ISSN:0975-9646

Data Based-Secure and Efficient Dynamic Clustering (DB-SEDC) for Data Aggregation in Wireless Sensor Network

Priya M R[1], Chinnaswamy C N[2], Sreenivas T H[3]

[1]*Research Scholar, Computer Network Engineering,National Institute of Engineering, Mysuru, India*
[2]*Associate Professor, Department of IS & Engineering,National Institute of Engineering, Mysuru, India*
[3] *Professor, Department of IS & Engineering,National Institute of Engineering, Mysuru, India*

***Abstract*: Secure and efficient data aggregation is very critical task in wireless sensor network. To overcome this problem, in this paper, we have proposed cluster-based WSN, where clusters are formed dynamically and periodically. And also cluster-head is elected dynamically. We propose a protocol called DB-SEDC (Data Based-Secure and Efficient Dynamic Clustering); which is having the capability of electing cluster-head periodically based on the number of data-bytes sense by sensors, data aggregation, data compression and RSA, Public-key based cryptographic algorithm is used for security. Finally, proposed protocol has longer life span, better performance over security overhead and energy utilization.**

***Keywords*:Sensors, Wireless Sensor Network, Clustering, Cluster-head, RSA.**

I. INTRODUCTION

The Wireless sensor networks are used in various applications like habitat monitoring, health monitoring, health monitoring, military and target tracking [1]. All sensor nodes in the wireless sensor network have restricted energy, estimation, memory and restricted communication capabilities. In WSNs, the data sensed by sensor nodes are transmitted to base station directly, when base station is located at too far, it takes more power to transmit data. And data aggregation at base station takes more computational work. Maintaining security is also a prime issue in WSNs [2].

In this paper, we proposed DB-SEDC protocol which is having the capability of forming the cluster and electing cluster-head periodically based on the number of data-bytes sensed by sensors. Periodically, sensors calculate the number of bytes of data which it has sensed, sensors which is having higher data-bytes is going to be elected as cluster-head. Cluster based WSN approach is used to reduce energy efficiency to send data and computational work at sink. After electing cluster-head, encrypted data at cluster nodes is send to cluster-head. Cluster-head carry out the data aggregation and compression on received data. Finally, data from cluster-head is transmitted to base station. This protocol provides data confirmation, interruption detection, secure data aggregation.

The rest of this paper is as follows. Section II discussed the related work. Section III tells about problem statement. Section IV introduces the proposed work. Last section V tells about conclusion and Future work.

II. RELATED WORK

In WSN, data aggregation is a difficult task. Data aggregation technique will reduce data traffic inside sensor networks, reduce amount of data that need to send to base station. The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced and decrease data redundancy. There are so many aggregate functions, e.g., MIN, MAX, COUNT, AVERAGE or COMBINE. There are different data aggregation networks. They are; flat, tree and cluster-based data aggregation networks [7] [6]. In flat data aggregation network [8], base station will send a query to all sensor nodes in network, sensor nodes will replay to the query. Finally, aggregation will do at base station. In this all sensors nodes implemented for particular application. The drawback of flat-based data aggregation network is computational loads at base station. In tree data aggregation network [10], all sensor nodes are arranged like a tree structure. Here root node is base station; tree structure contains so many levels. A node that does not have child is called as leaf node. Leaf nodes sends data to its high level nodes where the aggregation will take place, next to its higher level again data aggregation will take place, so on... Finally it reaches the base station. There are so many protocols proposed on tree-based data aggregation network i.e. GIT, SPT TAG [11] [12] [13] etc. The drawback of tree-based data aggregation network is it increases energy efficiency. In cluster-based data aggregation network; sensors nodes in network are grouped i.e. formation of cluster and then based on some criteria cluster head is selected. Cluster nodes send the data to cluster-head, cluster-head aggregates the data`s and send to base station. The cluster-based will decrease energy efficient compare to other two data aggregation networks. There are so many protocols proposed on cluster based data aggregation i.e. LEACH, HEED [14] [15] etc.

When we are implementing a protocol for data aggregation it has to satisfy security requirement. It is a challenging task to implement both data aggregation and security. For security we can use cryptography. There are single key cryptography and pair wise key cryptography. In

single key cryptography, statically single key is assigned to all sensor nodes using that sensor nodes will encrypt the data. This cryptography is very good for security in WSN due to resource constraints but security wise it has less security over data. In pair wise key cryptography, two key are used between nodes public and private key, using private key cluster nodes will encrypt the data and at cluster head using public key of cluster node it going to decrypt the data. Same way between cluster head and base station. The pair wire key is stronger in security compare to single key. There are so many protocols proposed on security S-LEACH, secureDAV [16] [17] etc.

