A Framework: Secure Data Aggregation in Wireless Sensor Networks

Vimal Pambhar¹, Bhoomi Bangoria², Bhavik Kataria³

Assistant professor, Dept. of CSE/IT, Dr. Shubhash Technical campus, Junagadh, Gujarat, India ¹
PG Student [CE], Dept. of CE, Noble Engineering College, Junagadh, Gujarat, India ²
PG Student [SE], Dept. of CSE, RKDF Institute of Science and Technology, Bhopal, Madhya Pradesh, India ³

ABSTRACT: Wireless Sensor Networks (WSNs) are used in many applications in the area of tracking and monitoring. WSNs have many constraints like low computational power, small memory, and limited energy resources. Most of the energy consumption is due to data transmission. For that we apply Data aggregation approach on the sensed data by the deployed sensor nodes. This approach helps to reduce the number of transmissions and improves the life time of wireless sensor network with less energy usage of sensor nodes and also to protect Data Aggregation process from various kinds of attacks becomes extremely critical. So we give some general framework for Secure Data Aggregation.

Keywords: wireless sensor network, sensor node, security, attacks, cluster, Data Aggregation.

I. INTRODUCTION

The Sensor Network can be described as a collection of sensor nodes which co-ordinate to perform some specific action. Unlike traditional networks, sensor networks depend on dense deployment and co-ordination to carry out their tasks. Sensor Networks consisted of small number of sensor nodes that were wired to a central processing station. However, nowadays, the focus is more on Wireless Sensor Networks.

In Figure 1 shows Wireless Sensor Network Architecture. Wireless sensor networks are consisting of numerous light weight and tiny sensor nodes with limited power, storage, communication and computation capabilities. Wireless sensor networks are being employed in civilian applications like habitat monitoring to mission critical Applications.

Fig. 1 Wireless sensor networks Architecture [1]

A sensor node is made up of four basic components as shown in Figure 2 a sensing unit, a processing unit, a transceiver unit and a power unit. They may also have application dependent additional components such as a location finding system, a power generator and a mobilizer Users.
II. GENERAL SURVEY OF WIRELESS SENSOR NETWORKS (WSNs).

Several attempts were made by the researchers to study the major challenges in WSNs, security requirements of WSNs, Constraints of WSNs. That survey mentions in below Table 1.

<table>
<thead>
<tr>
<th>WSNs Major Challenges</th>
<th>WSNs Constraints</th>
<th>WSNs Security Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility and topology changes</td>
<td>Limited Physical Resources</td>
<td>Availability</td>
</tr>
<tr>
<td>Due to mobility of Sensor nodes network topology would be changed dynamically.</td>
<td>like memory, computational power, energy (Battery).</td>
<td>Networks services are available even in the presence of denial-of-service attacks.</td>
</tr>
<tr>
<td>Energy constraints</td>
<td>Scalability</td>
<td>Authentication</td>
</tr>
<tr>
<td>Limited battery power</td>
<td>The protocols must be scalable</td>
<td>a malicious node cannot masquerade as a</td>
</tr>
<tr>
<td>of small tiny sensor nodes.</td>
<td>enough to respond and operate</td>
<td>trusted network node.</td>
</tr>
<tr>
<td></td>
<td>with such large number of sensor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>nodes.</td>
<td></td>
</tr>
<tr>
<td>Security Issues</td>
<td>Quality of Service</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>All the traditional networks</td>
<td>the data should be delivered</td>
<td>a given message cannot be understood</td>
</tr>
<tr>
<td>security approaches are</td>
<td>within a certain period of time</td>
<td>by anyone other than the desired</td>
</tr>
<tr>
<td>directly apply on WSNs.</td>
<td>from the moment it is sensed</td>
<td>recipients.</td>
</tr>
<tr>
<td></td>
<td>otherwise the data will be</td>
<td></td>
</tr>
<tr>
<td></td>
<td>careless.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. A Survey for Wireless Sensor networks.

III. DATA AGGREGATION

The architecture of the sensor network plays important role in the performance of data aggregation protocols. Several data aggregation protocols have been proposed. These protocols can be classified based on network models. There are two categories: Tree based data aggregation [9] and cluster based data aggregation.
Cluster based data aggregation [8] is the process of combining the data coming from various sources and en route them after removing redundancy such as to improve the overall network lifetime. The in-network processing is done on the aggregator node. The aggregator node aggregate the data received from its child node as per the required aggregation function (like min, max, average, sum etc.) and send the aggregated result to the other high level aggregated node.

An aggregation scenario using clustering shown in figure 3 in that cluster heads collect the data from all the neighbors sensor nodes and forwarded that data to the Base Station (Sink Node). Base station sends that information to the external network via Internet.

IV. CLASSIFICATION OF SECURE DATA AGGREGATION

The work on secure data aggregation can be classified based on encryption of data at specific nodes into three categories, hop-by-hop encrypted data aggregation end-to-end encrypted data aggregation [12] and Privacy Homomorphism.

