EVALUATING PURE NODES IN WIRELESS SENSOR NETWORKS

Jenifer.G[1], Ramya Dorai.D[2]

[1]*PG Scholar, Department of CSE, Adhiyamaan College of Engineering, Hosur,(India).*

[2]*Associate Professor, Department of CSE, Adhiyamaan College of Engineering, Hosur,(India).*

ABSTRACT

Sensor nodes perform continues monitoring of the event and gathers information regarding event and forwards to central authority which further process the event. If any node in the network is concedes for malicious attack then whole network will be fails. In this paper we proposed simple ordering algorithm and shares token messages for classifying nodes based on their performance of forwarding information from one node to the other node. According to this ordering mechanism each node will undergo three stages of ranking based on the rank pure nodes are identified and thus information is handled through pure nodes present in the network. Extensive analysis and simulations have been conducted to verify the effectiveness and efficiency of the scheme.

Keywords: ***Concede, Ordering, Malicious, Pure Node, Ranking.***

I INTRODUCTION

In wireless sensor networks the nodes are deployed to monitor the vast unattended environment and sense the medium gathers information and forwards to the sink. Sink may act as a central authority who control over the detection process and produces report depending upon their behavior. Based on the behavior it selects the un -concede nodes for forwarding the packet from the source to the destination. Most often the sensor nodes are compromised and lead to the in network disruption. Sensor nodes are affected by various attacks but here we are going to consider droppers and modifiers of the information in the network. So detection of pure nodes is most important task in deploying sensor networks in unattended environment. Pure nodes can be detected by using ordering algorithm. In this ordering algorithm each individual nodes undergoes three stages of ranking process and finally pure nodes can be identified in the network. This pure node information is stored in the sink which acts as a central authority for the whole. Sink determines the path for transmitting information from source to destination. Once pure node is identified in the network then forwarding the information takes place. Bad nodes are dropped in this ordering process.

II PROPOSED WORK

Proposed work is sending a token message between pair of nodes in order to ensure authenticity between nodes. The following activity diagram shows how bad nodes are eliminated by using sharing of token message

Proposed work can be carried by the following figure.

