ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Trust Ranking Based Safe and Secure Routing for Defending Against Collaborative Attacks in Wireless Sensor Network

Jasna Nazar[1], Sweety Kunjachan[2]

M.Tech Student[1], Assistant Professor[2]

Department of Electronics and Communication Engineering, A P J Abdul Kalam Technological University

[1]jasnanazar123@gmail.com,[2]sweetykunjachan88@gmail.com

***Abstract*-Wireless Sensor Networks have attracted a lot in wireless and mobile computing research community. Applications of WSNs ranges from indoor to outdoor deployments. Due to resource constraintin the sensor nodes, security mechanism with large overhead is difficult in WSNs .Trust Ranking Based Safe and Secure routing for Defending against Collaborative attacks in WSN, identify many attacks and resist them. Security can be ensured by secure routing and trust management.**

Keywords: Overhead, Collaborative attacks, Secure routing, Trust management

I. INTRODUCTION

Wireless Sensor Network consist of hundreds or even thousands of sensors. In these network a large number of sensor nodes are deployed to monitor a vast field. However the nodes in WSN have secure resource constraints due to lack of their processing power, limited memory and energy .In conventional security issues like secure routing, the security mechanism deployed in WSNs also involve collaboration among the nodes .WSNs with the characteristics of low cost, rapid deployment and self-organization plays vital role in facilitating the services of smart city . Sensor nodes can both collect the physical information of urban environment and control the public and private facilities in the context of smart urban environment. Due to the open distributed and dynamic characteristics of WSN, multihop routing is difficult.

The research shows that trust management is an effective way to solve security problems of WSN .In traditional routing protocol based on trust is difficult to ensure security of multihop information transmission .Each sensor node deployed in such networks has a limited energy and subjected to several attacks. The development of secure and energy efficient routing protocol to protect network against such attacks .WSNs has the following merits, evenly distributing the network load among the deployed sensor node and protecting network against attacks.

II.RELATED WORKS

Due to the natural constraints imposed on sensor nodes, several network layer protocols have been proposed to utilize sensor energy to propose to utilize sensor energy to improve the life time of WSNs.

According to Danyang QIN and Songxiang YANG,Trust sensing based secure routing mechanism for WSN to solve the network overhead and multihop information transmission. Results of TSSRM shows that it reduces routing overhead .The behavior of sensor nodes. The trust degree of sensor nodes evaluated according to these characters. The trust degree route is calculated and trust calculation nodes of network is established to node. The proposed routing algorithm is applied to secure routing mechanism to achieve the efficient and reliable transmission of data. The common attacks can be divided in to routing protocol attacks and trust model attacks. Routing protocol attacks can be classified in to soft and hard attacks. Soft attacks are black hole attack, gray hole attack, sink hole attack.Hard attack are DOS attack, tampering attacks.

TM handle attacks and improve the security of network by encryption and trust mechanism. Trust model attacks include on-off attack, selfish attack, badmouthing attack and collusion attack. TM is not applicable for all wireless sensor network because it focuses on trust calculation process. Watch dog is adopted for detecting mechanism .Trust model can be

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

established by direct trust calculation of nodes, indirect calculation of nodes and incentive factor.

The behaviour of sensor nodes can be monitored by neighbour nodesin WSN. Sensor nodes are constrained in computing power,energy, memory and bandwidth .Trust degree of nodes only monitoring the behaviour of nodes .Direct trust degree is the direct calculation of every node in communication .The nodes with high trust degree is used for conventional security model.

III.PROPOSED SYSTEM

Wireless Sensor Networks have been deployed in toa variety of applications including security and military systems. Sensor nodes deployed in networks are subject to several attacks such as sink hole and wormhole and spoofingattacks. Therefore it is very important to develop secure and energy efficient routing protocol for WSNs in which each sensor nodes forwards packet according to the data.

Each sensor node deployed in such networks has a limited energy and subject to several attacks such as sinkhole and wormhole and spoofing attacks .The development of secure and energy efficient routing protocol protect the network .It will avoid network overhead .Sensor nodes forwards the packets based on information collected from other nodes and malicious nodes allow the packets to forward through the other .The natural constraints imposedon sensor nodes .Several network layer protocols have been proposed .Energy efficient secure routing protocol provides security for data packets during way from source to destination .Energy efficient secure routing protocol can be achieved by roulette wheel routing protocol 1.The proposed protocol adopts three assumptions, 1.secret keys should be kept as secret 2.Seecret key shared among nodes 3.Sensor node should follow authentication.