A. Hop-by-Hop encrypted data aggregation

In the hop-by-hop encrypted data aggregation [13], intermediate nodes decrypt every message received by them. So, get the plaintext. Then aggregate the plaintext according to the aggregate function, and encrypt the aggregate result before transmitting it. In this all the intermediate sensor node has to decrypt the received data and apply aggregation function on it. Due to many decryptions perform by the intermediate node it’s consuming more battery power and not provide end-to-end security.

B. End-to-End encrypted data aggregation

In order to overcome the drawbacks of the hop-by-hop encrypted data aggregation [14, 15, 17] a set of end-to-end encrypted data aggregation protocols are proposed. In those schemes, intermediate nodes can aggregate the cipher text directly without decrypting the messages. Compared to the hop-by-hop one, it can guarantee the end-to-end data confidentiality and result in less transmission latency and computation cost. Adversaries will not be able to recognize what reading it is during data transmission. In terms of privacy, they designed aims to eliminate redundant reading for data aggregating but this reading remains secret to the aggregator.

C. Privacy Homomorphism

A Privacy Homomorphism (PH) [18] is an encryption transformation that allows direct computation on encrypted data. In homomorphic encryption certain aggregation functions can be calculated on the encrypted data. The data is encrypted and sent toward the base station, while sensors along the path apply the aggregation function on the encrypted data. The base station receives the encrypted aggregate result and decrypts it. Specifically, a homomorphic encryption scheme allows the following property to hold:

\[ \text{enc}(a + b) = \text{enc}(a) + \text{enc}(b) \]
This means that in order to calculate the SUM of two values, we can apply some function to their encrypted counterparts and then decrypt the result of the SUM operation at sink node. The data would be encrypted at the sensor node, the SUM or AVERAGE would be calculated as the aggregate result follows a path to the base station, and the final result would be decrypted at the base station.

V. A GENERAL FRAMEWORK OF SECURE DATA AGGREGATION IN WIRELESS SENSOR NETWORK.

In a general framework of Secure Data Aggregation, First, we discuss about the how to make clusters for the randomly placed nodes using Heartbeat node placement algorithm. We modify Appheartbeat protocol for the implementation of the clustering for the Data Aggregation. For the simulation we use Jist (java in simulation time)/SWAN (Scalable Wireless Ad-hoc Networks) Simulator.

Some of the nodes will work as cluster heads. These cluster heads are responsible to receive message or data from their neighbours. Each cluster head send hello message to all other nodes, those nodes which are in the range of cluster head they send the message back to cluster head and join with that cluster for further processing. We measure energy usage by every cluster head by the energy model which is integrated in the SWAN simulator and also show the comparison graph of energy usage by clusters heads between static and dynamic clusters heads selection procedure.

In below figure we mention the steps for the Data Aggregation using cluster based Data Aggregation for that we modify Appheartbeat protocol which is my default protocol given in SWAN simulator.

![Data Aggregation (SUM) Architecture in JiST/SWAN.](image)

We apply privacy on sending data by the sensor nodes to the Cluster head. We apply end to end symmetric cryptography based on Privacy Homomorphism on the sending data.

Figure 5 represents End to End privacy approach, in that S₁, S₂, ..., Sn nodes sense the data from the environment, before sending it to cluster head or aggregator node, It they apply encryption method on it and then send encrypted data to the cluster head. Perform SUM function on encrypted data using Privacy Homomorphism and sends this encrypted aggregated result to the base station. Base station applies decryption method on that data and gets original data. During this whole procedure we measure the energy usage by the cluster heads.
By reviewing the existing data aggregation in the WSN, an adversarial model that can be more useful to save the energy of Wireless sensor Nodes that lead to improve the life time of whole networks. An adversarial model for security on Data Aggregation its help us to give better performance compare to existing scheme.

VII. FUTURE WORK

In future work, this method can be made more scalable and fine-tuned with the multi level clustering where the cluster can have two to three level tree so the cluster can cover more number of nodes with lower energy consumption. It is also planned to evaluate more secure schemes and extend the framework if necessary. We hope that our work will encourage other researchers to consider the vital problem of secure information aggregation in sensor networks.

REFERENCES

Vimal J. Pambhar has completed the M.Tech in Computer Engineering from U.V. Patel College of Engineering, Ganpat University, and Gujarat, India. His Research area is Secure Data Aggregation in Wireless Sensor Network Subject. Right now he is work as Assistant Professor at CSE/IT Department in Dr.Subhash Technical Campus, Junagadh, Gujarat-362001, and India.

Bhoomi M. Bangoria is pursuing M.E scholar in Computer Engineering from Noble Engineering College, Junagadh, Gujarat-362001, and India.

Kataria Bhavikkumar M. is pursuing M.Tech. in Software Engineering from RKDF Institute of Science and Technology, Bhopal, Madhya Pradesh and He has completed his B.E. in Computer Engineering from C.U.Shah College of Engineering and Technology, Wadhwan City, Gujarat. Now days he is working as Assistant Professor in Dr. Subhash Technical Campus, Junagadh, Gujarat.