Selective Forwarding based Intrusion Detection System for Secure Wireless Sensor Network

Bharti Bains
CSE Department
M. M. Engineering College,
M. M. University,
Mullana, Ambala, Haryana, India-133207

Rohit Vaid
CSE Department
M. M. Engineering College,
M. M. University,
Mullana, Ambala, Haryana, India-133207

ABSTRACT
Security is the major threat in wireless sensor network. Deployment of sensor nodes in hostile environment makes vulnerable to a variety of potential attacks like Hello flood attack, wormhole attack, black hole attack and selective forward attack. In a black hole attack, compromised node drops all the packets forwarding through it. A special case of black hole attack is selective forwarding attack, where compromised node drops packets selectively, which may deteriorate 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. The proposed work is based on centralized intrusion detection scheme which uses multi level dynamic tree routing. It can detect both black hole attack and selective forwarding attack. The proposed scheme is compared with existing scheme and found that the packet delivery ratio in the proposed scheme is much more than the existing scheme.

Keywords
WSNs , Security, Selective Forwarding Attack.

1. INTRODUCTION TO WSNs

Wireless Sensor networks are composed o large number of small sensors nodes. These are designed for real time collection and analysis of low level data in hostile environment. Wireless Sensor applications include military command, intelligent communication, wildlife monitoring, industry quality control, traffic monitoring etc. Security is critical for sensor networks deployed in hostile environments. Providing security and privacy to small sensor nodes is challenging, due to the limited capabilities of sensor nodes in terms of computation, communication, memory storage, and energy supply. Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Theses attacks include Hello Flood , Selective Forwarding , Wormhole , Sybil, Acknowledgement Spoofing ,Node Replication, Eavesdropping. In a selective forwarding attack, malicious nodes behaves like black hole and may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a few selected nodes can reliably forward the remaining traffic and limit suspicion of its wrongdoing. It is very difficult to find out either the packet are dropped due to selective forward attack or due to any other network problem .There are different forms of selective forwarding attack[12]. In one form, the malicious node can selectively drops the packets coming form a particular node or a group of nodes which causes a Denial of Service attack**.** It also behaves like a Black hole [3] in which it refuses to forward every packet. In case of Black hole attack, all the packets are consumed by the malicious node .Hence it is easier to detect also. Another form of selective forwarding attack is called Neglect and Greed, where the malicious node arbitrarily neglecting to route some messages [11]. Moreover, another variance of selective forwarding attack is to delay packets passing through them, creating the confused routing information between sensor nodes.

2. LITREATURE REVIEW

Karlof et al. [4] first time discuss the selective forwarding attack and also suggest that Multi-path routing can be used to counter these types of attacks. Messages routed over n paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most n compromised nodes and still offer some probabilistic protection when over n nodes are compromised.

Xiao, Yu and Gao [5] have proposed a technique for identifying suspect nodes in selective forwarding attack. They have actually improved their previous technique for detection of selective forwarding attack and named it as CHEMAS (checkpoint-based multi-hop acknowledgement scheme).

K. Sophia et al [6] have proposed a centralized intrusion detection scheme based on Support Vector Machines (SVMs) and have used sliding windows for black hole attacks and selective forwarding attacks.

Jeremy Brown et al [7] have presented a centralized cluster based scheme for detecting the selective forwarding attack in sensor networks by applying Wald's Sequential Probability Ratio Test (SPRT) method. The scheme utilizes powerful high-end sensors and is based on the sequential probability ratio test. The simulations results show that the proposed scheme achieves high detection ratio and very low false alarm rate.

Huijuan Deng et al [8] have proposed a centralized detecting method by watermark technology using the trust value in the routing selected algorithm. They have improved geographic forwarding algorithm by combining the trust value with distance to choose an optimal data forwarding path. However, major downside of centralized scheme is compromise of the centralized node then the whole network will suffer. Wang Xin-sheng et al [9] have presented a distributed lightweight defense scheme against selective forwarding attack, which is based on a hexagonal WSN mesh topology.

Guorui Li et al [10] have proposed the sequential mesh test based selective forwarding attack detection scheme in wireless sensor networks. The scheme nature is centralized and works for cluster based sensor networks.

