Secure Clustering Algorithm for WSN

Poonam Vishal Sadafal, R. H. Borhade

Abstract*—In wireless sensor network, due to the high density of nodes, the redundant data will be detected by neighboring nodes while sensing an event. So energy consumption is key issue in wireless sensor network. In order to save energy all these redundant data will be aggregated at intermediate node and then it will send to sink node. Wireless sensor network has some key constraints such as limited energy resources, lack of infrastructure. All these constraints impose some security challenges. Now days wireless sensor network widely used in many civilian application areas which include environment and healthcare applications, home automation, habitat monitoring and traffic control. Security plays a fundamental role in many wireless sensor network applications. In this paper secure DRINA algorithm is implemented for routing purpose and security is achieved for secure data transmission. DRINA –Data routing in network aggregation, which gives best aggregation quality compared to previous algorithm i.e.InFRA and SPT. [1].

Index Terms*— Wireless Sensor Network (WSN), Data routing for in-network aggregation for WSNs (DRINA), Routing, Clustering, Security.

I. INTRODUCTION

Security plays an important role in wireless sensor network. The development of wireless sensor network was originally motivated by military applications such as battlefield surveillance where the security is main issue. In military sensor network, attackers are attempting to gain and detect as much as information about enemy movement. There are various techniques are used in order to achieve the security in wireless sensor network. So, in this project our aim is to provide security to an algorithm for wireless sensor network. We have chosen most recent clustering algorithm called as DRINA, on that algorithm we are providing security by using RSA and SHA algorithm.

2. DRINA: DATA ROUTING FOR IN-NETWORK AGGREGATION FOR WSNS.

The main goal of DRINA is to build a routing tree and find out the shortest path which connects all source nodes to the sink, while maximizing the data aggregations. In DRINA following roles are consider for building the routing tree.

1. Collaborator: - It is node which detects an event and reports the collected data to the Coordinator node.
2. Coordinator: - It is collaborator node detects an event but after using election algorithm it become a coordinator. This node is responsible for aggregating the collected data received from other collaborator and send results to the sink node.
3. Relay node: This node which is in route between coordinator and sink node, and forwards the data to the sink.

Sink Node: This node is interested in receiving the data from set of coordinator nodes & collaborator node [1].

DRINA algorithm is divided into three phase.

- Building Hop tree from sensor nodes to the sink node.
- Forming Cluster and electing a cluster head among the collaborator which becomes a coordinator.
- Routing means forwarding data towards to a sink node.

II. IMPLEMENTING SECURITY IN DRINA

In all previous clustering algorithms until now security constraints is not considered. Hence there is challenge to perform security on clustering algorithm for security purpose. For example in military, security is main constraint whenever there is need of WSN in military .In this project security is implemented on existing clustering algorithm DRINA.

III. SYSTEM MODEL

Here first of all we are calculating the false data sent by sensing node to the sink node

Let n nodes are attacker in total m nodes so probability of node being attacker is given by

$$P (A) = n/m \qquad (1)$$

Assuming every attacker sends false data, if attacker is coordinator then all data go through attacker is false data, so false data sent is

$$Dfalse = D(FS)+D(FC) \qquad (2)$$

Where

D(FS), Data false send by individual node

D (FC), data goes through attacking coordinator

False Data sent by individual node is given by

$$D(FS) = P (A)*SR = (n/m)*SR \qquad (3)$$

Where,

SR= sensing rate

Probability of attacker as coordinator is given by

$$P(FC) = P(A)*P(C) \qquad (4)$$

Where P(C) is probability of being coordinator

$$P(C) = 1/N \qquad (5)$$

Where N is number of neighbor

Putting (1) and (5) in (4)

$$P(FC) = n/m *(1/N) = n/(m*N) \qquad (6)$$

Probability of attacking coordinator on path of length l is given by

$$Pt(FC) = P(FC)*l = nl/(m*N) \qquad (7)$$

So false data send by coordinator (as data coming from loyal node to attacking coordinator is also falsely forwarded)

$$D (FC) = Pt (FC)*\sum_{K=0}^{N} ((1-P (A)) * SR)$$

$$D(FC)= n1/(m*N) *\sum^{N}((1-n/m) * SR)$$

Manuscript received December 15, 2013.

Poonam V.Sadafal, Dept. of Information Technology Sinhgad Institute of Technology & Science, Narhe, Pune-41, India

Prof. R. H. Borhade, Dept. of Information Technology Smt. Kashibai Navale College of Engg. Vadgaon, Pune, India

$$k=0 \qquad (8)$$

By putting (3) and (8) into (2) we will get total false data sent as

$$Dfalse = (n/m)*SR+ (n1/m*N)* \sum_{k=0}^{N} ((1-(n/m))*SR) \qquad (9)$$

This eq no. (9) Will give us amount of false data sent by coordinator.

