“IRDAT–Improved Data Aggregation Protocol for Sensor Networks”

Dinesh Kumar¹ and Kamal Parkash²

Department of Information Technology, Maharishi Markandeshwar University, Mullana, Ambala, India
¹dineshgarg82@gmail.com, ²jindalkamal@gmail.com

ABSTRACT: Data aggregation in wireless sensor networks is widely accepted as an essential paradigm for energy efficient routing but with low reliability under node and link failures. In wireless sensor networks, malicious sensor nodes send false data reports to distort aggregation results. Existing trust systems rely on general reputation to mitigate the effect of this attack.

This paper presents one of a reliable data aggregation protocol, called RDAT i.e Reliable Data Aggregation Protocol which associates packet’s reliability in data transmission with the amount of information it contains and gives higher reliability to the packet which has more information by adjusting the degree of redundancy. Therefore, RDA can jointly optimize both information reliability and energy efficiency in sensor networks with data aggregation. Especially, RDA is not banded with special routing schemes; hence it can be used with any kinds of routing schemes supporting data aggregation in wireless sensor networks.

Keywords: wireless sensor networks; reliability; routing; data aggregation

I. INTRODUCTION

Wireless sensor networks consist of large numbers of resource constrained sensor nodes communicating over the wireless medium for the purpose of information gathering. These networks have several unique properties that distinguish them from traditional wireless ad hoc networks. One such property of wireless sensor networks is that neighboring sensor nodes often have overlapping sensing ranges and therefore the data generated by neighboring sensor nodes are redundant. In addition, the amount of data generated in large sensor networks is usually enormous for the base station to process. To conserve the energy and bandwidth of resource constrained sensor nodes, redundancy in sensor data must be eliminated at intermediate sensor nodes by performing data aggregation. Data aggregation is defined as the process of combining data from multiple sensor nodes to eliminate redundant data transmission and provide fused information to the base station. Many wireless sensor networks are deployed in unattended hostile environments to perform mission-critical tasks and therefore security protocols are required for these networks. Despite this security requirement, physical security of sensor nodes cannot be provided because making sensor nodes tamper-proof is prohibitively expensive. Due to this lack of physical security, intruders can easily compromise one or more sensor nodes to subvert network operations. Compromised sensor nodes pose a challenging constraint for the protocol designer: a sensor network protocol must be highly energy efficient while being able to function securely in the presence of possible malicious compromised nodes within the network. However, cryptographic primitives alone cannot provide a sufficient solution to secure and reliable data aggregation problem because compromised nodes have access to cryptographic keys that are used to secure the data aggregation process. A reputation based system in wireless sensor network domain is a system in which the actions of every node are observed by the other nodes in an attempt to evaluate their trustworthiness. In this paper, effect of compromised nodes on data aggregation is mitigated using a reputation system which is built over functional reputation concept. A functional reputation of a sensor node is represented by the beta distribution of the sensor node’s actions with respect to a certain function. We propose an Improved Reliable DAT aggregation protocol, called IRDAT. IRDAT considers trustworthiness of sensor nodes to improve the reliability of aggregated data & based on clusters. Cluster is a collection of nodes.
II. METHODOLOGIES

Proposed Model for Data Aggregation

Beta Reputation System

As the success of Bayesian formulation in detecting arbitrary misbehavior of sensor nodes is, we select a Bayesian formulation, namely beta reputation system, for trust evolution. In this section, before giving the details of protocol RDAT, we present a brief information about beta reputation system.

Computing Functional Reputation and Trust

Functional reputation value \( (R_{i,j}X) \) is computed using beta density function of sensor node \( N_j \)'s previous actions with respect to function \( X \). Trust \( (T_{i,j}X) \) is the expected value of \( R_{i,j}X \). Let us take routing task as an example. If sensor node \( N_i \) counts the number of good and bad routing actions of \( N_j \) as \( \alpha \) and \( \beta \), respectively. Then, \( N_i \) computes the functional reputation \( R_{i,j}routing \) about node \( N_j \) as Beta\((\alpha + 1, \beta + 1)\). Its Equations are shown in the next topic that how it calculates these values.

Secure and Reliable Data Aggregation

In protocol RDAT, data aggregation is periodically performed in certain time intervals. In each data aggregation session, secure and reliable data aggregation is achieved in two phases. In the first phase, before transmitting data to data aggregators, each sensor node \( N_i \) computes \( R_{i,j}aggregation \) value for its data aggregator \( A_j \) and evaluate the trustworthiness of \( A_j \). If trustworthiness of \( A_j \) is below a predetermined threshold, then \( N_i \) does not let \( A_j \) to aggregate its data. To achieve this, \( N_i \) encrypts its data using the pairwise key that is shared between the base station and \( N_i \) and sends this encrypted data to the base station along with a report indicating \( A_j \) may be compromised. Based on the number of reports about \( A_j \) over the time, the base station may decide that \( A_j \) is a compromised node and it should be revoked from the network. In the second phase of data aggregation session, the following Reliable Data Aggregation (RDA) algorithm is run by data aggregators. Algorithm RDA depends on \( R_{i,j}sensing \) and \( R_{i,j}routing \) functional reputation values to mitigate the effect of compromised sensor nodes on aggregated data.

