Reliable and Secured Routing in Wireless Sensor Networks using Active Trust

Sneha K.
Dept. of Electronics and Communication
B.M.S College of Engineering, Karnataka

Akhila S.
Dept. of Electronics and Communication
B.M.S College of Engineering, Karnataka

ABSTRACT
A Wireless Sensor Network (WSN) comprises of devices that are autonomously distributed in space used to supervise the physical and environmental conditions with the help of sensors. They are mainly used in security critical applications such as monitoring the environment, tracking the surroundings and controlling areas. Security is an important requirement in WSNs. Because of the resource limitation and computational constraints the WSNs are transparent to various security attacks. Black hole attack is a serious attack which badly affects the packet transfer from source to destination. Here the Active Trust scheme is used to avoid the Black hole attack. The Active Trust scheme avoids the black holes through Active detection routing and data routing which improves the route security. The results obtained will indicate that the Active Trust scheme can achieve the same throughput as that of the normal Wireless Sensor Network without black holes. This shows the importance of Active Trust scheme in black hole attacks.

General Terms
Wireless Sensor Network, Black Hole Affect, Data Routing Protocol, Active Detection Routing Protocol.

Keywords
Active Trust, Black holes, Throughput.

1. INTRODUCTION
The Wireless Sensor Networks (WSNs) are very excessively used at present because of their all-inclusive applications. The nodes basically are very simple and low in cost. The sensor nodes suffer from different security attacks. A black hole attack (BLA) is one of the most serious attack. Black holes are the places in the wireless sensor network where the data packets are dropped silently in the middle of the transmission without even informing the source that the data did not reach the sink node or the recipient node [1]. When the architecture of the network is examined containing the black holes it reveals that the black holes are invisible by themselves. The black holes are identified only by keeping track of the lost traffic. The black hole attack frequently exploits wireless and adhoc networks. The black hole attack works as follows. The affected node drops all packets that are routed via that node, resulting in the data being discarded or unable to be forwarded to the sink. Our active trust scheme has better security performance. Here the nodes with higher trust is chosen to avoid potential attack using shortest routing protocol. When the nodes are attacked an immediately alternate route is taken to reach the sink. This improves the nodal trust and hence network security is improved. However the present trust based schemes face some challenging issues such as to obtain the route with high trust is very difficult. As the energy is very limited in WSNs .The trust acquisition consumes high energy which thereby leads to depletion of the network lifetime. Obtaining security is a challenge in the wireless sensor networks. Locating the malicious nodes is very difficult. So in this paper a secure and trustable routing called as the Active trust using active detection routing protocol and data routing protocol is proposed.

2. AD HOC ON DEMAND DISTANCE VECTOR ROUTING
Here AODV routing protocol is used to route the packets. AODV is classified as on demand routing system. Here the nodes which are not on the selected path, to route the packets to the sink do not maintain a routing table. These nodes do not contain routing information nor do they participate in routing table exchanges. When a source node intends to send a message or a data packet to the sink node and if the source node does not have a prior valid route to the destination it will initiate a path discovery process to find the sink node. The source node will broadcast a route request (RREQ) packet to its neighbouring nodes. The route request packet is forwarded along the communication path until it reaches the destination node or an intermediate node with a fresh enough routes to the destination node. AODV makes sure that it contains the most recent route information. It ensures that all routes are loop free. Each mode contained a separate sequence number as well as a broadcast id of its own. The broadcast id will increment for every route request packet. The RREQ contains the nodes own sequence number, the broadcast id and the most recent sequence number for the destination. The intermediate nodes can reply to the route request packet only if they have a route to the destination. The destination sequence number in the intermediate node should be greater than or equal to the sequence number contained in the RREQ, only then the intermediate node can route the packet to the destination node.