In proposed method, data is encrypted before transmitting to sink node as

DT= E(Kps, E(Kp, SD))

Where,

E is public key encryption function

Kps is public key of sink node

Kp is private key of Sensing Node

Because of above encryption attacking coordinator node can't read data and can't send data with other nodes identity. Attacker nodes are still able to send false data, so total false data coming to sink is

$$Dfalse=n/m*SR \qquad (10)$$

This is improved than existing system.

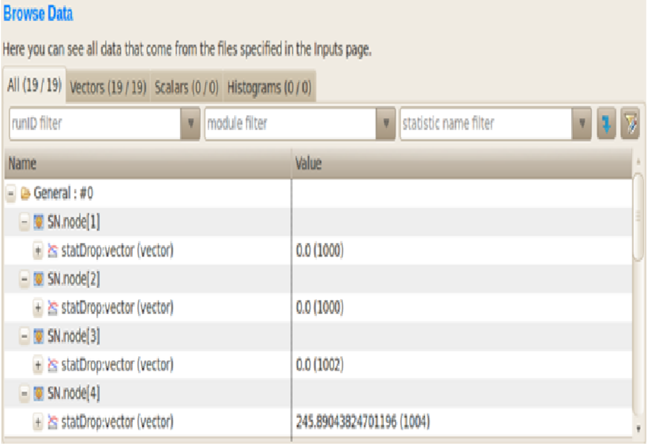
IV. SIMULATION RESULT

The simulation of the algorithm is performed using OMNET++.The nodes are placed randomly in given area. The simulation parameters are shown in Table 1.

Table 1.Simulation Parameter

Parameters	Value
Numbers of nodes	20
Number of Attacking nodes	02
Number of sinks	1
Initial Energy	18720 J
Transmission power	62mW
Receive power	62mW

Fig 5.2 shows the number of false packet detected by nodes. The no. of false packet detected by only those node which are in the already established routing route or which are closer to attacking node.

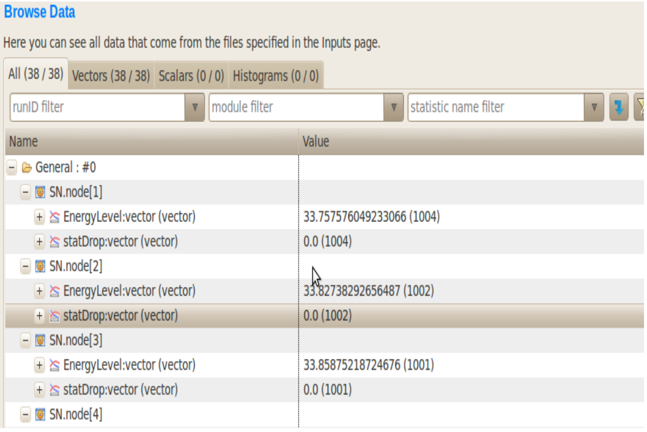


Here you can see all data that come from the files specified in the Inputs page.

Name	Value
General : #0	
SN.node[1]	
statDrop:vector (vector)	0.0 (1000)
SN.node[2]	
statDrop:vector (vector)	0.0 (1000)
SN.node[3]	
statDrop:vector (vector)	0.0 (1002)
SN.node[4]	
statDrop:vector (vector)	245.89043824701196 (1004)

Fig 5.2. False Packet detected by nodes

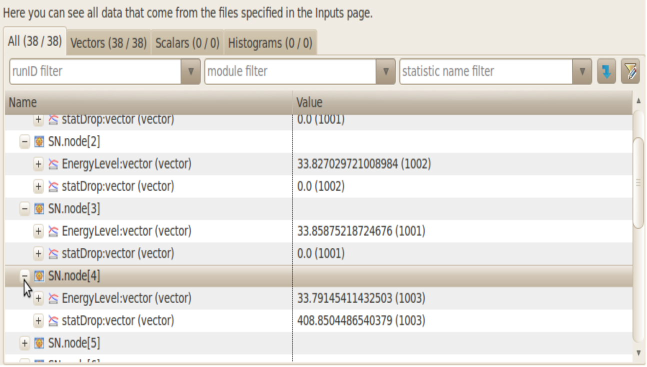
Fig 5.3 & 5.4 shows the comaprative result of existing DRINA and secure DRINA in tems of energy consumed by each node. This result shows that enery consumed by nodes in existing DRINA algorithm is not much varying in secure DRINA.



Here you can see all data that come from the files specified in the Inputs page.

Name	Value
General : #0	
SN.node[1]	
EnergyLevel:vector (vector)	33.757576049233066 (1004)
statDrop:vector (vector)	0.0 (1004)
SN.node[2]	
EnergyLevel:vector (vector)	33.82738292656487 (1002)
statDrop:vector (vector)	0.0 (1002)
SN.node[3]	
EnergyLevel:vector (vector)	33.85875218724676 (1001)
statDrop:vector (vector)	0.0 (1001)
SN.node[4]	

Fig 5.3. Energy level of nodes in Existing DRINA



Here you can see all data that come from the files specified in the Inputs page.

