RESEARCH ARTICLE OPEN ACCESS

Secure Data Aggregation in Wireless Sensor Network using Trust Model

M.Suraj [1], B.Raja [2], T.Vengattaraman [3]
Department of Computer Science [1] & [3]
Pondicherry University, Puducherry
Department of Computer Applications [2]
Bharathiar University, Coimbatore
Tamil Nadu - India

ABSTRACT

Wireless sensor networks usually consist of hundreds or thousands of inexpensive and low-powered sensing devices. In WSN, nodes have low computational power and communication resources to collect data to a specific function. Nodes have limited battery power and small data storage. In WSN, Security is an important issue, therefore its need to create a secure transmission model with minimum overheads and transmit the data securely to the Base station. In WSN, sensors are used to collect the data from the environment and pass it on to base station. Data aggregation is a technique to process and analyse the collected data from multiple sensor nodes and send the aggregated information to a base station through single route. Efficient Distributed Trust Model (EDTM) is a trust model for wireless sensor network used to provide the trustworthiness for each sensor nodes. The proposed model provides a secure data aggregation technique to avoid malicious node and false data generation during data aggregation in WSN. And also use to improve the average sensor lifetime, to eliminate redundant data transmission from multiple sensor nodes and to reduce the energy consumption during aggregation process. The simulation has been done in ns2.

Keywords: - Data Aggregation, Trust Model, Wireless Sensor Network.

I. INTRODUCTION

Wireless sensor networks are usually consists of hundreds or thousands of inexpensive and low-powered sensing devices. In WSNs, the basic function of sensor networks includes collaborative sensing, sampling, computing, broadcasting sensed information. However, sensors have severe resource constraints in terms of battery power, CPUs, storage, processing capability, finite radio range, and network bandwidth. It is a challenging task to provide efficient solutions to data gathering.

Several small and low cost devices are included in the sensor networks which are self-organizing ad hoc systems through which the information is collected and transmitted to one or more sink nodes by observing the physical environment. Thus, the data needs to be transmitted towards the sink node in a hop-by-hop manner. If the amount of data which needs to be transmitted is reduced, the energy consumption of the network is also minimized. To minimize this issue data aggregation technique is used in Wireless sensor network. Various data aggregation techniques are [4] Centralized Approach, Tree Based Approach, Cluster Based Approach and In-Network Approach. Data aggregation is the process of aggregating the sensed data from multiple sensor nodes and also uses to eliminate redundant data transmission and enhances the lifetime of energy in wireless sensor network. Aggregation is used to reduce network traffic energy consumption on sensor nodes. Main function of data aggregation is to suppress the duplication. Let two nodes source x and source y. All forwards same data to station z, now station z will send one of these forward, and used to save cost of data transmission. This can be done by one of the data aggregation technique that is In-network data aggregation. In this technique a number of sensor nodes act as a group which collects data or information from target region. Traditionally nodes send data individually when base station demands for network. Instead of that there is a special node called as aggregator which collects statistics from its neighbouring stations, adds them and forwards that combined information to base station in multi-hop pattern.

Efficient Distributed Trust Model (EDTM) [1] is a trust model for WSN, it is used for secure data aggregation in WSN. Here, every node locally calculates the trust value of all other nodes in the network by the calculation of direct trust, recommendation trust and indirect trust. The proposed system EDTM has been combined with In-network data aggregation to securely transmit the sensed data from multiple sensor nodes to the base station. EDTM provides trust worthiness for all sensor nodes by calculating the neighbour nodes in a distributed manner. The rest of the paper is organized as follows: section II presents the literature survey for data aggregation in wireless sensor network. In section III and IV data aggregation and its approaches are discussed. Section V covers the proposed system and section VI concludes the paper.

II. LITERATURE SURVEY

Jinfang Jiang [1] et al the authors have proposed the EDTM trust model to provide the trust worthiness to each sensor nodes in a WSN. EDTM has been compared with the previous trust model NBBTE while comparing, EDTM has been performed better than NBBTE. Direct and recommendation trusts are calculated to find the trust worthiness of each sensor node EDTM is used. Direct trust is calculated by considering the values of Communication trust, energy trust and data trust. EDTM is a multi-hop network which means the sensor nodes can only have direct communication with the neighbour nodes within their communication range. EDTM used to keep neighbourhood information which implies significant less memory space, less processing for trust level calculation, and lower energy consumption.