Data compression techniques are important in sensor networks [3] [8]. By compressing, the data size can be reduced and less bandwidth is required for sending data. There are so many techniques i.e. lossy and lossless compressions.

By this we can increase the network life span. The lossless compression method which does not tolerate any loss in data while compressing, mostly suitable for applications such as health monitoring, executable programs and source code *etc.,* and lossy compression methods which overcomes small amount of data loss during compression suitable for non critical applications like camera-based sensor networks [3].

III. PROBLEM STATEMENT

In WSN, data aggregation is very critical task, securing the data while transmission is very challenging task, reducing the bandwidth utilization while transmitting the data over network. All these are difficult task because wireless sensors have limited energy, limited memory limited computational and communication resources.

In WSN, their so many data aggregation network, they are flat, tree and cluster-based data aggregation networks. In this data aggregation networks cluster-based data aggregation network is good compare to other data aggregation networks. There are so many protocols which are cluster-based i.e. LEACH, S-LEACH, etc [5] [6], this protocols facilitates the nodes with more residual energy have more chances to be selected as cluster head. Data aggregation and securing the data is very critical task. In existing system, huge amount of data are flooding in network, there is the chance of data attack. In over proposed protocol we concentrate on securing huge amount of data, data aggregation and data compression.

IV. OUR PROPOSED APPROACH

The proposed DB-SEDC protocol provides secure and efficiency data transmission from sensor nodes to base station. The proposed DB-SEDC protocol has two phases. These Phases are discussed in section A and B are as follows.

A. Cluster formation and selecting a cluster-head phase.

Step 1: Forming a cluster where number of nodes in clusters is static.

Step 2: Each cluster node estimates the number of data-bytes which it has received.

Step 3: Each cluster nodes will compare data-bytes with its neighbors. One which is having higher data-bytes is elected has cluster-head. Here, node which is having higher data-bytes is elected has cluster-head dynamically. All the above steps repeated periodically. By doing this we can secure the huge amount of data transfer over the network, it reduces the time to transmit huge data between cluster node and cluster- head. By this we can prevent huge data from attacks.

B. Data Transfer Phase

Step 1: The cluster nodes will encrypt the data which it received.

Step 2: The cluster nodes send the encrypted data to the cluster head.

Step 3: Cluster-head will collect the data from all the members of their cluster. Cluster-head will decrypt the data`s perform data aggregation and apply compression techniques on aggregated data.

Step 4: Cluster-head send data to base station.

Working concept of DB-SEDC shown in below Fig. 1

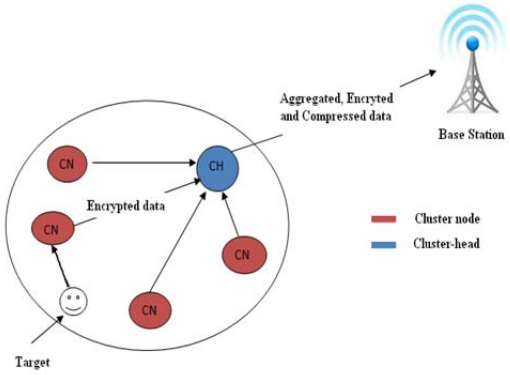

Fig. 1 working concept of DB-SEDC protocol

The DB-SEDC Protocol has the capability to protect the data. For, security Public-key based cryptographic algorithm i.e. RSA is used. In our proposed work, public and private keys are randomly and periodically generated in each sensor nodes. After generating the keys, sensor node will encrypt the data with it as received using private key, then it will send the encrypted data with attached public key to the sink. When sink receive the combined data, it will split both data and public key, using public key it is going to decrypt the data. This way we can secure the data.

The proposed DB-SEDC protocol has the capability to aggregate the data. Data aggregation is necessary to reduce the computational work at base station. In cluster-based network, cluster-head will receive the data from all its cluster nodes and it will combine the data and send to the base station. The data aggregation will reduce data redundancy, data transmission and improve data correctness [4] by this it will increase the network existence.

