www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242

Volume 3 Issue 6, June 2014, Page No. 6385-6388

Layer Based Secure Data Aggregation for Wireless Sensor Network

***Deepitha*[1]*, Manjunath C.R*[2]**

[1] M.Tech Student, Department of computer science and Engineering,
Jain University, Jakkasandra Post, Bangalore, India
deepithadeepu@gmail.com

[2] Assistant professor, Department of Computer Science and Engineering,
Jain University, Jakkasandra Post, Bangalore, India
manjucr123@gmail.com

Abstract: *Wireless sensor nodes are deployed to perform three main tasks: sensing, data processing and communication. Sensor nodes are usually constrained in energy, communication, storage, and computation capability, especially the ones powered by batteries, which cannot be replaced optionally. Due to the main characteristics of resource-constrained and battery-powered sensors in wireless sensor networks, energy consumption is always a major concern. Data aggregation is a method of collecting and aggregating the data to reduce the energy consumption and redundancy. Since data are transmitted through multiple hops security is very much essential. The proposed layered approach provides secure data aggregation by using slicing and mixing method and reduces the number of hopes required to transmit the data.*

Keywords: WSN, Data Aggregation, Layering, Slicing and Mixing

1. Introduction:

A wireless sensor network (WSN) is a collection of hundreds or thousands of these sensor nodes which are densely deployed in an unattended environment with the capabilities of sensing, wireless communications and computations [1]. These sensor nodes will forward the sensed data to the base station by communicating with other sensor nodes in the network. As the wireless sensor networks are small in size they constraints such as low battery, less computation speed and less memory. Wireless sensor networks are having some issues such as scalability, reliability and energy efficiency [2]. Because of these constraints and issues, efficient routing of data from source to destination is a major issue. Different routing protocols are designed for efficient routing of data. There are various techniques that are used to reduce the energy consumption in the network. Data aggregation is one of the techniques used to reduce the energy consumption and avoid data redundancy in the network. Data aggregation is the process of aggregating the data from multiple sensors to eliminate redundant transmission and provide fused information to the base station. Data aggregation usually involves the fusion of data from multiple sensors at intermediate nodes and transmission of the aggregated data to the base station [3]. The data Aggregation within the network increase the WSN's overall lifetime. In data aggregation scheme instead of sending each sensor node's data to sink node, one of the sensor nodes, called data aggregator collects the information from its neighbouring nodes, aggregates them and sends the aggregated data to the base station.

As the network is wireless and the sensor nodes are deployed in remote area the data is prone to various kinds of attacks, providing security to data while transmission is a major challenge [4]. Secure data aggregation is nothing but the providing security during data transmission between sensor nodes. Secure data aggregation protocols are mainly divided into 2 types they are 1) Hop-by-hop secure data aggregation: these protocols cannot provide data confidentiality and the overhead also increases. 2) End-to-end secure data aggregation: in order to overcome the limitations of hop-by-hop data aggregation end-to-end secure scheme is proposed. These protocols perform data aggregation without decrypting the sensor data at aggregator node [4].

2. Layer Based Approach

Layering is one of the technique used to reduce the hop count and in turn energy consumption in the network. When the network is first time deployed, the energy of all the nodes is same. As the network starts functioning, few nodes lose their energy faster and die earlier as compared to other nodes. The main problem is that how to manage the energy consumption among the nodes so that less energy could be consumed among nodes and we can increase the lifetime of the network.

In the layered architecture, nodes that have the same hop count to the sink are partitioned into one layer [5]. The number of layers and the number of nodes in each layer are determined by the geographical distribution of the nodes and the sink location. Nodes in the same layer select one node in its adjacent layer closer to the sink as the forwarding node.

Babu Ram, Narottam Chand, Prateek Gupta, Siddhartha Chauhan proposed a Layered architectural approach were sensor nodes are distributed among layers according to the distance from the BSC and each layer is consisting of many sensor nodes. Each layer is at R distance from the previous layer. The main purpose of layered approach is to communicate and send the data of higher level to the lower level sensor nodes using minimum transmission energy [6]. Sensor nodes are distributed among layers according to the distance from the BSC and each layer is consisting of many sensor nodes. Each layer is at distance R from its next layer. First layer is at distance R from the BSC, second layer is at R distance from the first layer, third layer is at distance R from the second layer. The main purpose of layered approach is to communicate and send the data of higher level to the lower level sensor nodes using minimum transmission energy. All sensor nodes of higher level will communicate to the lower level sensor nodes which are at the minimum distance R and hence reduces unnecessary energy consumption in the network.

Ioana Rodhe and Christian Rohner say that the nodes are organized into layers according to their hop distance from the base station. In the deployment phase, a wave algorithm starting from the base station is used to determine the layers in the network and that nodes exchange layer information with their neighbours.