3. ACTIVE TRUST SCHEME
3.1 Active Detection Routing Protocol
Through the active detection routing protocol the trust of the node can be easily obtained and it can increase the efficiency of the data route in choosing the nodes that are having high trust which can avoid black holes [1]. It refers to a route without any data packets, by sending a dummy data to the sink just to satisfy the attacker nodes to launch an attack so that the system can identify the attacker behavior and it can mark the black hole location. See Figure 1 which demonstrates the active detection routing protocol. By using this protocol decrease the trust of the malicious nodes is decreased and a different route is found to pass the packets to the sink node. It will guide the data route to choose the nodes that are having high trust to avoid the malicious nodes. In this scheme, the source node will select a neighbor node to create an active detection route [2]. The detection routing packet consists of six parts namely: packet head, packet type, ID of the source node, maximum detection route length, acknowledgment that is returned back to the source for every

hop and the ID of the packet. After sending the route request packets to the neighbours from the source to sink, the route request is acknowledged and a feedback packet is send back to the source from the sink. The route reply is send from the sink to the source. This leads to active detection of the route resulting in the shortest path from the source to the sink[5].

3.2 Data Routing Protocol

It is the process of packet data routing to the destination node. Here the route will select a node which is having high trust as the next hop to avoid black holes which thereby improves the success ratio of reaching the sink [1]. The figure 2 represents the data routing protocol. The core idea of data routing is when any node receives a data packet it will select any one node from its neighbors which is having higher trust than the present threshold as the next hop and which is nearer the sink. The encrypted data is send across the route which gets decrypted only at the sink. After the active detection routing protocol and the attacker trying to attack the dummy data the encrypted message is sent from the source to the sink using data routing protocol. This avoids the black holes leading to nodal trust improvement and data security.

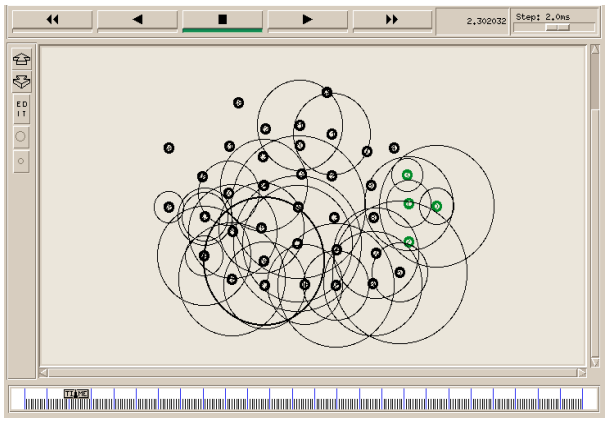

Fig 1: Active Detection Routing protocol

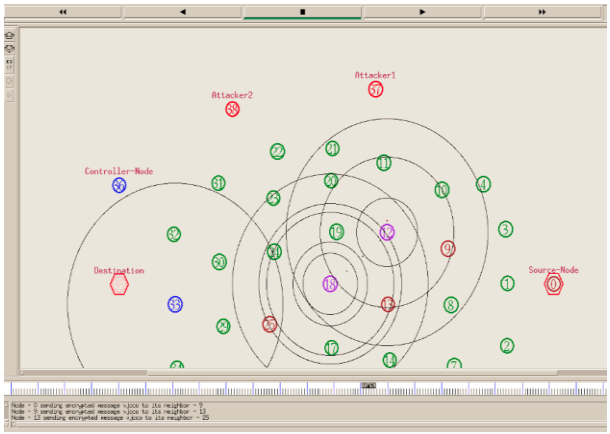

Fig 2: Data Routing protocol

3.3 System Model

The behavior of a system is a function of its parameters. The various parameters of the system design are time of design, resource availability, energy, time, packet size that is used during the communication [4]. The system model is used to develop wireless topology, network topology which consists of various mobile nodes and each node will work with multiple channels. The system model consists of various steps involved for communication such as setting up a network topology for communication to be initialized, various environmental settings, node configurations and creation of the topology network. Every node in the network will be given a preferred bandwidth. Euclidian distance concept is used to identify the neighbours for a particular node [3]. Every node is assigned with a threshold value of the trust. If the trust is below the threshold value the node is said to be a malicious node and if the trust is above the threshold value that node is taken for data routing. The pat for communication is specified. The system model specifies the source node, destination node and the data packets to be transferred along the intermediate nodes. The routing protocol used here is mainly developed for adhoc networks. The routing table information is exchanged between the nodes for communication.