Elena Fasolo et al, [4] in this paper the authors have described various, in-network aggregation technique and protocols. The aim of this paper is used to provide appropriate taxonomy of in-network aggregation. In one hand it provides the existing solutions and on other hand , it provides the solution for future use. The main goal of the paper is to motivate the researchers to use in-network aggregation.

V.Umarani and K.Soma Sundaram [5], in this paper the authors have discussed about trust models general structure such as Centralized, distributed and hybrid, next the author discussed about the design issues attacks and their defense mechanism in trust model. Finally they compared various existing trust model with each other. Therefore need of trust model in wireless sensor network is extensively discussed in this paper.

Suman Nathy, Phillip B. Gibbons et al, [11] here the author describes the synopsis diffusion general framework in an in-network aggregation. Synopsis diffusion uses order- and duplicate-insensetive (ODI) which avoids duplicate data and ODI synopses used to summarize the intermediate result during in-network aggregation.

Sumedha Sirsikar and Samarth Anavatti [12], in this paper the authors focus on various issues with respect to data aggregation process such as delay, redundant data elimination and reliability. Different data aggregation strategies has been studied. And various existing data aggregation has some different issues like redundancy, delay, accuracy, and traffic load. And this issues affect the performance of data aggregation. In this paper the author consider some methods to solve this issues by using different approaches and technique. For the above stated issues the comparative analysis have been done. And based on that, they proposed one model which performs data aggregation at two levels one is cluster head and another at storage node. By doing this the tradeoff is maintained between energy efficiency and accuracy and also it balance traffic load.

Nanthini.D and R.A.Roseline [13], in this paper the authors focus on various types of data aggregation in Wireless Sensor Network and also describes the general techniques and protocols used for it. A protocol have been proposed to route packets for facilitating data aggregation.

Sushruta Mishra and Hiren Thakkar [14], here the features of WSN and data aggregation have been discussed. Various architecture for data aggregation techniques are explained and simulation software is discussed in this paper.

III. DATA AGGREGATION

Data aggregation [4] is used for grouping the data from multiple sensor nodes by avoiding the redundant data transmission and that data has been sent to the base station in single route. Fig. 1 represents Data aggregation process, by this aggregation method can reduce number of redundant transmission and thus it improves the network performance and also provides bandwidth utilization.

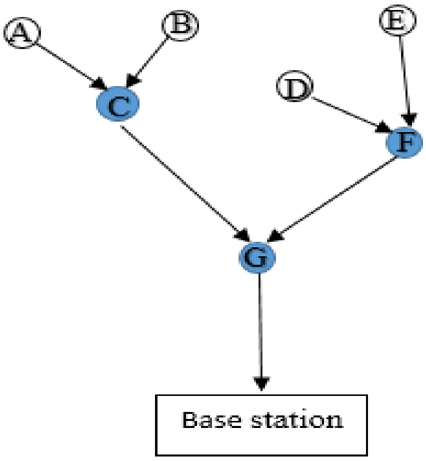

Fig.1 Data Aggregation

In WSN, traditionally nodes send data individually when the base station demands for network. Instead of that there is a special node called aggregator which used to collects statistics information from its neighbouring stations, adds them and forward that combined information to the base station in multi-hop manner. Various data aggregation algorithms are used to gather the sensed data from the sensor nodes and then aggregates the data and sent to the base station.

The main aspect of data aggregation is to collect and aggregate data in an energy efficient manner by which the network lifetime increases quietly. Aggregating data is a technique of compressing the transmitted packet, in the sense that the packet has only the necessary information.

A good aggregation function for Wireless Sensor networks need to have some additional requirements such as, they should take care of energy capabilities of the sensor devices, energy resources and computational capabilities. The topology of the network should be considered as important factor to construct aggregation function which is then used by the sensors.