Name	Value
statDrop:vector (vector)	0.0 (1001)
SN.node[2]	
EnergyLevel:vector (vector)	33.827029721008984 (1002)
statDrop:vector (vector)	0.0 (1002)
SN.node[3]	
EnergyLevel:vector (vector)	33.85875218724676 (1001)
statDrop:vector (vector)	0.0 (1001)
SN.node[4]	
EnergyLevel:vector (vector)	33.79145411432503 (1003)
statDrop:vector (vector)	408.8504486540379 (1003)
SN.node[5]	

Fig 5.3.Energy level of nodes in Secure DRINA

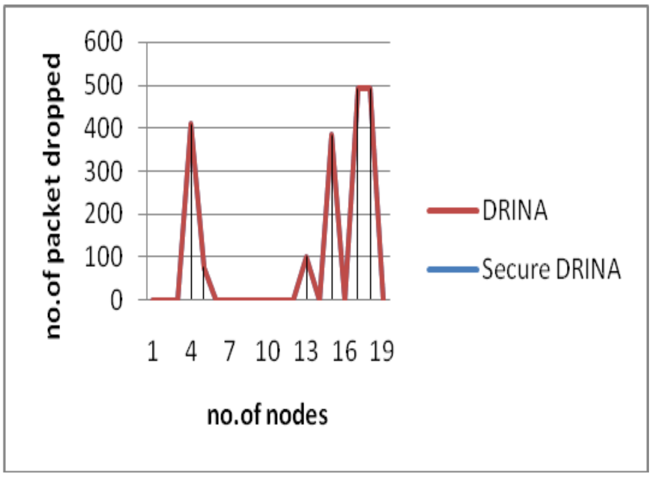


Fig 5.5 the comparative result of existing DRINA and secure DRINA in tems of no.of nodes versus no.of packet dropped.

V. CONCLUSION

Security is main constraint in wireless sensor network. So using RSA and SHA algorithm it is possible to provide security to any routing algorithm.

In this project security is provided to DRINA clustering algorithm in order to achieve two main goals of security which is nothing but confidentiality and Authentication.

REFERENCES

1. DRINA: A Lightweight and Reliable Routing Approach for in-Network Aggregation in Wireless Sensor Networks Leandro Villas1 2, Azzedine Boukerche1, Heitor S. Ramos1 , 2, Horacio A. B. F. de Oliveira3, Regina B. de Araujo4 and Antonio A. F. Loureiro2 ,2012 IEEE.
2. L. Villas, A. Boukerche, R. B. de Araujo, and A. A. F. Loureiro, “Highly dynamic routing protocol for data aggregation in sensor networks,” in Proceedings of the The IEEE symposium on Computers and Communications, ser. ISCC ’10. Washington, DC, USA: IEEE Computer Society, 2010,
3. H. S. AbdelSalam and S. Olariu, “A lightweight skeleton construction algorithm for self- organizing sensor networks.” in ICC. IEEE, 2009, pp. 1–5. [Online]. Available: http://dblp.uni-trier.de/db/conf/icc/icc2009
4. Boukerche, Algorithms and Protocols for Wireless Sensor Networks. Wiley-IEEE Press, 2008.
5. G. Anastasi, M. Conti, M. Francesco, and A. Passarella, “Energy conservation in wireless sensor networks: A survey,” Ad Hoc Networks, vol. 7, no. 3, pp. 537–568, May 2009.
6. Ameer Ahmed Abbasi Mohamed Younis “A survey on clustering algorithms for wireless sensor networks”, Department of Computing, Al-Hussan Institute of Management and Computer Science,Dammam 31411, Saudi Arabia Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, Baltimore, MD 21250, USA ,21 June 2007.
7. Boukerche, R. B. Araujo, and L. Villas, “Optimal route selection for highly dynamic wireless sensor and actor networks environment,” in MSWiM , Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems. NewYork, NY, USA: ACM, 2007.
8. E. F. Nakamura, H. A. B. F. de Oliveira, L. F. Pontello, and A. A. F. Loureiro, “On demand role assignment for event-detection in sensor networks,” in ISCC ’06: Proceedings of the 11th IEEE Symposium on Computers and Communications. Washington, DC, USA: IEEE Computer Society, 2006.
9. Dirk WESTHOFF, Joao GIRAO, “Security Solutions for Wireless Sensor Networks” Amardeo SARMA NEC TECHNICAL JOURNAL Vol.1 No.3/2006 .
10. S. Olariu, Q. Xu, and A. Zomaya, “An energy-efficient self-organization protocol for wireless sensor networks,” in Intelligent Sensors, Sensor Networks and Information Processing Conference (ISSNIP). Melbourne,Australia: IEEE, December 2004.