3.4 Network Simulator 2.35

Network simulator is an object oriented simulator. It basically uses OTcl script to perform simulation which contains simulation event scheduler and the network object libraries. The network simulator is programmed using OTcl script [7]. The OTcl script should be written to initiate an event scheduler, to set up the network topology using the network objects. The plumbing functions should be used which tells traffic sources when to start and stop transmitting packets through the event scheduler. Whenever a user wants to makes a new network object, it can be made easily by making an object either by writing a new object or by making a compound object from the object library, and to plumb the data through the object. The common arguments used in network simulator are AGT, MAC, and RTR. The AGT represents agent, MAC represents MAC and RTR represents routing. The various parameters that include in NS2 tracing are (1) Reason: The main reason for tracing (e.g., "NRTE" for No Route Entry) (2) Time to Send Data: The expected time required to transmit this packet over the wireless channel as indicated by the underlying MAC protocol.(3)Ethernet Packet Type: Currently, there are only two Ethernet packet types: A general IP packet: The value is "ETHERTYPE_IP" defined as "0x0800".(4)An ARP packet: The value is "ETHERTYPE_ARP" defined as "0x0860".(5)RREQ Type: type as indicated in the field "rq_type" of thehdr_aodv_request structure data type. By default, the value is "AODVTYPE_RREQ" defined as "0x02".

3.5 Node Deployment Algorithm

This algorithm is responsible for deployment of nodes in a particular area. This will position the nodes in the given area. Check for the number of nodes and the distance between the nodes. First node will have "0" distance. The next nodes distance will be previous node position plus the distance. Generate the node id as "i". Create a map of the node id and position of the node. The neighboring nodes are identified using the concept of Euclidian distance. Each and every node in the network topology will be assigned with certain bandwidth and topology. The source node and the destination node is to be specified. One controller node is to be specified which takes care of the network and is used in detecting the black holes in the network. According to the concept of Euclidian distance the nodes start detecting their neighbors by sending the route request packets to the neighbors[6]. The route request and the node acknowledgment is provided while detecting the shortest path from the source node to the sink node [8].

4. EXPERIMENTAL RESULTS

Here network simulator is used to simulate the results. Here a total of 39 nodes are used in the wireless sensor network. Two black holes are chosen for a total of 39 nodes. Any number of nodes and any number of malicious nodes can be taken. After the active detection routing protocol and after identifying the nodes the route request is send to the neighboring nodes (See Figure 3). The route request is accepted and acknowledged by sending a route reply across the nodes (See figure 4). This is done to find the shortest route from the source to the sink. The shortest route is calculated using the Euclidian Distance formula (See Figure 5).