3. SYSTEM MODEL

In the proposed work firstly construct a random wireless sensor network. Then find out the neighbors of each node using adjency matrix. Those neighbors which are within range are connected by links , while those nodes which are not in the range are disconnected from the network. Then Hello packets are sending by the base station to all the nodes for setting level of the nodes. Only those nodes which are in neighbor list of base station receive hello packets and are at level one. Then one by one Hello packets are move to individual nodes and set their level in increasing order. After setting level of each node, there is a need to find out route from each node to the base station. Now packets are transmitted from source to base station in such a way that only those nodes which are at immediate lower level can receive the packet. If more than one node is at same level and then chooses those nodes which have high trust value. Now a final path from source to destination is stored in farray and all packets move through it.

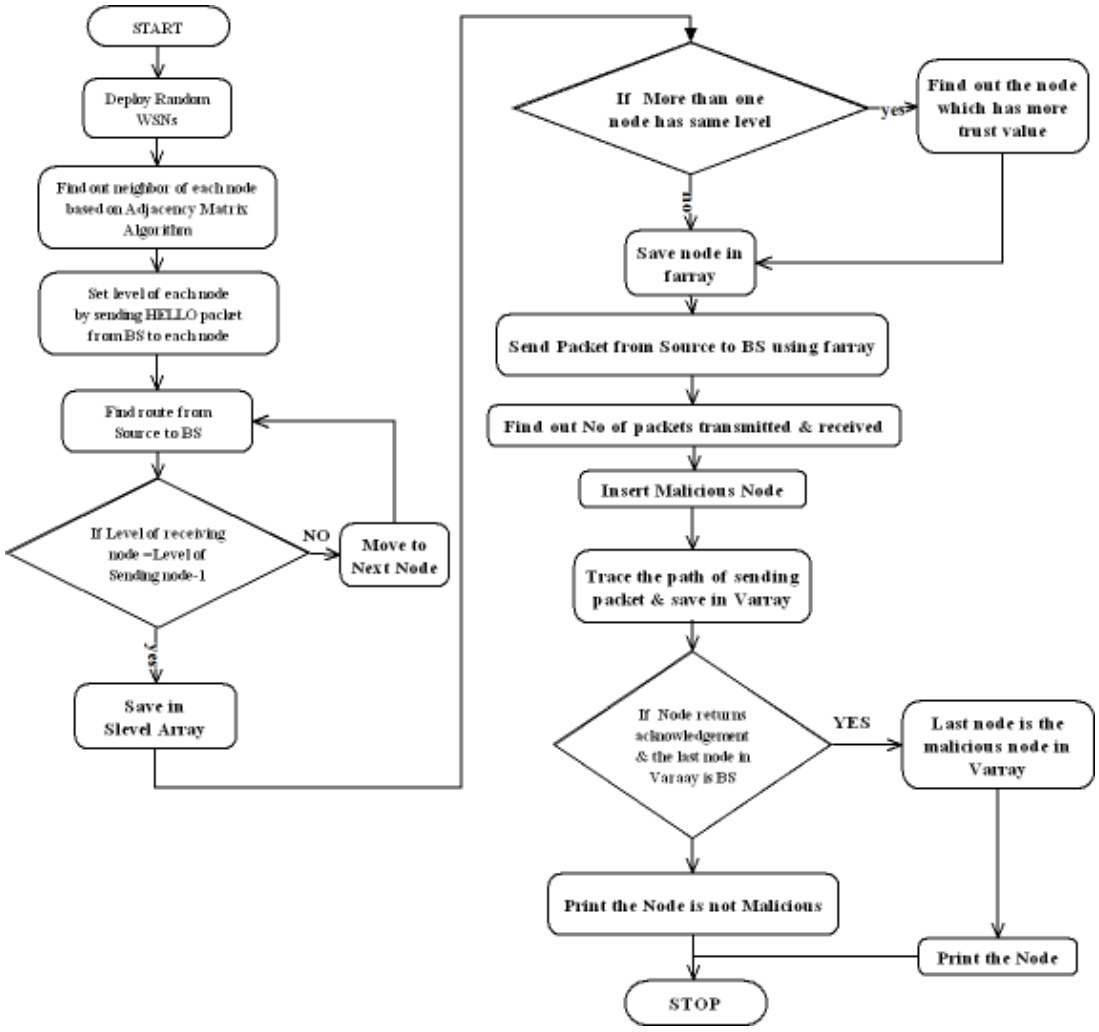

Fig 1: Flowchart of the system

4. PROPOSED SYSTEM

A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet it receives. In order to prevent selective forward attack certain measures are taken in order to detect the malicious node and make sure that the affected node would not be able to participate for the next event tracking process. Whole process has been divided into three steps:

A. Network Formation

B. Route Discovery

C. Malicious Node Detection

A. Network Formation

In the network construction phase, Base Station broadcast a Hello packet with Level field set to zero [3]. One hop neighbours of Base Station on receive the Hello packet update the value of their Level. Initially the value of Level at each node is set to infinity .These node again rebroadcast the Hello packet and the process continues until every node receives

Hello packet .Hello packets are send by the base station to all the nodes which are neighbours of base station Then selecting each neighbour one by one, packets are transmitted to further immediate neighbours of those nodes.

Algorithm 1: Network Construction Phase.
Step 1: Sink broadcasts a Hello packet with Source ID field set to its own ID and Level of node to zero.

Step 2: A node on receiving the Hello packet does the following.

If the currentLevel greater than value in NodeLevel + 1.

a. Set the currentLevel to NodeLevel + 1.

b. Rebroadcast the Hello packet with NodeLevel set field set to currentLevel, Source ID set to Node ID and HopCount to HopCount + 1.If the currentLevel less than or equal to NodeLevel + 1.

c. Discard the Hello packet.

Step 3: Repeat Step 2 until all nodes have received Hello packet.

In proposed system, each node has neighbors which are derived from adjency matrix. Neighbor table stores entries about neighbor id, node level and trust value of the neighbor node.

Table 1: Neighbor table

Neighbour_ID	NodeLevel	Trust Value
2	1	0.45
6	2	0.65
4	1	0.56

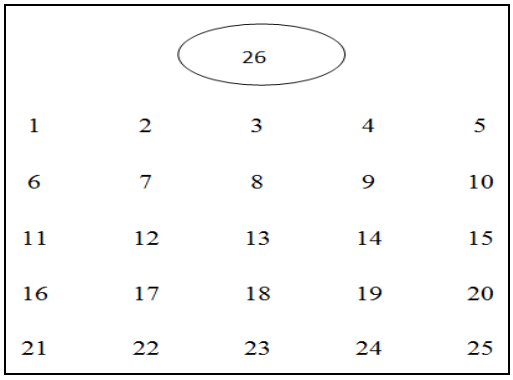

Fig 2: A network with 25 nodes in a 4X5 grid structure

The structure of the neighbour table is shown in Table 1. Consider a network with 25 nodes which are deployed in a 5x5 grid structure as shown in the Fig 2. Here S (26) is act as a sink node.

In the network construction phase, S broadcast a Hello packet with Level field set to zero as shown in Fig 3. One hop neighbours of S on receive the Hello packet update the value of their Level and necessary update is done in neighbour table. Initially the value of Level at each node is set to infinity. These nodes again rebroadcast the Hello packet and the process continues until every node receives Hello packet.

Hello packets are send by the base station to all the nodes which are neighbours of base station Then selecting each neighbour one by one, packets are transmitted to further immediate neighbours of those nodes.

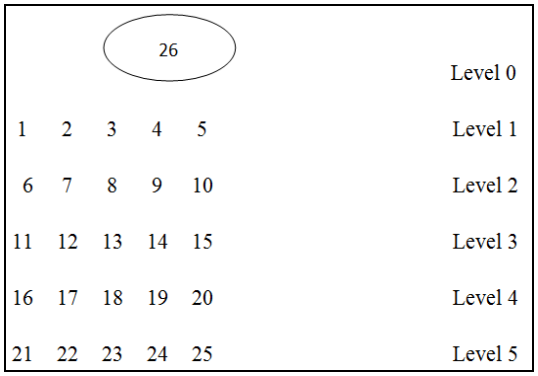

Fig 3: Leveling of each node

One hop neighbor of sink have the level is 1. Level is incremented by one for the further neighbors .Hello Packets are transferred from sink to those nodes whose level are more by one of the Sink node.

