

# Mitigating Selective Forwarding Attacks in WSN

Jaspreet Singh

*Department of Computer Science Engineering,  
RIMT IET, Punjab, India*

Anuj Gupta

*Head, Department of Computer Science Engineering,  
RIMT IET, Punjab, India*

**Abstract** - Security is the major threat in Wireless Sensor Networks (WSN) as they are being increasingly used due to their wide range of applications in military and civilian domains. These networks are prone to security attacks. Some of the inherent features like limited battery and low memory make sensor networks infeasible to use conventional solutions of security, which needs complex calculations and more memory. Deployment of sensor nodes in hostile environment makes them vulnerable to a variety of potential attacks like Hello flood attack, wormhole attack, black hole attack and selective forward attack. The attacks on these networks can be classified as routing attacks and data traffic attacks. Black hole attack is that in which compromised node usually drops all the packets being forwarded through it. A special type of black hole attack is selective forwarding attack, in which compromised node drops packets selectively, which may decrease the network efficiency. Selective forwarding attack is hard to detect, since packet drops in sensor networks may be caused by unreliable wireless communications or node failures. Selective forwarding attacks can corrupt some very critical applications. In these types of attacks, malicious nodes behave like normal nodes most of the time but selectively drop sensitive packets. The packet delivery ratio in the proposed scheme is much more than existing schemes.

**Keywords:** Wireless Sensor Network, Security, Selective Forwarding Attack, Sensor Network.

## I. INTRODUCTION

WSN is being emerged as a promising and interesting area. It is designed for real-time data collection and analysis of data in hostile environments so they are used mainly in monitoring and surveillance based applications. Most widely used applications of WSN are military appliance, area monitoring, environmental monitoring, industrial monitoring, machine health monitoring, water/waste water monitoring, fleet monitoring. Since, WSNs are mostly used in a hostile environment security is mainly concerned. The conventional security measures are not suitable to the wireless sensor networks due to resource constraints of both memory and energy. In WSN, sensor nodes use wireless communication to send packets. A sensor node uses multi-hop transmission to deliver the packet to the base station, due to its limited transmission range. so a packet is forwarded through too many hops/nodes to reach the destination. As, we discussed sensor networks are usually deployed in hostile environments, an adversary can launch attacks. Attacks can be classified into two types, inside attacks and outside attacks. The latter one can be easily detected and security solutions are provided. In former one, adversary compromises some internal nodes and launches attacks which will be difficult to detect. One kind of such attack is Selective Forwarding.

In Selective Forwarding Attack, internal nodes that are compromised selectively drops/forwards some of the packets passing through them. If any node drops all the packets, then it becomes black hole attack. Therefore, selective forwarding attack is sometimes called as a special case of black hole attack.

## II. SELECTIVE FORWARDING ATTACKS

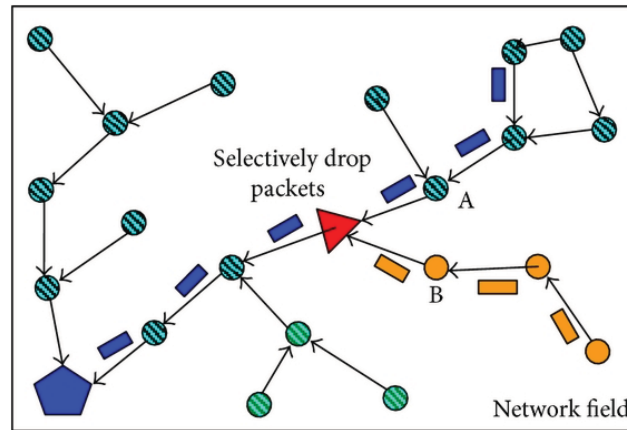


Figure 1. An example sensor network under selective forwarding attacks, when the adversary puts himself on the forwarding path

In selective forwarding attacks malicious nodes behaves like black hole and refuse to forward some messages and simply drop them and ensure that they are not propagate further. Such an attacker runs the risks that neighbouring nodes will conclude that they have failed and decide to seek another route. A more refined form of this attack is when an adversary selectively forwards some packets. An adversary interested in suppressing or modifying packets originating from a few selected nodes can constantly forward the remaining traffic and limit suspicion of its wrongdoing.