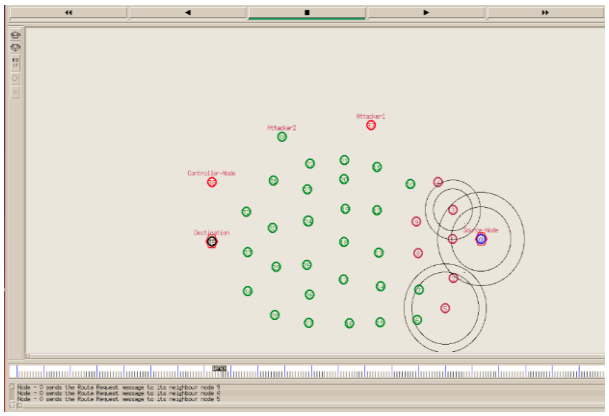

Fig 3: Sending Route Request to the Neighbors

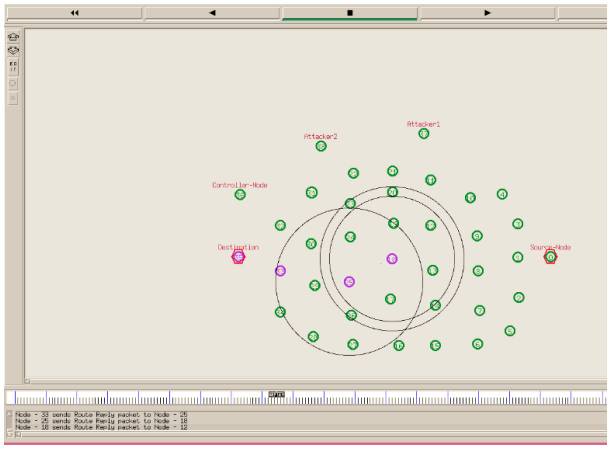

Fig 4: Sending Route Reply Back to the Source

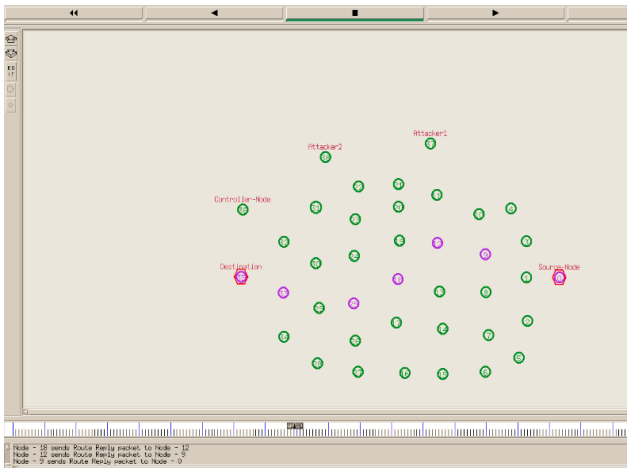

Fig 5: Shortest Path for Routing

In Figure 5, the nodes indicated in purple is the shortest path between the source node to the sink node. After finding the shortest path for routing the dummy data is sent across the shortest path just to see where the attacker launches the attack. The attacked nodes are identified as such. The dummy data that is "0000" is sent across the shortest path as shown in Figure 6. The attacked nodes are identified in the network as soon as the attacker launches the attack on the dummy data as shown in Figure 7. The nodes that are attacked are indicated in the Figure 7.

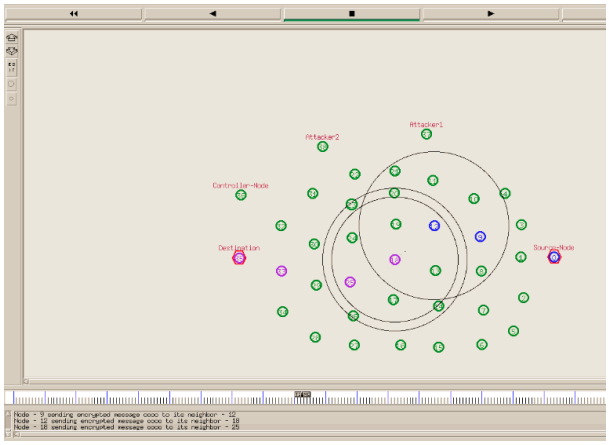

Fig 6: Sending Dummy data Across the Nodes

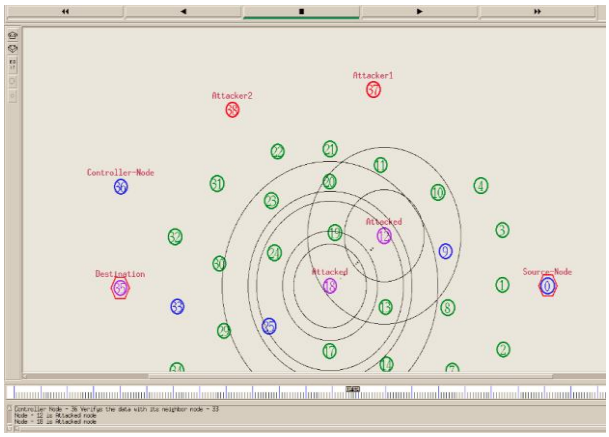

Fig 7: Attacked Nodes

The Figure 7 indicates that the node 12 and node 18 are the attacked nodes that are attacked by the attacker. The nodes 37 and 38 that are indicated in red are the attacker nodes. They try attacking the path that consists the packets. The controller node is used to control the network and it is used to verify the data with neighboring nodes to find if the data is proper and helps us in finding the attacked nodes. The node 36 here is indicated as the controller node. As soon as the black holes are detected in the network the network immediately changes the routing path and takes a different path with higher trust to reach the sink node. The nodes indicated in brown color are the new routing path to the sink. Thus the security routing is applied here. The encrypted message is routed to sink to ensure security of the packet as shown in Figure 8. The encrypted message is decrypted only at the sink node. Here the sink node is 35 and the source nod is 0. Thus the message gets decrypted only at node 35. The figure 8 indicates that as soon as the attacked nodes are found the routing path is changed from node 9 to node 13 instead of node 12 and node 18.

