ISSN:0975-9646

Secure and Efficient Data Transfer for Hierarchical Based Wireless Sensor Network

Akshada Deokar
ME Student
Department of Computer Engg.
Flora Institute Technology, Pune

Prof.Deepali Borade
Assistant Professor
Department of Computer Engg.
Flora Institute Technology, Pune

Prof.B.A.Tidke
Assistant Professor
Department of computer Engg.
Flora Institute Technology,Pune

***Abstract*— Now a day's security is an important issue in wireless sensor network. Clustering is effective way for energy efficiency. In this Paper we study secure data transfer for Hierarchical WSN. In Hierarchical WSN clusters are created dynamically and periodically. We proposed two secure data transmission protocol for Hierarchical WSN, called as SET-ABE and SET ABOOS, by using attribute based encryption Scheme and attribute based online offline encryption. During data transmission finds orphan node attack, misbehavour of node with the help of Diffie-Hellman algorithm.**

I. INTRODUCTION

WSN is demanding and large collection of distributed sensors nodes called as sensor devices, which are capable of senescing information like environmental condition, such as sound, temperature, motion. Sensor node senses environmental conditions and collect data from their domain area, processed them and send towards sink node.

Secure data transfer is most critical issue for WSN.Generally, most of WSNs are deployed with rough,crude,deffered physical environment for military and healthcare domain with trustless background. So, securely data transmission is necessary and most practical vision in WSN.

II. BACKGROUND AND MOTIVATION

Hierarchical based data transfer in WSN has been researched to achieve network scalability and maximizes node lifetime and low power consumption with energy efficient routing.

In hierarchical WSN every cluster has leader node called as cluster head node (CH).

A CH gathered all data which is collected by leaf node in respective cluster; this is generally called as data aggregation, send aggregate data to base station (BS) also called as sink node. The LEACH (Low Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelmal et. al. [1] is greatly known effectively used to reduce total system energy consumption and balanced energy by distributing the energy load randomly among all nodes in WSN and support to hierarchical WSN.

In LEACH protocol BS is fixed and located far away from sensors and all sensor nodes are same in nature. In cluster, one sensor node is cluster head (CH) acts as local BS, LEACH randomly select cluster head for energy balancing purpose.

So, all sensors consumes same battery power equally.BS is high energy node and leaf node is low energy node. LEACH performs in rounds, it has two phases: Setup Phase, Steady phase. In setup phase, clusters are created and CH is selected Randomly for each cluster, where as in steady phase leaf node send data to CH within certain time period using TDMA.

The ideas of LEACH protocol, number of protocols have been developed such as PEACH [3], APTEEN [2] and PEGASSIS [4] which uses same concept like LEACH. In this paper, for our convenience we used sort of hierarchical protocol as LEACH protocol. However, implementation of hierarchical based architecture in real world is complicated.

Providing security to LEACH protocol is very complex because they dynamically and periodically changes network, cluster head of network and data path[8].Therefore, providing steady and stable node to node trusted relationship and common key distribution is not feasible in LEACH like protocol. There some secure data transmission protocols are available based on LEACH protocol, like SEC-LEACH [6], GS-LEACH [7].But, many of them uses symmetric key management for network security, which suffer from orphan node problem. This problem occurs when node doesn't share pairwise key with other node in their cluster to serve the storage cost of symmetric key. The key ring in node is not able to share pairwise private key with all node in network. In such a case, the node can't participate in other cluster. So, that more CHs are elected by themselves which leads to more energy consume by network [1].The orphan node increases the overhead of network and the system energy consumptions by increasing number of CHs in network.

To overcome symmetric key management, Asymmetric key management has been recently used in WSN, with Attribute based encryption Technique (ABE).It based on set of attribute for which they implemented on group of bilinear attribute set, based on Diffie Hellman algorithm or Elgamal[12].

ABE allows users to encrypt message and decrypt message based on users attribute. It has two main type of ABE: Key policy ABE (KP-ABE) and Cipher policy ABE (CP-ABE).

