INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

DRINA: A SECURE CLUSTERING ALGORITHM

POONAM V. SADAFAL, RAHUL C. SALUNKHE

Dept. of Information Technology, Sinhgad Institute of Technology & Science, Narhe, Pune-41

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* Wireless sensor network consist of spatially isolated autonomous sensors to monitor physical or environmental conditions and to considerately pass their data through the network to a sink node. Mostly monitored conditions are temperature, sound, pressure etc. Wireless sensor network have many civilian application areas which include environment and healthcare applications, home automation, and habitat monitoring and traffic control. Security is major concern in all these applications. As the information provided by the networks has been increased, there is a need for secure transmission of information. Most wireless sensor network actively monitor their environment and it is often easy to presume information other than data monitored. There are various clustering algorithm was developed for wireless sensor network for data transmission. However, in all clustering algorithm, the security issues are not consider. In this paper we explore the existing DRINA algorithm along with security mechanism. DRINA is routing protocol which is designed for data aggregation. The key aspect of DRINA is data synchronization among the nodes. In DRINA security constraint is not considered. In order to achieve the security, in this paper we implement the security mechanism in existing DRINA algorithm.

Keywords: Security, clustering, Routing, DRINA, WSN

Corresponding Author: MS. POONAM V. SADAFAL

Access Online On:

www.ijpret.com

How to Cite This Article:

Poonam V. Sadafal, IJPRET, 2016; Volume 4 (9): 874-881

PAPER-QR CODE

INTRODUCTION

Security plays an important role in wireless sensor network. Wireless sensor network was highly motivated by military applications such as battlefield surveillance, where the security is most important. Each time attackers are attempting to gain and detect as much as information about enemy movement in military sensor network. In this paper we have used DRINA clustering algorithm for routing the data and for secure data transmission, we are providing security to it using RSA algorithm.

- Drina: data routing for in-network aggregation for wsn

Energy Consumption is key issue in WSN. In order to save energy redundant data detected by nodes should be aggregated at middle nodes while sensing an event, reducing the size and number of exchanged messages and, thus, decreasing communication costs and energy consumptions. DRINA is routing protocol. The main aim of DRINA is to build a routing tree and discover the shortest path which connects all source nodes to the sink node, while maximizing the data aggregations.

In DRINA following roles of nodes are consider for constructing the routing tree.

1. Collaborator: - The node which detects an event and sends the collected data to the Coordinator node.

2. Coordinator: - a node that also detects an event and is responsible for collecting all the gathered data sent by collaborator nodes, aggregating them and sending the aggregated data to sink node;

3**.** Relay node: It is intermediate node between coordinator and sink node, and forwards the data to the sink.

Sink Node: A node which is involved in getting the data from set of coordinator nodes & collaborator node

DRINA algorithm is divided into three stages.

Constructing Hop tree from sensor nodes to the sink node.

Grouping Cluster and selecting cluster head among collaborator nodes.

Routing the data towards to a sink node

- implementing security in Drina

The main aim of DRINA is to connect all nodes to sink node with shortest path while increasing the data aggregation. However it does not have security mechanism for data transmission. There is a need for secure transmission of information, as the information provided by networks has been increased. Several cryptographic and steganographic techniques are used in order to achieve security in wireless sensor networks. In this paper Secure DRINA algorithm is implemented. To achieve the security in existing DRINA algorithm, 'Public key cryptography' (RSA) algorithm is used and for message digest SHA algorithms is used. The RSA is Public key cryptography algorithm. Using **RSA** algorithm, user can creates the product of two large prime numbers, along with a supplementary value, as their public key. **SHA-1** is a cryptographic hash function which calculates 160 bit hash, value which is expressed as hexadecimal number. Using this two algorithms attacker not able to read and change the data.

- system model

At this point first of all the false data sent by sensing node to the sink node is calculated.

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

P (A) = t/m ………………………… (1)

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

Dfalse = D (FI) + D (FC) ………… (2)

Where,

D (FI), Data false send by individual node.

D (FC), data goes through attacking coordinator.

False Data sent by individual node is given by,

D (FI) = P (A)*SR = (t/m)*SR …… (3)

Where,

SR= sensing rate

Probability of attacker as coordinator is given by

P (FC) = P (A)*P (C) ……………… (4)

Where P(C) is probability of being coordinator

$P(C) = 1/N$ ……………………… … (5)

Where, N is number of neighbor.

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

$P\ (FC) = t/m * (1/N) = t/\ (m*N)$ …… (6)

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

$Pt\ (FC) = P\ (FC)*l = tl/(m*N)$……… (7)

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

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

$$D\ (FC) = t1\ (m*N)*\sum_{k=0}^{N} ((1-t/m)*SR) \ldots (8)$$

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

$$Dfalse = (t/m)*SR+ (t1/\ (m*N))*\sum_{k=0\ldots}^{N} ((1-t/m)*SR) \quad \ldots\ldots\ldots (9)$$

The equation 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 (Kpb, E(Kpr, SD))

Where,

E is public key encryption function

Kpb is public key of sink node.

