ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

A Secure and Advanced Data Gathering Pattern for Wireless Sensor Networks

Krupa A

Assistant Professor, Department of Studies in Computer Science, Pooja Bhagavat Memorial Mahajana Post Graduate Centre,K.R.S. Road, Metagalli, Mysuru, Karnataka, India

ABSTRACT: Contemporary trends in wireless networks brought many researchers to develop new protocols for data gathering. A secure and advanced data gathering pattern for Wireless Sensor Networks is introduced in this paper to secure data gathering. A modified Diffie Hellman Key Exchange algorithm is used in generation of keys and exchanging of keys between the sensor nodes in order to maintain security and avoid data from malicious nodes in the network. The performance is validated in terms of energy consumption, network lifetime, throughput, residual energy. The proposed scheme performs better than existing systems like SMART AND EEHA schemes.

I. INTRODUCTION

Wireless sensor networks (WSN) or wireless sensor and actuator networks (WSAN) are spatially distributed autonomous sensors used to monitor physical or environmental conditions, such as sound, pressure, temperature, etc. and to effectively pass the collected data over a network to main location. Wireless Sensor Networks grew in usage scale due to the military applications such as surveillance in battlefield and later many industries started using them for consumer applications such as process monitoring in industries, machine health monitoring, and so on.

The WSN is built of nodes – the nodes may scale from a few to several hundreds or even thousands, where each node is connected to one or more sensors. Each and every such sensor network node has typically several parts: a radio transceiver with either an internal antenna or an external antenna, a microcontroller, an electronic circuit for interacting or communicating with the sensors and an energy source, usually a battery or an embedded form of energy resource. A sensor node might vary in size from that of a computer size down to the size of a grain of dust. The cost of sensor nodes is variable, ranging from a few to hundreds of dollars, depending on the complexity, type of data gathered and various other factors. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as memory, computational speed, and energy and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

Sensor nodes on WSNs are operating with limited battery-power. The efficiency of the power source is one of the important factors for wireless sensor networks, since it is difficult to replace power source with new ones in large-scale wireless networks generally at sensor networks, gathered data is sent to a fixed base station. Since data transmission and reception consume most of node energy, middle nodes on the path consume more energy when they forward packets to the base station.

Applications of sensor networks can be classified based on its operational areas: data gathering and event driven. The data gathering application requires nodes to update their data to the base station on a timely basis. In event driven application, the nodes sends data to their base stations only when a certain event occurs, this event depends on application to application.

Wireless transmission is a vital source of power consumption. Hence a significant part of communication in WSNs is due to data gathering. Data gathering plays a vital role in WSN since the aggregation methodology reduces the amount of power consumed for data transmission between the sensor nodes. There are many gathering techniques used in WSN:

1. Tree based aggregation
2. In network aggregation

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Wireless Sensor Network is composed of sink node sometimes called as a Base Station and many small sensor nodes. The nodes monitor an assigned area and aggregate the information. Data collected by the sensor nodes are transferred to the base station using wireless transmissions. Aggregation policy reduces the amount of traffic; it helps to minimize the energy consumption. Two main concerns that bother in secure data gathering are confidentiality and integrity of data. While existing encryption is used to result end to end confidentiality in WSN. The aggregator node requires conducting the decryption process to decrypt the encrypted data to complete aggregation which in turn reveals the plain text at the aggregator nodes, which makes the data vulnerable to attacks.

This paper proposes an advance data gathering approach for aggregating location data on wireless sensor networks. One important factor is to reduce the energy consumption of the sensors in order to increase the lifetime of the network. Measures have been taken to provide superior level of data gathering with high security. The information of the node is constantly updated to find the nearest neighbor node for data transferring or forwarding. The Euclidean distance between the nodes is calculated to determine the neighbor node for data packet forwarding. Network lifetime is increased because of the lesser energy consumption.

The paper is divided into many sections as follows: Section 2 provides the previous work in secure energy based data gathering schemes. Section 3 describes about the proposed advanced data gathering approach for aggregating location data. Section 4 provides some performance analysis. And at last the conclusion and future work in section 5.

II. PREVIOUS WORK

This section provides the previous works targeting secure energy aware data gathering and routing schemes. *Yoo et al* [1] designed a secure energy and reliability aware data gathering protocol. This protocol provides protection against the network layer attacks. *Zhou et al* [2] work was to protect Wireless Sensor Networks from routing attacks with trust aware location based secure routing protocol. *Ahvar et al* [3] researched on the fuzzy based energy aware routing protocol for WSN. FEAR protocol concentrates on the energy balancing and energy saving. *Bahi et al* [4] suggested a secure data aggregation technique in WSN. This scheme was based on elliptic curve cryptography, which exploits a smaller size keys.