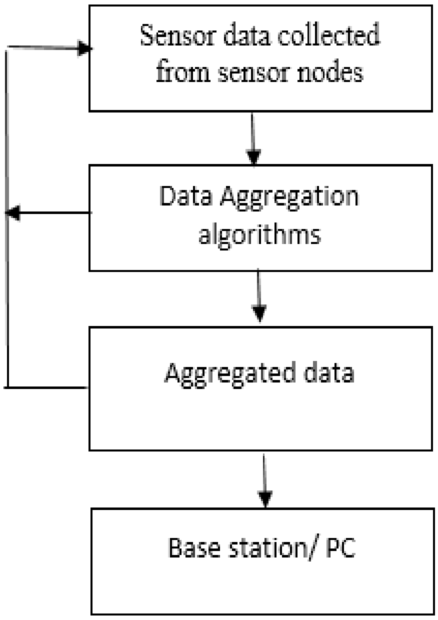
Sensor data collected from sensor nodes
Data Aggregation algorithms
Aggregated data
Base station/ PC

Fig. 2 General Architecture for Data Aggregations

Fig. 2 shows the architecture of data aggregation, in which the sensor nodes are collected from the different sensors and for the data aggregation we can use different algorithm as shown in the above figure. Then the data is aggregated ,that it used to sense the informatiom from multiple sensor nodes. And finally its send to the base station.

IV. DATA AGGREGATION APPROACHES

Aggregation techniques reduces energy consumption in sensor nodes and also used to avoid double counting problem. Many researchers have been identified different approaches. There are five Approaches for data aggregation [3]

A. Centralized Approach
B. Decentralized Approach
C. IN-Network Approach
D. Tree Based Approach
E. Cluster Based Approach

A. Centralized Approach

Centralized approach is an approach in which each sensor node sends its sensed data to a base station. The sensor nodes in wireless sensor network transmit the data packets to a leader node or base station, which is the powerful node with respect to energy and also acts as a central node. The leader node aggregates the data according to the queries. Each intermediate node has to transmit the data packets addressed to leader node from the child nodes. Then for the given query a large number of messages have to be transmitted in a best case equal to the sum of external path lengths for each sensor nodes.

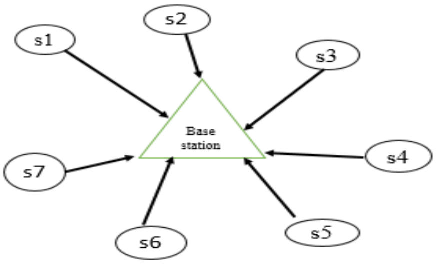

Fig. 3 Centralized Data Aggregation

B. Decentralized Approach

Decentralized approach is an approach in which all sensor nodes act as a aggregator to the sink node. In this approach there is no centralized node. In Fig. 4, all neighbour nodes can communicate with each other. It is more scalability when compare to other approaches.

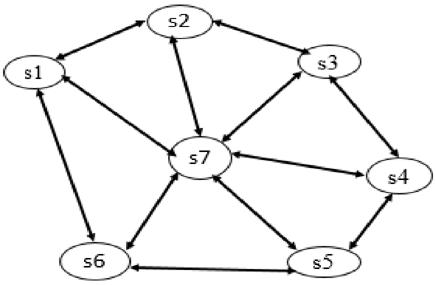

Fig. 4 Decentralized Data Aggregation

C. In-Network Approach

In-network aggregation is an approach for gathering and processing the data at intervening nodes and routing that processed information in a multi-hop network. The objective of this approach is to reduce resource consumption and to increase the network lifetime.

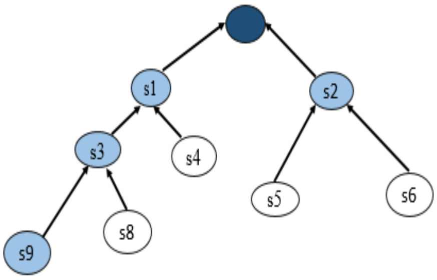

Fig. 5 In-Network Data Aggregation

There are two types of in-network aggregation: with size reduction and without size reduction.

i) With size reduction is used to reduce the packet size to be forwarded towards the sink node by combining & compressing the data packets received by a sensor node from its neighbours.

ii) Without size reduction will not process the value of data but merge all the data packets received from different neighbouring sensor nodes into a single data packet.

