APTIKOM Journal on Computer Science and Information Technologies
Vol. 1, No. 3, 2016, pp. 141~148
ISSN: 2528-2417
DOI: 10.11591/APTIKOM.J.CSIT.28

Detection of Compromised Nodes in Wireless Sensor Networks using GPSR Protocol and Iterative Filtering Algorithm

R. Ramalakshmi*, S. Subash Prabhu, C. Balasubramanian
Department.of CSE, P.S.R.R college of Engg, Sivakasi, India
*Corresponding author, e-mail: rlakshmi.cse70@gmail.com, subash.infotech@gmail.com, bala@psrr.edu.in

Abstract

The sensor network is used to observe surrounding area gathered and spread the information to other sink. The advantage of this network is used to improve life time and energy. The first sensor node or group of sensor nodes in the network runs out of energy. The aggregator node can send aggregate value to the base station. The sensor node can be used to assign initial weights for each node. This sensor node calculates weight for each node. Which sensor node weight should be lowest amount they can act as a cluster head. The joint node can send false data to the aggregator node and then these node controls to adversary. The dependability at any given instant represents an comprehensive behavior of participate to be various types of defects and misconduct. The adversary can send information to aggregator node then complexity will be occurred. These nodes are used to reduce the energy and band width.

Keywords*: Sensor network; Collusion attacks; Compromised node.*

1. Introduction

Wireless sensor network consists of individual node that are capable of interact with their environment by sensing or controlling physical parameters. These node have to collaborate physical task. Wireless sensor can be used to real world application the single technical solution encompasses entire design space. The roles of participants in wsn are source node and sink node. The source of node is the process of measure data or reports them and sink node can receive the information. They can be used to external entity and PDA, gateway. The deployment options of a wireless sensor network are random deployment and regular deployment. The random deployment is the process of sensor node deployed in random manner and regular deployment is used to the sensor node deployed in geographical area. The characteristic of wireless sensor network is the fault tolerance, life time, scalability, quality of service. The fault tolerance is the each sensor node operates in a battery power. The communication will be failure they can use to redundant node. The redundant node can avoid duplications. The redundant node is used to handle previous node. The sensor nodes are used to improve network life time. The scalability is the process of extent with node density, number and kinds of networks. The quality of service is sensor node should be quality one and energy efficient. The fraction of time to send information to sink node. They can be used to check information will be send correct source or not.

2. Related Works

The secure data aggregation [1] focus an sensor node are deployed in the hostile environment the sensor node are divide into the cluster .The cluster can send information to base station. The each sensor is based on the distance of readings of such a sensor from estimate of correct value. The each sensor node can assign initial weight. The weight will be compared of each node which node will be lower weight that node act as a cluster head. The remaining node can send information to aggregator node. The cluster head send information to base station. The sensor node are deployed in the hostile environment the sensor node are divide into the cluster .The cluster can send information to base station. The collusion attack occurred.

Received Aug 24, 2016; Revised Oct 21, 2016; Accepted Oct 26, 2016

The greedy perimeters stateless routing protocol is used location identify. The attacker high level knowledge about the data aggregation algorithm and it's parameter. They can conduct IF algorithm

2.1. Data Aggregation

The S.Ozdemir presents "Secure data aggregation in wireless sensor networks" the data aggregation is the process of summarizing combining sensor data [5]. In order to reduce the amount of data transmission in the network. They can be used to improve energy and bandwidth. It is used to tree based data aggregation protocol and cluster based data aggregation protocol. The tree based data aggregator protocol is used to construct energy efficient tree. The tree based data aggregator protocol is used to construct energy efficient tree. The cluster based data aggregation protocol is used to GIT, SPT.The GIT is the greedy incremental tree compared to other data centric routing scheme. The SPT is used parent selection of sensor node. The compromised node detection will.

2.2. IF Algorithm

The E.Ayday, presents "An iterative algorithm for trust and reputation management". The iterative filtering algorithm and reputation management techniques used to averaging scheme cluster approach [9]. The generic must and reputation model is used to specific characteristics they can be used to punish and reward method. The first parameter is the client who is requested and find most trustworthy or reputable server. The gathering information is used to path leading. The candidates to be selected as service providers. The score and ranking is used to receive the in formations. The performance transaction is used to evaluating satisfaction with received services.

2.3. Iterative Refinement

The P.Laureti, presents iterative filtering vs. iterative refinement algorithm is used to checking malfunction or misbehaves [10]. The cheating behavior will be increased the reputation is so much damaged by her misbehavior node. The entire network performance will be decreased.