Selective forwarding attack is hard to detect, since the wireless communications are unreliable because there is a loss of data packets due to noise also. In some cases, sensor nodes go into sleep state (mode) to save power and they are not able to send and receive data in this period. So, we have to be examine carefully whether the packet drop is due to selective forwarding or any other reason.

## III. PROBLEM FORMULATION

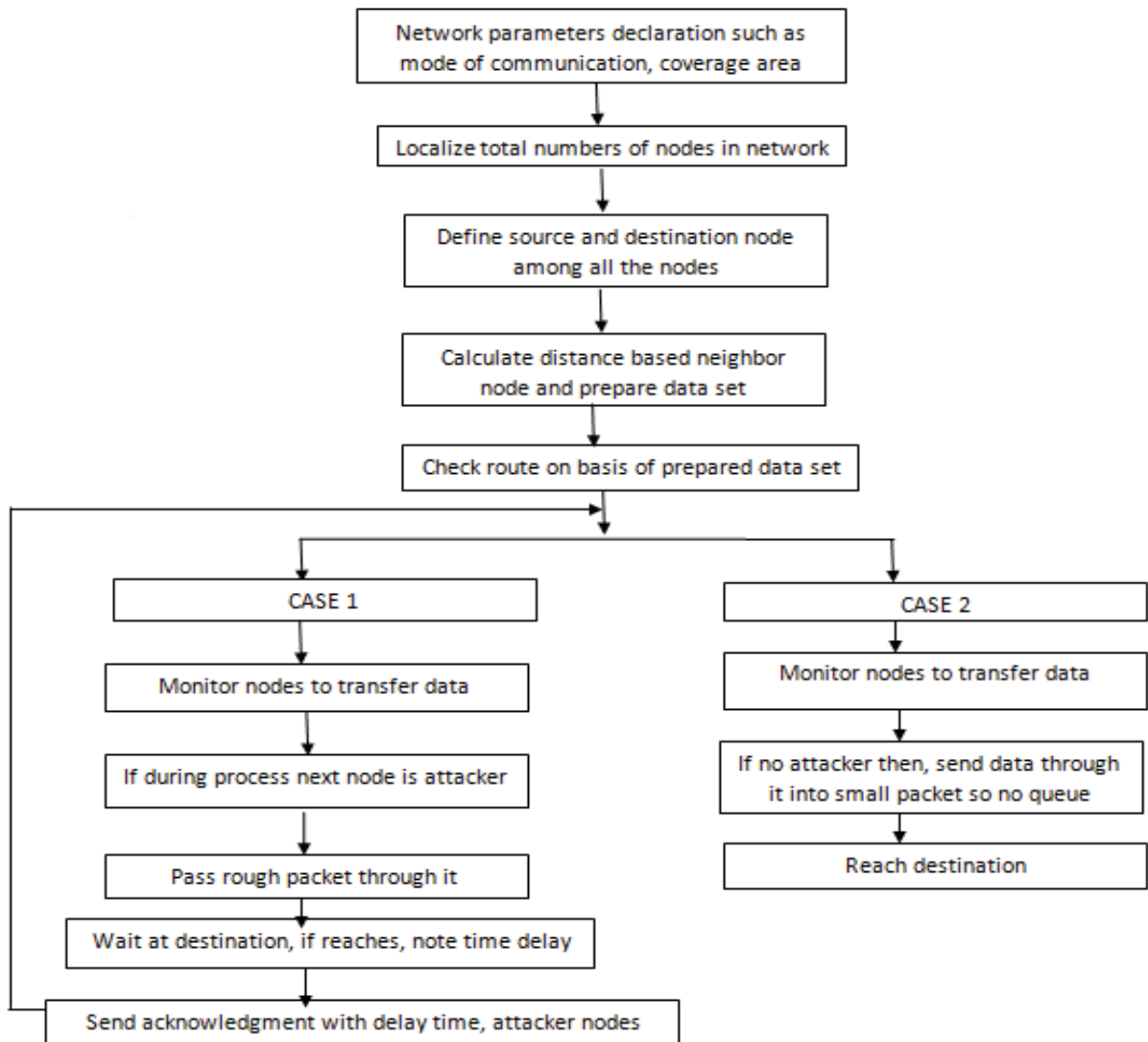
A network without physical link is termed as wireless sensor network. It consist of numbers of sensors nodes which act for spot of transmission in communication link. To transmit data from node to node in a wireless sensor network it requires determining best path of transmission. This suffers from various issues as:

- Malicious/ attacker nodes
- Fault transmission
- Delay in transmission
- Loss of data

Attack of malicious or attacker nodes causing loss of data and interferences in data were due to various factors which corrupt the transmission in Wireless sensor networks.

Due to this efficiency of the systems decreases and there was no security of successful transmission. Even there was no way to determine the attacker nodes in the network so as to decrease the delay time and enhance the network qualities with productive outputs.

## IV. FLOW DIAGRAM



## V. PROPOSED WORK

Proposed system performs a monitoring task of detecting attacker nodes on the basis of a doubt factor. Firstly source sends data to a node by detecting the position of the node and distance among all as done in previous systems. Now what path has to be followed for accurate /healthy communication is detected. Shortest way to select is determining the distance and energy of various nodes. After transmitting data to it again note the various factors as distance, other properties of nodes and repeat the process till data reach the destination. An acknowledgment is provided back to the transmitting node as the information regarding whether data is received properly or is lost.

As communication starts and data is send. A coverage area is defined and then the nodes distance is checked, for example if there lays three nodes which are very close to the source. Node with the shortest distance is selected to carry out the communication. The node which has receive the data, now for further communication will act as source and will transmit the data onwards. Now again the same features/ property is calculated. Data from node to node is transmitted by keeping a check on the distance until the data is received by the sink (destination). An acknowledgment is provided back to the transmitting node as the information regarding whether data is received properly or is lost.

Here proposed algorithm will keep a check on the attacker nodes and will inform about it to the sources so as not to send data by it and reduce delay with increasing the success transmission percentage.

## VI. METHODOLOGY

1. The very first step is to declare the network parameters for initialization such as coverage area and mode of communication.
2. Localization of nodes: means first determines the total number of nodes in the coverage area and then find their position.
3. Among total numbers of nodes, specify one source and destination node for data transmission and communication.
4. Now calculate the distances among all the nodes and find the neighboring nodes.
5. Few of the nodes, among total numbers of nodes may be malicious nodes or can say attacker nodes. We need to determine them in the network.
6. On the bases of distance, check for the shortest and healthy route of transmission. Means from source it will find the nodes which are closest, and among them, most nearest one will be selected for transmission and so on will keep determining distance based nodes to follow up the route.
7. The very next step is to monitor this entire network's nodes to start transmission of data from source to sink node.

Here comes two cases:

**With Attacker node case:** While transferring data from node to node, if the coming next node is an attacker node, then pass any rough packet through that attacker node and to see its output. If this packet reaches the destination with a delay or if the packet didn't reach the destination, then send an acknowledgement back to the system for monitoring the nodes once again. This acknowledgement contains information about the positive or negative output with delay time and information of the nodes which are attacker, so as not to transfer any more data from them.

