CHAPTER-8

CONCLUSION AND FUTURE DIRECTIONS

This PhD thesis presents a framework for secure wireless sensor networks. This chapter concludes the thesis by summarizing the main contributions and discusses about the extendibility. The system models discussed in this thesis is an attempt to enhance the efficiency of WSNs with respect to security as the main parameter. The context and the scope of the problem considered in this research are confirmed through a detailed and comprehensive survey of previous work on security modeling in WSNs.

Since security is based on encryption function and the key, therefore so the matter presented in this thesis is closely related to encryption function and key management schemes. In short, techniques for securing wireless sensor networks have been presented in this thesis that includes secure data aggregation, efficient key management, removal and replacement of compromised sensor nodes, dynamic encryption function along with lightweight encoding schemes for WSNs. Analysis of the system model validates the effectiveness and efficiency of the various techniques presented in this thesis.

This chapter summarizes the work that has been carried out in this thesis and discusses some directions for future work. Section 7.1 provides the summary of contributions in this research work. In Section 7.2, some of the possible future work has been described.

7.1 CONTRIBUTIONS

In this research, followings are the main contributions of this thesis based on the problem definition under consideration:

- *Secure Data Aggregation for WSNs:* The general issues in designing a secure data aggregation for wireless sensor networks are discussed. A survey is conducted on some of the existing data aggregation protocols focusing on energy efficiency and security.
- *Efficient Key Management Scheme for Wireless Sensor Networks:* Developed model is used for WSNs where more than one key is required and used to ensure the security in the WSNs. Virtual Location based Key Management scheme (VLKM) based model reduces the number of communications required for rekeying operation. Model presented

in this work maintains key uniqueness in the network to avoid key duplicacy and to allow different keys for the proper functioning of the network.

- *Compromised sensor Key revocation scheme:* Most of the key revocation schemes focus on removing the compromised node from the network by redistributing the keys or keying material to every node in the network. In presented scheme, Key Updation for Removal & replacement of Compromised Sensor nodes uses key updation techniques to update the keys of few sensors in the network rather updating the keys of entire network, thus a compromised sensor is automatically removed from the network.
- Dynamic Encryption Function*:* Developed a model for lightweight encryption mechanism by introducing a dynamic encryption function to achieve forward and backward secrecy (DESFB) in WSNs. The presented function is dynamic in nature, i.e. it produces different output irrespective of the inputs for different runs. The simulation results show that a dynamic encryption function with 8 bit key size is more secure than static encryption with 128 bits key size.
- *Pairing Based Encoding Scheme for WSNs:* Several types of pairing based encoding schemes introduced for wireless sensor networks. Each type of encoding scheme requires a very small amount of storage for its functioning. The use of multiple encoding schemes along with light weight encryption function is very economical in comparison to a heavy cryptographic algorithm with no encoding scheme. The concept of encoding scheme is introduced to increase one step complexity in lightweight encryption function which works in a similar way as that of heavy static encryption function.

7.2 FUTURE DIRECTIONS

Although a complete framework for secure wireless sensor network has been presented in this research work, still there is scope for lot of work to be done in this area. In this section, we briefly identify the areas of future research work based on this thesis. Following are the future directions that can be taken up for the further improvement in this research:

- *Secure Data Storage and Retrieval:* Securing stored information and retrieval becoming an issue in some of the WSNs applications. In this thesis, we focused on securing the information during communication. Securing information in storage is not addressed

properly in this research work. Hence, more research efforts should be made on secure data storage and retrieval when it is on storage medium.

- *Privacy-aware Security Services:* This thesis considers only data security. However, security for network services like network communication privacy is still a research potential in the field of wireless sensor networks.
- *Security in dynamic clustering:* The presented framework provides security in static clustering but there is a requirement for security framework in dynamic clustering where the size and member of any cluster is flexible and changed after the cluster formation.
- *Data Aggregation for Heterogeneous WSNs*: Scheme describes in this thesis provides data aggregation in homogenous network, but it is recommended that further research for data aggregation based on heterogeneous wireless sensor networks needs to be taken care of in the form of memory, processing power and energy exists in the network.
- *Security framework for Mobile WSNs:* The presented framework provides security for static WSNs where the location for any sensor is random but once decided, it is freezed. There is a requirement for security framework in mobile WSNs where nodes in the network are mobile thus their location is updated with respect to time. Hence a security framework for mobile WSNs is designed in future research.
- *Security from insider attacks:* This research work provides security from outsider attackers with the help of cryptography but cryptography is not sufficient for defending the network against insiders and attackers; thus designing the protocols for insider attacks carefully is required as well.