The neighbor table at node 22 and 26 is shown in Fig 4. Neighbor table of a node maintains the same, higher by 1 and lower by 1 level in the multi level tree. In this section, route is discovered for forwarding packet in such a way that it defends the selective forwarding attack. The routing scheme is a dynamic one. A node forwards a packet to one of its neighbors that have a lower level and more trust value. If two nodes of the same level have same trust value, then one of them is selected at random.

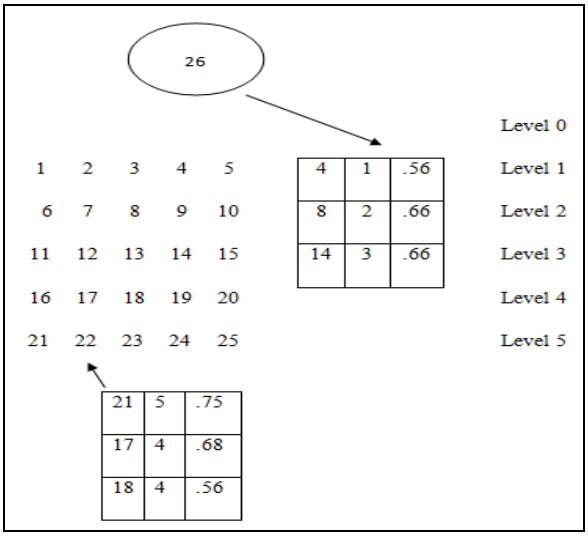

Fig 4: Network after construction Phase

B. Route Discovery

A node want to send the packet to base station will find out its immediate neighbour whose level is less than one of its levels. If more than one node has same level on that route, then that node which has large trust value is selected. In this way, a route is selected based on decreasing value of level from a node towards the base station.

Algorithm 2: Route Discovery
function send(i,next2)

INPUT: level, slevel, big, tv, next, next1, m, p, r, farray;

WHERE

level : level of each node

slevel: Nodes with same level.

big: Trust value from nodes at same level in slevel array.

m, r, i, j, k: temporary variables.

next2: movement to different nodes in neighbour array.

OUTPUT

farray: Final route of each node from source to sink.

Step 1: m=1

Step 2: farray{i}(r)=next2

Step 3: r=r+1

Step 4: If (next2==n+1) then

return

end if

Step 5: for j=1 to length(neighbours{next2}))

next=neighbors{next2}(j)

Step 6: if (level{next}==level{next2}-1) then

slevel{m}=next

m=m+1

end if

end for

Step 7: big=slevel{1}

Step 8: if (big==0) then

next2=n+1

return

end if

Step 9 for k=2 to n-1

next1=slevel{k}

Step 10: if (next1~=0 and big~=0) then

Step 11: if(tv(next1) > tv(big)) then

big=next1

end if

else

break

end if

end for

Step 12: for k=1 to n

slevel{k}=0

end for

Step 13: calling to send1

Step 14: end

The path from source node to sink node are shown in the Fig 5 below. Let us consider an example as shown in Fig 4, where node 22 wants to send data. Its immediate neighbors are 21, 17 and 18. But level o 21 is equal to 22.So a node with lower level to be chosen. Hence it selects a node that has greater trust value from nodes 17, 18 which are in lower node level than that of node 22. In this way, the path to sink node is chosen from node 22 as shown in Fig 5. Here, the arrow shows the path selected to sink node .So the path from source node to base station consist of the nodes 22-17-13-8-4-26 as shown in Fig 5.

