International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 3 Issue 6, May 2016

ISSN: 2394-4404

Secure Scheme For Wireless Sensor Networks By Watchdog Location And Frequency Optimization

Apeksha Balakrishna
M.Tech (DCN),
Department of Telecommunication Engineering,
Dr.AIT, Bangalore

Usharani M A
Assistant Professor,
Department of Telecommunication Engineering,
Dr.AIT, Bangalore

Abstract: ***Wireless sensor networks are typically deployed in an unattended environment. These gives promising future for many sensitive application such as defence, health monitoring, early bushfire detection etc. since the sensor nodes are kept unattended it causes serious security concern. The main aim of this paper is to optimize watchdog technique for malicious nodes in the network. Watchdog is a monitoring technique which is used to detect misbehaviour node in the network. By optimizing watchdog we minimize the energy consumption while keeping security system in sufficient level.***

Keywords: wireless sensor network, watchdog technique, trust node.

I. INTRODUCTION

Wireless Sensor Networks have been used in challenging, hostile environments for various applications such as forest fire detection, battlefield surveillance, habitat monitoring, etc. sensing computation and communication is done by tiny piece of electronic device in wireless sensor network. One common assumption in traditional Wireless Sensor Networks is that a trusted third party, e.g., a sink, is always available to collect sensed data in a near-to-real-time fashion. Although many Wireless Sensor Networks operate in such a mode, there are Wireless Sensor Network applications that do not fit into the real time data collection model. A Wireless Sensor Network comprises battery-powered sensor nodes with extremely limited processing capabilities. With a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multihop path. However, the multihop routing of Wireless Sensor Networks often becomes the target of malicious attacks. An attacker may tamper nodes physically, create traffic collision with seemingly valid transmission, drop or misdirect messages in routes, or jam the communication channel by creating radio interference.

A critical complement to security mechanisms trusts systems are widely applied to protect wireless sensor networks from being attacked by trust sensor node. Those nodes can bypass traditional security protections using their trust identities, but can be possibly captured by trust systems due to their poor reputation or past misbehaviour. Building trust system is not easy task. The problems which are found while building these trust system are. First, sensor nodes may not be located in the communication range for base station or cluster head. Second, some sensor node may not be communicating with other nodes or it may be communicating with low frequency. Third, the information obtained from one sensor node cannot be used to build trust system for other sensor nodes.

Although the watchdog technique has been proved as a very effective approach to build up Wireless Sensor Network Trust System foundations, it introduces a large amount of additional energy consumptions which conflict the energy efficient design principle of Wireless Sensor Networks. Recharging or replacement of these unattended nodes' power is very difficult and expensive. Due to those challenges, energy saving plays a very important role in the design of modern Wireless Sensor Networks. However, to our best knowledge, no existing Wireless Sensor Network Trust Systems give appropriate solutions to save the energy consumed by the watchdog technique. In particular, some

Wireless Sensor Network Trust Systems do not discuss how to schedule watchdogs in their proposals, while some others implicitly suggest letting sensor nodes launch neighbor-flooding watchdog tasks to monitor all their neighbors and do not study which frequency is appropriate for their monitoring. This watchdog technique consumes much energy and they do not give correct solution for energy consumption. Thereby network life time is decreased.

II. RELATED WORK

Trust systems are designed and deployed in wireless sensor networks for a general security and can protect particular wireless sensor network functionalities.

In the literature, wireless sensor network trust system is usually applied to avoid unreliable and corrupted sensing data, or secure multi-hop routing or protect both of them. In this paper [2] they proposed a storage-efficient trust model by applying a geographic hash table to identify trust managers this was mainly designed for storage purpose rather than energy, while [3] implemented an energy watcher to help sensor nodes estimate their neighbor nodes' energy cost for each packet forwarding and thus enable the selection of the most efficient node as their next hop in the route, although proposes an energy-efficient secure routing algorithm to choose efficient and trustworthy next-hop node in a route, it cannot reduce the energy used to build up wireless sensor network trust system, which is the major problem. Moreover, a clustering technology is widely used in [4] to make wireless sensor network and wireless sensor network trust systems energy-efficient. By electing a number of cluster heads to manage sensor nodes on behalf of the base station, energy consumption can be reduced due to shorter communication distance, clustering techniques which save energy by reorganizing wireless sensor network topology to a hierarchical architecture, our research saves energy by means of reducing redundant trust foundations in wireless sensor network trust system. And even better, our solution can also be applied to clustered wireless sensor network to further reduce energy cost. Based on the clustered topology, [5] further reduced energy by cancelling feedback between cluster members or between cluster heads, and thereby proposed a more lightweight wireless sensor network trust system, designs an energy-efficient wireless sensor network trust system by reducing unnecessary communications of trust recommendations. This paper has taken watchdog technique into consideration which is the largest energy consumption unit. Therefore we are going to optimize watchdog technique to reduce the energy consumed by the nodes and to keep the security is sufficient level