In this paper, we proposed two protocols based on ABE that is SET-ABE, SET-ABOOS.The ABOOS scheme could be effective for key management, the offline phase can be executed on sensor node while online phase executed during communication [8].

III. RELATED WORK

Abdul Gani khan & Abdur Rohan et al. [4] stated data transmission protocol for hierarchical based WSN, such as LEACH,TEEN,APTEEN,PEGASSIS.It distribute data as per need to any router that can receive. Based on this comparative analysis of protocol is presented.

Table1: Comparision of different hierarchical protocol in WSN

Routing Protocol In WSN	LEACH	TEEN	APTEEN	PEGASIS
Classification	Hierarchical			
Data Delivery	Cluster Head	Active Threshold	Active Threshold	Chain Based
Data Collection	Yes	Yes	Yes	No
Power consumption	High	High	High	Max
Scalability	Good	Good	Good	Chain Based
Overhead	High	High	High	Low
Network Life time	Very Good	Good	Good	Good
Resource Availability	Yes	Yes	Yes	Yes
Mobility	Fixed BS	Fixed BS	Fixed BS	Fixed BS

Online/offline Attribute Based Encryption scheme discussed by Susan Honerberger & Brent water [5].They developed new “correct and connect” technique with two phases: preparation phase and online/offline encryption. This technology reduces battery power on nodes & reduce bottleneck on master authority task.

Huang Lu, Jili et.al. [8] Proposed two data transmission protocol named as SET-IBS & SET-IBOOS based on Digital Signature to achieve security parameter also it solve problem of orphan node with symmetric key management.

Attribute based Encryption proposed by Sahani and B. Waters [13] they states that identity of user is viewed as group of attribute. They proved scheme under the Selective-ID model that can be viewed as a modified version of the Bilinear Decisional Diffie-Hellman assumption.

IV. DESIGN

WSN consisting of fixed BS and all leaf nodes, which are homogeneous in nature with same functionality. The BS is always reliable and trusted authorized user, where the sensor nodes may compromised by unauthorized user and transmission path may be interrupted by unauthorized user. In WSN, sensor nods are grouped into clusters and every cluster has CH nodes, which can be selected randomly. A Non-CH node (leaf node) joins clusters depending on strength of received signal from BS. CH performs data collection and transmission towards BS with high energy than leaf node.

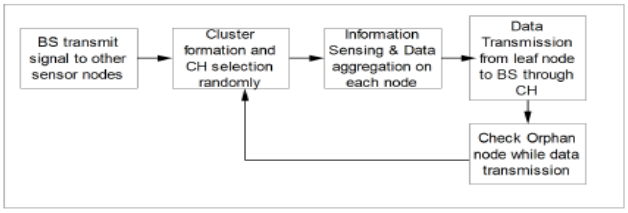

Fig: Working Block Diagram of System

The LEACH protocol used for implementation of WSN. Operation of LEACH protocol divided into two phases that can be carried out within number of rounds each round include separate setup phase for forming clusters and steady phase for data transmission from sensor nodes to BS through CH. Time is divided into number of time slot, for data transmission and cluster formation it uses TDMA scheme. In each round the time line is divided into consecutive time interval by TDMA control.

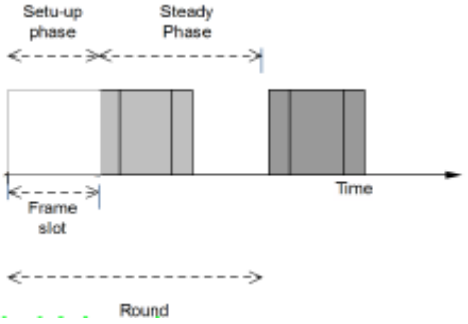

Fig: Diagram of TDMA slots

Sensor nodes sends sensed data to CHs in each time slot of steady phase, CHs are elected randomly for balance energy and non-Ch sensor nodes join clusters using two hop transmissions depending on higher receiving signal. To select CH in new round each leaf node determines random number and compare with threshold value. If value is less than value of threshold then sensor node becomes CH for current round. This is the way for new CHs are self selected based on their own local decision [8].