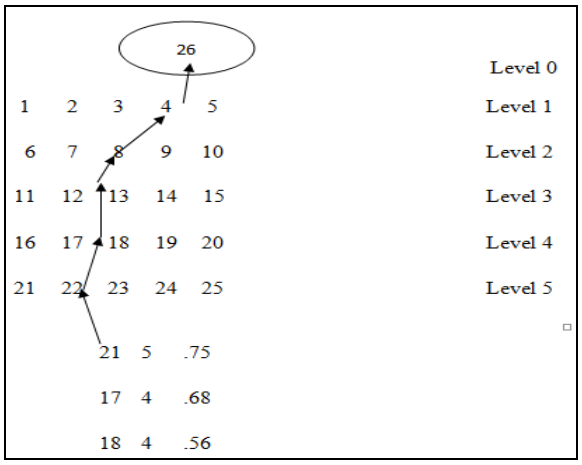

Fig 5: Route selection in a network

C. Malicious Node Detection:

Each time whenever a source sends a packet to the base station, it sends through the path of farray called final array to find the route. Sequence number of each node to which packet transmitted is stored in varray called visited array. Where path is such that , the first and the last node in varray for each individual node is the source and base station. While in case of malicious node, path is broken and any intermediate node be at the place of base station .If the last node on the route of source is replaced by any other node, rather than the base station then that replaced node is malicious one.

5. RESULTS AND DISCUSSION

5.1. Simulation Model:

In the proposed system, field size of 25x25m^2, where 50 nodes have been deployed randomly. There is a single base station located on the field. The detection range of each sensor is 7 meter. Each node has an initial energy of 100 micro Joules. All the energy parameters are given below.

Table 2: Energy parameters for wireless sensor network

Operation	Energy Dissipated
Transmitter Electronics (ETX) Receiver Electronics (ERX)	50 Nj/bit
Transmit Amplifier(Efs)	100 pJ/bit/m^2

5.2. Performance Metric

The metrics considered for comparison are Energy left and packet delivery ratio in presence and absence of malicious node. The transmission and receiving energy is given by:

$$Et1 = ETX * (CM + DM) + Efs * (CM + DM) * d * d \quad .....(1)$$

$$Energy(n) = Energy(n) - Et1 \quad .....(2)$$

$$Er1 = ERX * CM \quad .....(3)$$

$$Energy(n) = Energy(n) - Er1 \quad .....(4)$$

Where d is the distance of transmission, CM and DM are the constants. Efs is the energy dissipated by the transmit amplifier .From the above equation it becomes apparent that in order to reduce transmission energy , sensor node needs to select its next hop based on distance .Only those nodes that have sufficient energy can received and further transmit data packet. While those nodes that have not sufficient energy is dead. Dead nodes are shown by red circles and base station is shown by green circle as shown in Fig 6.

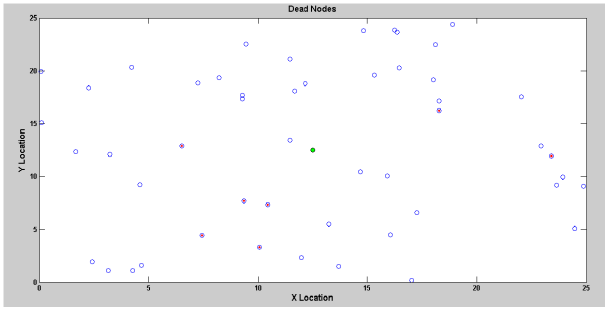

Fig 6: Dead nodes in a Wireless Sensor Network

Packet Delivery Ratio (R): This metrics represents the ratio between numbers of data packets that are received by base station to the data packets sent by the source.

$$Packet\ Delivery\ Ratio = \frac{Packet\ Received\ by\ Base\ Station}{Packets\ Transmitted\ by\ Source}$$

5.3 Simulation Results:

Wireless sensor network have very less lifetime so it is necessary that sensor nodes should consume minimum energy in radio communication. From the result given below, it is find out that the proposed algorithm takes minimum energy as compared to the existing scheme.

5.3.1 Comparison between energy efficiency in existing and proposed scheme

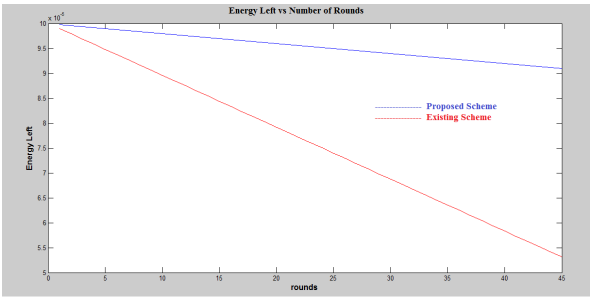

Fig 7: Comparison B/W Energy Left v/s Number of Rounds

5.3.2 Comparison between packet delivery ratio in presence of malicious nodes

In the proposed scheme, four runs have been performed. In the first run the hacker does not interfere with network communications, this is referred to as the normal run.