III. OBJECTIVES

The main objectives of this paper are

- ✓ To reduce energy consumption by the sensor nodes by optimizing watchdog in location and frequency.
- ✓ By optimizing we are going to increase network lifetime.
- ✓ Maintaining the security in sufficient level.

IV. PROPOSED METHOD

Proposed work is about balancing the energy efficiency and security of wireless sensor network. To make this possible we are using watchdog optimizing technique in two levels.

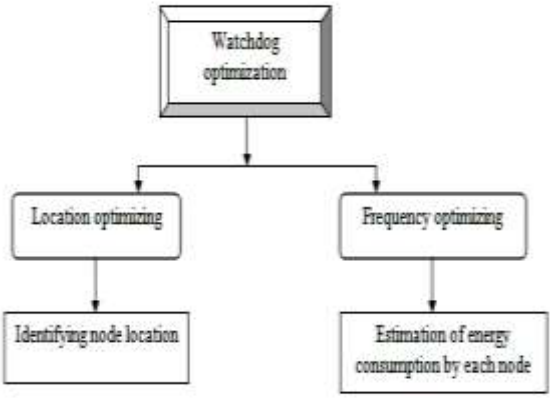

Figure 1: Levels of Watchdog Optimization

First level of optimization is watchdog location optimizing. This level of optimizing technique use distance based probabilistic algorithm. This algorithm can find a set of watchdog nodes by considering those nodes' locations in a probabilistic manner and to create shortest path between source node and destination node. It identify misbehaving node in the network and prevent those nodes from being used by future routing.

Second level of optimization is watchdog frequency optimizing. Watchdog Frequency Optimization technique uses Heuristic Watchdog Frequency Adjustment algorithm to estimate energy units for each node. Based on this energy consumption node transfer the data to intermediate nodes. It defines the number of task to be performed by watchdog node within a time window. Below flow chart shows the flow of data transaction from source node to destination node using watchdog optimizing technique for selecting the shortest path

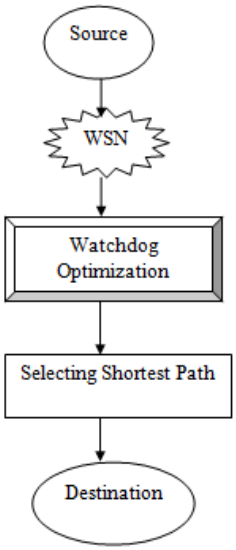

Figure 2: Flow chart of data transaction in WSN

ISSN: 2394-4404

III. DESIGN METHODOLOGY

This section consists of design model of the proposed system. We design our methods by considering a flat wireless sensor network topology, let each node be within the communication range and to formalize a watchdog task we first separate time space into a sequence of consecutive time slots with equal size. And we are going to estimate the energy consumed by the nodes we implement energy watcher to help sensor nodes estimate their neighbour nodes' energy cost for each packet forwarding and thus enable the selection of the most efficient node as their next hop in the route. In our network every node is being monitored by set of watchdog nodes. At first only one watchdog node will be monitoring the particular node, if any misbehaviour is found in that node then all other watchdog nodes monitor this fault node.

Here we are going to calculate the trust value of each node. Trust value is calculated using the factors like amount of energy the node is going to consume, distance between the nodes, attacks that may be caused by this nodes etc., are been considered. After calculating this trust value the nodes are going to perform transaction. The nodes for multi hopping purpose are selected using this trust values.