Leligou et al [5] proposed a routing protocol with trust and location information in WSN. This protocol was utilized for balancing trust and location information. *Zhan et* [6] *al* suggested a trust aware routing model. It provides trusted and energy efficient route. It opposes the harmful attacks established out of identity trick. *Crosby et al* [7] designed a setup where the system detects all the compromised nodes in the network with the help of a verification algorithm for the verification of the location information of the sensor nodes. *Feng et al* [8] formulated a node behavioral strategies banding belief theory of the trust evaluation algorithm. A trust factor and the coefficients were established to attain the direct and indirect trust values by estimating the weighted average of trust factors. The fuzzy set method was applied to form the vector evidence. The evidence difference was determined between the indirect and direct trust values that combine the revised D-S evidence combination rule.

Zhao et al [9] formulated a secure geographical routing protocol. This protocol utilizes the location pair wise keys for secure routing of packets. *Mao and Yuxin* [10] proposed an algorithm which combines a counter based intrusion detection algorithm and key based secure routing algorithm. *Duan et al* [11] designed a Trust aware Secure Routing Framework (TSRF). Firstly, the features of known attacks were analyzed on trust routing approaches. Then, the trust derivation scheme and specific trust calculations were formulated based on the analysis. *Huang et al* [12] proposed a secure encrypted data aggregation scheme to remove the redundant sensor readings without the encryption policy. Security and privacy aggregation were provided and the duplicate instances were composed as a single packet.

III. SECURE ENERGY EFFICIENT LOCATION AWARE DATE GATHERING APPROACH

Due to the nature of hostile environmental condition and vulnerabilities of the WSN, it is really tough task to protect the complex information. Moreover, wireless sensor networks faces security issues which is very crucial for a network that the traditional networks do not face. Because of these factors it demands a lot of research on various ways to create a secure environment for the nodes to communicate among themselves. The proposed system uses the Elliptic Curve Diffie Hellman Key Exchange (ECDHKE) Algorithm. Figure.1. shows the flow of the proposed method. The following sections describe the interaction between the energy consideration and data gathering process.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

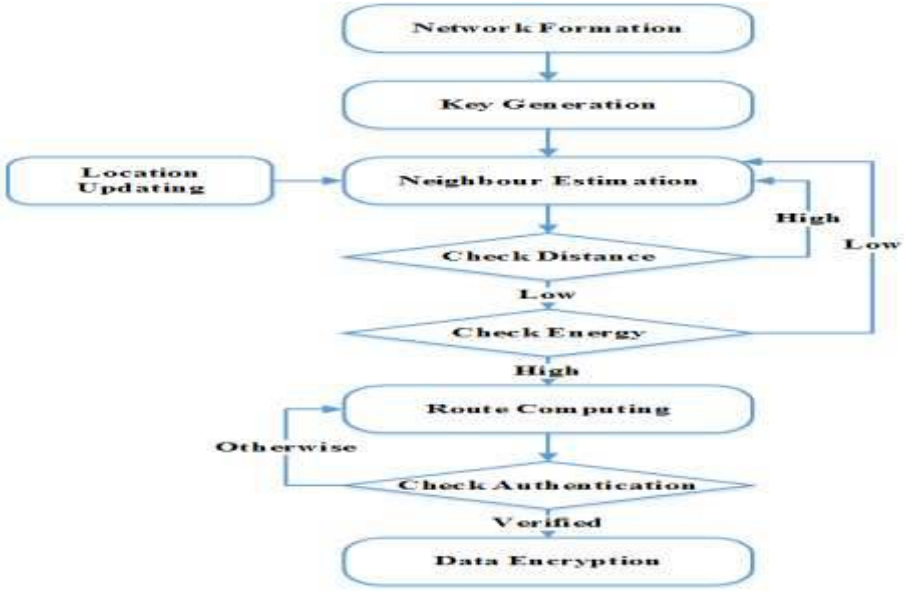

Figure 1. Flow of the proposed system.

1. Security Requirements

Data confidentiality, data integrity, availability and source authentication are the major security requirements for wireless sensor networks.