D. Tree Based Approach

In this approach, Data Aggregation Tree (DAT) is formed at first for data transmission. An aggregation tree is constructed for each data transmission with minimum spanning tree. Each node in a network has a parent-child relationship in which the data is forwarded in a bottom-up approach. Data flow starts from leaf nodes to the sink and the aggregation is done by parent nodes in the network.

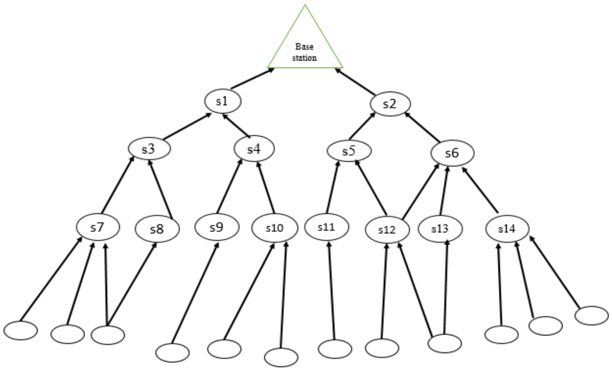

Fig. 6 Tree based Data Aggregation

E. Cluster Based Approach

In cluster-based approach, the entire network is formed as clusters. Cluster head is selected among the sensor nodes within a cluster. Cluster heads is used to receive and transmit data among sensor nodes present in a cluster. Cluster head acts as an aggregator which aggregates the data received and send to the base station.

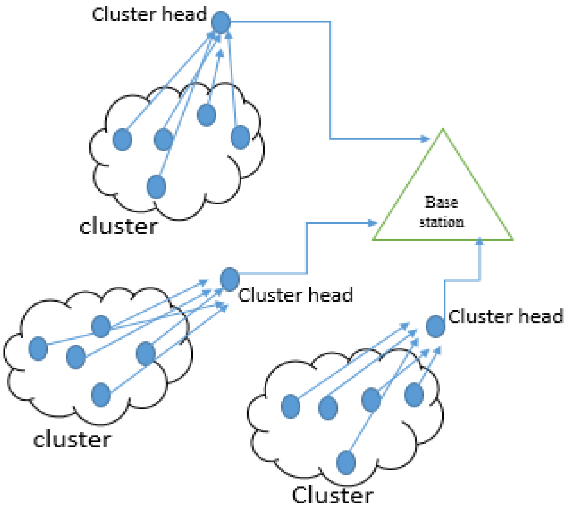

Fig. 7 Cluster based Data aggregation

Table 1 show the comparison of different data aggregation algorithms. The algorithm Synopsis Diffusion based on In-Network Aggregation is used for multi-hop network.

TABLE 1: Comparison of data aggregation algorithms

Algor. Char.	TAG	Directed diffusion	PEGASIS	LEACH	Synopsis Diffusion	Tributaries and Deltas
Aggregation Method	Tree Based	Tree Based	Centralized	Cluster Based	In-Network, Multi hop	Tree/ In-network
Overhead to setup	High	High	High	Medium	Medium	Medium
Scalability	Low	Medium	Very Low	Low	High	Medium
Timing Strategy	Periodic per hop adjusted	Asynchr onous	Periodic per hop adjusted	Periodic per hop adjusted	Asynchron ous	Asynchronous
Resilience to Link Failures	Low	Medium	Very Low	Low	High	Medium

In-Network Aggregation approach is used for the proposed system which uses synopsis diffusion algorithm for data aggregation. In the next section the proposed systemis discussed in detail.

V. PROPOSED SYSTEM

The proposed work is used to provide secure data aggregation by combining trust model and in-network aggregation in WSN.