IV. EXPERIMENTAL RESULTS

This model is coded in NS2 and is made run in VMware workstation. First we are going to create nodes using flat topology. After creating nodes watchdog nodes for every nodes is been assigned. This is shown in figure below. This watchdog node monitors the sensor nodes. And data transmission is made from node 12 and node 17. While transmitting the shortest path is been obtained using trust value of every node. It is analysed that by watchdog optimization the energy consumption is reduced and the security is maintained. Initially every node is provided with the energy of 100 joules. After transaction of data it is found that the energy consumption by nodes is decreased as shown in figure below

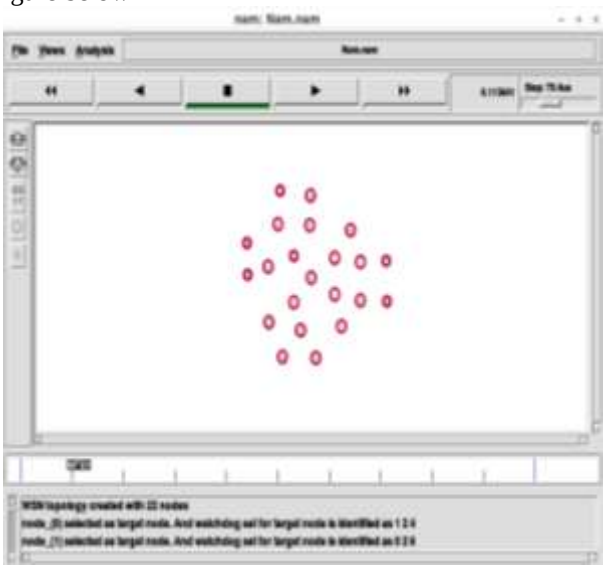

Figure 3: Creation of nodes

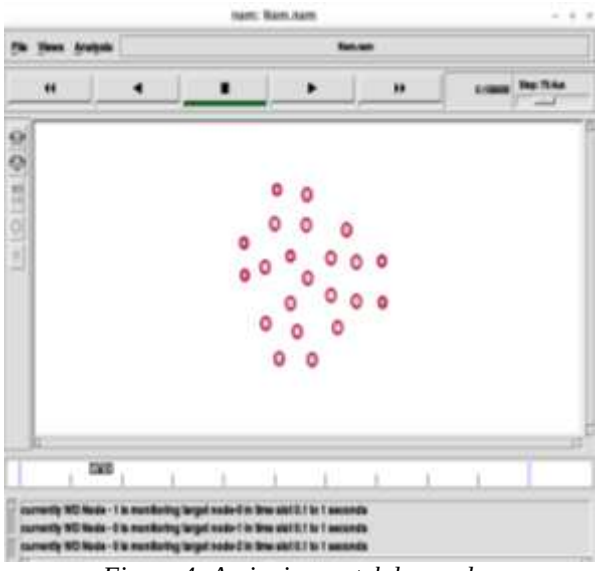

Figure 4: Assigning watchdog nodes

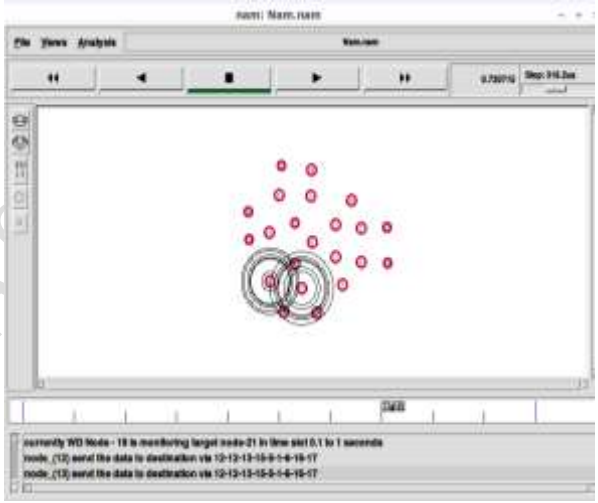

Figure 5: Transmitting data

It is found that the shortest path for transmitting data from node 12 to node 17 is 12-13-15-5-6-16-17