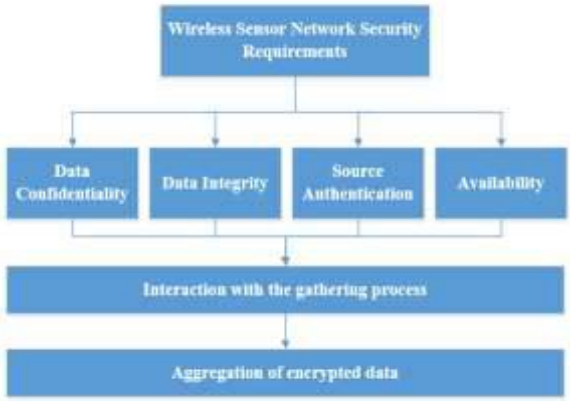

Figure.2. Interaction between wireless sensor network security and data gathering process

1.1 Data Confidentiality

Unauthenticated nodes/parties should never be given access to the data, if nodes can access the data that are not supposed to be exposed, and then the data loses its confidentiality. Confidentiality of the data improves the secrecy of the data gathered and this data is more valued than that of the leaked data. Hence, it is essential to build the secure communication channels between sensor nodes. The data like sensor ids and public keys must be encrypted to protect against the security attacks. The traditional method to keep the sensitive data is to encrypt the information with some kind of encryption technique with higher encryption key size to increase the complexity of the decryption process. The proposed scheme uses the ECDHKE algorithm to exchange the keys between the nodes. This results lesser delay and energy consumption and also provides the end-to-end confidentiality.

1.2 Data Integrity

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Data confidentiality prevents only from data not being accessed by unauthorized nodes or users, but it won't stop from data being changed where as data integrity guarantees that a data being transferred are never corrupted.

1.3 Source Authentication

Authentication is the process where the nodes have to identify themselves to the network in order to restrict any unauthorized nodes getting into the network. The sensor network uses a shared medium and the sensor nodes need standard authentication mechanisms to identify the unauthenticated packets. Without the source authentication policy, an adversary node can attack the network and access the sensitive information. If two nodes are communicating there are lots of authentication mechanisms available to identify the nodes themselves in the communication network.

1.4 Availability

Denial of Service (DOS) is a kind of attack where a node or a resource is made unavailable in the network. And hence availability is a major constraint that guarantees the stability of network performance against Denial of Service attacks.

2. Route Formation

The sensor nodes broadcast the HELLO packet throughout the network to discover the nearest node and live nodes in the network and the energy of the particular node. There are two major criteria used for route selection.

1. Distance among the nodes.
2. Energy computation

2.1 Neighbor node selection

The neighbor nodes are found based on the Euclidean distance. The packets are forwarded to the nodes with shortest distance. Consider the two points x = (x1, x2,…,xn) and y= (y1, y2,…,yn). The distance from x to y or from y to x is given by:

$$d(x,y) = d(y,x) = \sqrt{\sum_{i=1}^{n} (y_i - x_i)^2} = \sqrt{(y_1 - x_1)^2 + (y_2 - x_2)^2 + \ldots + (y_n - x_n)^2} \quad \ldots\ldots\ldots (1)$$

Equation for computing the distance between the sensor nodes is given in Equation (1). The shortest distanced neighbor nodes are selected to forward the data.

Neighbor Discovery Algorithm

1: func Neighbor discovery
2: Broadcast the RTR packet with source information
3: end func

Receiver side RTR packet algorithm

1: Receive RTR ()
2: Retrieve the sender location from RTR packet
3: Retrieve the receiver location
4: Calculate the distance between Source to Destination (d(S, D) and Receiver to Destination (d (R, D)
5: if (d (S, D) < d (R, D))
6: if (packet type! = broadcast)
7: add the entry to neighbor table with flag 1
8: else
9: add the entry to neighbor table with flag 0
10: Send RTR reply packet to sender with receiver information
11: end if
12: end

RTR packet algorithm is established at the receiver. The sender location is retrieved from the RTR packet. The receiver location is also noted. Then, the distance from source to destination and receiver to destination is estimated. If the distance from (S, D) is lesser than (R,D) then the algorithm checks the packet type. Then, a value 1 will be appended to the neighbor table else it will be 0. At last, the RTR reply packet will be forwarded to the sender with the receiver information.

