Research Paper

Controlling Residual Energy of WSN With Secure Routing Protocal

Engineering

KEYWORDS : Wireless Sensor Networks, intrusion detection, intrusion prevention, efficient routing protocol.

K. Imrana Banu M.Tech, Computer Science and Engineering, JNTUA college of engineering pulivendula, Andhra Pradesh, India

Sri G.Murali Assistant professor, Computer Science and Engineering, JNTUA college of engineering pulivendula

ABSTRACT

Wireless Sensor Network (WSN) is a developing technology that is anticipated to change the human life in future. This sensor network is composed of small sensing objects called sensors that are scattered in the environment. Because of wireless nature and having limited lifetime there are many difficulties for researcher to make this technology more useful.Mostly in wireless sensor network, easily affect by malicious activities.Energy is the main factor in WSN, most of the times sensor will lose due to energy problems.Routing scheme, always network will choose shortest path for data forwarding.So, which are the nodes placed in the same path will lose their energy in an exceedingly fast interval. In our proposed scheme, we introduce both intrusion detection and prevention in energy efficient routing protocol. Initially all the nodes and BS will construct the network with route construction messages and neighbour instruction messages. Then sensor sense the environment and it forward the data with randomly selected nodes by check nodes. Based on the energy the route will change dynamically. So we can enhanced energy routing with secure intrusion detection scheme.

1. INTRODUCTION

A wireless sensor network (WSN) consists of large number of sensor nodes that are capable of assembling the data from the environment and act with each other through wireless transceivers. These collected information will be sended to one or more sinks, generally through multi-hop communication [1]. Due to the limited features of sensor network such as memory, battery, CPU. Since the sensor nodes are expected to work with batteries and these are often deployed in the hostile environment. It can be very difficult and impossible to replace the batteries when the nodes die . Due to the nature of wireless sensor network these are affected by many malicious activity.

Energy is the main factor in WSN, because most of the times sensors will lose due to the energy problems. Since the sensor nodes are deployed to gather data and desired that each and every nodes works endlessly and transmit data as long as possible. Routing Scheme, always network will choose shortest path for forwarding information. so, which are the nodes placed in the same path will lose their energy continuously.

As Wireless sensor networks address the lifetime problem, mainly energy is spend during transmitting the information, relaying and receiving packets [2]. Hence, the main aim is to reduce the energy consumption and improve the network lifetime by increasing the individual energy of all the nodes.

Here we have introduced introduce both intrusion detection and prevention in energy efficient routing protocol. Initially all the nodes and BS will construct the network topology with route construction messages and neighbour instruction messages. Then sensor sense the environment and it forward the information with randomly selected nodes by check nodes. Based on the energy the route will change dynamically. So we can enhanced energy routing with secure intrusion detection scheme.

In wireless sensor network information gathering and are the difficult tasks because of their dynamic nature and distinctive properties. several routing developed, however among those protocols cluster primarily based routing protocols are energy economical, scalable and prolong the network lifetime. In the event detection surroundings nodes are idle most of the time and active at the time once the event occur [3]. Routing is a critical issue in information gathering sensor network, were as on the opposite hands sleep-awake synchronization is the key problem for event detection sensor networks.

2. RELATED WORK

2.1 Literature Survey

I.F. Akyildiz et. al. [1] has presented "A Survey on wireless technology" This paper Surveys recent advancement of wireless networks that has enabled the development of very low-cost sensor nodes. sensor nodes are used to sense the environment condition such as humidity, temperature, images and sounds. So these are use in various application areas such as military, health, home, etc. but for different application areas there are different, technical issues that are solved by the researchers currently.

C. Karlof et. al. [2] has presented "Secure routing in wireless sensor networks: Attacks and countermeasures," our attention is on routing security in WNS. Current proposition for routing protocols in sensor networks upgrade for the limited capacities of the nodes and the application particular nature of the networks, however don't consider security. Despite the fact that these protocols have not been outlined with security as a goal, we feel it is imperative to examine their security properties. At the point when the safeguard has the liabilities of insecure wireless communication, possible insider threads, furthermore, limited node capabilities, and the foes can utilize powerful tablets with long range communication and high energy to attack the network , outlining a protected routing protocol is non-trivial.

Y. Hu, A. Perrig, and D. B. Johnson et. al. [3] has presented "Packet leashes: A defence against wormhole attacks in wireless networks," in 2003. In the wormhole attack, an attacker records packets at one area in the network, tunnels them to another area, and re-transmits them there into the network. The wormhole attack can frame a serious danger in wireless networks, particularly against numerous ad hoc network routing protocols and location based wireless security frameworks. so the researcher has introduced another, general mechanism, called packet leaches, for distinguishing and in this manner defending against wormhole attacks, and we present a particular protocol, called TIK, that implements leaches.