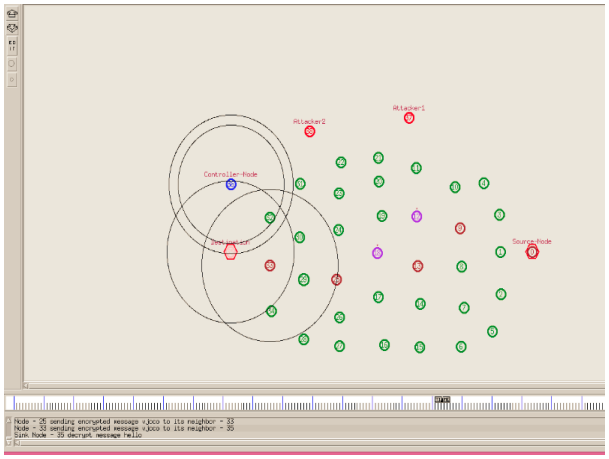

Fig 8: Path Changes

Similarly there are other different paths to route the packet to the sink node. The nodes indicated in yellow and orange Figure 9 are the new paths to the sink with higher trust and with avoiding the black holes are routed to the sink node. The encrypted message is only send across these paths to ensure the security of the packets and the data. The nodes indicated in purple are the attacked nodes. The nodes indicated in brown, yellow and orange are the alternative paths to the sink to avoid black holes. Figure 10 indicates the complete active trust scheme output with various alternative paths to the sink from the source node. Even though there are black holes the routing is successful without any loss of data.

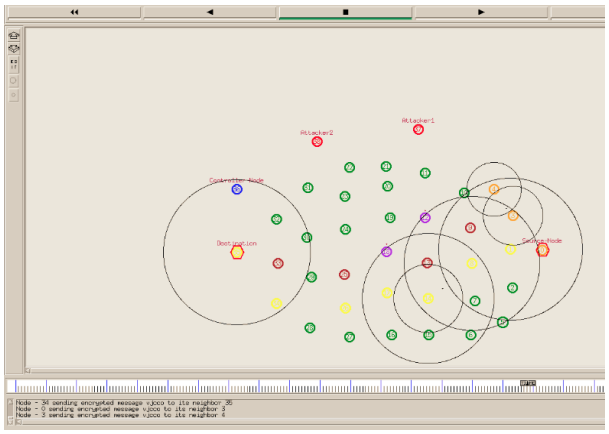

Fig 9: Alternative Paths to the Sink

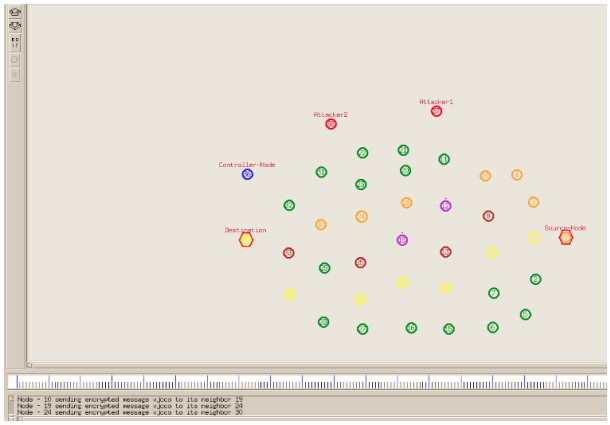

Fig 10: Trust Routing Final Output

4.1 Output Parameters

The various output parameters that are calculated, simulated and compared with the Active trust scheme are: throughput, overhead, packet delivery ratio, end to end delay and the average energy. Theses parameters are compared with the network without any malicious nodes and the network containing malicious nodes but using the active trust scheme. The Table 1 indicates the comparison between the Active trust scheme with malicious nodes and a healthy network without any malicious nodes.

