Secured Transmission of Attribute Aware Aggregated Data In Wireless Sensor Network

B.Muthulakshmi[1], G.Mervin George[2]

PG scholar[1], Assistant Professor[2]

Department Of Computer Science And Engineering

Kalasalingam Institute of Technology, Krishnankoil.

Abstract

Wireless sensor nodes can be deployed in various environment to collect the information in an autonomous manner, that it can various applications such as traffic monitoring, pressure and temperature sensing etc. Different kind of sensor nodes can be embedded in the same network. Transmission of data from different sensors without any collusion and redundancy is an difficult process. Security in data transmission is an another major problem in WSN. In existing schemes data packets were transmitted via shortest path without any redundancy, but they assume that there is only homogeneous application in the network. In my proposed system data packets were transmitted in a dynamic environment with a maximum accuracy by using minimum energy. Here the security also provided to the data packets using diffie hell-man algorithm.

Keywords: *Wireless sensor network, data aggregation, attribute-aware, dynamic routing, diffie hell-man.*

I.INTRODUCTION

A Wireless Sensor Network (WSN) can be used to monitor the environment and provide the information about the environment which are useful in military applications. Wireless network consists of thousands of inexpensive miniature devices capable of computation, communication and sensing capacity.

Wireless sensor network provide a bridge between virtual and real physical world. It allow the ability to observe the previously unobservable at affine resolution over a large spatio and temporal scales. Wireless sensors can be used in wide range of potential applications to industry, science ,civil infrastructure and security.

To do this process sensor nodes require more energy, which is more economic also. Since wireless network is a connectionless, responsiveness and robustness is a major problem WSN. Most of the existing scheme in data transmission does not support the scalability in are WSN.

Privacy and security in data transmission is a difficult process in sensor network, since all data were transmitted via an air medium, so there is more chance to hack the data by man-in-middle Attack and also there is a chance for missing of data because of collusion in data.

II.RELATED WORK

In WSN sensed data must be transmitted to the base station where it is further processed by end user queries. Our existing scheme use the concept of Power efficient data gathering and aggregation protocol in which data where gathered in an efficient manner. But it support data aggregation in the network with homogeneous sensors and a single application .But these existing schemes cannot provide effective communication in heterogenous environment.

Localization of nodes in a dynamic environment is a challenging process in wireless network. There are many algorithms were described to find the location of sensor nodes in the dynamic environment such as local broadcast algorithm[2], by this algorithm we can achieve a constant quality transmission without using the position information.

In this algorithm status of all nodes are decided on the sport, so it does not require additional memory to store the information about the location of all the nodes. But it only applicable for small kind of network.

Data aggregation is the efficient method to reduce the transmission energy, the routing

ISSN: 2278 – 7798

protocols employed by most of existing data aggregation scheme are static. They properly support data aggregation in the network with Homogeneous sensors and a single application. But they cannot conduct a effective data aggregation when the data from different applications or from heterogeneous sensor nodes.

In our proposed scheme we borrow the concept of potential based dynamic routing algorithm[1],in which potential field for each node were calculated based on that potential information data were transmitted to the destination via an intermediate node which has maximum potential.

To provide a security in data transmission in this paper we use the concept of differ-hellman algorithm.

III.SYSTEM ARCHITECTURE

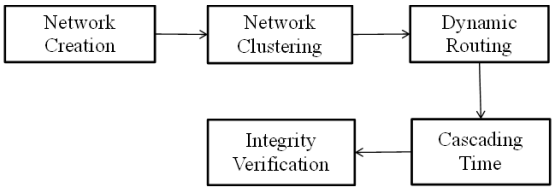

Fig 1:System Architecture

Heterogeneous sensors can be used to gather different information from an environment. Different sensor nodes can be embed in the same WSN for different application.. Data gathered by various application has unique attribute. The packets from same sensor has same attribute and the packets from different sensors has different attribute. The packets on the same application are gathered together.

In this fig:1 describes the overall architecture of the system, by this architecture different kind of sensor nodes can be embed in the same network.

IV.NETWORK CREATION

This module deals with creation of the N number of nodes that is mainly used in this project. The nodes are created dynamically according to the query type required by the sink node. Each node has unique ID and the node type. While creating a node, the details about neighbor nodes are stored.

Given wireless sensor network nodes current capabilities, we set out to design a data-collection network that would meet the scientific requirements. Before deploying network we are going to collect sensor node details. Based on that network is formed.

V.NETWORK CLUSTERING

Clustering can be loosely defined as the process of grouping objects into sets called clusters, so that each cluster consists of elements that are similar in some way. Clustering is used for multiple purposes, including natural clusters (modules) and describing their properties, classifying the data, and detecting unusual data objects (outliers). In addition, treating a cluster or one of its elements as a single representative unit allows us to achieve data reduction. Here clustering was done based on the sensor types. To reduce energy waste in the sensor networks.

