RESEARCH ARTICLE OPEN ACCESS

Implementation of Data Aggregation Protocol for Wireless Sensor Networks and Ai to Minimize the Energy Consumption in Surface and Underground Mining

Prof. Amar Nath Singh [1], Mr. Rishi Raj [2]
Department of Computer Science & Engineering
Department of MCA,
Amity University, Ranchi
Jharkhand – India

ABSTRACT
The wireless sensor network is a vast, wide range application in which many researches are continuing now a days. In WSN, the most prominent area of research is, how the WSN imparts a important role in the modern era of technology.
As we know that, In WSN the sensor nodes which are used is a kind of hardware device which always require some amount of energy for its operation. This energy is called as operational voltage for sensors. As we know that each node in the arrangement requires some energy for its operation, so as an arrangement they took a huge amount of energy for their operation.
In this paper, we are proposing to design an Energy Efficient Secure Data Aggregation Protocol for wireless sensor networks to minimize the consumption of energy. In this protocol, we incorporate the authentication and security to maintain the efficiency of the data aggregation. To make our experiment more effective, First the network is divided into clusters which is a combination of some nodes where one node is called as a master node and other are called as slaves node, here each cluster is headed by an aggregator and the aggregators are connected to sink either directly or through other aggregators. The selection of the aggregator node is purely based on the nearest distance to a set of sensor nodes and its energy level. Separate keys are distributed to the two levels i.e., sensor node to the aggregator and aggregator to the sink.
Whenever a sensor node wants to send data to another node; first the sensor node encrypts the data using a key and sends it to the aggregator. Here the Source and sink nodes are the most vital node which are used to transmit the information in terms of energy mode.
Keywords:- Wireless Sensor Networks, Artificial Intelligence, Data Aggregation, Aggregator, Energy factor, MAC energy, Surface mining and Underground Mining.

I. INTRODUCTION

The Wireless sensor networks comprises with the upcoming technology that has attained noteworthy Consideration from the research community. It is applied in most of the research area of science now a day. As we know that the sensors are the hardware devices which are used to require some energy for its operation. The sensor networks comprise of many small, low cost devices and are naturally self-organizing ad hoc systems. In the Mines area, to sense the environmental data we are usually mount the sensors which are driven by AI logic-based algorithm. The most important function of the sensor network is monitoring the physical environment, collect and transmit the information to other sink nodes. After collecting the information, these data are to be send to the host machine for further processing. Here to send the data we are using the radio transmission whose ranges must be optimal for the sensor networks in the orders of the magnitude which is smaller than the geographical extent of the intact network. Hence, the data has to be transmitted hop-by-hop towards the sink in a multi-hop manner. The consumption of energy by the sensor present in the network is directly proportional to the amount of data it is being transmitted. So the

consumption of energy can be reduced if the amount of data to be relayed is reduced. [11]. Wireless sensor network comprises of a great number of minute electromechanical sensor devices which posses the sensing, computing and communication abilities. These devices can be utilized for gathering sensory information, like measurement of temperature from an extended geographical area [2]. Many of the features of the wireless sensor networks give rise to challenging problems [3]. The most important three characteristics are:

• Sensor nodes are the ones which are prone to maximum failures.
• Sensor nodes make use of the broadcast communication pattern and have severe bandwidth restraint.
• Sensor nodes have limited amount of resources.

1.2 Data Aggregation:

As we know that, the mines area are very sensitive area because the soil strength factor are not identical at everywhere. So to make the mining process safe and to identify the geological and environmental condition, we usually mount the sensor nodes in the mines. But by implementing the sensors it consumes huge amount of energy for its operation and hence data transmission rate is increases. So we now trying to implement the Data aggregation, which is considered as one of the most fundamental distributed data processing procedures for saving the energy and minimizing the medium access layer contention in wireless sensor networks [4]. Data aggregation technique is considered as an important pattern for routing in the wireless sensor networks. The basic idea is to merge the data from various sources, reroute it with the elimination of the redundancy and thus reducing the number of transmissions and saving the energy [5]. The inbuilt redundancy in the raw data gathered from various sensors can be prevented by the in-network data aggregation. Additionally, these operations use raw materials for obtaining application specific information. To preserve the energy in the system for maintaining longer lifetime in the network, it is important for the network to maintain high incidence of the in-network data aggregation [6].