Table 1. Comparison Table with Active Trust Scheme and Healthy Network

Parameters	Active Trust Scheme With Black Holes	Healthy network without black holes
Throughput	475	475
Overhead	3.2	2.6
Packet Delivery Ratio	71	98
End to End Delay	36	191
Energy	5.119 J	**4.857**

4.1.1 Throughput Comparison

In wireless technology, throughput is amount of work a network can do. Network throughput is the average number of successful message delivery over a wireless channel. Users of communications devices, systems designers, and researchers into communication theory are often interested in knowing the expected performance of a system. This is a benchmark for many calculations. The main aim of the paper is to prove that, by using active trust scheme the throughput of the malicious nodes or black nodes is exactly equal to the throughput of the normal healthy network. The Figure 11 shows us that the throughput is exactly same for with and without malicious nodes, but using active trust scheme for the network with malicious nodes. Thus active trust scheme plays a very important role in maintaining network security and keeping the data delivery rate maximum. Figure 12 indicates that the throughput remains constant even though the number of black holes increases. This proves the strength of the active trust scheme in a black hole attack.

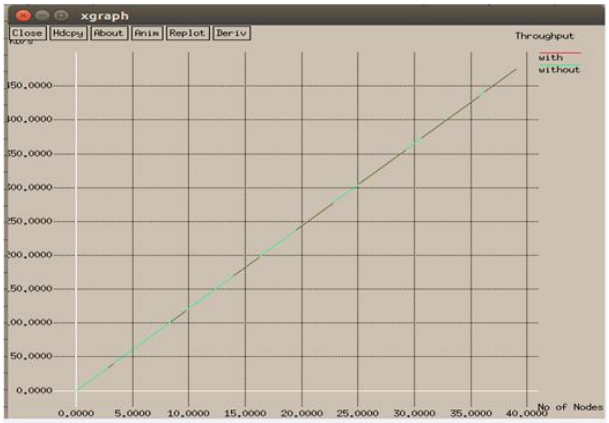

Fig 11: Throughput Comparison

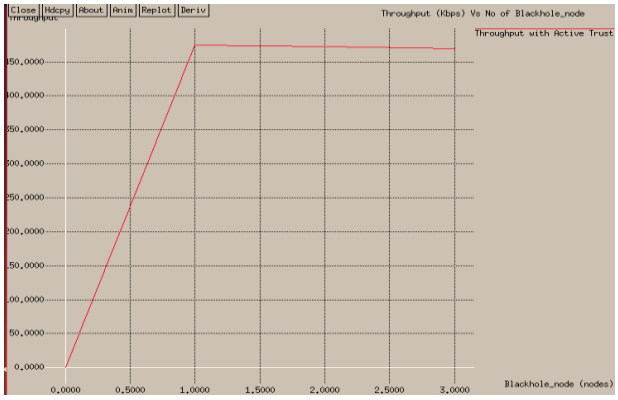

Fig 12: Constant Throughput with Increased Black Holes

4.1.2 Overhead Comparison

Overhead defines the number of routing packets that are required for communication. First the communication between node 0 and all the other nodes is to be defined. The route request is send to all the neighboring nodes and the route acknowledgement is received. Routing Overhead= Routing packets count/ Received packet count. The overhead energy is very important and an intrinsic factor of energy dissipation in sensor nodes. If this important parameter is neglected while making routing decisions it will result in worst routing leading to unwanted multihop communications which thereby results in a significant amount of waste of energy. The lifetime of the network will decrease if the overhead energy dissipation is not considered in the routing algorithm. Figure 13 indicates that the overhead with black holes is 3.2 and without black holes is 2.6.The overhead is comparatively high with black holes rather than without black holes which is acceptable.