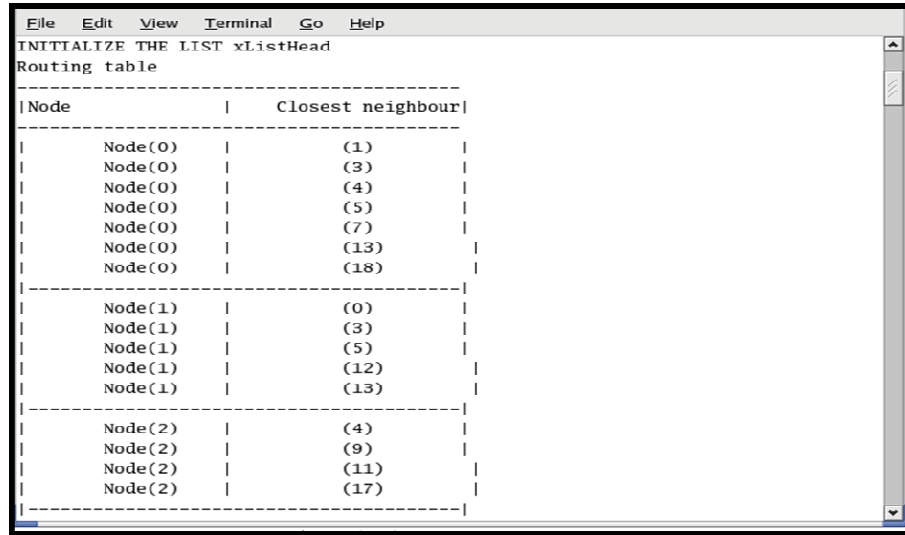
**Without attacker node case:** But if in node to node transmission, the coming node is not an attacker node, then send the data through it by converting them into small packets so as to reduce the delay. It will reduce the delay by minimizing the queue in the buffer. Packets will reach at the destination node and hence the packet is transferred from source to sink by following the shortest path based on distance.

Proposed methodology is having two cases in which the results are determined

1. Case1:- when the attacker node is detected in path
2. Case2:- when there is not any attacker node in path

On the basis of this methodology implementation is done which is described step by step with some of the sanpshots taken from the simulator as shown below:-

**Step 1:** in first step the parameters of network are determined as number of nodes, area etc. then after distance based neighbor nodes of the individual nodes are determined as shown below



Node	Closest neighbour
Node(0)	(1)
Node(0)	(3)
Node(0)	(4)
Node(0)	(5)
Node(0)	(7)
Node(0)	(13)
Node(0)	(18)
Node(1)	(0)
Node(1)	(3)
Node(1)	(5)
Node(1)	(12)
Node(1)	(13)
Node(2)	(4)
Node(2)	(9)
Node(2)	(11)
Node(2)	(17)

Figure 2: Individual nodes closest neighbor node table

**Step 2:** After determining the neighbor node the source and the destination node is defined. user will input the source node number and destination node number and on basis of that the algorithm will determine the path that it has to follow to transfer the data from source to destination.

**Step 3:** this step include the case 1 study the source node will check the next node to transfer data upto destination if next node determined is worm hole attacker node which is determined by the monitoring module of the network. Then the source node will transfer a rough packet of data from the attacker node and wait for acknowledgement.

**Step 4:** in this step as the packet is sent to attacker node it will pass the data to next attacker and so on to the destination. the destination will send a data acknowledgement which will include the time consumption and the data dropage of the attacker node and save it for further transmission in the network.

**Step 5:** this step include the network animation to show the demonstration in real time by network animation tool of the NS2 where green color of node represent the source node and blue as a destination and red color as the attacker nodes.