1.3 Secure Data Aggregation:

Whenever the data aggregation are done in mines area, then due to environmental condition, the security of data became the major issue. As we know that the waves so far used in the mines area are highly defected by the moisture so now we are going to used the Secure Data Aggregation approach to secure our data transmission. We also know that, The issues related to the security in the data aggregation of WSN using AI logic are many, out of which some are listed below:

1.3.1 Data Confidentiality:

In particular, the basic security issue is the data confidentiality which safeguards the transmitted data that is sensitive from passive attacks like eavesdropping. The importance of the data confidentiality is in the hostile environment, where the wireless channel is more susceptible to eaves dropping[8].

1.3.2 Data Integrity: The purpose of using it to prevent the alteration of the final aggregation value by the compromised source nodes or aggregator nodes. As we know that, when the data from various nodes are integrated, the there is a chance to get data error. The sensor nodes can be easily compromised due to the lacking of the expensive tampering-resistant hardware. The otherwise used hardware may not be reliable at times. So there is a chance that, the compromised message is capable of modifying, forging and discarding the messages.

So, whenever we think for secure data aggregation in wireless sensor networks using AI logic, we usually refer two methods, such as

1.3.2.1. Hop-by-Hop encrypted data aggregation: In this technique, the encryption of the data is performed by the sensing nodes and decryption by the aggregator nodes. The aggregator nodes aggregate the data and again encrypt the aggregation result. At the end, the sink node on obtaining the final encrypted aggregation result decrypts it[10].

1.3.2.2. End to End encrypted data aggregation: In this technique, the aggregator nodes in between have no decryption keys and can only perform aggregation on the encrypted data.

1.4 Adopted Methodology:

By considering the existing technique, in contrast to the modern scenario, the following are the biggest problems were found when we are going to mount the sensor in the mines area. Few of the problems are mentioned as below:

1. The communication overhead is maximum on sensor

nodes.
2. It has more complexities.
3. High bandwidth consumption during the operation.
4. Reducing energy consumption is not optimal.
5. There is no integrity and authentication of data.

Hence, It became a challenge to the miners, how to go for secure data aggregation in mines. So we are going to propose a system, where we are using the cluster technology of WSN driven by AI logic to identify the gap and try to resolve the problem issues.

II. PROPOSED SYSTEM

As we know that, the environmental condition at mines are not identical at every places, hence we can't depends on a single sensor to get our service. In most of the time due to because of temperature the sensors are get damage and we can't receive the proper information. So to resolve the problem, thus we are trying to go for the cluster technology. In a clustered WSN, the network is grouped into clusters. In each cluster, there is an aggregator which consists of a very powerful wireless transceiver that is capable of transmitting the data directly to the backend server. Here each sensor performs the transmission of the data only to the aggregator[10]. As a result, each sensor will be able to reduce the overhead in transmitting the data packets

The verification information is built by the source using the shared key. Verification information is included with data packet during the transmission. On reception of the packet, the source is verified by the aggregator using the shared key. If we need then we may also use the MAC based authentication code, for our authentication of data, which is used in order to maintain the integrity of the data packet. The sink can detect any changes performed by the aggregator including the verification information, by checking of the MAC value using its shared key. If the data packet is found to be modified, then it will be discarded[2].

III. DEPLOYMENT TECHNIQUE

In order to identify the system, we need to deploy the system first. Here the most important factor is energy consumption. To we are using the AI based logic to implement the system.

