proposed and random walk



Snapshot 8- Graph describing energy consumption

REFERENCES

[1.] D.-Y. Qin, L. Ma, X.-J. Sha and Y.-B. Xu, “An Effective Survivable Routing Strategy for MANET,” Tamkang Journal of Science and Engineering, Vol. 14, No. 1, 2011, pp. 71-80.

[2.] Hawbani et. Al.,“Wireless Sensor Network Routing Based on Sensors Grouping”, Wireless Sensor Network,2014, 6, 8-17

[3.] H. L. Nguyen and U. T. Nguyen, “Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Net- works,” Networking, International Conference on Sys- tems and International Conference on Mobile Communications and Learning Technologies, 23-29 April 2006, 149 p.

[4.] Kumar et. Al., “Simulation & Performance Evaluation of QoS Routing Protocol for Ad-hoc Networks Using Directional Communication”, Int. J. Communications, Network and System Sciences,2012, 5, 825-833

[5.] Meng et. Al.,“ Swarm Intelligence in Power System Planning” , International Journal of Clean Coal and Energy, 2013, 2, 1-7

[6.] R. H. Jhaveri, S. J. Patel, et al., “DoS Attacks in Mobile Ad Hoc Networks: A Survey,” 2nd International Con- ference on Advanced Computing & Communication Technologies, 2012.

[7.] .Yih-Chun Hu, Adrian Perrig, and David B. Johnson— “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks”, In Proceedings of the IEEE Conference on Computer Communications (Infocom), 2003, p. 1976-1986.

[8.] L. Hu and D. Evans. “Using directional antennas to prevent wormhole attacks,” Proceedings of Network and Distributed System Security Symposium, pp. 131−41, Feb. 2004.

[9.] Hon Sun Chiu and King-Shan Lui, “DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks”, International Symposium on Wireless Pervasive Computing (ISWPC), 2006.

[10.] T Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoung Lee, and Heejo Lee,“Transmission time-based mechanism to detect wormhole attack”,In Proceedings of the IEEE Asia-Pacific Service Computing Conference, Dec. 11-14, 2007, p. 172-178.

[11.] Mohammad Rafiqul Alam and King Sun Chan, “RTT-TC: A Topological Comparison Based Method to Detect Wormhole Attacks in MANET”, 12th IEEE International Conference on Communication Technology, 2010, p. 991-994.

[12.] S. Capkun, L. Buttyán, and J.P. Hubaux, “SECTOR: Secure trackingof node encounters in multi-hop wireless networks,” Proceedings of the 1st ACM workshop on Security of ad-hoc and sensor networks (SASN 03), pp.21−32, Oct. 2003.

[13.] S. Brands and D. Chaum,“Distance-bounding protocols,” In Theory and Application of Cryptographic Techniques, pp. 344−59, 1993.