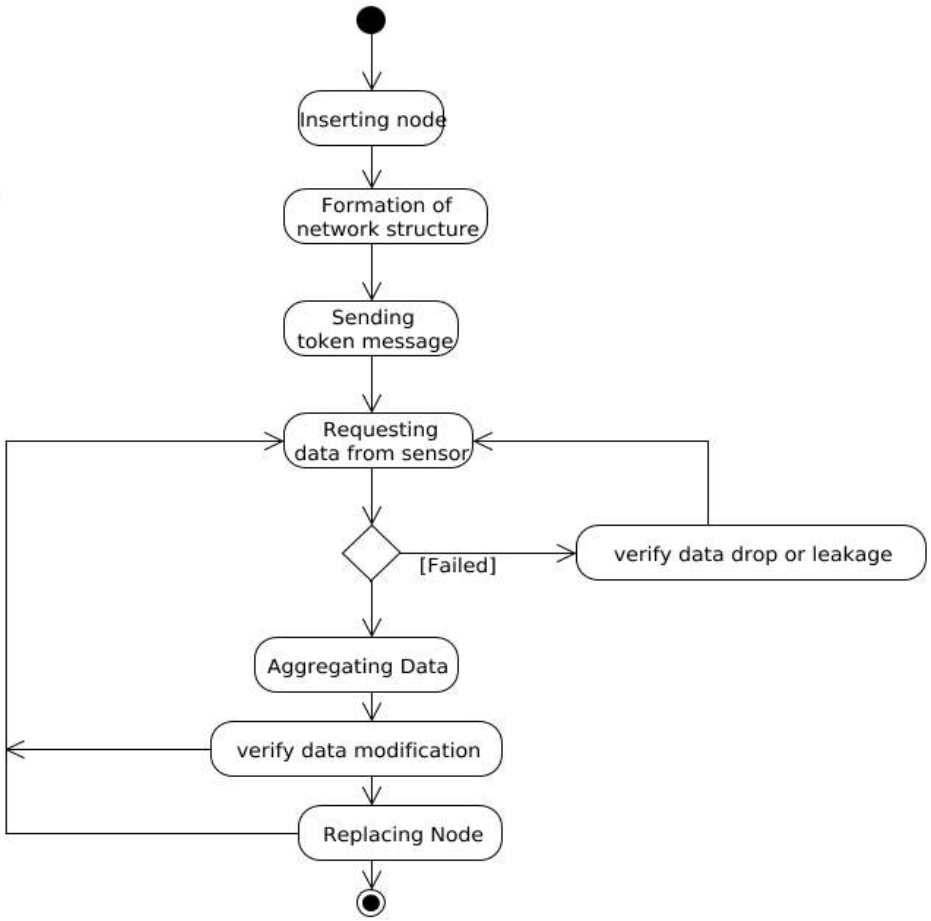

Fig 1: Flow Graph

This flow graph shows how token messages are used to eliminate bad nodes from the network.

III DISTRIBUTION OF NODES

This distribution phase explains how the nodes are arranged as a network and information transmission takes place between them. The below figure 2 shows how nodes are deployed as network and source destination and sink are established. Once they are established packet or information are started to transmitted between source and destination if any malicious act of node is identified then whole network undergoes three types ordering in-order to identify pure node for transmission.