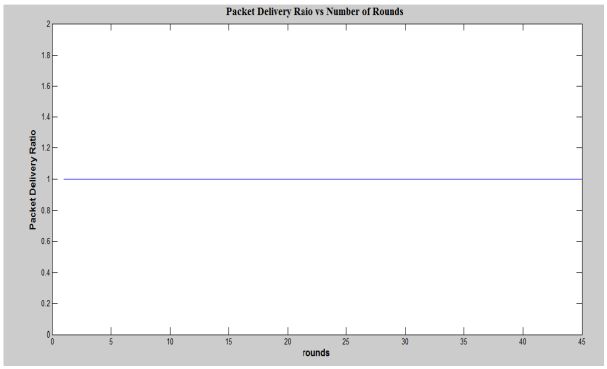

Fig 8: Packet delivery ratio vs Number of rounds without malicious node

In the second, third and fourth run , malicious nodes are incremented in a network .Then packet delivery ratio is compared one by one.

a. Packet Delivery Ratio in the presence of one malicious node

Behavior of the system is observed when malicious node is inserted in WSNs.

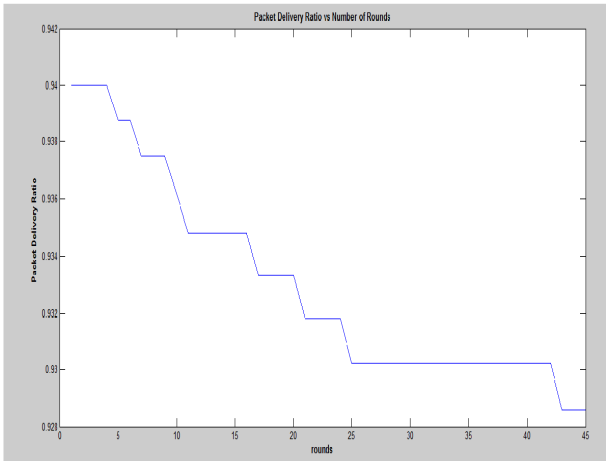

Fig 9: Packet delivery ratio v/s Number of rounds in presence of one malicious node

It found that when no any malicious node is present in the network then number of packet transmitted by source nodes is equal to the number of packets received by base station. Hence no any packet drop is there. After inserting a single malicious node in a network, packet delivery ratio drops.

b. Packet Delivery Ratio in the presence of two malicious nodes

Here two malicious nodes are inserted in a wireless sensor network .Then the packet delivery ratio is compared in different rounds to find out the behavior of the system.

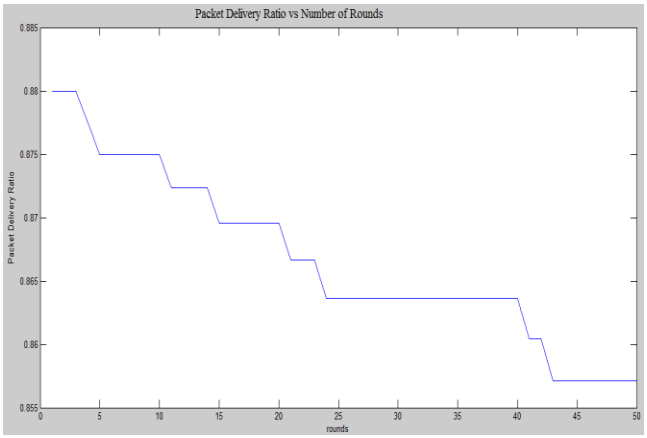

Fig 10: Packet delivery ratio v/s Number of rounds in presence of two malicious nodes

c. Packet Delivery Ratio in the presence of four malicious nodes

Behavior of the system when number of malicious nodes are increased from two to four is shown in Fig 11.