B. Xiao, B. Yu, and C. Gao et. al.[5] has presented "CHEMAS: Identify suspect nodes in selective forwarding attacks," in 2007. As the wireless sensor networks are vulnerable to many attack due to its nature. The researcher has proposed checkpoint based multi-hop acknowledgement scheme (CHEMAS**)**. Based on the previously fixed probability the check nodes are selected. The security intensity and energy efficiency of WSN are affected due to the selection of checkpoint nodes. So researcher has proposed fuzzy rule system and feedback concepts these are the control method for the selection of checknodes

J. Deng, R. Han, and S. Mishra et. al. [6] has presented "INSENS: Intrusion-tolerant routing for wireless sensor networks," in 2006. The researcher has exhibit an adaptable and mathematically rigorous modeling framework for breaking down the security of WSN routing protocols. At that point, the researcher has demonstrated the use of this network by formally proving that INSENS (Intrusion-Tolerant Routing in WSN), which is a secured WSN routing protocal proposed in the writing autonomously of researchers work , can be demonstrated to be secure in this model.

Fan Ye and Haiyun Luo et. al. [7] has presented "Statistical en-route filtering of injected false data in sensor networks," in 2005. The researcher has proposed a statistical en-route filtering (SEF) mechanism. While forwarding process this mechanism is used to detect and drop the false report in the network. If the same event is detected by the multiple sensors and in SEF keyed MAC is generated for each detected sensor nodes then multiple MACS are attached to the event report. As the report is forwarded the invalid MAC are dropped based on correctness of MAC probability. SEF exploits the network scale to channel out false reports through aggregate decision making by multiple detecting nodes and aggregate false detection by multiple sending nodes.

3. PROPOSED SYSTEM

The proposed method is composed of five phases: Create a Wireless Sensor Network, Initial Construction, Sensing data transmission, Re-Construction, Secure Data Transmission. Creating a wireless sensor networks, initial construction are designed based on [6] and sensing data transmission is based on [5].

3.1 Create a Sensor Network

Create a group of nodes and form a sensor network. As the sensor network consists of large number of sensor nodes and one or more sink node. Each node have the capability of collecting the information from the environment and communicate with each other through wireless transceivers. Sensor node will forward the data through relay communication to sink node. For forwarding the data sensors will prefer a shortest routing path.

Wireless sensor nodes

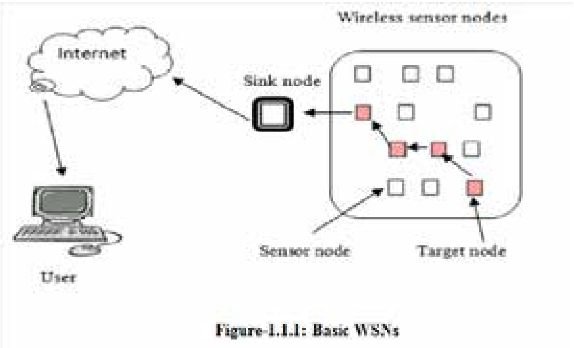


Fig -1 wireless sensor network

3.2Initial Construction

The topology and routing path of the whole network are constructed in initial construction phase. Using topology and route construction message (TRC) and the neighbor information response message (NIR), BS and each node in the network communicate with each other. First the TRC message is broadcasted by the BS within the transmission range. Each node which receives these message records the sender as its neighbor node. In the current round if the sender is the first node from which it gets TRC message, it records the sender as its neighbor node.

After that, node changes the sender's ID and MAC of the TRC message and re-broadcast this message. After all the nodes gets the TRC message, each of them generates neighbor information responds message. (NIR message) and send it to BS. This BS construct neighbor information table using NIR message. After the network topology is f finished, routing table for the each node is constructed by BS based on the routing path. Using routing table update message BS sends the routing table to each and every node.

3.3 Sensing Data Transmission

In this phase an event report is generated by the sensing node and forwarded to the BS. Few nodes on the way are randomly chosen as check nodes during forwarding process. These check node sends back an acknowledgement message in direction to the source node. Based on the Time- To- live (TTL) value the ack is send to limited number of hops. On the off chance that if Time- to- live value is one, an ack message is send to the next check node in the direction to the source node. If the sufficient number of ack is not received by the sensor node an ALERT message is transmitted to the first check node in the direction to the source node.

Using the report path the first node which receives the ALERT message sends ALARM to report that harm had occurred in the main path.

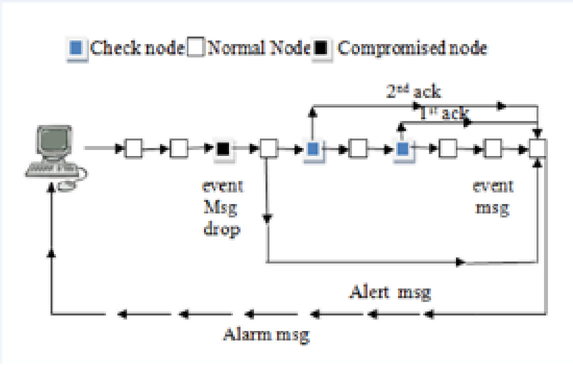


Fig-2 : Data Transmission

3.4 Re-Construction Phase

In this phase based on the ALERT and the ALARM messages the network topology and the routing path are reconstructed. However base station gets path and node information from the previous phase based on this BS selects a path modifies the routing table and topology.