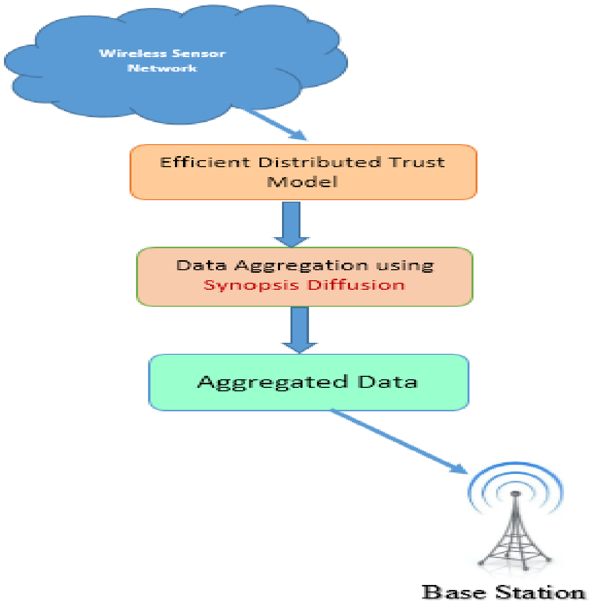
Wireless Sensor Network
Efficient Distributed Trust Model
Data Aggregation using Synopsis Diffusion
Aggregated Data
Base Station

Fig. 8 Architecture of proposed work

In figure 8, Sensor nodes in wireless sensor network is secured by EDTM trust model using which malicious nodes are avoided in data aggregation process and data aggregation for multi-hop WSN is done by using synopsis diffusion which aggregates the data and sent to the base station. The modules involved in the proposed systemare

A. Efficient Distributed Trust Model (EDTM)

B. Data Aggregation using Synopsis Diffusion

A. Efficient Distributed Trust Model:

Efficient Distributed trust model [1] is used to calculate the direct trust and recommendation trust based on the number of packets received from sensor nodes in wireless sensor network. While calculating direct trust, the other trusts like communication trust, energy trust and data trust are considered. Recommendation trust is checked for its trust reliability to improve the accuracy of recommendation trust for sensor node. This existing EDTM trust model has been compared with the previous NBBTE model and the simulation result shows EDTM has provide more security than the previous model. Therefore the EDTM model detects the malicious nodes based on the trust value calculated.

The wireless sensor network designed for the proposed system is a multi-hop network. Therefore each sensor node could only have a directly communicate with the other neighbouring sensor nodes within their communication range. EDTM model provides more security and increase the packet delivery ratio in WSN.

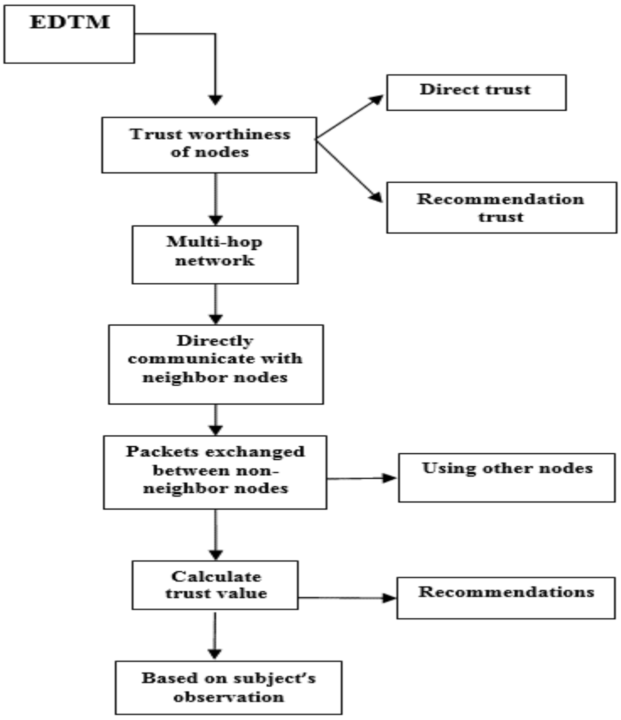
EDTM
Trust worthiness of nodes
Direct trust
Recommendation trust
Multi-hop network
Directly communicate with neighbor nodes
Packets exchanged between non-neighbor nodes
Using other nodes
Calculate trust value
Recommendations
Based on subject's observation

Fig. 9 EDTM Flow Chart

As shown in Figure 9, there are three kinds of nodes in the network: subject nodes, recommender and object nodes. If a sensor node A wants to obtain the trust value of another sensor node B, the evaluating sensor node A is reference as subject node and the evaluated node B is the object node. The trust value is calculated based on a subject node's observation on the object node and recommendations from a third party. The recommendations provided by third party for object node is referred as recommender. Thus, EDTM provides trustworthiness for all the sensor nodes in the network and the nodes used for data aggregation may not be malicious node. Therefore by using EDTM in wireless sensor network before data aggregation process can help in avoiding false data aggregation.