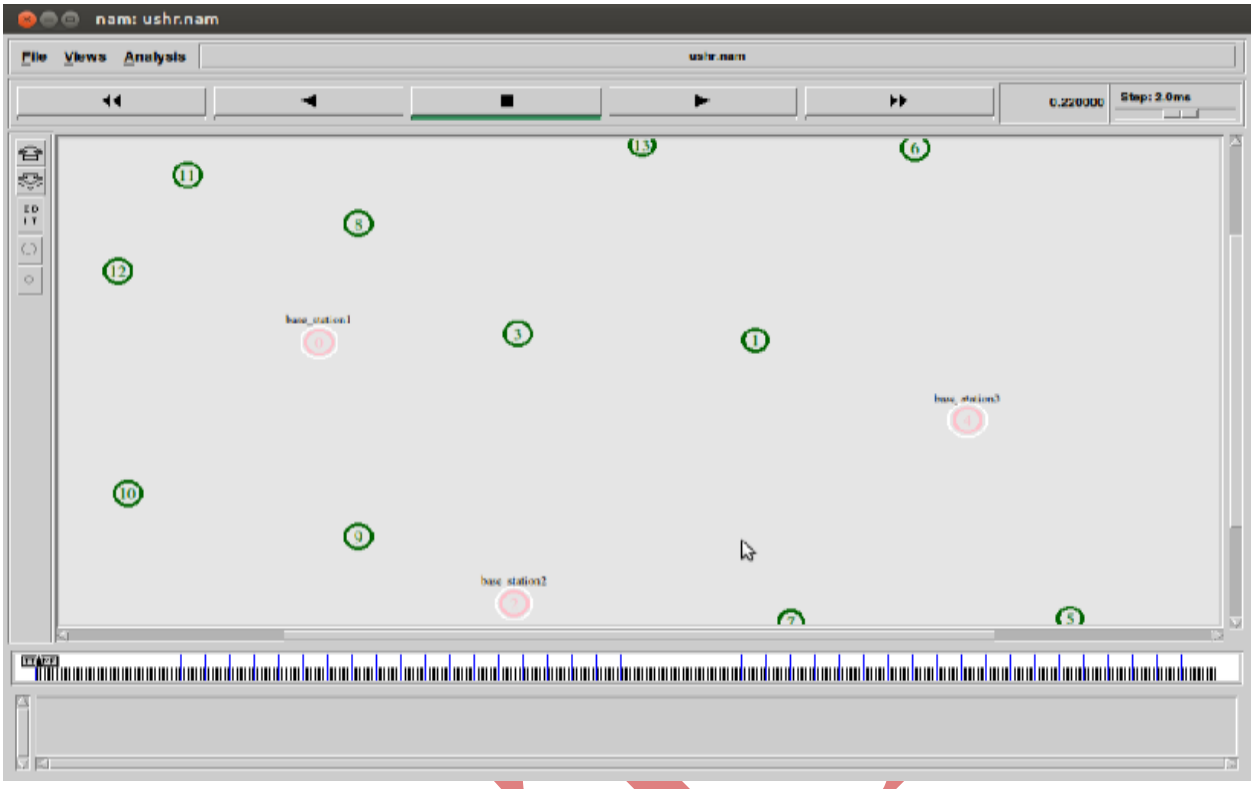

Fig 2: Distribution of Nodes

IV PURE NODE SELECTION

The selection of pure nodes involve in the following steps.

1. Packet transmission
2. Identify bad nodes
3. Evaluating pure nodes.

4.1 Packet Transmission

Once nodes are deployed in the network transmitting of packets are starts from sender node to the receiver node. The packet which is send by sender node is sealed with token message in it and it is forwarded to the neighbour nodes. Neighbour nodes verify the token message and check the sender node is intended sender or not and stores the packet in their forwarding table. The fig 2 explains how packets are transmitted from sender node to neighbour node along with token message.