Finally, proposed protocol DB-SEDC , which is having the capability of electing cluster-head periodically based on the number of data-bytes sensed by sensors, data aggregation, data compression and Public-key based cryptographic algorithm, i.e., RSA, is used for security. Advantage of using this protocol is:-since we are electing the cluster–head which is having large data-bytes we can

secure the large data to transmit over the network, proposed protocol have longer life span, better performance over security overhead and energy consumption.

V. CONCLUTION AND FUTURE WORK

The proposed protocol DB-SEDC (Data Base-Secure and Efficiency Dynamic Clustering); which is having the capability of electing cluster-head periodically based on the number of data-bytes sensed by sensors, data aggregation, data compression and Public-key based cryptographic algorithm, i.e., RSA, is used for security. Using this protocol we can avoid huge data flooding over the network. Finally, proposed protocol has longer life span, scalability, better performance over security and energy utilization. In future work, same idea can be implemented for heterogeneous network and also for hierarchical cluster-based network.

The Proposed protocol has a technique to compress the data using lossless data compression algorithms integrated with the shortest path routing technique to reduce the raw data size and to accomplish optimal trade-off between data-rate, power, and correctness in a sensor network .This is made before sending the data to base station and after data aggregation at cluster-head.

REFERENCES

[1] Giuseppe Anastasi, Marco Conti, Mario Di Francesco, Andrea Passarella, Energy conservation in wireless sensor networks: A survey, Computer Networks, Elsevier, Volume 7, Issue 3, Pages 537–568, May 2009.

[2] S. Ganesh and R. Amutha. Efficient and secure routing protocol for wireless sensornetworks through SNR based dynamic clustering mechanisms. Journal of Communications and Networks, 15(4):422–429, 2013.

[3] Energy Efficient Data Compression in Wireless Sensor Networks, Ranganathan Vidhyapriya1 and Ponnusamy Vanathi2 1Department of Information Technology, PSG College of Technology, India 2Department of Electronics and Communication Engineering, PSG College of Technology, India.

[4] Suat Ozdemir and Hasan Çam, "Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks," IEEE/ACM Transactions on Networking, Vol. 18, NO. 3, pp. 736-749, JUNE 2010.

[5] A Comparative Study on Advances in LEACH Routing Protocol for Wireless Sensor Networks: International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014. Alakesh Braman, Umapathi G. R

[6] Y. Zhang and L. Xu. An efficient secure ondemand routing in clustered wireless ad hoc networks. In International Conference on Wireless Communications, Networking and Mobile Computing. IEEE, 2008.

[7] Secure data aggregation in wireless sensor networks: A comprehensive overview Suat Ozdemir, Yang Xiao.

[8] Bajwa W., Haupt J., Sayeed A., and Nowak R.,"Compressive Wireless Sensing," in Proceedings of Information Processing in Sensor Networks, USA, pp. 134-142, 2006.

[9] S. Ozdemir, Secure data aggregation in wireless sensor networks via homomorphic encryption, Journal of The Faculty of Engineering and Architecture of Gazi University 23 (2) (2008) 365–373. ISSN:1304-4915.

[10] M. Lee and V.W.S. Wong, "An Energy-aware Spanning Tree Algorithm for Data Aggregation in Wireless Sensor Networks," IEEE

[11] B. Krishnamachari, D. Estrin, S. Wicker, The impact of data aggregation in wireless sensor networks, in: Proceedings of the 22nd International Conference on Distributed Computing Systems Workshops, 2002, pp. 575–578

[12] M. Ding, X. Cheng, G. Xue, Aggregation tree construction in sensor networks, in: Proceedings of the 58th IEEE Vehicular Technology Conference, vol. 4, 2003, pp. 2168–2172.

[13] S. Madden et al., TAG: A Tiny AGgregation Service for Ad Hoc Sensor Networks, OSDI, Boston, MA, 2002.

[14] W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, An application-specific protocol architecture for wireless microsensor networks, IEEE Trans. Wireless Commun. 1 (4) (2002) 660–670.

[15] O. Younis, S. Fahmy, HEED: a hybrid, energy-efficient distributed clustering approach for ad hoc sensor networks, IEEE Trans. Mobile Comput. 3 (4) (2004) 366–379

[16] A. Mahimkar, T.S. Rappaport, SecureDAV: a secure data aggregation and verification protocol for wireless sensor networks, in: Proceedings of the 47th IEEE Global Telecommunications Conference (Globecom), November 29–December 3, Dallas, TX,2004.

[17] Enhancing S-LEACH security for wireless sensor networks,2012IEEE International conference, El-Saadawy, Shaaban.