International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

Dynamic Clustering for Energy Efficient Data Aggregation Technique using Secure Data Encoding Scheme for WSN

Pradeep Kumar CTM
pradeep.ctm@gmail.com

CTM Praveen Kumar
ctm.praveen@gmail.com

Chinnaswamy C. N.
chinnaswamynie@gmail.com

Abstract: The main factor in wireless sensor networks communication is to transfer information with high security. With increase in number of nodes, the cluster are formed dynamically and the data transmission between these dynamically created cluster, cluster heads and base station has to achieved with high security. The limitation in WSN resources like bandwidth, battery backup, speed and size of information will play a major role in forming clusters and its heads, which will affect the security aspects associated with packet transmission. The dynamically changing cluster size needs to constantly update its cluster head which will affect the packet size formed and security provided to it. The current work developed will provide security to the information (packet) transfer between the cluster and base station. The security is achieved by applying the RSA-Chinese Reminder Theorem for the packet sent from cluster head to base satiation. This algorithm provides multiple private key and single public key. Each cluster head will be provided with different private key and the base station will have single public key. Each cluster head will assign its private key with every message it sends towards base station. Base station will decrypt the message using its public key,

Keywords-Secure data transfer in WSN, dynamic clustering; differential data aggregation

I. INTRODUCTION[1]

From past few decades, wireless sensor network (WSN) is expanding at rapid pace. With each day passing number of devices added to the WSN increasing and making it one of the major player in carrying out the day to day activates. Around the globe, over next decade the estimated number of wireless devices shall cross 25 billion. This avalanche of devices in the network comes up with even bigger challenges in providing vital service called security for each device, each group and each message which transmitted over network. In our research work prioritized the work to deal with the security of the data transmitted between the devices which are dynamically grouped and placed in hierarchy level.

In an ever expanding network, each device will gather, share information and collaborate with other devices in the network to use the network resources efficiently. The number of devices is grouped dynamically called as dynamic clustering and each cluster will select a cluster head (CH). The CH will collect the data from all the nodes of its cluster and aggregate the data into single packet and send the aggregated data packet to base station. This data packet needs to be secured. Here clusters are not evenly distributed and hence the data collected at regular interval will also varies, this variation should be taken into consideration while providing security to the dynamic data packet length. The fig 1 shows the simulated output from of LEACH algorithm [5], in which CH are concentrated in one area rather than evenly distributing across the area of interest.

II. EXISTING SYSTEMS

In the literature survey for data aggregation with dynamic clustering, we found that clustering in derived into two categories which are having their own limitations and disadvantages. The categories are 1.Low energy Adoptive Clustering Algorithm [LEACH] 2. Grid Based Algorithm.

In LEACH algorithm, there is hierarchical cluster-based routing technique being used for wireless sensor network where nodes are partitioned into clusters, a cluster head will be selected for each cluster which is responsible for creating and sending aggregated data from cluster head to base station. Leach has two phases 1. Set-Up Phase 2. Steady phase.

In Set-Up phase, each node decides independent of other nodes if it will become a CH or not. Here control heads sends data packet to Base Station based on its time slot assigned to it.

And when Data transmission begins; Nodes send their data during their allocated time slot to the CH. This transmission will use minimal amount of energy. The radio of each non-CH node can be turned off until the nodes allocated Time slot, thus reducing the energy dissipation in these nodes. After receiving all the data, the CH shall aggregate these data and send it to the BS. LEACH has a drawback which is due to random selection of control head which leads to increase in energy consumption, limits the scalability and control heads are not uniformly distributed. These draw backs of LEACH lead to modified LEACH protocols like E-LEACH, TL-LEACH, M-LEACH, LEACH-C and V-LEACH.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

In Grid Based Clustering, the sensor filed is divided into grid of square shape of defined size. And the algorithm will selects one cluster head per grid as a coordinator which stays active until it runs out of energy. All other nodes power down or will be in sleep mode to save energy. The base station starts flooding the network with a query message to every cluster head. once the cluster head receives the message it sends info back to base station by finding a way back to base station. Here there is no rotation of cluster head and the cluster will die once all its energy is lost. This not only results in waste of energy and also affect whole cluster once CH dies leaving other nodes floating.

In this paper we are using another method called virtual grid based algorithm where grid is not considered as cluster and CH are not selected based only on grid. Here we need stable, steady sized and localized clusters without any extra energy being consumed and without any centralized system.
The selection of CH is not only based on energy levels of the nodes within a grid but also total no. of nodes available inside the grid which are active. And also clusters are formed based on the nearest CH which includes cluster having nodes from other grids also. With this we get one CH per grid to have even distribution of cluster with low energy maintained across the network.

In this paper we are introducing data security aspects for the packets sent from CH to base station. So far in previous methods where LEACH or Grid based or Virtual Grid based algorithm are discussed, there is no security provided for the packets sent from CH to base station. With this drawback, we came up with a data security protocol called RSA Algorithm to secure the data packets sent from CH to BS. Here after data encoding and aggregation, the CH will encode the packets using extended Chinese Reminder Theorem for RSA Algorithm, which generates multiple private and one public key. Where each CH will get private key and BS will have one public key.

III. PORPOSED SYSTEM

The proposed implementation is having stages as a precondition application and will help in implementing the proposed security aspects of the system.
Stage 1 deal with balancing of load across cluster, which can be achieved. And stage 2 and 3 are in progress.

Along with this we are extending our experiment by introducing security for the packets sent between cluster heads and base station y using RSA algorithm.