2.4. Robust Ranking Algorithm

The correlation based ranking algorithm is used to two kinds of rating [8]. The random rating spamming techniques is used to sensor node are deployed in the random manner. The push rating spamming is used to maximum or minimum allowable of rating items. The push rating spamming is used to maximum or minimum allowable of rating items. The positive correlation and negative correlation is used to it.

The positive correlation is the degree in the value of one variable will be predicted in the same direction in the second variable. The data will be changed in the same direction. The negative correlation is used to degree in the value of one variable will be changed in the opposite directions. In this paper trust and reputation system is used to credential based trust management .They can be used to identification of node the will be access in a restriction.

3. System Description

The secure data aggregation techniques used to tree topology. The tree topologies are used to type of network topology that includes three specific levels in a topology hierarchy.

3.1. Tree Topology

This involves variety of single nodes connected to central node. Each node in a hierarchy level has point to point links with each neighboring node on its below level. The drawback of the tree topology is used to entire system can be crippled by any damage or failure of primary node. Figure 1 shows system architecture.

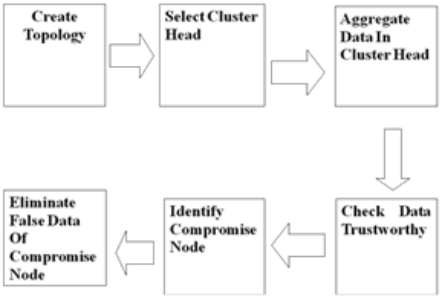


Figure 1. System Architecture

3.2. Weight Factor Assign To Each Source

In this module the weight factor is assigned to each source in the network. The individual id specifies the node location by allocate weight factor to each node. Each node is specific by their locality by transfer weight factor. The allocate of weight factor is based on the liveliness need in any form of network.

3.3. Cluster Formation

The cluster head formation is the process of first step, indiscriminately select c cluster head with their xi, yi coordinates. Then calculate the distance between each sensor node and the arbitrarily selected cluster head and also get the energy of each node. In the next step, re-compute the cluster head by using cancroids method. The sensor nodes which have the minimum distance from the cancroids point is a new cluster head.

3.4. Secure Data Aggregation

The hierarchical secure data aggregation is used to join the data from different source, transmit it with the elimination of the duplication and thereby reducing the number of transmissions and also saves energy. The inbuilt duplications in the raw data gathered from various sensors can be banned by the in-network data aggregation.

3.5. Collusion Attack With False Data

The Collusion attack scenario is used to visualization techniques. In scenario 1, all sensors are dependable and the result of the IF algorithm is secure to the significant value. In scenario 2, adversaries compromises two sensor nodes, and change the readings of these values such that the simple average of all sensor readings is slanted towards a lower value. In scenario 3, is used to computes the slanted value of the uncomplicated average of all sensor readings and information the third compromised sensor to report such slanted average as its readings.

4. Implementation

In this module the weight factor is assigned to each source in the network. The individual id specifies the node location by allocating weight factor to each node. Each node is specifies by their location by assign weight factor. The distribution of weight factor is based on the liveliness need in any form of network. In this module the number of nodes connected into the network can also be identified.

The secure data aggregation techniques can be used to weighted average techniques. In first module used to the five coefficient values are set as follows: $p1$=0.5, p2=0.1, p3=0.05, p4=0.05 and p5=0.3.Where the summing up of the weights is equal to 1. For this example, of the proposed algorithm proceeds.

Step1

The neighbors of every sensor node *v* are search and its degree *dv* is obtained.

Step2

The degree difference of every node *v* is computed formula

$$\Delta v = |dv - M| \quad (1)$$

Step 3
The sum of the distances *Dv* between an SN and all its neighbors is

$$dv = \sqrt{(x2 - x1)^2 + (y2 - y1)^2} \quad (2)$$

Step 4
The mobility speed *Mv* of every sensor node *v* is calculated. For example, assume in the past 2 time blocks

$$Mv = \frac{1}{T}\sum_{t=1}^{T}\sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2} \quad (3)$$

Step 5
The *Tv* is a cumulative time for a node *v* to act as an application node is obtained.

Step 6
The characteristic *Cv* of every node *v* is derived Assume this example, the Cv constant of amplification *c* is set at 1000.

$$Cv = c * \frac{r1}{E1} \quad (4)$$

Step 7
The combined weight of each sensor node *v* is calculated by the formula.

$$Wv = p1\Delta v + p2Dv + p3Mv + p4Tv + p5cv \quad (5)$$

Step 8
The node with a minimum *Wv* is chosen as the cluster head.