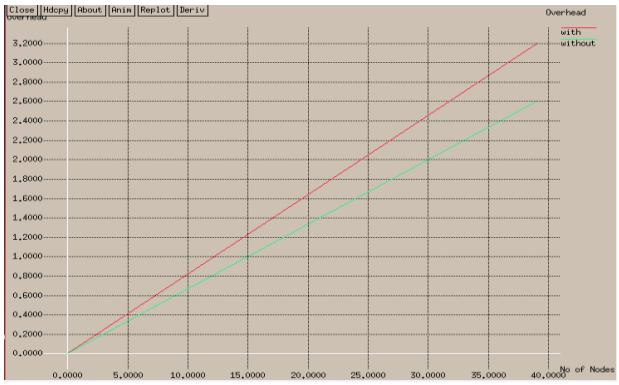

Fig 13: Overhead Comparison

4.1.3 Packet Delivery Ratio Comparison

Packet Delivery Ratio is defined as the ratio of the packets that are successfully received at the sink node to the number of packets that are send by the sender. The packet delivery ratio is calculated using the awk scripts to produce the results. It will process the trace file and then it will produce the result. It is defined as the ratio of received packets divided by the send packet. It is multiplied by 100 to find the percentage. The Figure 14 indicates that the packet delivery ratio is 98% without malicious nodes and 71% with malicious nodes. This is very much desirable because even with malicious nodes using the active trust scheme the delivery is 71%.

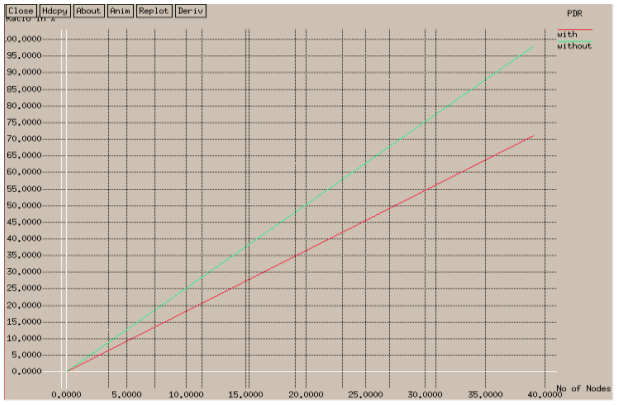

Fig 14: Packet Delivery Ratio Comparison

4.1.4 End to End Delay Comparison

Delay is the time at which the sender has generated the packet for transmission and the time at which the receiver received the packet. If "i" is the packet sequence number. If count is the total packet count then

Delay[i] = Receiving time[i]-Sending time[i]

Total delay= Total delay between packets + delay[i]

Average delay= Total delay/count.

This figure 15 indicates that the delay with black holes is less compared to the delay without black holes. In active trust scheme the black holes are detected and an alternative route is taken to reach the sink, but in a healthy network it needs to trace every neighbouring node. Therefore the delay increases for a network without any malicious nodes.

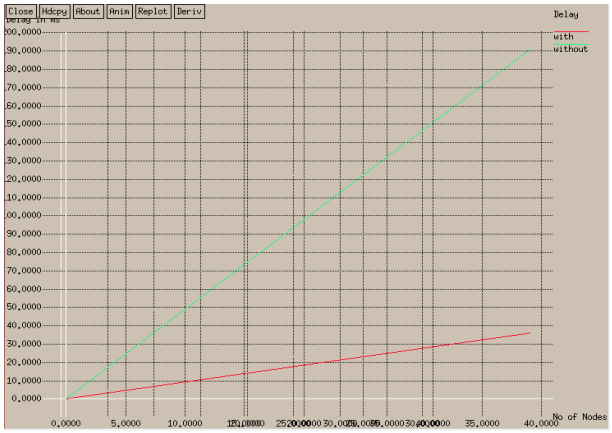

Fig 15: End to End Delay Comparison

4.1.5 Energy Comparison

The energy model represents the level of energy in a mobile nodes. The energy model in a node has an initial value which is the level of energy the node has at the beginning of the simulation. This is known as initial energy. They have a given energy usage for every packet it transmits and receives. These are called Transmission power and Reception power. The energy model only maintains the total energy and does not maintain radio states. It is generic enough for future simulations such as the CPU power consumption. The Figure 16 indicates that the average energy is compared with malicious nodes using active trust and without malicious nodes. The energy utilized is very similar which is equal to 5Joules. The energy model represents the energy level of the nodes. The amount of energy consumed to travel from the

source to the sink. This indicates that the energy consumed will increase as the network size increases. But the energy utilized remains same for both the malicious nodes using active trust scheme and without malicious nodes. The energy consumed here is 5J for 40 nodes.