The Algorithm Improved RDA is

Input: Data aggregator \( DA_j \), \( DA_j \)'s neighboring nodes \{\( N_1, N_2, ..., N_i \}\), trust values of neighboring nodes computed by \( DA_j \) \{\( T_{i,j}Sensing \), ..., \( T_{i,j}Sensing \)\} and \{\( T_{i,j}Routing \), ..., \( T_{i,j}Routing \)\}.

Output: Aggregated data \( Dagg \).

Step 1: \( DA_j \) requests each \( N_i \) to send its data for data aggregation.

Step 2: Sensor nodes \{\( N_1, N_2, ..., N_i \}\} transmit data \{\( D_1, D_2, ..., D_i \)\} to \( DA_j \).

Step 3: \( DA_j \) updates trust values \( T_{i,j}Sensing \) and \( T_{i,j}Routing \) of each \( N_i \) based on the first and second hand information regarding \( N_i \).

Step 4: when \( DA_j \) receives data packet

\[
\text{If (this packet is never received before) Then} \]

\[
\{ \]

\[
DA_j \text{ weighs data } D_i \text{ of sensor node } N_i \text{ using the } T_{i,j}Sensing \text{ and } T_{i,j}Routing \]

\[
H_1 = \text{the amount of information a source senses;} \]

\[
H_k = \text{the amount of information after aggregation;}
\]

\[
\alpha = (1/(1 – e)), \quad p = \alpha \ast (H_k/H_1)
\]

\[
A_j \text{ aggregates the weighted data to obtain } Dagg.
\]

\[
}\]

Step5: If (all packets are received or this round is over) Then

\[
\{ \]

\[
\text{Send the aggregation packet to parent } p \text{ times;}
\]

\[
}\]

Since compromised nodes send false sensing reports in order to deceive the base station, Algorithm RDA considers trustworthiness of sensor nodes with respect to sensing function to increase the reliability of aggregated data. To achieve this, \( A_j \) weights data of each sensor node \( N_i \) with respect to the sensor node’s trust value \( T_{i,j}sensing \) and \( T_{i,j}routing \). By weighting sensor data based on trust levels, data aggregators reduce the compromised sensor nodes’ effect on the aggregated data.
III. RESULTS

A. Figure: Flow chart of IRDAT.

- Generate the Functional Reputation Table and Data for all the Nodes
- Divide Nodes into Clusters
- Select Data Aggregator for Each Cluster
- Each Cluster Head will send Request for Data to its Cluster Nodes
- Each Node will Check the Trust Worthiness of Data Aggregator and Send Data Accordingly
- Data Aggregator Calculates Trust Values for Routing and Sensing for each Node and Weights the Data of that Node Accordingly
- Each Cluster Head Aggregates the Data and Sends it to the Base Station
- Base Station will Aggregate the Data

B. Result
With the simulation result, it can be shown that the protocol implemented in this paper is Improved Reliable Data Aggregation Protocol and more energy efficient & secured.

C. Figure: Data Aggregator for all Cluster

D. Figure: Final Data Aggregator

IV. DISCUSSION
In this paper the protocol is discussed after its implementation in C. A structure called NODE has been used to describe a node which contains the array of functional reputation table and also the values of node id, first and last node in the cluster and the node’s data. One node is made the Base station and the remaining nodes are divided into clusters. A Data aggregator for each cluster is selected using Random() function. Then the Random() function is again used to generate values for the functional reputation table and the data for each node. After this the algorithm RDA is implemented. Each data aggregator will request all other nodes in its cluster to send it the data. Each node in the cluster after receiving this message will calculate the trustworthiness i.e of the data aggregator. Only if it is above the threshold level, it will send its data, else it will increment the value in the array of errors for that data aggregator.

Data aggregator will gather the second hand value for each node and then combining it with first hand
value, it will calculate trust values of Routing and Sensing for each node i.e. Then using these values of trust, it will weight the data received from each node accordingly. There is also a factor “v” the aging factor which is used in calculation of trust values and its value is varied from 0.2 to 0.9. The effect of change in value of ‘v’ on the aggregated data is plotted on the graph.

V. CONCLUSION

In wireless sensor networks, compromised sensor nodes can distort the integrity of aggregated data by sending false data reports and injecting false data during data aggregation. Since cryptographic solutions are not sufficient to prevent these attacks, general reputation based trust systems are proposed in the literature. The Improved Reliable Data Aggregation Protocol (IRDAT) introduces Cluster based Functional Reputation Data Aggregation concept. In this System total processing is based on cluster & a cluster is a collection of nodes & the aggregator node is selected automatically.

Future work includes the simulation of this protocol on any simulation software such as Network Simulator (NS-2) or QUALNET or any other simulation software and get the exact results and compare these results with the implementation results of another reliable data aggregation protocol i.e “Ant Colony data gathering protocol”. Carrying out more detailed simulator runs would also allow the protocols to be evaluated in more detail.

REFERENCES