Kpr is private key of Sensing Node

Because of above encryption, attacking coordinator node can't read data and send data with other nodes identity.

Attacker nodes are still able to send false data, so total false data coming to sink is

Dfalse = (t/m)*SR …………………………… (10)

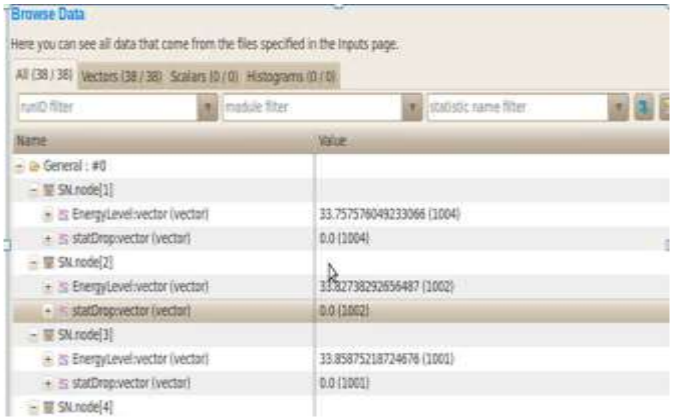
The equation no. (10) is improved than existing system.

- simulation result

For simulation of an algorithm OMNET++ is used .The nodes are placed randomly in given area. 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
MAC	Bypass MAC
Routing Protocol	DRINA

Fig 5.1 and 5.2 shows energy consumption of nodes in existing DRINA and in secure DRINA . This result shows that energy consumed by nodes in Existing DRINA algorithm is not much vary in secure DRINA.

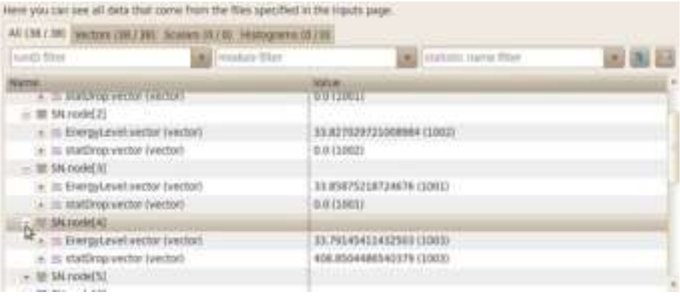


Browse Data

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 5.1: 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)	33.791454112432503 (1003)
statDrop:vector (vector)	406.85044865403379 (1003)
SN.node[5]	

Fig 5.2: Energy level of nodes in Secure DRINA

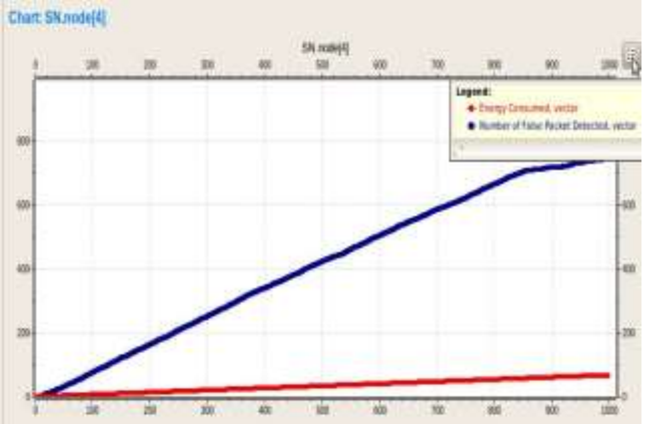


Fig 5.3: Energy consumed v/s number of false packet detected in Secure DRINA

Fig 5.3 shows the energy consumed and number of false packets detected by node 4 in secure DRINA

CONCLUSION

Wireless sensor networks (WSNs) have attracted considerable attention over the past few years. In military and civil application WSN is widely used; especially in hostile and remote areas. Examples include combat field surveillance, disaster management, and border protection. In all these applications a large number of sensors are expected, requiring careful planning and management of the network.

In previous clustering algorithm security was not considered. In this paper we presented secure DRINA algorithm. Our secure DRINA algorithm was extensively compared to existing DRINA algorithm regarding security, energy consumption, communication costs, delivery efficiency, and aggregation rate and aggregated data delivery rate.

REFERENCES

1. Azzedine Boukerche, Heitor S. Ramos Horacio A. B. F. de Oliveira, Regina B. de Araujo and Antonio A. F. Loureiro, "DRINA: A Lightweight and Reliable Routing Approach for in-Network Aggregation in *Wireless Sensor Networks*" Leandro Villas, 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 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.
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. Dirk WESTHOFF, Joao GIRAO, "Security Solutions for Wireless Sensor Networks" Amardeo SARMA NEC TECHNICAL JOURNAL Vol.1 No.3/2006.
8. 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.
9. 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.

10. G. Gaubatz, J.-P. Kaps, and B. Sunar. "*Public key cryptography in sensor networks*" revisited in 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), 2004.