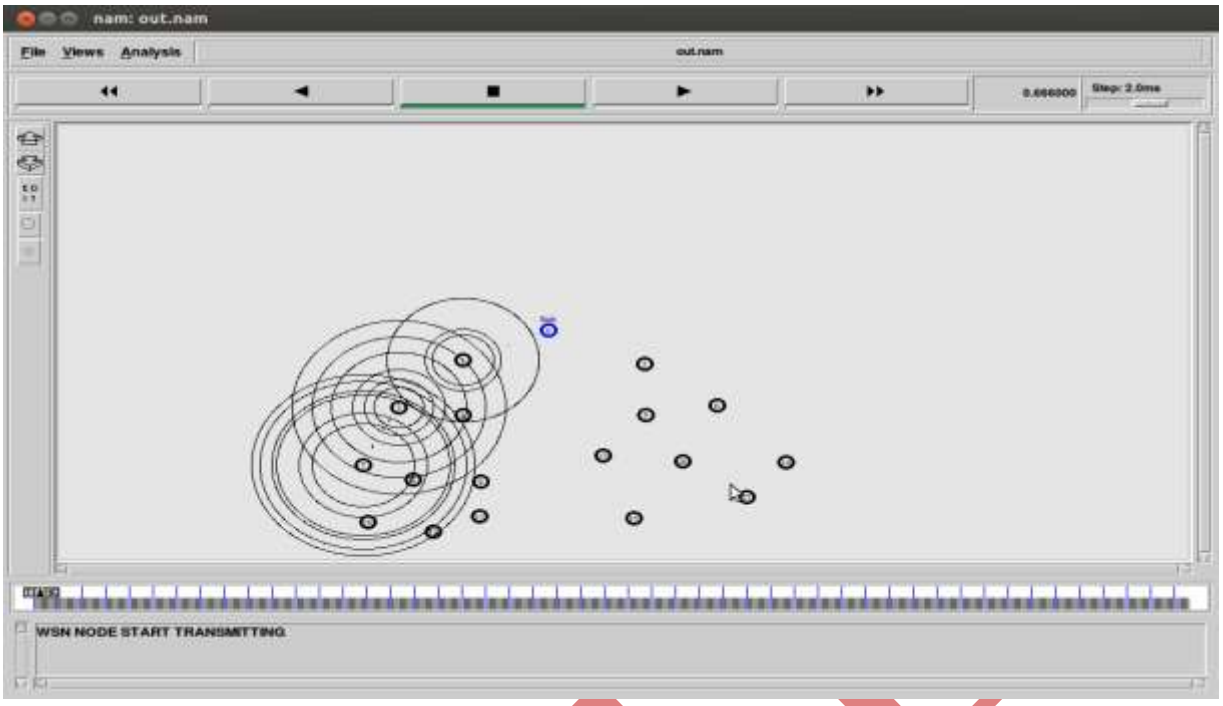

Fig 3: Packet Transmission

4.2 Identify Bad Nodes

Once packet transmission started all the nodes in the network will start involve in transmission. The identification of bad nodes will be processed by using RC5 algorithm. The main reason for nodes to act as bad node is to save battery power the most important constraint of sensor node because commonly sensor nodes are deployed in large unattended environment so nodes will drop the packet which is supposed to be transmitted.

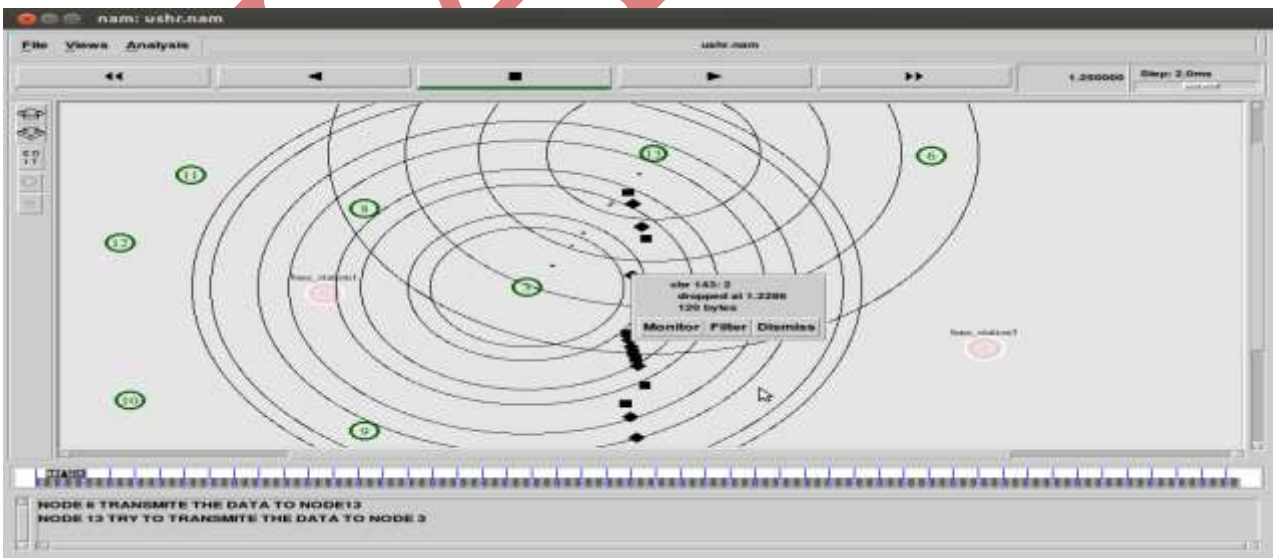

Fig 4 : Packet Drop

In this fig 4 node 13 starts dropping the packet which is supposed to forward to its neighbour. Continues monitoring of node 13 takes place. After certain time if it's still keep on dropping the packet then node 13 is marked as dropper in the network.

Fig 5: Dropper Identified

From fig 5 once dropper is found and labelled communication between dropper node and all other node in the network is stop.

4.3. Evaluting Pure Node

Pure nodes can be evaluated by using ranking algorithms these ranking algorithm consists of following scheme [11].