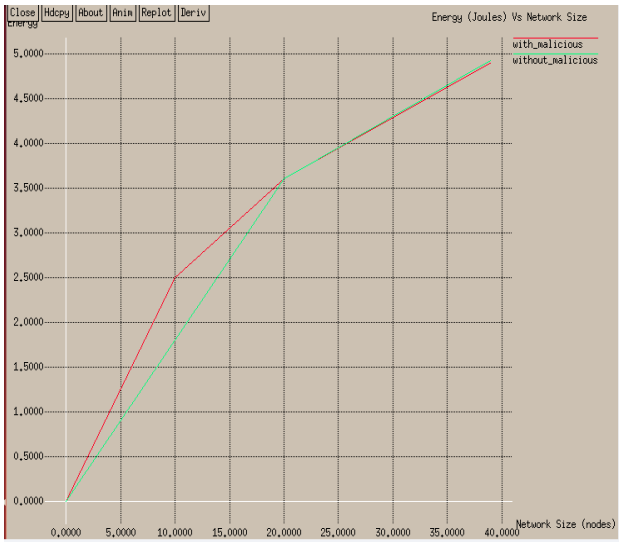

Fig 16: Energy Comparison

4.1.6 Conclusion and Future Scope

The Active trust protocol has the following excellent properties: (1) High successful routing probability, security and scalability. The trust of the route is very high throughout the transmission of packets. (2)Nearly 100% successful routing even with black holes. (3)Throughput is similar to a healthy network throughput. (4)It makes use of the residue energy of the nodes. (5)It improves the network security performance which is very important in wireless sensor networks.

The future scope of the active trust scheme would be to improve the energy efficiency and the network security performance. To use the residue energy present in the nodes to construct the various detection routes.

5. ACKNOWLEDGMENTS

This work would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them. My sincere gratitude to all who have contributed to my work. With profound reverence, I sincerely thank Dr. K. Mallikarjuna Babu, Principal, BMSCE Bengaluru and Dr. G. Poornima, Professor and Head of Department of Electronics and Communication, BMSCE Bengaluru for giving me an opportunity to undertake this project work. I am thankful to all the members of ECE department for their continuous cooperation during my project work. Finally my whole hearted gratitude to my loving parents who were a constant source of moral support, love and encouragement throughout my studies.

6. REFERENCES

[1] Yuxin Liu, Mianxiong Dong, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks," IEEE, vol.11, No.9, September-2016,pp.2013-2027.

[2] J. Wang, Y. Liu, and Y. Jiao, "Building A Trusted Route In A Mobile Ad Hoc Network Considering Communication Reliability And Path Length," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1138–1149, 2011.

[3] Y. Hu, M. Dong, K. Ota, A. Liu, and M. Guo, "Mobile Target Detection In Wireless Sensor Networks With Adjustable Sensing Frequency," IEEE Syst. J., to be published, doi: 10.1109/JSYST.2014.2308391.

[4] H. C. Leligou, P. Trakadas, S. Maniatis, P. Karkazis, and T. Zahariadis, "Combining Trust With Location Information For Routing In Wireless Sensor Networks," Wireless Commun. Mobile Comput. vol. 12, no. 12, pp. 1091–1103, 2012.

[5] M.-Y. Hsieh, Y.-M. Huang, and H.-C. Chao, "Adaptive Security Design With Malicious Node Detection In Cluster-Based Sensor Networks," Comput. Commun., vol. 30, nos. 11–12, pp. 2385–2400, 2007

[6] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "Energy And Memory Efficient Clone Detection In Wireless Sensor Networks," IEEE Trans. Mobile Comput., vol. 15, no. 5,May 2016,pp.1130–1143, doi: 10.1109/TMC.2015.2449847.

[7] Network Simulator 2.35 available at http://www.NS-2.35.org/

[8] S. Mandala, K. Jenni, A. Ngadi, M. Kamat, and Y. Coulibaly, "Quantify- Ing The Severity Of Blackhole Attack In Wireless Mobile Adhoc Networks,"in Security in Computing and Communications. Berlin, Germany: Springer, 2014, pp. 57–67.