Step 9
Steps 1 to 8 are repeated for processing the remaining nodes until each node is assigned to a cluster.

The cluster head selection process can be used centroid method. The cluster head selection can be used to two phases. The one is set up phase and second is steady state phase.The cluster set up phase is each level divide into the cluster for each level k each node can decide the cluster head for the present surrounding by choosing a nodes randomly.

The node which has the higher energy level will be consider as cluster head (CH). The one cluster is formed and TDMA schedule is fixed for all nodes in cluster by cluster head and data broadcast.

The cluster set up phase algorithm is n is no of sensor node to the base station (BS).
1. For each level k, message transmitted by BS.
2. If (Nodes does not assigned the earlier level and received new message or BS transmit level k=1).
3. Assign level k.
4. End if.
5. End for.
6. BS broadcast hello message, which contains the
in sequence of higher limit and minor limit of each level.
7. Each node estimate the distance from the BS based on received signal strength.

The cluster steady state phase algorithm is used to no of sensor node.
1. for each (node N)
2. if node N has uppermost energy level
3. N become CH.
4. N broadcasts a message for its cluster nodes.
5. Else
6. N becomes a NCH node.
7. N informs the selects CH and become a member of its cluster.
8. End if.

9. for each (CH).
10. CH generate TDMA schedule for each cluster member.
11. Each cluster associate communicates to the CH in its time
12. End for

The hierarchal protected data aggregation is the process of combine the data from different sources, redirects it with the removal of the duplication and thereby reducing the number of transmissions and also saves energy. The inbuilt duplication in the raw data gathered from various sensors can be excluded by the in-network data aggregation.
The collusion attack scenario is used to IF algorithm.
Input: X, n, m;
Output: The reputation vector r;
L ← 0;
W (0) ←1;
repeat;
Compute $r^{(L+1);}$
Compute d;
Compute $w^{(L+1)}$;
L ← L+1;
Compute d;

Where**,** X-Value of sensor node, n–No of sensor nodes, m–No of intervals, L-No of iterations, r-Reputation vector, w-Weight age assigned to each sensor node.

5. Performance Analysis

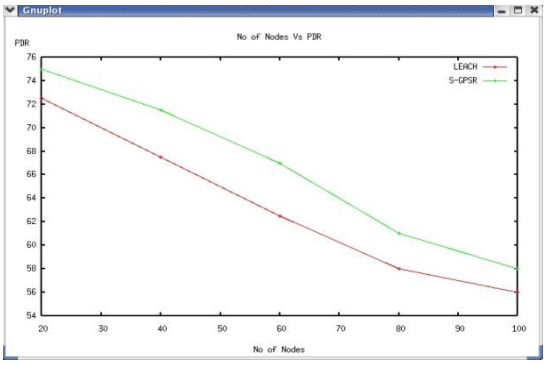
The following metrics are employed for the performance analysis.

5.1. Packet Delivery Ratio

The performance analysis is used to very important factor to measure the performance of the network. The packet delivery ratio is based on the various parameters. The packet delivery ratio is the total number of received packet at destination divide by the total number of send packets. The performance is better and packet delivery ratio is high. Table 1 shows packet delivery ratio.

Table 1. Packet delivery ratio

S.No	No of Nodes (x-axis)	Packet Delivery Ratio (y-axis)
1	20	72.50
2	40	67.50
3	60	62.00
4	80	60.00
5	100	59.50



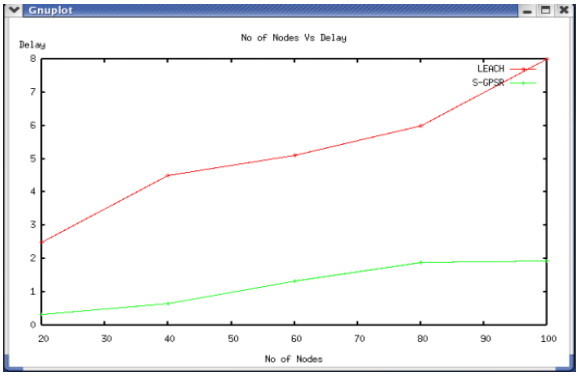
Screen shot 1. Packet delivery ratio

5.2. Average End to End Delay

The average end to end delay is used to destination. The end to end delay computes all message successfully delivered. The distance between source and destination the probability of packet drop decrease. Table 2 shows delay.