A. Network Model

The network model consist of base station, sinknode, distributed wireless sensor nodes.It is required that every deployed sensor in the network have unique identification number. The base station can be inserted anywhere in field. It is usually connected to sink node through a wired or wireless network. Sink node is a wireless sensor node with high capabilities in terms of memory, processing, power. The sink node works as an intermediate node between the base station and the other sensors .It receives commands from the base station and conveys them to the deployed sensors .And also collects data from sensor and sends them to the base station. The sensor nodes, have limited battery power, memory, processing are distributed all over the area.

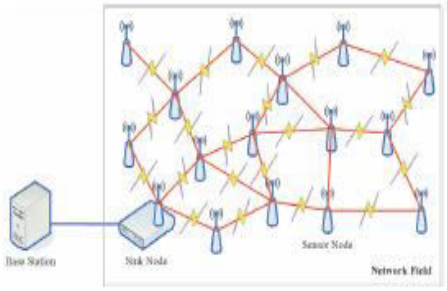

Figure 1: Network Model

The line between any two nodes means these nodes are within the transition range of each other.

B. Roulette –Wheel Routing Protocol

This section introduces Roulette – Wheel Routing Protocol that is forwarding data packets to next hop towards the sink node during the routing process. The significance of this protocol is that routing decision of a forwarding node is not affected by any other nodes and network load is evenly among all sensors. The RWRP considers the number of packets sent by the forwarding node to each neighbor node. It implement the roulette –wheel selection algorithm to select the forwarding node. In roulette – wheel selection algorithm, an individual is given probability of being selected that is directly proportional to measured metric. The individual is chosen randomly based on its probability. In this protocol, the individuals are the set of nodes of the forwarding node.

Mainly there are 8 steps for the roulette wheel routing protocol. (1)Network topology creation ,(2) Configuration of sender and receiver,(3)initial data collection , (4) Routing table establishment,(5) DES encryption ,(6) Data routing is source with roulette wheel routing protocol , (7) DES encryption in receiver node, (8) Data routing in receiver with roulette wheel routing protocol.

The secure routing protocol provides the security for data packets by (1) nodeinitialization, (2) routing table establishment (3) excluding malicious nodes, (4) routing data packets. The protocol implements the security by using the data encryption standard algorithm. DES provide confidentiality.

The EESRP protocol provides protection for WSNs against most of attacks on both application data and routing protocols. The protection against application data attacks, such as revealing, tampering, repeating, spoofing of data, is achieved

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

by providing encryption, digital signature and freshness features for conveyed data between a source and the sink node. Also the EESRP provides security feature to guard in particular against attacks on routing protocols that traffic by advertising high quality path to the sink node. This security feature of EESRP comes from the distinctive way used to construct the path between the source and the sink node. In addition, each node is permitted to only receive from and send to authentic nodes.

The path is constructed from the source tothe sink. That is each node along the route starting from the source randomly selects a next node towards the sink form its routing table. The routing table of each node contains only its authentic neighbour's. It is extremely hard to a malicious node to include itself on a path during its establishment.The attacks include tampering routing information, sinkhole attacks, selective forwarding attacks, wormhole attacks and spoofing attacks.

Tampering attack is explained by the EESRP protocol. The execution of the malicious nodesphase, the behaviour of the EESRP protocol does not allow any node to update its routing. Consequently, a malicious node cannot tamper with the routing tables of other nodes.

In selective forwarding attacks, malicious nodes droppart or all received packets so that they are not propagated. These attacks are typically most effective the attacker in the routing path. The ESRP protocol prevents a malicious nodes. A forwarding node randomly selects a next node towards the sink from routing table.

IV. RESULT AND DISCUSSION

In this section we describe our simulation and comparison based on assumptions.

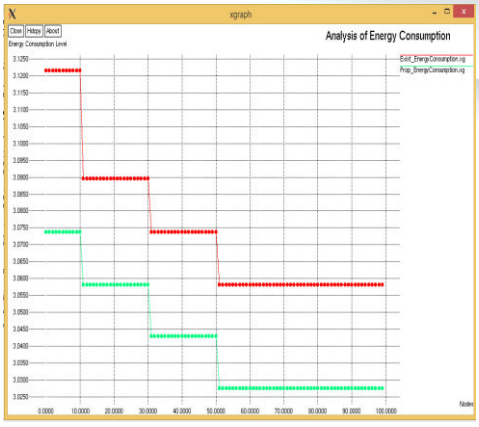

Figure 2: Analysis of energy consumption

The algorithm are compared using energy consumption.Network life time, network delay. The simulation time is 400s.

Energy consumption is the amount of energy or power used. From the figure, energy consumed is low compared to previous works.