Xiaoqing ZHANG; Zhongtang HE, Tongkai JI proposes a approach which divides nodes into layers. BS broadcasts one *HELLO* message with a fixed sending power. After all sensor nodes have received this message, they calculate the distance from BS according to the signal strength. This distance helps sensor nodes to choose a suitable Sending power for saving energy when they transmit data to BS

3. Privacy Preserving Techniques in Data Aggregation:

Data aggregation is designed to reduce the volume of traffic being transmitted over the network by fusing or compressing data in the intermediate sensor nodes (Aggregator nodes). Aggregation is a common and effective method to preserve private data against an external adversary, because the process compresses large inputs to small outputs at the intermediate sensor nodes [7]. Data aggregation also leads to vulnerability against internal adversaries. In particular, if an aggregator node is compromised, it may undergo either passive or active attacks:

- In passive attacks, the malicious aggregator node properly follows the protocols defined by a WSN, with the only exception that it might record all intermediate computation and communication. Since an aggregator is supposed to perform the aggregation operations, it can decrypt the transmitted data and compromise with the content privacy.
- In active attacks an aggregator node may inject bogus data or tamper with raw data, leading to the irrelevance of collected data at base station with original data. Unlike passive attacks which aim to compromise the confidentiality of data, active attacks aim to destroy the integrity of collected data.

Different privacy preserving techniques are proposed which aims at providing the confidentiality to the data in the network.

3.1. Cluster-based privacy data aggregation (CPDA):

The basic idea of CPDA is to introduce noise to the raw data sensed from a WSN, such that although an aggregator can obtain accurate aggregated information but not individual data points. CPDA classifies sensor nodes into two categories: cluster heads and cluster members. There is a one-to-many mapping between the cluster heads and cluster members. The cluster heads are responsible for directly aggregating data from cluster members, with the communication secured by a different shared key between any pair of communicating nodes.

3.2. Slice-mixed aggregation (SMART)

SMART [8] is another solution to protect individual data in the SUM aggregation. The main object is to preserve privacy by slicing original data into pieces and recombining them randomly. There are three steps in this approach. In the first step (Slicing), each sensor randomly selects J neighbour nodes within h hops to form a set S. Then it slices its data into J pieces, keeps one piece for itself and then sends the j - 1 encrypted pieces to j - 1 sensors randomly selected from the set S. In the second step (Mixing), after a sensor receives pieces of data from some other sensors, it decrypts the data using the key shared with the data sender. Each sensor waits for a while to make sure that all of the round aggregation data have already been sliced and received separately. In the third step (Aggregation), the intermediate sensor aggregates all pieces of data and transmits it towards the base station. Joyce Jose, M Princy, Josna Jose proposes a secure data aggregation scheme [9] which guarantees the privacy, authenticity and freshness of individual sensed data as well as the accuracy and confidentiality of the aggregated data without introducing a significant overhead on the battery limited sensors. This scheme involves aggregation tree construction, slicing, mixing and aggregation.

4. Proposed work:

Since sensed data contains the redundant information, data aggregation is a technique which aggregates the sensed data and forward to the base station which eliminates the redundancy. The proposed work mainly focuses on secure data aggregation. Initially an aggregation tree is constructed by ordering nodes into layers. The secure data aggregation is achieved by using slicing and mixing techniques.

The proposed approach uses small scale network. Base station is placed at the centre of the network. All the sensor nodes are deployed around the base station as shown in figure 1.

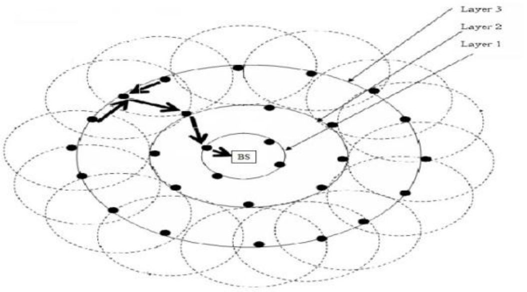

Figure 1: Network Architecture

4.1. Layer Formation:

Layers are formed based on the hop distance.
Aggregation tree is constructed by ordering nodes into layers based on hop distance.
Three layers are formed as shown in the figure 1.