Table 2. Delay

S.No	No of Nodes (x-axis)	Delay (y-axis)
1	20	2.50
2	40	4.50
3	60	6.00
4	80	8.00
5	100	10.50



Screen Shot 2. Delay.

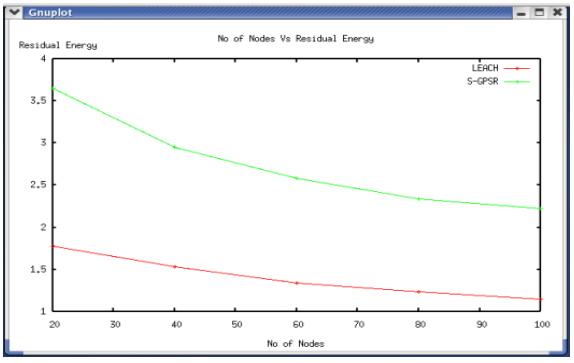
Average end to end delay=∑ (arrive time-send time) /∑ (no of connections).

5.3. Throughput Analysis

The average throughput is used to receive packet size divided by stop time and start time.Average throughput=(received size)/(stop time–start time)*(8/1000). Where, received size=store received packets, stop time=simulation stop time, start time=simulation start time. Table 3 shows residual energy.

Table 3. Residual Energy

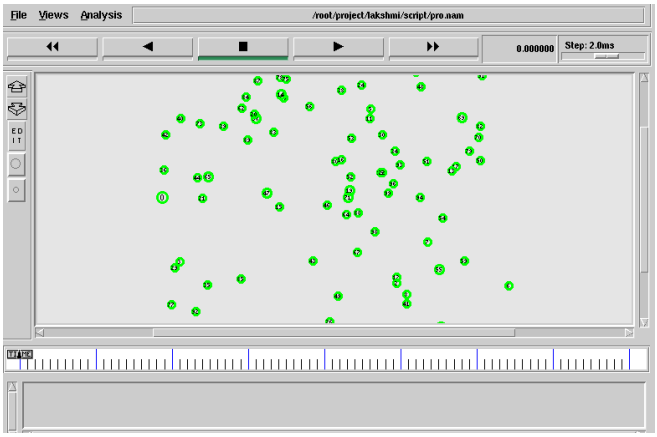
S.No	No of Nodes (x-axis)	Residual Energy (y-axis)
1	*20*	1.78
2	*40*	1.62
3	*60*	1.53
4	*80*	1.45
5	*100*	1.32



Screenshot 3. Residual Energy.

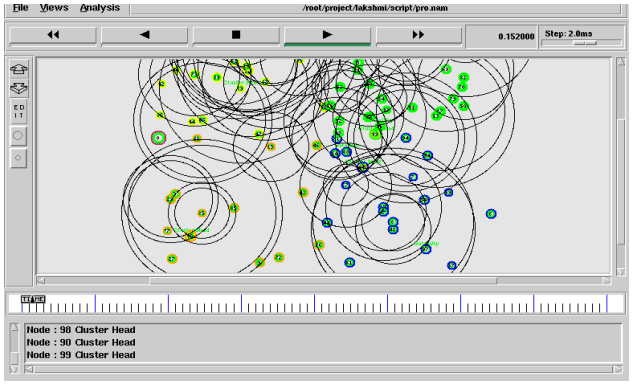
6. Simulation Result

The simulations results show that first of all form a cluster. Thereare four clusters are formed. The every node senses the sensor field and initializes the location of sensor nodes. All sensor nodes get the communications. The dependency on their nearest position connected to each other. This process done in all cluster is shown below,



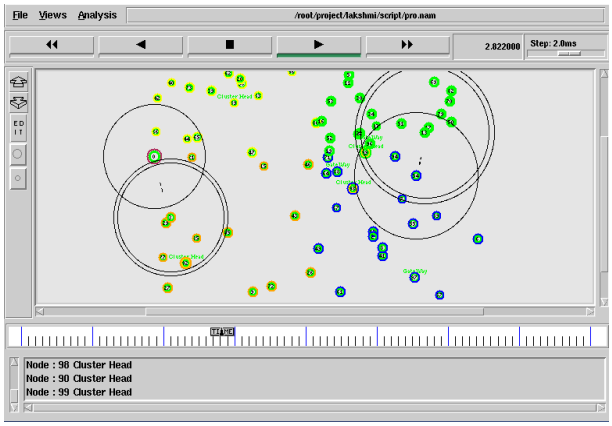
Screenshot 4. Number of Sensor Node

In next step of nodes are connected to each other the process of sending time and receiving time of pending request. The some node is missed due to their long distance. The figure shown below,