B. Data Aggregation using Synopsis Diffusion:

The main contribution of the proposed work is to define a secure data aggregation function which is to prevent the false data generation due to malicious node and to avoid data redundancy. In-Network data aggregation approach is used for data aggregation in the proposed system which is designed as a multi-hop network.

Data Aggregation Synopsis Diffusion:

Synopsis diffusion is one type of In-network aggregation which is a general framework for combining multipath routing into a single route and to avoid double counting problem. This approach defines Order and Duplicate Insensitive (ODI) properties, which is responsible for the final aggregated result is independent of duplicate data. The final aggregate computed must be the same as of the order in which the sensed data are merged. A synopsis is defined as a brief summary of the partial result of the aggregation process received at a given node. Three functions are used for synopses and possible to perform for in-network data aggregation.

i) Synopsis Generation: SG(sensor)=Synopsis generation. Synopsis generation function SG (Sensor Reading) produces the corresponding synopsis for that data.

ii) Synopsis Fusion: SF (s1, s2) = Synopsis fusion Given two synopsis, a synopsis fusion function SF (s1, s2) generates a new synopsis that summarizes both s1 and s2.

iii) Synopsis Evaluation: SE(s) = Synopsis Evaluation
Given a synopsis, a synopsis evaluation function
SE (s) produces the final result.

Synopsis diffusion consists of two phases:

First, distribution phase in which the query for aggregation is flooded throughout the network and topology for aggregation is constructed, and Second, aggregation phase where the aggregate values are continually routed toward the querying node. Each node periodically uses the function Synopsis Generation within the aggregation phase, to convert sensed data to a local synopsis and the function Synopsis Fusion to merge two synopses to create a new local synopsis. For example, whenever a node receives a synopsis from a neighbour, Synopsis Fusion SF is applied to update its local synopsis to its current local synopsis. Finally, Synopsis Evaluation SE is used by the querying node to translate its local synopsis to the final result.

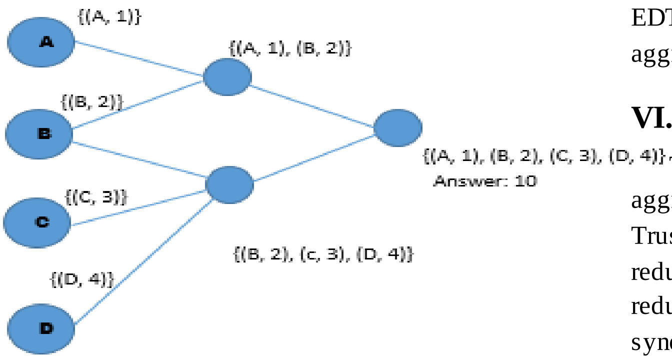

Fig. 10(a) Synopsis Diffusion without redundant data

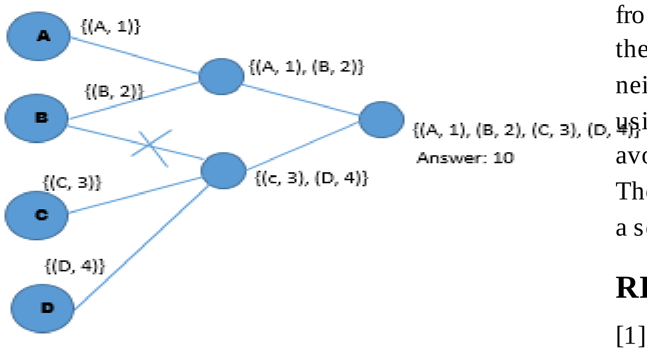

Fig. 10(b) Synopsis Diffusion with redundant data

From the following figure 10a and 10b, come to know that the synopsis function has been applied and energy efficiently the final result has been produced. The aggregated result must be ODI-correct which are based on the following four properties mentioned below:

i) Preserves duplicates: if two readings contain the same values, the algorithm generates the same synopsis.

