The International Journal Of Engineering And Science (IJES)
||Volume|| 3 ||Issue|| 01 || Pages || 52-55 || 2014 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Ranking Wireless Sensor Networks

Jenifer.G
PG SCHOLAR, Department of Computer Science, Adhiyamaan College of Engineering, Hosur, Tamil Nadu
Ramya Dorai.D
Associate Professor, Department o f Computer Science, Adhiyamaan College of Engineering, Hosur, Tamil Nadu

ABSTRACT

Wireless sensor network are often deployed in unattended and vast environment for monitoring the environment and sending information to base station. If any node in the network is compromised then the whole working of the system is collapse and lead to the failure of the network. In our proposed scheme ranking of nodes take place based on the rank node can be identified for malicious and that can be removed. This ranking is made through three stages like global ranking, stepwise ranking and hybrid ranking. The extensive analysis and simulation can be carried by ns2 to verify effectiveness and efficiency of the network.

Keywords- *collapse, heuristics, sensor node*

Date of Submission: 06 January 2014 Date of Acceptance: 15 January 2014

I. INTRODUCTION

The Wireless sensor network consists of sensing node and sink. They are deployed in unattended and vast environment. The purpose of such node is to sense medium and gathers information and forwards that information to base station or central authority that controls all nodes in the network. The most important constraint of sensor node is to retain battery power for long time because replacement of battery is very cost effective and also hard. Hence some of the nodes in the network will act selfish and intentionally drops the packet which is supposed to forward to next node in the network in order to save energy and also some nodes maliciously modifies the content of the packet by simply compromising the innocent nodes. This is known as security attack. To avoid these two kinds of attack we need to provide rank to all nodes present in the network. By providing rank to nodes each node undergoes three heuristics process in order to provide rank and remove the malicious and compromised node in the network. The proposed heuristics ranking algorithm are used to categorize nodes in the network. The algorithm is of three kinds universal ranking, iterative ranking, hybrid ranking. Thus the effectiveness and efficiency of the network can be verified by using network simulator2(NS2) tool.

II. PROPOSED METHOD

Proposed method of providing ranking to nodes can be explained by using figures. Let’s consider the general deployment of nodes in the network and then by implementing our ranking schemes how nodes are ranked in the network. This ranking scheme is of about four phases.

1. Deployment phase
2. Universal ranking phase
3. Iterative ranking phase
4. Hybrid ranking phase

1. **DEPLOYMENT PHASE:**

In the deployment phase all nodes are positioned in the network. Locating nodes in the network is the first stages of deployment nearly 17 nodes are taken as a network. Identifying the source and destination node for transmitting and receiving the packet through intermediate nodes.

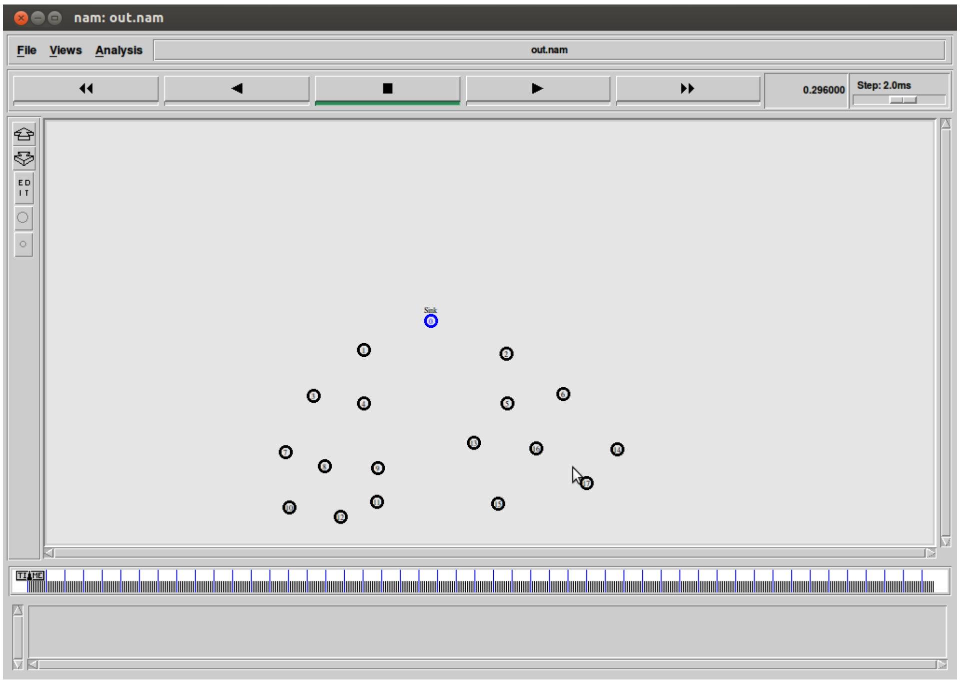
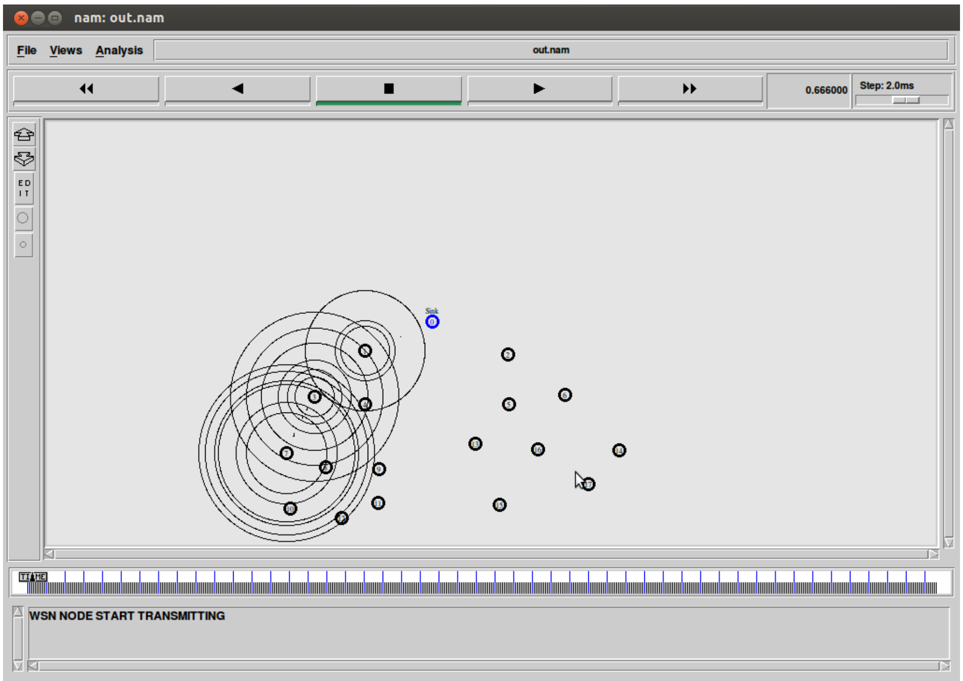