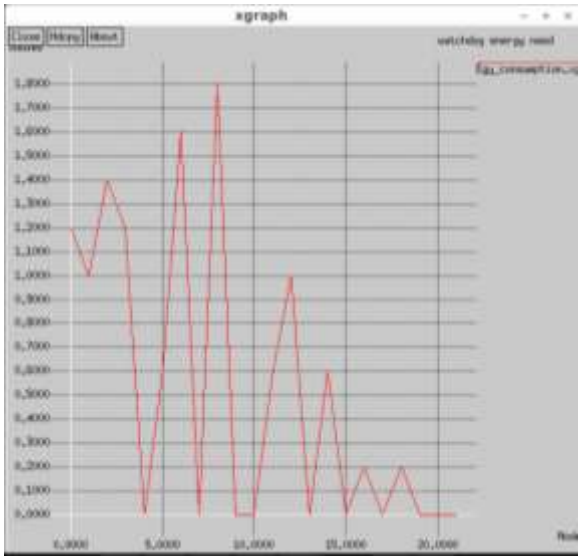

Figure 6: Energy consumption by watchdog node

Here we can observe that the near node 5 the amount of energy consumed is more. This is because in this experiment we made node 5 as the misbehaving node and its watchdog

nodes are monitoring this node. The watchdog nodes for node 5 are node 6 and 15. At first node 6 finds that node 5 is misbehaving and it keeps monitoring this fault node and node 15 also starts to monitor this node.

V. CONCLUSION

In this paper we propose Watchdog Optimization algorithm by considering a new approach. It can be used to solve several optimal problems. It is aimed to minimize the length of the tour and find the target path. The inefficient and inappropriate use of watchdog technique in existing trust systems leads to propose a suite of optimization methods to minimize the energy cost of watchdog usage, while keeping the security level of whole system in a sufficient level.

VI. FUTURE WORK

The watchdog optimizing technique can also be applied to vehicular ad-hoc network and all other networks which are similar to wireless sensor network. And it can also be applied to mobile wireless sensor network. For mobile wireless sensor network we will have to redesign the data based probabilistic algorithm.

REFERENCES

[1] Peng Zhou, Siwei Jiang, Athirai Irissappale "Toward energy-efficient trust system through watchdog optimization for WSNs" IEEE Transactions on Information Forensics and Security, volume 10, No 3, March 2015.
[2] Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, "A novel approach to trust management in unattended wireless sensor networks," IEEE Transaction. Mobile Computer, volume. 13, no. 7, pp. 1409–1423, July. 2014.
[3] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: A trust-aware secure routing framework in wireless sensor networks," International Journal Distribution Sensor Network volume 2014, Art. ID 209436, January 2014.
[4] F. Bao, I. R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust based routing and intrusion detection," IEEE Transaction Network Service Manage., volume 9, no. 2, pp. 169–183, June 2012.
[5] X. Li, F. Zhou, and J. Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," IEEE Transaction Information Forensics Security, volume 8, no. 6, pp. 924–935, June 2013.
[6] Seung-Jun Kim, Xiaodong Wang, and Mohammad Madihian, "Distributed Joint Routing and Medium Access Control for Lifetime Maximization of Wireless Sensor Networks", IEEE transactions on wireless communications, vol. 6, no. 7, July 2007.
[7] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol, Member, IEEE Computer Society, Heejo Lee, Member, IEEE, Sungyoung Lee, Member, IEEE, and Young-Jae Song, "Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks" IEEE transactions on parallel and distributed systems, vol. 20, no. 11, November 2009
[8] Xiaoyong Li, Feng Zhou, and Junping Du, "LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks", IEEE transactions on information forensics and security, vol. 8, no. 6, June 2013
[9] [9] Chen X. Makki K. Yen K. and Pissinou N. 'Sensor network security: A survey', IEEE Communication Survey Tuts, volume 11, no. 2, pp. 52–73, June 2009.
[10] Das M. L. 'Two-factor user authentication in wireless sensor networks', IEEE Transaction. Wireless Communication volume 8, no. 3, pp. 1086–1090. March 2009
[11] Marti S. Giuli T. J. Lai K. and Baker M. 'Mitigating routing misbehavior in mobile ad hoc networks', in Proc. 6th Annual International Conference Mobile Computer Network pp. 255–265, 2000