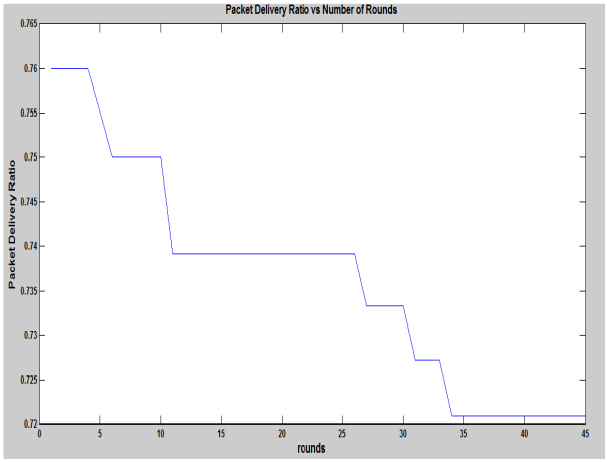

Fig 11: Packet delivery ratio vs Number of rounds in presence of four malicious nodes

As the number of malicious nodes is increased, packet delivery ratio starts decreasing as shown in Fig 10 and Fig 11.

5.5.3 Comparison between packet delivery ratio in existing and proposed scheme

Existing scheme is based on shortest distance where shortest path is found from source node to the base station and packets are forwarded through that path. In proposed scheme, packets are transmitted on the path of final array. Final path from source to he base station is derived based on the level and trust value of each node. When no any malicious node is inserted in a network then packet delivery ratio is one for both the scheme. But as soon as malicious nodes are increased in a wireless sensor network correspondingly decrease in packet delivery ratio as discussed above. Now the packet delivery ratio in the presence of malicious nodes is compared between existing and proposed scheme as shown in Fig 12.

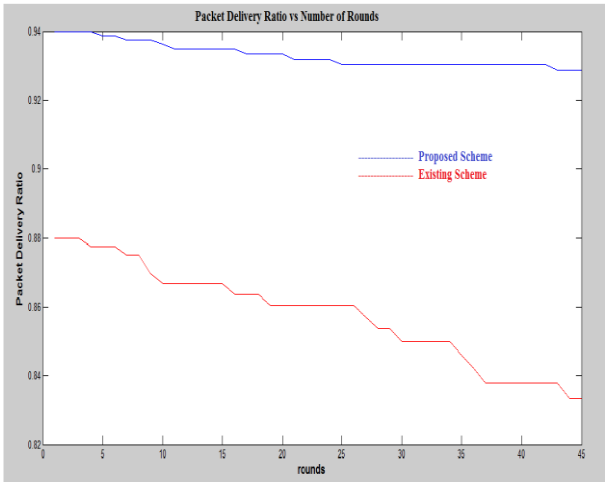

Fig 12: Comparison B/W Packet delivery ratio v/s Number of rounds in presence of malicious nodes

It is found that packet delivery ratio in proposed scheme is larger as compared to existing scheme in presence of malicious node.

5.3.4 Comparison between packets drops in existing V/S proposed scheme

Packets are transmitted on shortest path that is totally derived from the distance between different nodes. While in proposed scheme it is based on level and trust value of a node.

a. Number of packets transmitted by nodes

Packets transmitted by nodes against number of rounds in case of existing and proposed scheme are shown in Fig 13.

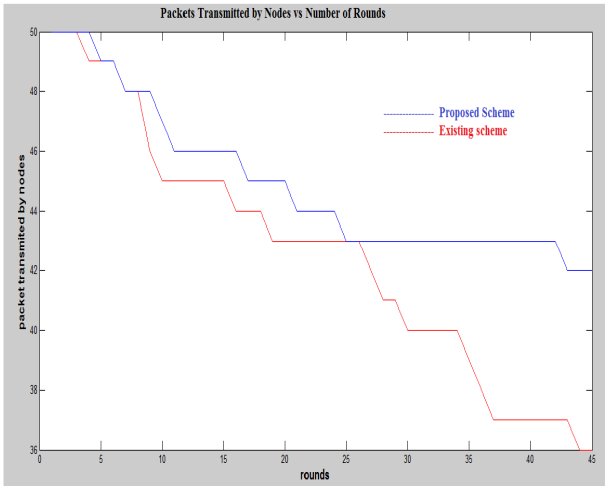

Fig 13: Comparison of packets transmitted v/s number of rounds

It is found that only 36 packets are transmitted in the 45th round in case of existing scheme as compared of proposed scheme which are 43 as shown in Fig 13. While packets received by base station in existing scheme at the end of 45th round is 30 much smaller than proposed scheme which is 39 shown in Fig 14.

b. Number of packets received by base station

Packets received by base station in case of existing and proposed scheme are compared to find out which one is better as shown in Fig 14.

