ENERGY EFFICIENT SECURE ROUTING ALGORITHM FOR WIRELESS SENSOR NETWORKS

ANURAG

M.Tech (Computer Science and Information Security)
E-mail: anurag.smit@gmail.com

Abstract- Popularity of wireless sensor networks (WSNs) is increasing continuously in different domains of daily life, as they provide efficient method of collecting valuable data from the surroundings for use in different applications. Routing in WSNs is the vital functionality that allows the flow of information generated by sensor nodes to the base station, while considering the severe energy constraint and the limitations of computational and storage resources. Indeed, this functionality may be vulnerable and must be in itself secured, since conventional routing protocols in WSNs provide efficient routing techniques with low power consumption, but they do not take into account the possible attacks. As sensor nodes may be easily captured and compromised, we present an energy efficient secure data transmission in WSNs where we divide the area of interest in four quadrants and then uses the techniques of both public and private key cryptography using four Mobile Base stations for energy saving. We also use data compression techniques for reducing the amount of bit transmission. We also employ Monitor Nodes to detect the internal attacks.

Keywords- Cluster Based Wireless Sensor Network, Cryptographic Techniques, Data Compression technique, Mobile Sink nodes, Monitor Nodes.

I. INTRODUCTION

Wireless sensor network connects the large number of sensor nodes using wireless network. It consumes energy when the sensor senses the data, transmit the data between the sensor nodes and process the data. It has major concerns about energy, security and routing. Sensor is used to sense and track in the military, collect the data during disaster management, finding the fire in the forest, find the defect in the manufacturing process, monitoring the temperature of the building and many more applications like monitoring, tracking, detecting, collecting or reporting. The medical and military solutions require more security than other solutions. The military application uses sensor data for enemy tracking and targeting and medical solutions store the individual medical related information.

Secure data transmission deals with preventing the interception, injection and alteration of malicious data during the course of transmission. Security in WSNs is not easy compared with conventional desktop computers; severe challenges meet these sensor nodes. The sensor node which deployed in a hostile environment has limitation in processing power, storage, channel bandwidth and computational energy, prone to failure and the network topology changes frequently.

We attempt to overcome these challenges, due to importance of security. Sensor networks are used sometime in very sensitive applications such as healthcare and military. With this in mind we must address the security concerns from the beginning of network design. Sensor networks pose unique security challenges because of their inherent limitations in communication and computing abilities. Deployment of sensor networks in an unattended environment makes them vulnerable to potential attacks .Attackers can compromise the network to accept malicious nodes as legitimate nodes. Hardware and software improvements will address these issues at some extend but comprehensive security requires development of countermeasures such as secure key management, lightweight encryption techniques; secure routing protocols and malicious node detection mechanism. This paper presents an energy efficient algorithm for secure data transmission in sensor networks.
The rest of the paper is being organized as follows: In the next section, we will discuss about related work done till now in this field. In Section III, we will discuss about proposed work. Finally, in the last section, we will discuss the conclusion and future research direction.

II. RELATED WORK

Various research work done till now related to secure routing protocol, but here we will discuss some few of them.

Multipath routing can be used to avoid several types of attacks. When, one path is bogus, packets route through another probable secure path. This way is also more reliable if the primary path includes disconnecting nodes.

Energy efficient Secure Multipath Routing Protocol (EESM) protocol have been proposed. The EESM

protocol divided into three phases Route construction, Transfer data and Route maintenance and security. It uses Ant Colony optimization algorithm for finding the shortest path between the sensor nodes. This source initiated (Base Station) protocol which uses public cryptography for secure the data and introduce the protocol schema to transfer the data from sink to source. EESM uses multipath routing protocol which gives energy efficiency and security. The average energy consumption for data processing including Authentication and average energy consumption for each bit of data transmitted.
SEER assumes the energy spend each node has the same value. It uses public key cryptography for authentication and authorization with pre deployed private key in sensor node.

Ambient Trust Sensor Routing (ATSR) algorithm has been proposed which has been shown to detect fast malicious nodes by using the neighboring trust information and reacts in their detection, finding alternative paths. As soon as the malicious nodes are detected, the network performance becomes identical to the one observed for no malicious nodes in the network. Additionally, its energy awareness allows for better load balancing which improves the network lifetime and is considered a measure against traffic analysis attacks.