2.2 Energy Analysis of proposed routing protocol

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

In the proposed protocol, nodes route the data packets to the destination through the intermediate nodes and the selection of intermediate nodes is a crucial process. The intermediate nodes are selected such that the transmit amplifier energy is minimized. Hence node 1 transmits to node 3 through node 2 if and only if:

$E_T\ k,d = d_{12} + E_T\ k,d = d_{23} < E^T\ k,d = d_{13}$ …… (2)

Or

$d^2_{12} + d^2_{23} < d^2_{12}$ …… (3)

The messages are encrypted based on the key generation algorithm and the resulted encrypted data are combined at the base station shown in Figure.3.

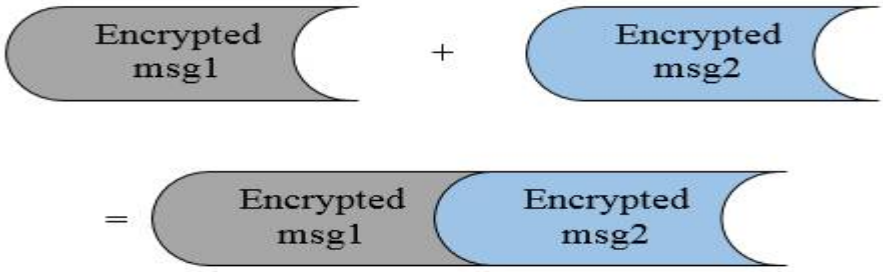

Figure.3 Final encrypted data

IV. PERFORMANCE ANALYSIS

This section presents the results gathered during the simulation of the environment using the secure and advanced data gathering pattern for Wireless Sensor Networks. Here a source location estimate is obtained through the periodic HELLO packets. The simulation was performed in NS2 and the total number of nodes is 500 nodes in the area of 1000m x 1000m. Table 1 shows the simulation parameters.

Table 1 Simulation Parameters

Parameters	Values
Total number of sensor nodes	500
Simulation area	1000 X 1000m
Node distribution	Random
Simulation Time	50ms
Initial Energy	15J

The performance of the proposed data gathering scheme is validated and compared with the existing data gathering scheme without security measures. Following parameters have been considered for performance evaluation which involves: packet drop, network lifetime, throughput and residual energy.

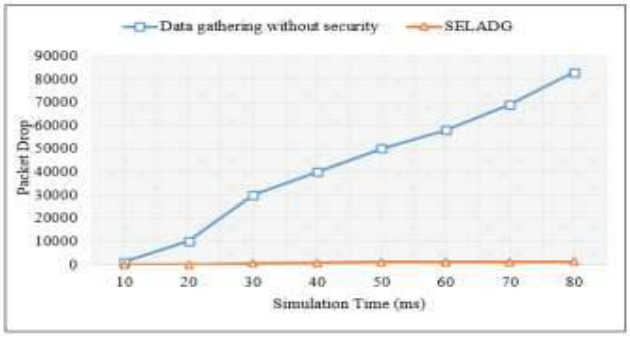

Figure.4. Packet drop

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Figure 4 shows the difference between the existing system and proposed system. As shown clearly the performance with packet drop metric is very much high compared to the previous systems.

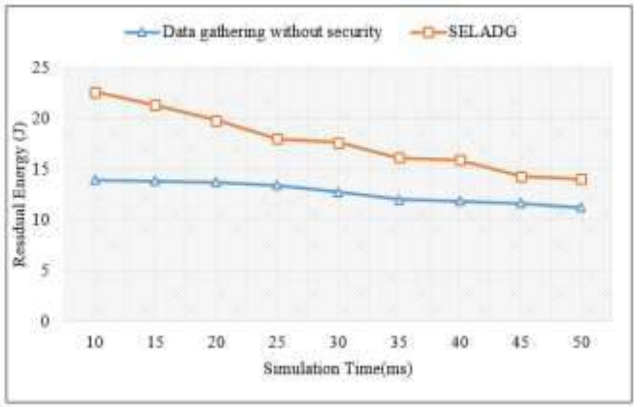

Figure.5. Residual energy

Figure 5 shows the difference between the performances of existing system and proposed system with respect to residual energy is concerned.