- Layer 1 – Aggregator Nodes
- Layer 2 – Intermediate Nodes
- Layer 3 – Leaf Nodes

4.2. Slicing and Mixing:

Leaf nodes will sense the data and divide/slice the sensed data in to three pieces. A leaf node will distribute the slices to its neighbouring nodes of the same level by keeping one slice on itself. One of the *m* encrypted slices is kept on the node itself and the remaining *m-1* encrypted slices are appended with the node ID and transmitted to *m-1* neighbour nodes within the *h* hop (for a dense network *h=1*) except the encrypted slices to its parent. The encrypted slice with its ID to the parent is appended with the encrypted slice kept on the node, and it is transmitted to its parent with the aggregation result from leaf node. All the slices are encrypted

$$Encryption\ C_{ij} = (\sum_{i.j=0}^{N} (d_{ij} + K_{ei}))\ mod\ M$$

Where $d_{ij} = 0$, when there is no data transfer between node, i to node j.

$$Aggregation\ d_{iA} = (\sum_{i,j=1}^{N} C_{ij})\ mod\ M$$

$$Decryption\ f_R = \left(\sum_{i,j=1}^{N} C_{ij} - \sum_{i=1}^{N} K_{ei}\right) mod\ M$$

If *M* is smaller than the sum of all sample values and encryption keys, the sink fails to reproduce the real sum, instead it produces a smaller number than *M*. So, in order to avoid this problem take *M* as large *M=n*t*, where *n* is the number of nodes and *t=max (di)*, i.e., maximal value, which may appear in the measurement.

All the data slices from each leaf nodes are sent to the intermediate nodes in the next level for mixing process. Each intermediate node will collect the slices from respective leaf nodes, sums them along with their sensed data and encrypt it to send the mixed data to the aggregator node in the next level.

4.3. Aggregation of Data:

Each intermediate node will send the mixed encrypted data to the aggregator node for data aggregation. Aggregator node will check whether the received data is from the valid member nodes or not. Each node in a sensor network is assigned with a common secret key (K), node specific key (K_i) and a unique ID_i. If any changes occur in the sensing region of the leaf node, the leaf node will sense the changed data and follow the same procedure as discussed above to keep the aggregator node updated. The aggregated data at the aggregator node is encrypted. When the base station requires data, it sends a request to the aggregator node. Aggregator node will in turn send the requested data to the base station. The received data at the base station is decrypted to obtain the original aggregated data.

5. Analysis

The proposed approach is mainly based on reducing the energy consumption by minimizing the number of hops and providing the secure data aggregation. A centralized base station is placed at the centre of the network and the sensor nodes are placed around the base station. Layers are formed based on hop distance of the nodes from the base station. While transmitting data from the leaf nodes to the base station a forwarding node will select a node which is in the higher level and hence minimizing the cost of unnecessary computation at the forwarding node. Here privacy of data is preserved using slicing and mixing methods. The leaf node in the network will sense the data slice it and forward to its neighbouring nodes at the same level. Received data from the neighbouring nodes are encrypted and sent to the intermediate nodes placed at the next level along the aggregation tree. Finally all the mixed data in the intermediate nodes are encrypted and sent to the aggregator node for data aggregation. When the base station sends request to the aggregator node for data, aggregator node will send the encrypted data to the base station. The base station will decrypt and obtain the original data and hence preserving the privacy of data by providing end to end security to the data.

6. Conclusion

Wireless sensor networks are resource constrained where the energy efficiency is a major issue. Many techniques are used to reduce energy consumption like data aggregation. Aggregation reduces redundancy of data and hence minimizes energy consumption. As the sensor nodes are wireless security is major issue that has to be addressed. The proposed approach achieves efficiency by reducing the number of hops and provides security by using slicing and mixing techniques. Efficient end to end security is achieved in this method.

7. References

[1]. Yazeed Al-Obaisat, Robin Braun, “On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management”, 2006.

[2]. R.Devika, B.Santhi, T.Sivasubramanian, “Survey on Routing Protocol in Wireless Sensor Network”, International Journal of Engineering and Technology, 2013

[3]. Ahmed Sardouk, “data aggregation in WSNs: A survey”, material science research, 2010

[4]. A.S.Poornima, B.B.Amberker, "SEEDA : Secure End-to-End Data Aggregation in Wireless Sensor Networks", 2010 IEEE

[5]. Mei Yang, Jianping Wang, Zhenguo Gao, Yingtao Jiang, Yoohwan Kim*,"* Coordinated Robust Routing by Dual Cluster Heads in Layered Wireless Sensor Networks"

[6]. Babu Ram, Narottam Chand, Prateek Gupta, Siddhartha Chauhan, "A New Approach Layered Architecture based Clustering for Prolong Life of Wireless Sensor Network", International Journal of Computer Applications, 2011

[7]. Na Li, Nan Zhang, Sajal K. Das, Bhavani Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey", 2009

[8]. Chaoran Li and Yun Liu, "ESMART: Energy-Efficient Slice-Mix-Aggregate for Wireless Sensor Network", Hindawi Publishing Corporation, 2013

[9]. Joyce Jose, M .Princy, Josna Jose, "PEPPDA: Power Efficient Privacy Preserving Data Aggregation for Wireless Sensor Networks", 2013 IEEE International Conference on Emerging Trends in Computing.