A Novel Approach for Load Balancing and Privacy Preservation in Real-Time Wireless Sensor Networks

Jeena P Abraham[1] Lidiya Raju[2]
[1],[2]Assitant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Mount Zion College of Engineering, Kadammanitta, Kerala

Abstract— Wireless sensor networks are collection of small sensing self-powered nodes organized into a supportive network which have certain processing capabilities and the nodes communicate wirelessly. Securing data and proper load balancing is a challenging task in wireless sensor networks. This paper propose a new mechanisms for privacy preservation and load balancing in real-time wireless sensor networks, i.e. DA (Data Aggregation) and MHCM (Multi-hop communication mechanism), which combines data aggregation and multi-hop communication mechanisms. Using this mechanisms a proper load balancing is possible using clusters and it also provide protection against collusion attacks in real- time wireless sensor networks.

Key words: Wireless Sensor Networks, Data Aggregation, Privacy Preservation, MHCM, Load Balancing

I. INTRODUCTION

Recently, continuous improvement in wireless communication technologies have enabled the organization of large scale wireless sensor networks (WSNs). Sensor networks have one or more sensor nodes which communicates between each other using wired or wireless medium to perform distributed sensing tasks [1]. Each sensor may have the abilities to sense, communicate and process data either locally or remotely. Wireless sensor networks are one of the largest growing type of networks used in many features including environmental analysis and monitoring, security and health monitoring [2].

The wireless sensor networks depends upon different network protocol like multi-path based routing, query based routing etc. Among these multi-path routing protocol is commonly used for reliable data transfer. Sensor networks, is a complex task, since it involve not only reducing the energy consumption of a single sensor node, but also maximizing the life time of an entire network. To maximize network life time of the WSN, a dynamic tradeoff among various factors, energy consumption, and system performance [3].

Secure data aggregation mechanisms can be classified into two, namely hop-by-hop and end-to-end mechanisms. Data aggregation is an essential mechanism used in sensor networks to preserve the battery power of the sensor network device [1]. A secure data aggregation mechanism that protect against collusion attacks in a real-time wireless sensor networks.

The focus of this paper, propose a mechanisms data aggregation (DA) and multi-hop communication mechanism (MHCM) providing a proper load balancing and securing data in real-time wireless sensor networks. Here, assume that all the sensor nodes of the network are equipped with a different amount of energy. Each sensor node transmits sensing data to the base station (BS) through a cluster head (CH). The CHs are selected periodically by different weighted probability. After the selection of CHs, member nodes in their respective clusters, aggregate the received data , and send it to the BS using data aggregation (DA) and multi -hop communication (MHCM) mechanisms.

II. LOAD BALANCING

Single-hop and Multi-hop communication mechanism are two simple communication forms which are used in wireless sensor networks. In the load balancing to use multi- hop communication mechanism are used. Multi – hop communication mechanism (MHCM) helps to proper load balancing in real- time wireless sensor networks.

A. Multi-Hop Communication Mechanism (MHCM)

The network model is composed of different types of nodes. Each sensor node transmits sensing data to the base station (BS) through a selected cluster heads (CHs). All the CHs are selected periodically by different weighted probability in the network. Each member nodes communicate with their respective CHs. The CHs collect the data from the member nodes in their respective clusters, aggregate the data, and send it to the BS using multi-hop communication mechanism.

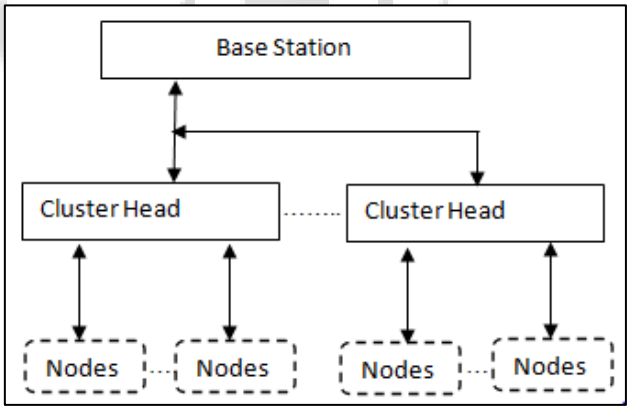

Fig. 1: MHCM Architecture

To use the data transmission network by a directed weighted graph G={V,E}, where V is a set of nodes and E is a set of edges. Let us assume V_i and V_j are two nodes in the graph. For the edge e=(V_i,V_j), W(e)=W_{ij} , which indicates the weight of e. W_{ij} represents the wasting energy of nodes. Similarly, if V_j is the second hop node chosen by another node and V_t is the BS, then W_{ij} represents the wasting energy of node V_j because it includes a receiving consumption. Therefore, the shortest path weight, also called distance, from V_i and V_t, denoted d_{st} is the minimum weight of all possible directed paths with origin V_s and destination V_t. Let G={V,E} be a directed weighted graph with V a set, whose elements are called vertices or nodes and E is a set of ordered pairs of vertices, called directed edges . It repeatedly