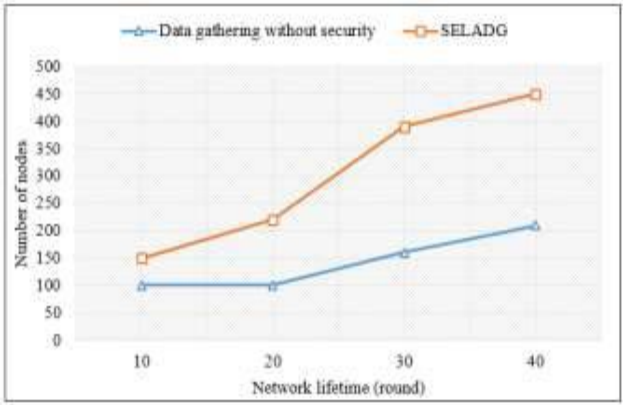

Figure.6. Network lifetime vs number of nodes

The proposed system has better residual energy due to the proposed energy criteria which is shown in Figure.5. Hence the lifetime is improved for the proposed methodology. The comparison graph is shown in Figure.6. It shows the proposed method can result better network lifetime than the existing approach.

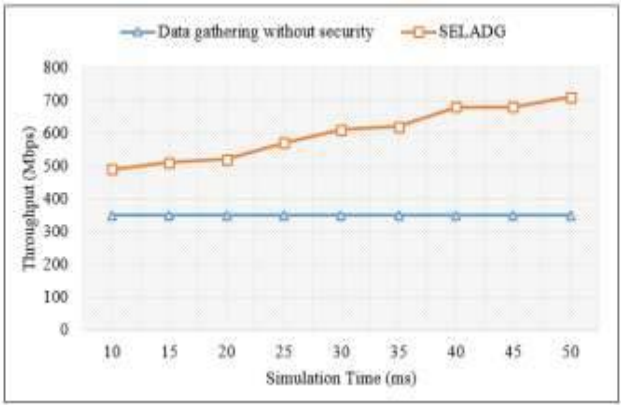

Figure.7. Throughput vs simulation time

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Throughput is the total number of data packets that have been received at time *t* by a destination. Figure.7.shows that the proposed scheme can result better throughput than the existing approach.

V. CONCLUSION AND FUTURE WORK

In this paper, a secure and advanced data gathering pattern for Wireless Sensor Networks is proposed. The lifetime of the node and network is increased with the help of the node location and energy. Secure data gathering algorithm termed Elliptic Curve Diffie Hellman Key Exchange is used for secure data gathering between source and receiver. Comparison of the performance with the existing system is shown in separate section. Performance parameters like packet drop, throughput, residual energy and network lifetime is improved compared to existing systems. In future work, the proposed structure is incorporated with a super node and clustering concepts to provide better and secure data gathering.

REFERENCES

1 S. Yoo, S.-h. Kang, and J. Kim, "SERA: a secure energy reliability aware data gathering for sensor networks," Multimedia Tools and Applications, pp. 1-30, 2011/01/29 2011.
2 Y. M. Zhou and L. Y. Li, "A Trust-Aware and Location-Based Secure Routing Protocol for WSN," Applied Mechanics and Materials, vol. 373, pp. 1931-1934, 2013.
3 E. Ahvar, A. Pourmoslemi, and M. J. Piran, "Fear: A Fuzzy-based Energy-aware Routing Protocol for Wireless Sensor Networks," arXiv preprint arXiv:1108.2777, 2011.
4 J. Bahi, C. Guyeux, and A. Makhoul, "Secure Data Aggregation in Wireless Sensor Networks: Homomorphism versus Watermarking Approach," in Ad Hoc Networks. vol. 49, J. Zheng, D. Simplot-Ryl, and V. M. Leung, Eds., ed: Springer Berlin Heidelberg, 2010, pp. 344-358.
5 T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," Wireless personal communications, vol. 69, pp. 805-826, 2013.
6 H.-C. Leligou, P. Trakadas, S. Maniatis, P. Karkazis, and T. Zahariadis, "Combining trust with location information for routing in wireless sensor networks," Wireless Communications and Mobile Computing, vol. 12, pp. 1091-1103, 2012.
7 G. Zhan, W. Shi, and J. Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," Dependable and Secure Computing, IEEE Transactions on, vol. 9, pp. 184-197, 2012.
8 G. V. Crosby, L. Hester, and N. Pissinou, "Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks," IJ Network Security, vol. 12, pp. 107-117, 2011.
9 R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory," Sensors, vol. 11, pp. 1345-1360, 2011.
10 J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2014, 2014.
11 H. Zhao, Y. Li, M. Zhang, R. Zheng, and Q. Wu, "A New Secure Geographical Routing Protocol Based on Location Pairwise Keys in Wireless Sensor Networks," International Journal of Computer Science Issues (IJCSI), vol. 10, 2013.
12 Y. Mao, "A secure mechanism for data collection in wireless sensor networks," Applied Mathematics & Information Sciences, vol. 5, pp. 97-103, 2011.