Energy efficient multipath routing protocol has been proposed .The secure Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) finds the multiple paths between the source and destination based on the rate of energy consumption. It uses a crypto system which uses the MD5 hash function and RSA public key algorithm. The public key distributed freely and private key distributed for each node. It has Route construction phase, Data transmission phase and transmits the data in wireless sensor network.

In addition to the above cryptographic techniques, various methods has been proposed to detect internal attacks by the help of Monitor Nodes Present researches are much more oriented to the development of logical intrusion detection systems.

An intrusion detection system (IDS) is by definition a system that handles the detection and the isolation of intruders present in the network through a collection of monitor nodes (MNs). A MN is a sensor node which has to control network's traffic and to transmit alarm messages on detecting misbehaviors. In, Threshold Hierarchical Intrusion Detection system has been proposed in which Monitor Node has the responsibility of sending alarm to the base station when the no. of blacklisted sensor nodes of reaches the threshold. The base station then stops receiving notification from malicious nodes.

III. PROPOSED WORK

As discussed above, secure data transmission in many cases involve the use of cryptographic techniques. Our proposed method is based on Cluster based Wireless Sensor Network. As the public key cryptography is energy consuming, we only apply public key cryptography to the cluster head and private key cryptographic technique is being apply to the rest of the sensors. We have divided the test coverage area into four quadrants and will install the sink node at each quadrant and only the sink node at particular quadrant has the responsibility to transmit the keys to its respective area and performing computation. We have used mobile base stations to reduce the amount of energy consumed. We will also used Existing THIDS approach to detect the internal attacks. As the data transmission of each bits consumes energy, we decreases the amount of bit transmission by applying data compression techniques to each cluster heads. The proposed algorithm uses the concept of Mobile sink nodes, data compression and public and private key cryptography.

Our proposed method is based upon the following assumptions, which are as follows:
1. It is based on cluster based WSNs, especially those where clusters are dynamically and periodically formed.
2. Number of Cluster heads defined in each quadrants according to the tradeoff between detection effectiveness and energy savings.
3. The number of Monitor nodes deployed in this case according to the tradeoff between detection effectiveness and energy saving.
4. Whether it reports bogus data messages or it reports no messages, it can't affect, significantly, data consistence and/or network performance, unless the number of intruders is large.
5. Data compression techniques are being applied to each cluster head. It does not loses the original meaning during transmission

At each quadrant, the sensor nodes are deployed to sense the targets. These sensors are being deployed in cluster based network, in which each cluster contains a cluster head, whose function is to aggregate the data from gathered from each sensors and send them to the other cluster head .A quadrants contains more than one cluster head. Sink nodes in each quadrant become mobile to save some energy.

We have used four sink nodes. We assume an area in which sensor network being deployed is divided into four quadrants, each quadrants containing a sink node. The large numbers of sensors being deployed in an area, and there is a cluster head of each sensor-set. This cluster head has the responsibility of sending the

data to the sink node at its respective quadrants via the other cluster head. Initially, all the sink nodes are static. The sink node at each respective quadrant starts sending the private keys to each sensor and public/private key pairs to the respective clusters head .The sink nodes than starts become mobile. The sensors after sensing sends the data to the cluster head via other sensor nodes authenticating with each other by using private key cryptography .It then sends the data to the respective cluster head. Cluster head sends the data to the other cluster head authenticating each other by using public key cryptography, and finally it sends the data to the sink nodes at its respective quadrant.

The path from the cluster head to the sink nodes is via the shortest possible routes, which is the function of distance, sensing, communication and transmission energy. We also have used the data compressor at each cluster head to compress the data being transmitted to each other and to sink node and hence less number of bits being spent in transmission. We have used existing THIDS approach were monitor nodes beside each sensor nodes is being deployed to detect the internal attacks, and when the number of malicious nodes being detected reaches the threshold, the information is being sent to the sensor and blacklisted nodes will stop its participation.

In the course of time, when the energy of the cluster head reaches less than the certain threshold value, than that cluster head will be in sleep mode and other cluster head will be activated. The base station will then provide the new public /private key pairs.