3.5 Secure data transmission

In this phase keys are initially shared by all the nodes. While forwarding the data source will encrypt the data, this encrypted data is only forward through the route. If any misbehaviour node is detected in then the network will eliminate the malicious node.

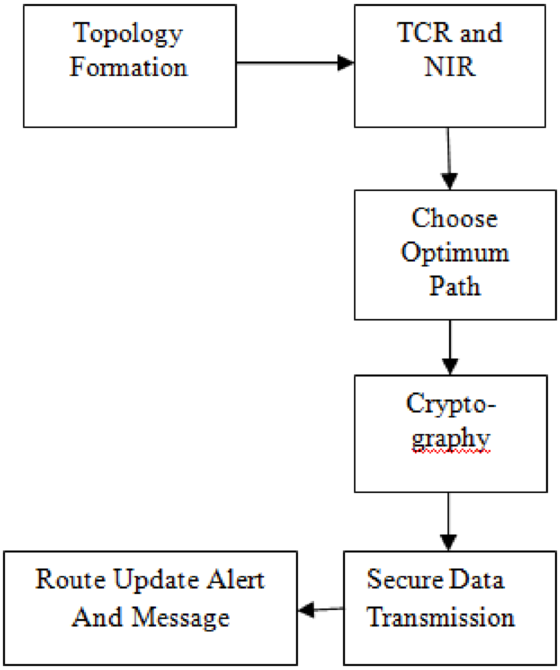
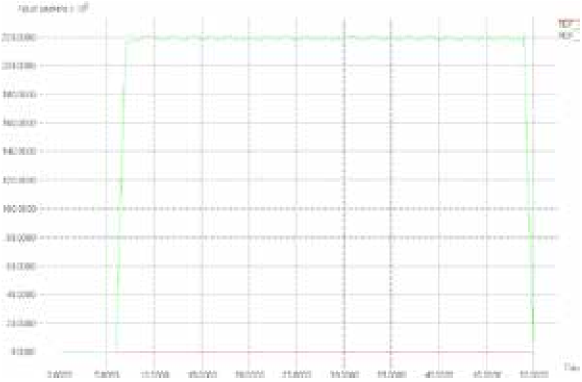


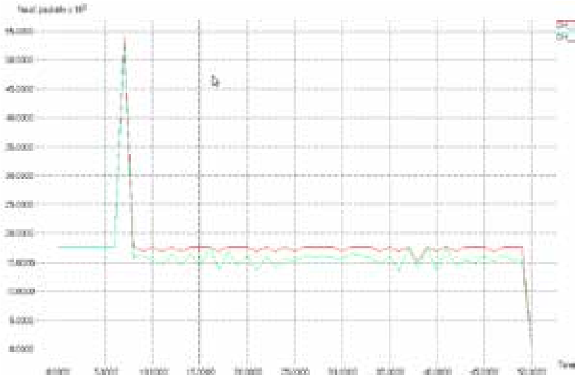
Fig-3 Block diagram

4. RESULT ANALYSIS

Proposed Energy efficient routing protocol is compared with the existing protocols. Packet delivery ratio of proposed method is very high compared to existing one .In the Graph-1 the red lines shows the packet delivery ratio of Existing which is very low compared to proposed method. Second graph shows the packet overhead which is very low in proposed method compared to existing method. Proposed method achieves lower energy consumption. This improves the lifetime of the nodes in the network. Thus proposed routing protocol provides better lifetime and with secure data transmission than existing one.



Graph-1: Packet delivery ratio



Graph-2: Overhead

5. CONCLUSION

Proposed Energy efficient routing protocol is compared with the existing protocols. Proposed protocol achieves the higher energy consumption. This improves the lifetime of the nodes in the network. Quality of Service of the communication network is also improved by achieving the lesser end-to-end delay. Thus proposed routing protocol reduced the energy consumption and increased the network lifetime compared to existing one.

REFERENCE

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," Communications magazine, IEEE, vol.40, no.8, pp.102-114. | [2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad hoc networks, vol.1, no.2, pp.293-315. | [3] Y. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense againstwormhole attacks in wireless networks,"INFOCOM 2003. Twenty-SecondAnnual Joint Conference of the IEEE Computer and Communications. IEEESocieties, pp.1976-1986. | [4] J. R. Douceur, "The sybil attack," in Peer-to-peer SystemsAnonymous ,pp.251-260, Springer, 2002. | [5] B. Xiao, B. Yu, and C. Gao, "CHEMAS: Identify suspect nodes inselective forwarding attacks," Journal of Parallel and Distributed Computing,vol.67, no.11, pp.1218-1230, 2007. | [6] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing forwireless sensor networks," Comput.Commun., vol.29, no.2, pp.216-230, 2006. | [7] Fan Ye, Haiyun Luo, Songwu Lu, and Lixia Zhang, "Statistical en-routefiltering of injected false data in sensor networks," IEEE Journal on SelectedAreas in Communications,2004. |