If a connection probability of connectivity requirementσ_0 for any sensor node (SN) is required, i.e., $p_R \geq \sigma_0$ the minimum number of aggregators, *aggr* is expressed as:

$$N_{aggr} \{\min\} \geq \ln(1-\sigma_0)/\ln(1-\Pi r_{SN}^2/|A|)2 \qquad (1)$$

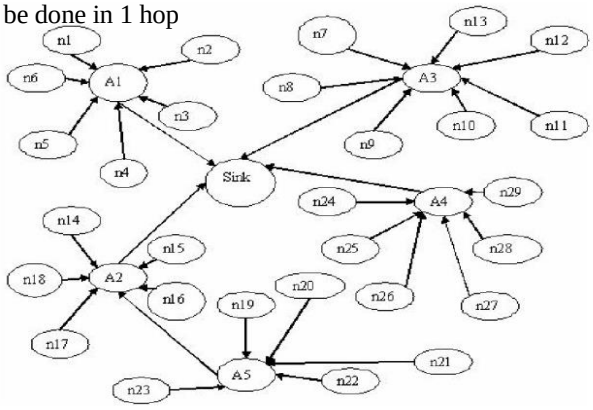
where r_{SN} : transmission radius

If the connectivity probability σ_0 is required, letting $p_R \geq \sigma_0$, and solving for N_{aggr}, we have

$$N_{aggr} \{\min\} \geq \ln(1-\sigma_0)/\ln(1-\Pi r_{SN}^2 EI/J) \quad (2)$$

where *EI* is the energy index of an area defined as the ratio of the energy consumption rate of the area to the size of the area.
J is the integral of *EI* .

where $E_{\text{int } ra}$: total energy spent on intra cluster communication by all the *aggr*
$E_{\text{int } er}$: total energy spent on inter cluster relay by all the *aggr*
r_{aggr} : radius around the *aggr* where the transmission can be done in 1 hop



IV. ALGORITHM FOR AGGREGATOR

1. The sensors send its data to the nearest aggregator, aggr since each sensor node has a aggr to ensure its connectivity
2. Each sensor node encrypts the data using the symmetric key Kch,i and sends it to its aggr .
3. When aggr receives the data packet from any node S , it decrypts the data using the symmetric key Kch,i

4. The aggr then calculates the MAC using the hash functions MAC(aggr) .
5. By calculating the MAC , the aggr ensures that the sensor sending the data is valid and
authenticates the sensor, else the sensor is considered to be invalid and it is deauthenticated
6. aggr again encrypts the data along with the MAC by the symmetric key Kch,s and transmits it to the sink.
7. When all the aggregated data from aggr reaches the sink, it decrypts the data using symmetric key Kch,s
8. The sink checks if the aggregated data is valid without any change in its content by checking its
MAC .
9. If the MAC is not valid, the aggr is prohibited from further transmissions

V. SIMULATION SETUP AND RESULT

The performance of Energy Efficient Secure Data Aggregation (EESDA) protocol in cluster technology based on WSN and AI logic is evaluated through NS2 simulation [12]. A random network deployed in an area of 50 X 50 m is considered. We vary the number of Attackers as 1, 2,..5. Initially the nodes are placed randomly in the specified area. The base station is assumed to be situated 100 meters away from the above specified area. The initial energy of all the attackers assumed as 3.1 joules. The IEEE 802.15.4 MAC layer is used for a reliable and single hop communication among the devices, providing access to the physical channel for all types of transmissions and appropriate security mechanisms. The IEEE 802.15.4 specification supports two PHY options based on direct sequence spread spectrum (DSSS), which allows the use of low-cost digital IC realizations. The PHY adopts the same basic frame structure for low-duty-cycle low-power operation, except that the two PHYs adopt different frequency bands: low-band (868/915 MHz) and high band (2.4 GHz). The PHY layer uses a common frame structure, containing a 32-bit preamble, a frame length. The simulated traffic is FTP with TCP source and sink. The number of sources is varied from 1to 4. And it has been found that the saving of the energy is of about 3.1J .