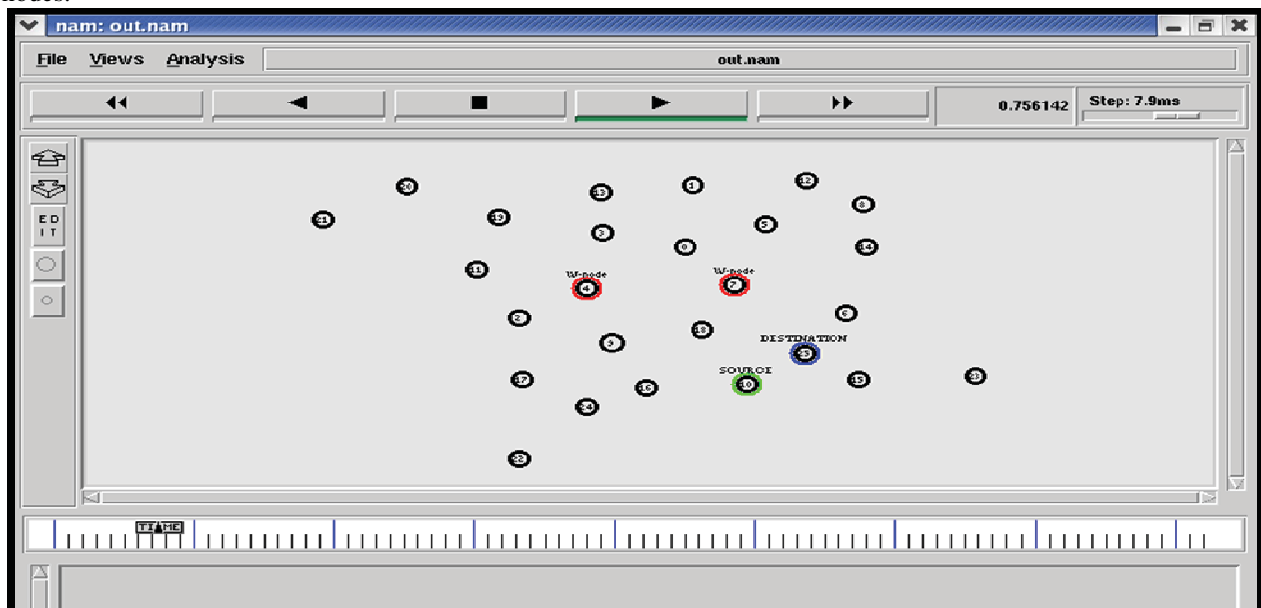


Figure 3: selection of source and destination node for the data transmission

**Step 6:** as shown in the snapshot the data is transmitted from source to the attacker node and so on upto destination with temporary data packet

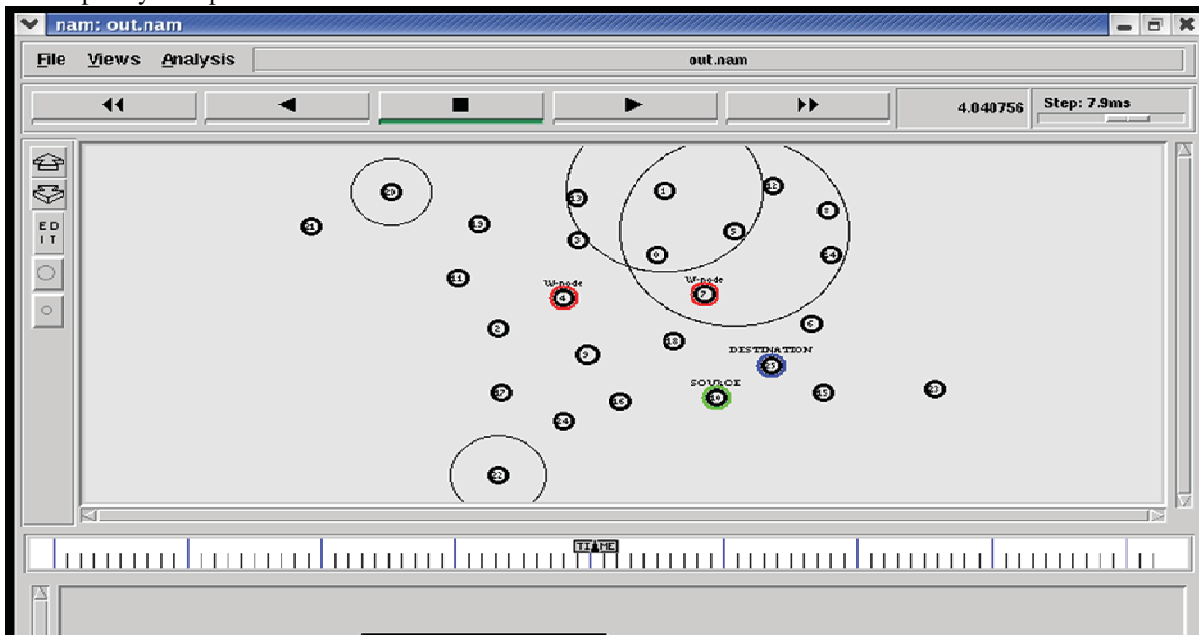


Figure 4: transfer of rough data packet from source to destination as malicious node detected