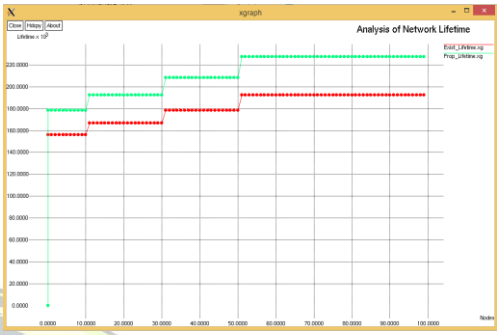

Figure 3: Analysis of network lifetime

The amount of time that a wireless sensor network is fully operative or network life time is the time which the network node runs out of energy to spend a packet.Network lifetime is improved compared to previous works.

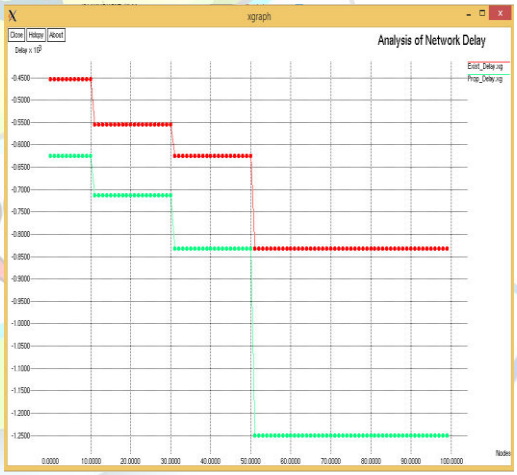

Figure 4: Analysis of network delay

Network delay is an important design .The delay of a network specifies how long it takes for a bit of a data to travel across the network from one node or end point to another. Usually measured in multiples or fractions of seconds .In this paper, network delay is lower compared to existing system.

V.CONCLUSION

WSN is an important part of modern communication systems .Energy efficient secure routing protocol provides security for data packets during the way from source to sink transmission. Trust ranking based safe and secure routing for

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

defending against collaborative attacks improves the security and also reduces routing overhead and improve the reliability of data transmission compared with traditional mechanism. The secure routing mechanism handles the network attacks

REFERENCES

[1] o. ozel, k. tutuncuoglu, j. yang, s. ulukus, and a. yener, ”transmission with energy harvesting nodes in fading wireless channels: optimal policies,” *ieee journal on selected areas in communications*, vol. 29, no. 8, pp. 1732-1743, sep. 2011.

[2] N. Marlon, C. Jose, A. B. Campelo, O. Rafael, V. C. Juan, and J. S. Juan, ”Active low intrusion hybrid monitor for wireless sensor networks,” *Sensors*, vol. 15, no. 3, pp. 23927-23952, 2015.

[3] G. Ottman, A. Bhatt, H. Hofmann, and G. Lesieutre, ”Adaptive piezoelectric energy harvesting circuit for wireless, remote power supply,” *IEEETransactions on Power Electronics*, vol. 17, no. 5, pp. 669-676, Sep. 2002.

[4] A. K. A. Mohammad, and S. Gadadhar, Enhancing cooperation inMANET using neighbourhood compressive sensing model,” *EgyptianInformatics Journal*, vol. 6, no. 1, pp. 1-15, 2016.

[5] G. Uttam G, and D. Raja, ”SDRP: secure and dynamic routing protocol for mobile ad-hoc networks,” *IET Networks*, vol. 3, no. 2, pp. 235-243, 2014.

[6] W. K. K. Chin, and K. L. AYau, ”Trust and reputation scheme forclustering in cognitive radio networks,” *International Conference onFrontiers of Communications, Networks and Applications (ICFCNA)*, KualaLumpur, Malaysia, Nov. 2014, pp. 1-6.

[7] Y. Gao, H. W. Chris, J. J. Duan, and J. R. Chou, ”A novel energy aware distributed clustering algorithm for heterogeneous wireless sensor networks in the mobile environment,” *Sensors*, vol. 15, no. 10, pp. 31108- 31124, 2015.

[8] J. G. Choi, S. Bahk, ”Cell-throughput analysis of the proportional fair scheduler in the single-cell environment,” *IEEE Transactions on VehicularTechnology*, vol. 56, no. 2, pp. 766-778, 2007.

[9] K. B. Sourav, and M. K. Pabitra, ”SIR: a secure and intelligent routing protocol for vehicular ad hoc network,” *IET Networks*, vol. 4, no. 6, pp. 185-194, 2015.

[10] E. Adel, K. Abdellatif, and E. Mohammed, ”A new trust model tosecure routing protocols against DoS attacks in MANETs,” *The 10th International Conference on Intelligent Systems: Theories and Applications (SITA)*, Taiwan, Oct. 2015, pp. 1-6.