1. Universal ranking scheme
2. Iterative ranking scheme
3. Hybrid ranking scheme

4.3.1 Universal Ranking Scheme

Once deployment of nodes in the network had over the ranking of nodes takes place. First scheme of ranking is universal in this universal ranking method all participating nodes are provided with rank based on their performance of forwarding packets from the source to destination. This is the first stage of screening bad nodes in the network. The algorithm for universal ranking scheme as follows

ALGORITHM 1:

1: Sort all suspicious nodes into queue Q according to the descending order of their accused account values

2: $S \leftarrow N$

3: while *n*

i=1 *Si* = *N* do

4: *u* ← *deque*(*Q*)

5: *S* ← *S N {u}*

6: remove all *u*, *N* from *n*

i=1 *Si*

In this algorithm, S_i is the set of nodes in the network and u is the suspicious node which is further checked with the accused account in the network.

4.3.2 Iterative Ranking Scheme

Nodes that are processed by universal ranking scheme is then further processed by iterative ranking algorithm. The main purpose of the iterative ranking is to reduce false positive ratio . The algorithm is as follows

ALGORITHM 2:

1: *S* ← *N*

2: while *n i*=1 *Si* = *N* do

3: *u* ← the node has the maximum times of presence in

*S*1, · · · , *Sn*

4: *S* ← *S {u}*

5: remove all *u*, from *n*

i=1 *Si*

by using this algorithm false positive of nodes get reduced .

4.3.3 Hybrid Ranking Scheme

Hybrid ranking scheme is the combination of both universal and iterative algorithm. The algorithm helps to find out collusion among the participating node and reducing it. The algorithm is as follows

ALGORITHM 3:

1: Sort all suspicious nodes into queue *Q* according to the descending order of their accused account values 2: *S* ← *N*

3: while *n i*=1 *Si* = *N* do

4: *u* ← *deqeue*(*Q*)

5: if there exists u, $N<n$

i=1 Si then

6: $S \leftarrow S\{u\}$

7: remove all u, N from n

i=1 Si

by using this algorithm collusion among nodes are identified and reduced

V CONCLUSION

In this paper we concluded three ranking scheme for identifying pure nodes among n nodes participating in communication network. This ranking scheme also used to identified the droppers and modifiers which disturbs the in network communication of the network. Extensive analysis and simulation will improve the performance of the algorithm and it can be used for large communicating networks.

REFERNCES

[1] Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang, "Catching packet droppers and modifiers in wireless sensor networks", IEEE TRANSACTION on parallel and distributed computing, vol 23 no 5, may 2012.

[2] M.Kefayati, H.R Rabiee, S.G.Miremadi and A.Khonsari, "Misbehavior resilient multipath data transmission in mobile ad hoc networks," ACM SASN,2006.

[3] R.Mavropodi,P.Kotzanilolauo and C.Douligeris, " Secmr- a secure multipath routing protocol for ad hoc networks", vol 5, no 1,2007.

[4] I.Khalil and S. Bagchi, "Mispar: mitigating stealthy packet dropping in locally monitoring multihop wireless ad hoc networks", in SecureComm,2008.

[5]S.Ganeriwal, L.K Balzano and M.B.Srivastva, " Reputation based framework for high integrity sensor networks," ACM TRANSACTION on sensor networks (TOSN), vol 4 no.3,2008

[6] B.Xiao,B.Yu and G.Cao, "Chemas: identify suspects node in selective forwarding attacks," Journal of parallel and distributed computing, vol.67, no 11,2007.

[7] X.Zhang,A.Jain, and A.Perrig, "Packet dropping adversary identification for data plane security," in ACM CONTEXT, 2008.

[8]F.Ye,H.Yang and Z.Liu, "Catching moles in sensor networks," in IEEE ICDCS,2007

[9]N.Vanitha, G.Jenifa , "Detection of packet droppers in wireless sensor network using node categorization algorithm", journal of advanced research in computer science vol 3, issue 3,2009.

[10]RonRivest"RC5encryptionalgorithm"http://people.csail.mit.edu/rivest/Rivest-RC5.pdf".

[11]G.Jenifer,D.Ramya Dorai, "Ranking Wireless Sensor Networks" International Journal of Engineering Science" volume 3,issue 1,version 2,2014