CHAPTER 7

CONCLUSION AND FUTURE RESEARCH

7.1 Summary of research

By using the process of encryption (RAC algorithm), we provide security to the data being passed through the network. This is further enhanced by providing a secure network by using Concealed Data Aggregation, Secret Sharing and Dispersive Randomized Routing methods. By using these methods, the packet interception probability can be easily reduced. Also in our approach we have reduced the energy consumption by using data aggregation that reduces the amount of packets transferred from the nodes to the sink. Though the secret sharing mechanism increases the amount of data transferred from the aggregator node to sink, by optimizing the M value of (T, M) approach to be equal to the number of nodes from which data is aggregated we can overcome this overhead. Thus our approach remains secure and at the same time energy efficient compared to the classic deterministic routing approaches.

This can be further made foolproof by using dynamic routing techniques for transmission of packets. Dynamic routing can be performed on the shares, rather than randomized routing, to provide better efficiency and security. By using the Backpressure
algorithm and Reactive Routing methods the packet interception probability can be easily reduced. DoS [Zhan et al. 2009] attacks can be made almost impossible by using our approach.

7.2 Recommendations for further work

The algorithm can be further optimized by fixing a max hop count during the first phase such that the packets are not passed to nodes that are at long distances. The user can also encrypt packets such that even if an adversary obtains a group of packets, they might still not be able to retrieve the information.