Fig 1: sensor network.

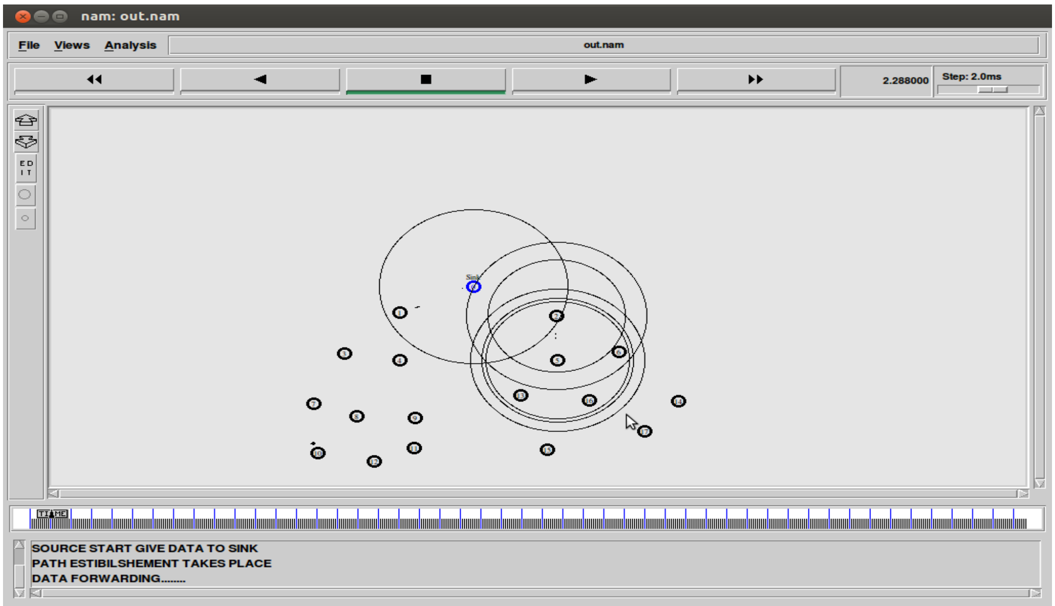
The fig 1shows a set of sensor nodes involved in the transmission and forms the network. The packet transmission in the network is carried by sensing the neighbors and gathers information about node and starts transmitting the packet.



WSN NODE START TRANSMITTING

Fig 2 packet transmission from source

From the fig 2 it shows source node 1 starts sending packet to the destination node 17. Initially source node start sensing its neighbor for forwarding packet to the destination in this figure nodes start sensing and sink establishment also occurs.



```
SOURCE START GIVE DATA TO SINK
PATH ESTIBILSHEMENT TAKES PLACE
DATA FORWARDING........
```

Fig 3 packet forwarding to destination

Once neighbor information is gathered then source node starts transmitting the packet to destination. The purpose of sink is to determine the path between source and destination.

III. 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: $u \leftarrow deque(Q)$
5: $S \leftarrow S\ N\ \{u\}$
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.

IV. 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 are as follows

ALGORITHM 2:

```
 1: $S \leftarrow N$
2: while $n$ $i$=1 $Si = N$ do
3: $u \leftarrow$ the node has the maximum times of presence in
$S1, \cdots , Sn$
4: $S \leftarrow S\ \{u\}$
5: remove all $u$, from $n$
$i$=1 $Si$
```

by using this algorithm false positive of nodes get reduced .

V. 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 are as follows

ALGORITHM 3:

```
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: $u \leftarrow deqeue(Q)$
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.

VI. 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.

REFERENCES

[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 V.Bhuse,A.Gupta

[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.