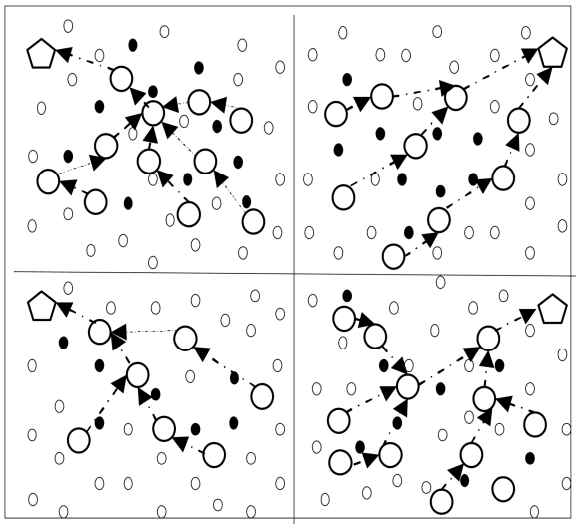
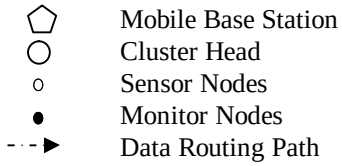


Fig. The proposed scenario



A. Pseudo Code:

1. Consider an area (0,0),(100,0),(0,100)(100,100) divided into four quadrants.
2. Install the base stations at each quadrant.
3. Set status=static
4. Begin
2. For active Sensor Set $S=(S_1,S_2,\ldots.S_j)$.
3. For active CHid=$(CH_1,CH_2,\ldots,CH_n)$
4. Send $E(K_{in},P)$ and $D(K_{in}\text{-}1,C)$ to each cluster Head
5. Send $E(k_{ij},P)$ to each active sensors
6. Set status=mobile
7. Sensor nodes starts sensing and communicate with each other and also to the cluster head by private key $E(k_{ij},P)$.
8.Cluster head compresses the data and starts communication with each other via public key cryptography $E(K_{in},,P)$ and $D(K_{in}\text{-}1,C)$
9. Shortest route from each cluster head is being formed which is a function of distance, sensing, communication and transmission energy.
10. Cluster heads then sends data to the base station currently at its vicinity.
11. Execute existing THIDS approach.
12. When $E_{CHi}<E_{thresh}$
13. remove CH_i from the cluster head
14. Set other CH_k = active
15. Supply the new $E(K_{ik},P)$ and $D(K_{ik}\text{-}1,C)$ to this CH_k.
16. End.

CONCLUSION

In this paper, we have presented an algorithm were we have used four sink nodes at each quadrants, which has the responsibility of distributing keys to the sensors as well as cluster heads at it respective quadrant.

These sink nodes becomes mobiles in its own quadrants and hence save the energy to considerable extent. We have used combination of public and private key cryptography which provides the robust security against various types of attacks. We have also used Monitor Nodes for detecting internal attacks.
We also have compressed the data so that less no. of bits could be transmitted from one cluster head to the other. In the next section, we will simulate the result and will compare it with the existing approach graphically.

In the future work, we can increase the number of base stations so that it could get enough power to distributed public keys individually to each sensor nodes also and hence could be more secure with maximum lifetime. However, more work be needed to done in this field so that global solution could be achieved.

REFERENCES

[1] Gay, D., Levis, P., and Culler, D. 2007. Software design patterns for TinyOS. Published in Journal ACM Transactions on Embedded Computing Systems (TECS), Volume.6, 2007.

[2] Dr. A. Senthilkumar, "Energy Efficient Secure Multipath Routing Protocol For Wireless Sensor Networks ", International Journal of Engineering Research & Technology (IJERT)Vol. 2 Issue 4, April – 2013

[3] Nidal Nasser and Yunfeng Chen, Secure Multipath Routing Protocol for Wireless Sensor Networks, 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07), 2007, IEEE

[4] THEODORE ZAHARIADIS, HELEN C. LELIGOU, STAMATIS VOLIOTIS,SOTIRIS MANIATIS, PANAGIOTIS TRAKADAS, PANAGIOTIS KARKAZIS,An Energy and Trust-aware Routing Protocol for Large Wireless Sensor Networks ,Proceedings of the 9th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS , (AIC '09).

[5] Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad. : Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks, IEEE SENSORS JOURNAL, VOL. 12, NO. 10, (2012)

[6] A. Abduvaliyev, et al, "On the Vital areas of Intrusion Detection Systems in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, pp. 1223-1237, 2013.

[7] Somia Sahraoui, Souheila Bouam , Secure Routing Optimization in Hierarchical Cluster-Based Wireless Sensor Networks,International Journal of Communication Networks and Information Security (IJCNIS), Vol. 5, No. 3, December 2013.

★★★