In our project network clustering was formed based on the service type of each sensor node. So that nodes on the same cluster have the same service type.

VI.DYNAMIC ROUTING

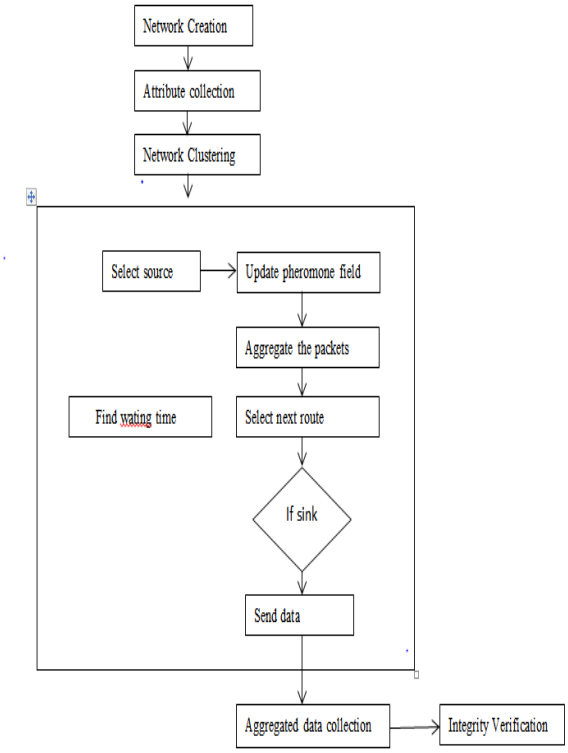

Fig 2:Data Flow Diagram

In this figure 2 shows the data flow of the entire process. Route was found by using attribute aware aggregation algorithm[2]. First source node was selected. For that node set of neighbors found. From that neighbor next forwarding node is the node that has same attribute as current forwarding node. In the process of finding the next forwarding node potential field of all node such as bandwidth,

ISSN: 2278 – 7798

depth ,waiting time of each node was considered. This process was continued until reaching the sensor node. Finally data was transferred though that path.

VII.CASCADING TIME

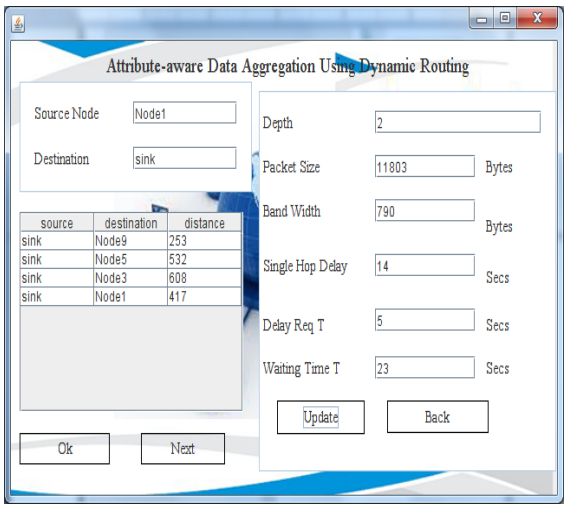

Fig 3:Potential Fields of a Node

Network congestion is a major problem in wireless sensor network. To avoid congestion, after selecting forwarding node waiting time is calculated for each node .so that current forwarding node can wait that much time before sending data. Cascading time was calculated for each node based on the depth of node and packet size. so that time will be different to all the nodes. This cascading time to avoid network congestions.

VIII.INTEGRITY VERIFICATION

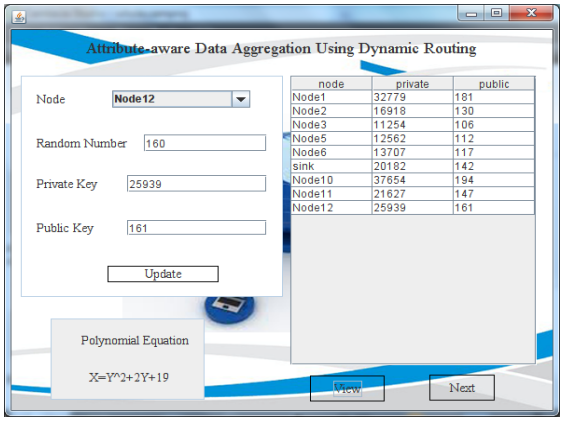

Fig 4:Public and Private Key Generation

Before receiving data from source node sink did validation for the received file. For that diffie-hellmen key exchange algorithm was used to generate secret keys. By using that key hash value was generated for each file. By using hash value verification was done at sink node.