selects from the unselected vertices, vertex *V* nearest to source *S* and declares the distance to be the actual shortest distance from *S* to *V*. The edges of *V* are then checked to see if their destination can be reached by *V* followed by the relevant outgoing edges.

III. PRIVACY PRESERVATION

To achieve accurate data aggregation with reasonable communication overhead to preserve data privacy. The data aggregation mechanism should satisfy the following measures.

Efficiency: Data aggregation achieve bandwidth efficiency through in-network processing.

Accuracy: It should be a criterion to estimate the performance of private data aggregation mechanism.

It include efficiency of privacy and integrity protection, and accuracy of aggregated, provide a mechanism by using data aggregation (DA). Privacy preserving mechanism is performed through two phases; encryption phase and data aggregation phase.

A. Data Encryption Phase

In data encryption phase, use curve key exchange algorithm which exchanges its own data by using a public key, an arbitrary point and its secret constant key [1]. A source node and its receiving node set a private constant key ie. pSender and pReceiver. Each node makes a result R by multiplying an arbitrary point (E) and the private constant key having public curve. Each node transmits the result R to the receiving node. Finally it calculates the seed data by multiplying R with its private constant key. The curve key exchange algorithm can make each node communicate without redundant message, its own data can be preserved during the communication from the attacker.

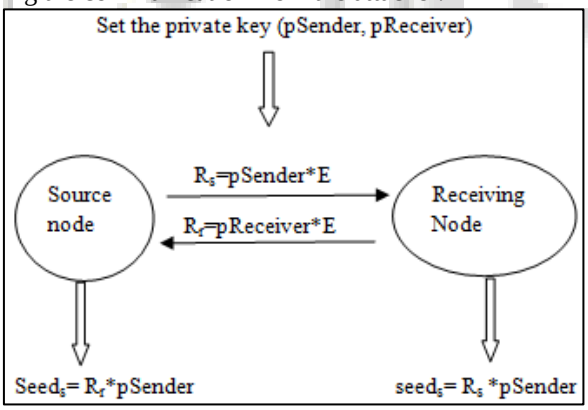

Fig. 2: Curve key exchange algorithm

The seed is used for hiding an original data from an adversary. The original data can be changed by extracting some part of a seed value which is sent to other nodes. Some part of the seed value which is sent to other nodes. Some part of the seed value is also added from other node. The sensed data can be hidden among seed exchange group members.

B. Data Aggregation Phase

In data aggregation phase, each node sends the encrypted data to its parent node. Then, the parent node analyses the encrypted data which received from child node. If the cure direction and level of its child node are different from its own ones, they should be changed into the curve direction and level of its parent ones. A sink node aggregates all of the encrypted data from the hierarchy of nodes.

IV. CONCLUSION

As discussed about, security and load balancing is challenging task in real-time wireless sensor networks. The proposed mechanisms DA and MHCM can provide better load balancing and also enhance security to some extent. The security can be assured using data aggregation mechanism, the effective load balancing can be acquired through multi-hop communication mechanism. However real-time wireless sensor networks still suffer from high computation cost. As a future work, next focus on reducing overhead of computation cost.

REFERENCES

[1] Ahmed Alghamdi , Mesfar Alshamrani " secure data aggregation scheme in wireless sensor networks for IoT" IEEE 2016.
[2] D.Kumar, R.B.Patel "Multi-hop Data Communication Algorithm for Clustered Wireless Sensor Networks" International Journal of Distributed Sensor Networks ,February 2011.
[3] Shiv Prasad Kori, Dr.R.K.Baghel, "Evaluation of Communication Overheads in Wireless Sensor Networks" IJER Volume No.2,Isuue No.2,pp:167-171.
[4] W.He,X.Liu, H.Nguyen, K.Nahrstedt, and T.Abdelzaher, "PDA: Privacy-preserving Data Aggregation in WSNs." In IEEE INFOCOM,2007.
[5] Hu and D.Evans," secure aggregation for wireless networks," in workshop on security and assurance in Ad hoc Networks, January 2003.