VI. CONCLUSION

In this paper, we have developed a secure data aggregation protocol for wireless sensor networks which maintains energy efficiency. For data aggregation, the system is grouped such that each group is headed by an aggregator. This aggregator acts as a link between the sensor nodes and the sink. During the transmission of the data, first encryption is performed by the sensor nodes when transferring data to the aggregator. The aggregator on reception of the data decrypts it using the key and reads it. The aggregator then determines the MAC value using hash function to check the validity of the source sensor. If the estimated MAC value is valid then the source is authenticated. Second encryption is performed by the aggregator when transferring data along with the MAC value to the sink. Hence integrity of the system is maintained. Due to the double encryption of the data during data aggregation, adversaries cannot affect the system. Hence the system remains secure even in the wireless environment. Simulation results show that our proposed protocol has reduced energy consumption while attaining good packet delivery ratio.

REFERENCES

[1] Dorottya Vass, Attila Vidacs, "Distributed Data Aggregation with Geographical Routing in
[2] Wireless Sensor Networks", Pervasive Services, *IEEE International Conference* on July 2007.
[3] Jukka Kohonen, "Data Gathering in Sensor Networks", Helsinki Institute for Information Technology, Finland. Nov 2004.
[4] Gregory Hartl, Baochun Li, "Loss Inference in Wireless Sensor Networks Based on Data Aggregation", IPSN 2004.
[5] Zhenzhen Ye, Alhussein A. Abouzeid and Jing Ai, "Optimal Policies for Distributed Data Aggregation in Wireless Sensor Networks", Draft Infocom2007 Paper.
[6] Bhaskar Krishnamachari, Deborah Estrin and Stephen Wicker, "The Impact of Data Aggregation in Wireless Sensor Networks", *Proceedings of the 22nd International Conference on Distributed Computing Systems*, 2002.
[7] Kai-Wei Fan, Sha Liu, and Prasun Sinha, "Structure-free Data Aggregation in Sensor Networks", *IEEE Transactions on Mobile Computing*, 2007.
[8] Yingpeng Sang, Hong Shen, Yasushi Inoguchi, Yasuo Tan and Naixue Xiong, "Secure Data Aggregation inWireless Sensor Networks: A Survey", *Seventh International Conference on*

Parallel and Distributed Computing, Applications and Technologies, 2006.

[9] Prakash G L, S H Manjula, K R Venugopal and L M Patnaik, "Secure Data Aggregation Using Clusters in Sensor Networks", *International Journal of Wireless Networks and Communications* Volume 1, Number 1 (2009), pp. 93-101.

[10] Tamer AbuHmed and DaeHun Nyang, "A Dynamic Level-based Secure Data Aggregation in Wireless Sensor Network", Information Security Research Laboratory Graduate School of IT &Telecommunication InHa University.

[11] Wenbo He, Xue Liu, Hoang Nguyen, Klara Nahrstedt andTarek Abdelzaher, "PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks", 26th IEEE International Conference on Computer Communications. IEEE INFOCOM 2007.

[12] Shih-I Huang and Shiuhpyng Shieh, "SEA: Secure Encrypted-Data Aggregation in Mobile Wireless Sensor Networks", *International Conference on Computational Intelligence and Security* 2007.

[13] Network Simulator: www.isi.edu/nsnam/ns

ABOUT THE AUTHOR

Prof. Amar Nath Singh is presently working at Amity University, Ranchi, Jharkhand as a reader in the department of Computer Science and Engineering. His research area is Underground Mines and Surface mining using Artificial Intelligence, Fuzzy Logic. His research area includes cloud computing, WSN, Machine Learning and Data Science. He has produced more than 60 M.Tech scholars till date.

Mr. Rishi Raj, is presently the scholar in MCA department at Amity University, Jharkhand.