CHAPTER 8

CONCLUSION

WSNs are a class of ad hoc network consisting of tiny low cost resource constrained devices that have the ability to sense their environment, process, aggregate and to send the data to the destination. The deployment nature, resource constraint and the wireless communication channel make WSNs susceptible to a variety of attacks. Deployment of WSNs has been envisioned in many sensitive applications such as military operations and health care. Despite advances in miniaturization and other developments in WSNs occurring at a very fast pace, security and fault tolerance within WSNs has not gained significant interest. This is due to the lack of commercial motivation.

Traditional security and fault tolerant schemes require heavy communication and computational resources which is beyond the resource starved SNs. Instead, WSNs need a balanced and comprehensive solution, which is efficient, effective and has low, security and fault tolerance overheads. Keeping these factors in mind, few protocols/Schemes have been developed and presented in this thesis.

8.1 Contributions: The followings are the contributions of this thesis.

(a) Group Aware Network Management (GANM) Protocol: GANM protocol minimizes the energy consumption of SNs by not allowing all of them to sense and transmit the sensed data at the same time either locally or globally. GANM protocol also enables a fault tolerant scheduling scheme among the group members such that there is always one member awake to listen to the surrounding, i.e., to sense and to transmit. Simulation results shows that when GANM is applied at lower level in Direct, LEACH and PEGASIS a significant gain in network life is achieved.
(b) Timestamp Firewall based misused key detection (TFMKD) protocol: TFMKD is designed to detect key being misused by an adversary and revoked these keys from the network. TFMKD prevents WSNs from various types of attacks viz. selective forwarding, wormholes, sinkholes and Sybil attacks. The simulation results show its performance over some existing schemes.

(c) Secure and Energy Efficient Adaptive Routing (SEEAR) protocol: Communications from BS to SNs, between neighboring SNs and from SNs to BS is protected by SEEAR. SEEAR have been designed with keeping in mind the various parameter viz., network size, energy consumption at SNs, hot sink problem, network setup time, network scalability, etc. Analysis shows that SEEAR outperform than Q-composite and peer to peer scheme on most of the parameter.

(d) Framework for Energy Management, Fault Revocation And Homogeneous Distribution Of Static SNs: The presented Framework provides ample amount of energy to the BS and SNs in the deployment area. Fault revocation is provided by removing the dead SNs from the network with the help of mobile fault revoking SNs. Framework also distributes static SNs throughout the network equally to avoid partitioning of the network. Simulation results show the effect of concentration of FRNs on time taken to revoke fault in the deployment area and effect of ratio between SNs and mobile SNs on time taken to establish homogeneous network.

8.2 Future work
Secure and fault tolerant protocols presented in this thesis are promising still there are significant scope for future research. In future we extend this research work in the following direction.

- We develop trust model for the presented security protocols.
And testing will be done by developing an integrated system of real life applications.

- We explore security issues in multimedia and biometric security, cyber security and information assurance, protection against identity theft and forensic computing and testbed will be developed for testing the security requirement of different applications.

- We propose issues such as quality of service (QoS) posed by video and imaging SNs and real-time applications. Energy aware QoS routing in WSNs will ensure guaranteed bandwidth (or delay) through the duration of connection as well as providing the use of most energy efficient path. QoS routing in WSNs have several applications including real time target tracking in battle environments, emergent event triggering in monitoring applications, etc. Currently, there is very little research that looks at handling QoS requirements in a very energy constrained environment like WSNs.

- We can think about more good security and key management algorithms, irrespective of the energy which the network will consume. Moreover, we can also work upon some good robotics technology to develop even more compact RSVs that suits to real life applications.