IX.RESULT

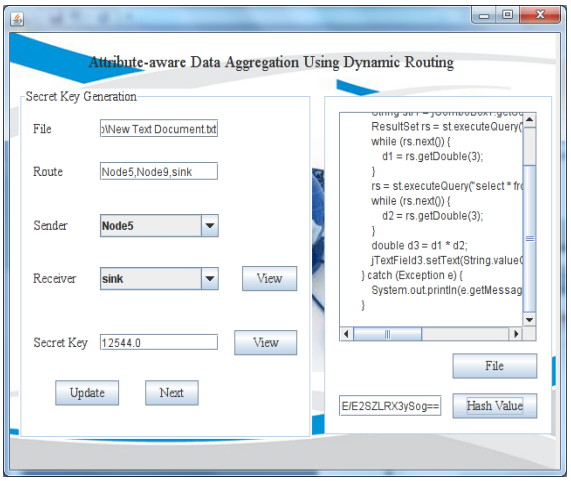

Fig 5:Integrity verification

Diffie-Hellman key exchange algorithm uses asymmetric key principles for the distribution of symmetric keys to both parties in a communication network. Key distribution is an important aspect of conventional algorithm and the entire safety is dependent on the distribution of key using secured channel. Diffie-Hellman utilizes the public & private key of asymmetric key cryptography to exchange the secret key.

By using diffie-hellman algorithm integrity of the file was verified successfully at the receiver side.

X.CONCLUSION

Energy efficiency is the challenging process in wireless sensor network, in order to reduce the energy consumption our paper cluster the nodes based on the service attribute of each sensor node. By these data were transmitted via the related cluster to the sink node. To achieve efficient transmission in dynamic sensor network, our paper consider the potential field of each node to select the next forwarding node.

To avoid the congestion in wireless network, in our paper waiting time was calculated based on the packet size and bandwidth of each node during every transaction. To provide security in data transmission, integrity verification also performed at the receiver side using diffie hellman algorithm. Thus our paper provide solution to efficient and secuired transmission in wireless sensor network.

XI.REFERENCES

[1] Fengyuan Ren, Jiao Zhang, ongwei Wu, Tao He, Canfeng Chen, and Chuang Lin, "Attribute-Aware Data Aggregation Using Potential-Based Dynamic Routing in Wireless Sensor Networks" IEEE Transactions On Parallel And Distributed Systems, VOL. 24, NO. 5, MAY 2013

ISSN: 2278 – 7798

[2] K. Romer and F. Mattern. The design space of wireless sensor networks. *IEEE Wireless Communications*, 11(6):54–61, December 2004.

[3] O. Younis, M. Krunz, and S. Ramasubramanina. Node clustering in wireless sensor networks: Recent developments and deployment challenges. *IEEE Network*, 20(3):20–25, December 2006.

[4] G. Anastasi, M. Conti, M. Francesco, and A. Passarella. Energy conservation in wireless sensor networks: A survey. *Ad Hoc Networks*, 7(3):537–568, May 2009.

[5] K. Akkaya and M. Younis. A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, 3(3):325 – 349, 2005.

[6] E. Fasolo, M. Rossi, J. Widmer, and M. Zorzi. In-network aggregation techniques for wireless sensor networks: a survey. *Wireless Communications, IEEE*, 14(2):70–87, April 2007.

[7] S. R. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, ―TAG: a tiny aggregation service for ad-hoc sensor networks,‖ in *Proceedings of the Symposium on Operating Systems Design and Implementation,OSDI*, pp. 131–146, Dec. 2002.

[8] H. F. Salama, D. S. Reeves, and Y. Viniotis, ―Evaluation of Multicast Routing Algorithms for Real-time Communication on High-speed Networks,‖ *IEEE Journal on Selected Area in Communications*, vol. 15,no. 3, pp. 332–345, April 1997.

[9] A. Basu, A. Lin, and S. Ramanathan, ―Routing Using Potentials: A Dynamic Traffic-Aware Routing Algorithm,‖ Proc. ACM SIGCOMM, pp. 37-48, 2003.

[10]. Di Caro G. Ant Colony Optimization and its application to adaptive routing in telecommunication networks. PhD thesis. Universite´ Librede Bruxelles: Brussels, Belgium, 2004.

[11] Dorigo M, Di Caro G, Gambardella LM. Ant algorithms for discreteoptimization. Artificial Life 1999; 5(2):137–172.

First Author Ms.B.Muthulakshmi
The author is currently a ME Student in Computer Science and Engineering Department at Kalasalingam Institute of Technology.She had completed BE from SCAD college of engineering and Technology.

Second Author Mr.G.Mervin George
The author is an Assistant Professor in Computer Science Engineering Department at Kalasalingam Institute of Technology. He received his BE from CSI Engineering College; affiliated To Anna University, and M.Tech. Degree from SRM University. His Research interests are in the areas of Data Mining and network security.

ISSN: 2278 – 7798