**Step 7:** this step demonstrate the packet received at the destination transferred by attacker nodes from source.

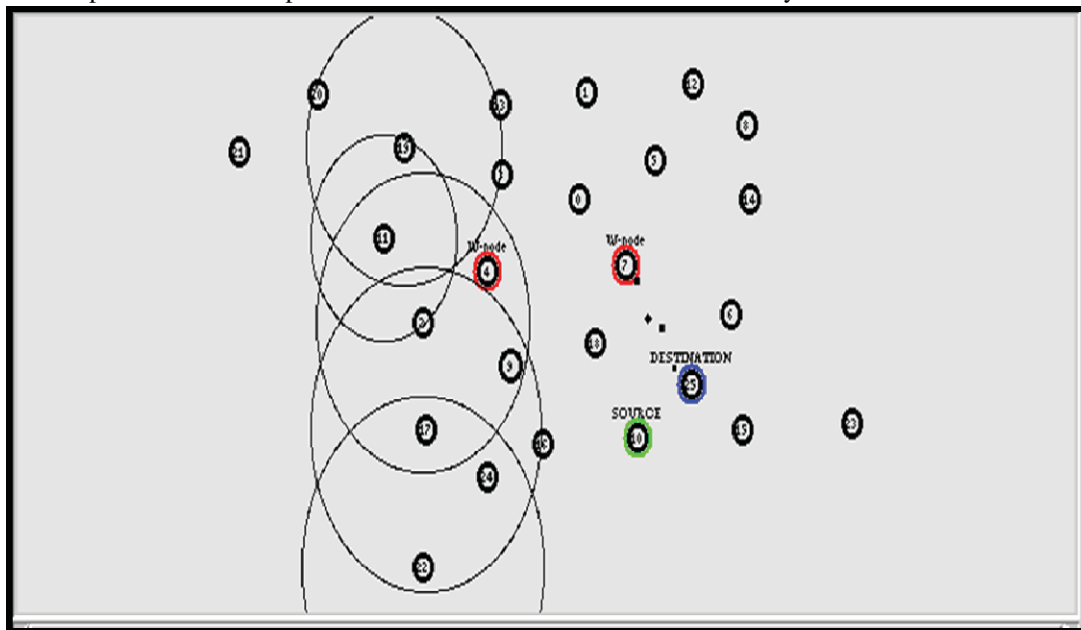


Figure 5: after travelling only attacker node's data received at destination

**Step 8:** this step is study of case two in which there is not any attacker node in route found by the algorithm of neighbor node vector. The monitoring system determine that there is not any malicious node in route of closet node data transfer module.

**Step 9:** this step shows that how data transfers from source to destination with including the attacker node as it is detected in case1 so data is received in actual form at destination sent by any source node by secured path.