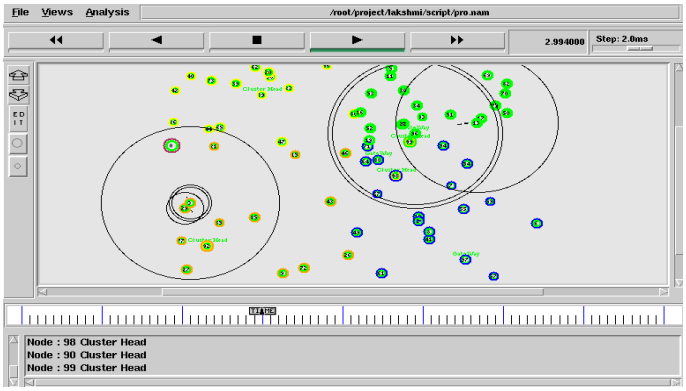
Screenshot 5. Sensor Node Connected to Each other

In next step every sensor node are connected to the cluster head. All data are send to the cluster head.



ScreenShot 6. Sends Data to Cluster Head.

The cluster head can send information to base station. The figure shows below,



Screenshot 7. Cluster Head Send Data to basestation

7. Conclusion

To provide secure authentication for various message transmission in the network. The proposed work is for enhancing the life time of wireless sensor network using IF algorithm. The IF algorithm is used to improve network life time. They can be used to reduce the energy and the system will be energy efficient. WSN are of two types. One is static sensor node and another one is mobile sensor node. In this paper, static node is implemented in WSN and energy is saved, delay is minimized. Same algorithm (GPSR) is used for mobile WSN to save energy, increase packet delivery ratio and to minimize delay.

References

[1] H.S. Lim, E.Bertino And M.Kantarcioglu, "*A Game Theoretic Approach For High Assurance Of Data Trustworthiness In Sensor Networks*," In Pro.IEEE 28th Int. Conf Data Eng., Apr 2012.
[2] Y. Yu "Trust Mechanisms In Wireless Sensor Networks: Attack Analysis And Countermeasures,"*J. Netw. Compute. Appl*.Vol. 35, 2012
[3] L. Shi, K. M. Hou, H. Ying Zhou, And X. Liu, "*Energy Efficient And Fault Tolerant Multicore Wireless Sensor Network: EMWSN*,"In Proc. 7th Int.Conf. Wireless Commun, Netw. Mobile Compute, 2011, Pp. 1–4.
[4] C. De Kerchove And P. Van Dooren, "Iterative Filtering In Reputation Systems*," SIAM J. Matrix Anal. Appl*., Vol. 31, No. 4, Pp. 1812, 1834, Mar, 2010.
[5] S.Ozdemir and Y. Xiao, "Secure Data Aggregation In Wireless Sensor Networks: A Comprehensive Overview," *Comput. Netw*.Vol. 53, No. 12, Pp. 2022–2037, Aug. 2009.
[6] A. Jøsang And J. Golbeck, "*Challenges For Robust Trust And Reputa-Tion Systems*," In Proc. 5th Int. Workshop Security Trust Manage., Saint Malo, France, 2009, Pp. 253–262.
[7] R.Roman, C. Fernandez- Gago, J. Lopez,"Trust And Reputation Systems For Wireless Sensor Networks," In Security And Privacy In Mobile And Wireless Networking, S.Gritzalis, T. Karygiannis, U.K: Troubador Publishing Ltd, 2009 Pp. 105–128.
[8] K. Hoffman,"A Survey Of Attack And Defense Techniques For Reputation Systems," *ACM Compute. Surveys*, Vol. 42, No. 1, Pp. 1:1–1:31, Dec. 2009.
[9] E.Ayday, H. Lee, And F.Fekri, "*An Iterative Algorithm For Trust And Reputation Management*,"Proc. IEEE Int. Conf.Symp. Inf. Theory, Vol. 3, 2009, Pp. 2051–2055.
[10] P.Laureti,Y.-C. Zhang, And Y.-K. Yu, "Information Filtering Via Iterative Refinement," *Europhys. Lett*, Vol. 75, Pp. 1006–1012, Sep. 2009.