SET-ABE algorithm is implemented for secure data transfer in WSN.In has four operations: setup, key Generation, Encryption, Decryption.

1) Set up: The authority user as BS generates Master Key and public key parameter for generation of private key and send them to all sensor nodes in cluster.
2) Key Generation: The authority executes and generates private key for data user.
3) Encryption: Data owner encrypt messages with set of attributes.
4) Decryption: Data user decrypt the encrypted message with private key and verifies receiving output is acceptable or not which depends on attribute matching.

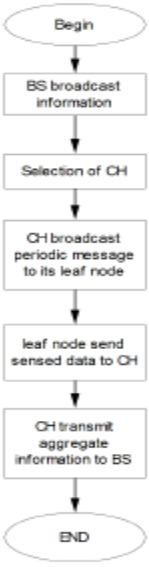

Figure: Flowchart for operation in SET-ABE

SET-ABOOS operates similar way to that of SET-ABE. The main goal in online/offline setting is to allow precomputation of attribute based chipher text as possible without knowing about cipher policy or attribute set

SET-ABOOS implemented with five operations: Setup, Extract, Offline Encryption, Online Encryption and Decryption.

1) Set up: This algorithm takes input as security parameters and set of attributes in system and generates master key and public parameters.
2) Extract: This algorithm takes input as set of attribute and master key in order to generate private key associated with set of attribute.
3) Offline Encryption: This algorithm takes parameter and generates output as intermediate cipher text.
4) Online Encryption: This algorithm takes input as public parameter, set of attribute and intermediate cipher text and generate output as session key and cipher text.
5) Decryption: this algorithm takes input as private key and cipher text in order to decapsulate cipher text to get original message and to recover session key only if it satisfy attribute constrain.

CONCLUSION

In this paper, we have design and developed two protocol scheme in order to get secure and efficient data transfer over WSN, such as SET-ABE and SET-ABOOS based on Attribute based encryption. As well as it provide security towards orphan node problem in secure data transmission. Due to use of hierarchical architecture provides balanced energy consumption on every sensor node.

REFERNCES

1. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “An Application-Specific Protocol Architecture for Wireless Microsensor Networks,” IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.
2. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, “An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol,” IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.
3. S. Yi et al.,” PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks ” Computer Comm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.
4. Abdul Gani Khan,Abdur Rahman, Neeti Bisht ”Classification of Hierarchical Based Routing Protocols for Wireless Sensor Networks”, International Journal of Innovations in Engineering and Technology, ISSN:2319-1058,Special Issue-ICAECE-2013.
5. Susan Hohenberger, Brent Waters “Online/Offline Attribute-Based Encryption”,2007.
6. L.B. Oliveira et al., “SecLEACH-On the Security of Clustered Sensor Networks,” Signal Processing, vol. 87, pp. 2882-2895, 2007.
7. P. Banerjee, D. Jacobson, and S. Lahiri, “Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks,” Proc. IEEE Sixth Int’l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.
8. Huang Lu, Jie Li, Mohsen Guzani “Secure and Efficient Data Transmission for Cluster-Based Wireless sensor Networks”,IEEE TRANSACTION ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2004.
9. Cheng-chi Lee,Pei-Shan chung,and Min-Shiang Hwang “Asurvey on Attribute-based Encryption Scheme of Access Contol in Cloud Environment”, International Journal of Network Security, Vol.15,No.4,PP.231-240,July2013.
10. Susan Hohenberger, Brent Waters “Online/Offline Attribute-Based Encryption”,2007.
11. Susan Hohenberger, Brent Waters “Attribute-Based Encryption with Fast Decryption”,8 may 2013.
12. Shraddha U. Rasal,Bharat Tidake”Improving Revocation Sheme to Enhance the Performance in Multi-Authority ABE”,International Journal of computer Application(0975-8887) Vol 90-No 18,March 2014.
13. Shai and B.Water,”fuzzy Identity based Encryption,” Advance in Cryptogyaphy Eu-rocrypt, LNCS, Spinger, vol.3494, pp.475-473, 2005.