Stage 1: here virtual grid based clustering technique is used as basis for this proposed work. In this method selection of CH is not only based on energy level of nodes within grid but also the total no. of nodes within the network. Based on distances between the CHs clusters are formed. In this case, a cluster head can have its member node from other grid also.

Here CH is selection has two phases, in first phase using modified LEACHs algorithm and using the equation

$$T(n) = \begin{cases} \dfrac{p}{1 - p * \left(r \bmod \left(1/p * G_T \right) \right)} & \text{for } n \in X \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

We can find the CH, where n is no. of nodes and p requiring percentage of CH. On every node a random no. is generated, if no.is less than *T* (n), then that node is chosen to be CH. Here X total no, of nodes which are not yet became CH in the last 1/ (p*GT) rounds. Addition of GT in the actual LEACH equation has increased the probability of each node getting selected by GT times.
In the second method CH is selected based on highest energy exerted by node within a grid. Node with highest energy will be selected as CH.
With the current implementation phase of this paper we are noticing that, selecting of one CH per grid will be smooth for small no. of grids but as grid no. increases this setup will get disturbed. Keeping one CH per grid and using the below formulae one can suggest minimum no. of nodes that can be suggested.

$$G_{CH} = ([0.24 \square n + 5])^2$$

Equation says "*For n number of nodes within a finite size of area, we should not have more than GCH grids if we want to have one CH in almost every grid*"

Stage 2: Keep redundant nodes into Sleep Mode depending on Threshold sensing range

To perform sensing or monitoring, there are more no. of devices than the required. In such cases it is inevitable to avoid redundant nodes and bring the clusters size down. We can use a threshold sensing range as a parameter to decide the redundant node buy using the formula

TSR = SR – RSR

Where TSR is Threshold sensing range, SR is Sensing Range and Required Sensing Range (RSR). Two adjacent nodes within grid having inter-distance less than TSR, need not to send data to CH. One can estimate the TSR assuming the uniform distribution of nodes and SR > RSR.

Stage 3: To aggregate the correlated data into single packet at each CH, method called differential encoding has been proposed, assumptions are made that cluster will be smaller in

size and will be a stable one. Proposed technique will be flexible enough to adjust the incoming data which of 1.variable in size 2.having correlation between the data sensed within cluster 3. No of nodes within cluster.

We are extending the work by proving the security for data transfer by encrypting the encoded data at the cluster and then stream the data to the base station. The data transformation scheme used in this project is extended Chinese Reminder Theorem for RSA Algorithm which provides multiple private for single public key. After the cluster formation, the cluster heads will receive the private key generated by the base station, each cluster head will get a different private key for a single public key of the base station. After data encoding and aggregation the cluster head sends the aggregated data to the base station by encrypting the data by the private key provided by the base station so that the base station can decrypt the data sent by the clusters using the public key

IV. PROPOSED WORK OUTPUT

In this paper we are extending our work and research on security aspects of data packets sent from cluster head to base station. To achieve this, we are using 'Chinese remainder algorithm', which provides multiple secret keys and a single public key. This algorithm is sophisticated and hard to break. This will not consume network resources which are critical. The analysis and implementation of the above work is in progress.

V. WORK CONTRIBUTION

Increases the security of the packets sent from CH to BS.
Further research work can be done on to work with different and more efficient security algorithms. This will not consume critical network resources but provides security to the packets.

REFERENCES

[1]. "Eliciting truthful measurements from a community of sensors" by Boi Faltings ,Jason Jingshi Li and Radu Jurca in 3rd International Conference on the Internet of Things (IoT) 2012
[2]. "Energy Efficient Round Rotation Method for a Random Cluster Based WSN" Rabia Noor Enam, Syed Misbahuddin, M. Imam, International Conference on Collaboration Technologies and Systems.
[3]. "Overlapping Multihop Clustering for Wireless Sensor Networks For Wireless Sensor Networks", M.Youssef, A.Youssef and M.Younis, IEEE Transactions on Parallel and Distributed Systems
[4]. "Distance Distribution Approach of Minimizing Energy Consumption in Grid Wireless Sensor Network,", Ketki Ram Bhakare, R.K.Krishna, Samiksha Bhakare, International Journal of Engineering and Advanced Technology (IJEAT).
[5]. "Grid-based coordinated routing in wireless sensor networks", R. Akl and U. Sawant, 4th IEEE Consumer Communications and Networking Conference
[6]. "Cross-Layer packet Size Optimization for wireless Terrestruial, Underwater and Underground Sensor Networks", Mehmet C. Vuran, Ian F. Akyildiz, 27th IEEE
[7]. "Efficient and Secure Routing Protocol for Wireless Sensor Networks through SNR based Dynamic Clustering Mechanisms", S.Ganesh, R.Amutha Sathyabama University, Chennai , Tamil Nadu, India
[8]. "On the Security of Cluster-based Communication Protocols for Wireless Sensor Networks", Adrian Carlos Ferreira1, Marcos Aur´elio Vila¸ca1, Leonardo B. Oliveira1, Eduardo Habib1, Hao Chi Wong1, Antonio A.Loureiro1, Federal University of Minas Gerais, MG,Brazil
[9]. "Novel Secure and Dynamic Clustering Protocols in Wireless Sensor Networks" Rui Jiang, Purdue University, Southeast University Mehdi Azarmi, Purdue University, ACM Student Member Tao Gong, Purdue University Bharat Bhargava, Purdue University, ACM and IEEE Fellow