ii) Commutative: for any two synopses s1 and s2 if SF (s1, s2) = SF(s2, s1) then the synopsis function SF (s) is commutative.

iii) Associative: if any triple (s1,s2,s3) then SF(s1,SF(s2,s3)) = SF(SF(s1, s2), s3).

iv) Synopsis Idempotent: The synopsis function SF(s) is same for any synopsis s we have that SF(s1, s2) = s

The above said four properties helps in achieving an energy efficient result by applying this synopsis diffusion framework for aggregating data in Multi-hop Wireless sensor network which is secured by using EDTM for avoiding malicious nodes and false data aggregation.

VI. CONCLUSION

This paper presents a new approach to secure data aggregation technique by using the Efficient Distributed Trust Model (EDTM) to avoid data falsification and to reduce the energy consumption by avoiding multiple redundant data transmission from multiple sensors using synopsis diffusion during aggregation process and from this the average sensor lifetime of the overall bandwidth utilization is less. From the proposed system the data from multiple sensors nodes are securely aggregated to the base station in a distributed manner, so the neighbour nodes can communicate among themself. By using EDTM the malicious nodes are detected and avoided based on the trustworthiness of the sensor node. Therefore data is aggregated using synopsis diffusion in a secured manner.

REFERENCES

[1] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, Member, "An Efficient Distributed Trust Model for Wireless Sensor Networks" IEEE, and Mohsen Guizani, Fellow, IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 5, May 2015.

[2] Wei Zhang, Sajal K. Das, and Yonghe Liu "A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks", 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 2006.

[3] Mousam Dagar and Shilpa Mahajan, "Data Aggregation in Wireless Sensor Network: A Survey", International Journal of Information and Computation Technology, Volume 3, Number 3, 2013. ISSN 0974-2239.

[4] Elena Fasolo, Michele Rossi, Jorg Widmer and Michele Zorzi, "A new In-network data aggregation technology of wireless sensor networks.", Proceedings of the Second International Conference on Semantics, Knowledge, and Grid (SKG'06) IEEE 2006.

[5] V.Umarani, K.Soma Sundaram, "Survey of Various Trust Models and Their Behavior in Wireless Sensor Networks", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 10, pp. 180-188, October 2013.

[6] S. Nath, P. B. Gibbons, Z. R. Anderson, and S. Seshan, "Synopsis Diffusion for Robust Aggregation in Sensor Networks," in ACM SenSys 2004, Baltimore, MD, US, Nov. 2004.

[7] V.Vineel Kumar, K.Ananda Brahmi, "Data Aggregation Using Synopsis Diffusion Approach In Wireless Sensor Networks" International Journal of Innovative Engineering Research (E-ISSN: 2349-882X) Vol 2, Issue 1, September 2014 .

[8] Mr.Rakesh, Kr.RanjanMrs., S.P.Karmore, "Survey on Secured Data Aggregation in Wireless Sensor Network" IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems 2015.

[9] Suat Ozdemir , Yang Xiao ,"Secure data aggregation in wireless sensor networks: A comprehensive overview" Science direct Volume 53, Issue 12, August 2009.

[10] Nandini. S. Patil, Prof. P. R. Patil, "Data Aggregation in Wireless Sensor Network" in IEEE International Conference on Computational Intelligence and Computing Research, 2010.

[11] Suman Nathy; Phillip B. Gibbons, Srinivasan Seshany, Zachary R. Anderson, "Synopsis Diffusion for Robust Aggregation in Sensor Networks" ACM Transactions on Sensor Networks, Vol. V, No. N, September 2007.

[12] Sumedha Sirsikar, Samarath Anavatti, "Issues of Data Aggregatiom Methods in Wireless Sensor Network: A Survey" in Proceedings of 4th International Conference on Advances in Computing, Communication and Control (ICAC3'15) Science direct 2015.

[13] Nanthini.D and R.A.Roseline, "Aggregation Protocols in Wireless Sensor Network- A Survey" by International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 7, July 2014.

[14] Sushruta Mishra and Hiren Thakkar, "Features of WSN and Data Aggregation techniques in WSN: A Survey " International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.