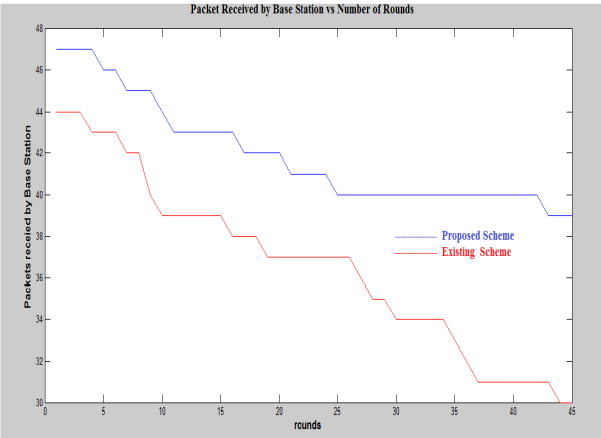

Fig 14: Comparison B/W packets received by base station v/s rounds

Packet drop in the first round in existing scheme is six, while in case of proposed scheme its value is three only. Packet drop is more in case of existing scheme as shown in Fig 14. Hence proposed scheme is better than existing scheme.

6. CONCLUSION

The proposed work described multi level secure routing scheme for detecting selective forward attack. This scheme is centralized in which detection is implemented in the base station. This scheme is reactive also, which finds the path and send the packets dynamically .The proposed scheme is compared with the existing scheme and it is found that packet delivery ratio in the proposed scheme is much higher as compared to existing scheme in the presence of attack .It is also found that proposed schemes saves much more energy as compared to existing scheme .Thus Proposed Scheme effectively detect the attack and saves energy also.

7. REFRENCES

[1] Padmavathi, Dr G. and Mrs Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks", arXiv preprint arXiv:0909.0576 (2009).

[2] Kalita, Hemanta Kumar and Avijit Kar, "Wireless sensor network security analysis", International Journal of Next-Generation Networks (IJNGN) 1.1 (2009): 1-10.

[3] Bysani, Leela Krishna and Ashok Kumar Turuk, "A survey on selective forwarding attack in wireless sensor networks", Devices and Communications (ICDeCom), 2011 International Conference on. IEEE, 2011.

[4] Karlof, Chris and David Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Ad hoc networks 1.2 (2003): 293-315.

[5] Xiao, Bin, Bo Yu and Chuanshan Gao "CHEMAS: Identify suspect nodes in selective forwarding attacks", Journal of Parallel and Distributed Computing 67.11 (2007): 1218-1230.

[6] Kaplantzis, Sophia, et al. "Detecting selective forwarding attacks in wireless sensor networks using support vector machines", Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on. IEEE, 2007.

[7] Brown, Jeremy and Xiaojiang Du. "Detection of selective forwarding attacks in heterogeneous sensor networks", Communications, 2008. ICC'08. IEEE International Conference on. IEEE, 2008.

[8] Deng, Huijuan, et al. "Selective forwarding attack detection using watermark in WSNs", Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on. Vol. 3. IEEE, 2009.

[9] Xin-Sheng, Wang, et al. "Lightweight defense scheme against selective forwarding attacks in wireless sensor networks", Cyber-Enabled Distributed Computing and Knowledge Discovery, 2009. CyberC'09. International Conference on. IEEE, 2009.

[10] Li, Guorui, Xiangdong Liu and Cuirong Wang. "A sequential mesh test based selective forwarding attack detection scheme in wireless sensor networks", Networking, Sensing and Control (ICNSC), 2010 International Conference on. IEEE, 2010.

[11] Anthony Wood and John A. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, 35(10):54-62, October 2002.

[12] W z khan, "comprehensive study on selective forward attack".