CHAPTER 5

CONCLUSION AND SCOPE FOR FUTURE WORK

5.1 CONCLUSION

A wireless sensor network is a collection of nodes organized into a cooperative network. The nodes communicate wirelessly and often self-organize after being deployed in an Ad-hoc fashion. Many wireless sensor networks also utilize minimal capacity devices which places a further strain on the ability to use past solutions.

Data aggregation is one of the important fundamental distributed data processing procedures in WSN. The goal of data aggregation is to merge the data from various sources, reroute it with the elimination of the redundancy and thus reducing the number of transmissions and saving the energy. In addition, secure authentication is an important technique in WSN. The objective of secure authentication technique is to rectify the security threat of node capture attacks which meant the process of getting hold of the sensor node through a physical attack.

In practice, in the sensor node compromise technique, there is a initiation of node capture attack where the adversary physically captures the sensor nodes, removes them, compromises and redeploy them in the network. Following the redeployment of the compromised nodes, it builds up a variety of attacks through compromised nodes. The forceful attacker weakens the sensor network protocols along with the formation of clusters,
routing and data aggregation and hence resulting in recurrent disruption of network operations. Therefore, the node capture attacks are unsafe, hence secure authentication technique for data aggregation protocol is designed to reduce the damages caused by them.

This research attempts an investigation into the existing secure data aggregation protocol proposed for WSN. The research focuses on reducing energy consumption while attaining good packet delivery ratio, achieved by Energy Efficient Secure Data Aggregation (EESDA) protocol and eliminates more attacks and increases the packet delivery ratio attained by Secure Authentication Technique for Data Aggregation (SATDA) protocol.

In the first part of this research, an energy efficient secure data aggregation protocol for wireless sensor networks was proposed. For data aggregation, the system is grouped such that each group is headed by an aggregator. This aggregator acts as a link between the sensor nodes and the sink. During the transmission of the data, first encryption is performed by the sensor nodes when transferring data to the aggregator. The aggregator on reception of the data decrypts it using the key and reads it. The aggregator then determines the MAC value using hash function to check the validity of the source sensor. If the estimated MAC value is valid then the source is authenticated. Second encryption is performed by the aggregator when transferring data along with the MAC value to the sink. Hence, integrity of the system is maintained. Due to the double encryption of the data during data aggregation, adversaries cannot affect the system. Hence, the system remains secure even in the wireless environment. The protocol has performed well to reduce energy consumption while attaining good packet delivery ratio.
In the second part of this thesis, secure authentication technique for data aggregation in wireless sensor networks is proposed. During first round of data aggregation, the aggregator upon identifying the detected nodes selects a set of nodes randomly and broadcasts a unique value which contains their authentication keys, to the selected set of nodes. When any node within the set wants to send the data, it sends slices of data to other nodes in that set, encrypted with their respective authentication keys. Each receiving node decrypts, sums up the slices and sends the encrypted data to the aggregator. The aggregator aggregates and encrypts the data with the shared secret key of the sink and forwards it to the sink. In the second round of aggregation, the set of nodes is reselected with new set of authentication keys. The proposed approach rectifies the security threat of node capture attacks.

Simulation was carried out to evaluate its performance of the proposed algorithm. To further evaluate the practical performance of the proposed algorithm, simulation based experiments were conducted. The simulation framework was based on the NS2. In the simulation, the proposed protocol Energy Efficient Secure Data Aggregation (EESDA) was tested against Cluster-based Private Data Aggregation (CPDA) and Secure Authentication Technique for Data Aggregation (SATDA) protocol was tested against Energy Efficient Secure Data Aggregation (EESDA) protocol. In addition, robustness of various attacks such as Sybil Attack (SY), Selective Forwarding Attack (SF), Replay Attack (RE) and Spoofed Data Attack (SD) was tested.

For EESDA and SATDA of the protocols, the following performance metrics were tested.

- Averages over all surviving data packets from the sources to the destinations.
• Ratio of the number of packets received successfully and the total number of packets transmitted.

• Average energy consumption of all nodes in sending, receiving and forward operations.

• Average number of packet dropped at each receiver.

• Number of packets successfully received by the receiver.

From the simulation results it is shown that the proposed protocols EESDA and SATDA performs better.

5.2 SCOPE FOR FUTURE WORK

Main goals of energy efficient secure data aggregation protocol and secure authentication technique for data aggregation protocol in WSN are to avoid redundant transmission of packets to minimize energy consumption and to eliminate more attacks and increases the packet delivery ratio. However, this research work does not take into account about the node capture attacks in hierarchical data aggregation for heterogeneous sensor nodes. Hence, it is recommended that further research on hierarchical data aggregation approaches for heterogeneous nodes should be conducted for the existing protocols.