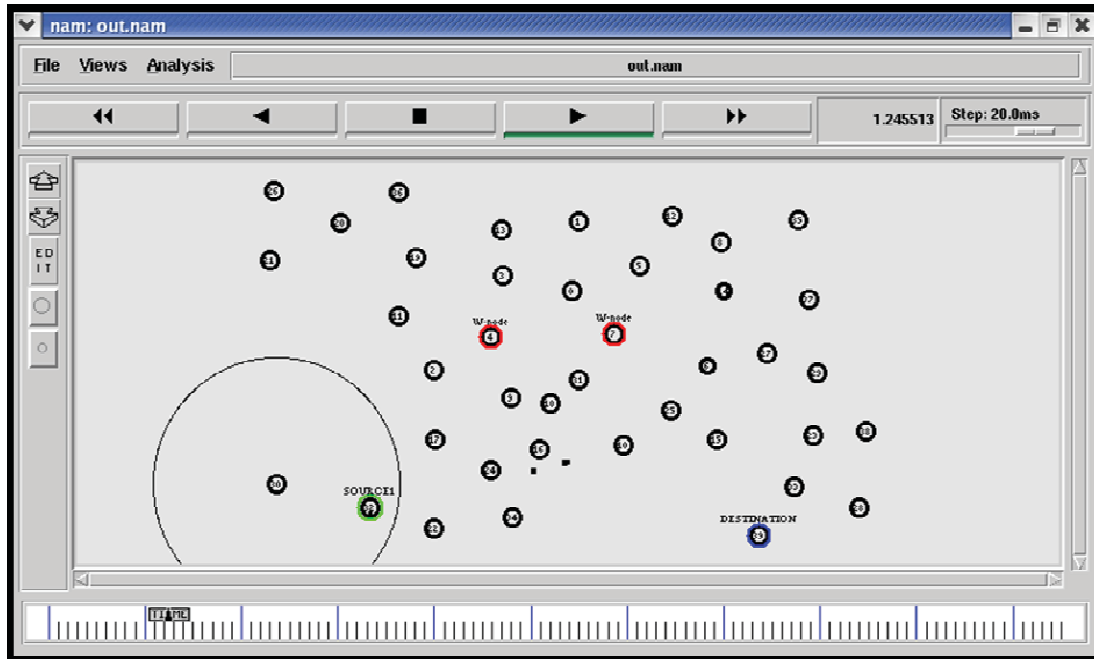


Figure :6 the data packets are transferred from secured path

## VII. CONCLUSION

Security in network during data transfer is main concern for QOS in the network. After simulation of proposed methodology the results demonstrate the security of data transfer in network with more effective approach by editing the monitoring module in the network which will help the further transmission in network without considering the attacker node in route as those are determined earlier by monitoring. So the proposed system is more secured and efficient for performing data transmission in network. As a future scope key based approaches for node selection and dedicated link provision can be used for providing intrusion less path.

## ACKNOWLEDGEMENTS

We wish to thank the editors and reviewers for their valuable suggestions and expert comments that help improve the quality as well as quantity of the paper.

## REFERENCES

- [1] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Ad Hoc Networks*, Vol. 1, No. 2, 2003, pp. 293-315.
- [2] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in *Proc. of the 2nd International Workshop on Security in Systems and Networks*, April 2006, pp. 1-8.
- [3] B. Yu and B. Xiao, "CHEMAS: identify suspect nodes in selective forwarding attacks," in *Journal of Parallel and Distributed Computing*, Vol. 67, No. 11, 2007, pp. 1218-1230.
- [4] Navjot Kaur, Amandeep Kaur, Anuj K. Gupta, "Security attacks on Mobile Ad hoc networks", Proceedings of 7th International Conference on upcoming trends in IT (ICUTIT 2011), PCTE, Punjab, pp. – 66 – 71, 26 March 2011.
- [5] H. Sun, C. Chen and Y. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in *Proc. Of IEEE TENCON 2007*, Oct. 2007, pp. 1-4.
- [6] Tran Hoang Hai, Eui-Nam Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbour Knowledge" Seventh IEEE International Symposium on Network Computing and Applications, 2008, pp.325-331.
- [7] G.Padmavathi, D.Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" international Journal of Computer Security, Vol. 4, No. 1 & 2, pp. 117-125, 2009
- [8] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, Wang Liang-min, "Lightweight Defence Scheme against Selective Forwarding Attacks in Wireless Sensor Networks" pp.226-232, IEEE, 2009.
- [9] Yenumula B Reddy, S. Srivathsan, "Game Theory Model for Selective Forward Attacks in Wireless Sensor Networks" 17th Mediterranean Conference on Control & Automation Makedonia Palace, Thessaloniki, Greece June 24 - 26, 2009, pp. 458-463

- [10] Guorui Li, Xiangdong Liu, and Cuirong Wang, "A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks", pp.554-558, 2010.
- [11] S.-B. Lee and Y.-H. Choi, A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks, In Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN'06), pp. 59-70, 2006.
- [12] Jaspreet Singh, Anuj Gupta, "Different Approaches to Mitigate Selective Forwarding Attacks in WSN", International Journal of Innovations in Engineering and Technology (IJJET), ISSN: 2319 – 1058, 3(4): 40-46, April 2014.