7.1 Conclusion

In this thesis, secure communication techniques, attack detection and prevention schemes have been focused. These techniques are discussed in various sections of this thesis. There are various application areas for secure data communications and its attacks detection techniques. One of the important application areas of these techniques has been identified as defense secret communication. The growing demand for highly secured secret communications is the driving force behind improving the established security techniques and deployment of a new worldwide communication standard. The security of the communication system is mainly limited by the number of various types of attackers. The conventional approaches of data security for wireless communication may not be good in many ways. Here, a proposal has been given to show that the problems in conventional or classical cryptographic approaches may be avoided, if the proposed secure communication techniques handling with different types of attacks are adopted in various wireless networks. In this thesis, problems like key distribution among communicating parties, localization and prevention of various types of attackers during data communications have been considered.

Many works related to similar problems have been surveyed and presented in the thesis. The performance of the various key distribution techniques and routing protocols have been analyzed and discussed in literature survey. Various data communication techniques in wireless network have been briefly discussed in Chapter 2 of this thesis.
The modern secret sharing algorithms for different types of wireless networks and prevention techniques for different types of attacks have been discussed in this thesis. Classical cryptography methods for information sharing require more complex operations during the communication. The improved performance can be obtained from quantum mechanics-based quantum cryptography. The proposed method’s performance has been obtained for qubit utilization and it reduces the memory of users by means of simulations. The simulation results of enhanced three party quantum key distribution protocol with untrusted center is compared with the existing quantum communication system and it is presented in Chapter 3. The proposed unconditional security over WMN provides better PDR and packet delivery latency. It is concluded that the quantum cryptography based unconditional secure communication protocol provides better PDR and qubit utilization compared to the conventional system.

Secure routing strategies are mainly affected by different types of attacks. This thesis is concentrating on Black Hole (BH) attack during routing over WSN. The performance is improved by employing randomized multipath encrypted routing. Here, the data delivery mechanism provides a high possibility of avoiding the BH attack. The proposed method’s simulation results are obtained and provided in Chapter 4. The source node sends data through one route and suddenly changes route over time. Thus, the probability of identifying the current route by the BH attacker is less. The proposed system provides higher PDR and throughput. It is used to reduce Control Packet Overhead (CPO) and also End-to-End delay.

A strategic placement of the wormhole can result in a significant breakdown in communication across a wireless network and the security is at high risk. The prevention is carried out by broadcasting the identity of the attacker node. This
message should be transmitted by an anchor node to the normal nodes within the communication range. By receiving the message, each and every node should update their conflict set and then identify the attacker node from the conflict set. Further, every node drops the packet coming from the attacker node and hence better security is ensured. This thesis presents a method for the prevention of WH attack with various number of attacker’s nodes such as 1 or 2 or 5, and their performances are analysed. The simulation results show that this scheme produces high PDR and CPO. The simulation result of this method is verified and it is presented in Chapter 5.

In Chapter 6, various types of different number of attackers are employed in the multipath reactive routing protocol. This routing scheme is based on trust evaluated on neighbouring nodes. This chapter considers the wormhole, blackhole, misrouting and flooding attacks. To measure the neighbour’s behaviour, to forward the packets and to reduce the effect of malicious attackers, the node trust model is used in MANET. The proposed trusted path-based ad hoc on-demand multipath distance vector (TAOMDV) routing protocol is discovered trustworthy forward paths and can prevent the blackhole, wormhole, flooding and misrouting attacks using passive acknowledgement. The highest trusted path is selected to send the data. When there is any change in the behaviour of any node, then it will update the trust value of the nodes and detect the attack node accordingly. TAOMDV protocol is a hop-by-hop routing method, in which the source is not capable to know all the nodes in the path to a destination, but it is enough for the source to recognize which neighbour is the next hop. It provides higher detection ratio of the attacker. The simulation result shows that the throughput achieved is little lower since there is more number of attacks in the network. TAOMDV protocol achieves high PDR, reduces the packet overhead and average end-to-end delay of packet is reduced.
7.2 Future Scope

The capacity and performance of Wireless Ad hoc NETwork (WANET) could be improved by incorporating ways to resist against attacks in the self-preventing and self-adjusting fashion, as well as to enhance the attack tolerance of the network. This preventive and tolerance mechanism can be achieved by employing a special expert system called Adaptive Fuzzy Petri Net Agent at each node, which may have the ability to learn and adjust to fit into the dynamic environment. The capability of sensing and transmitting process in WSN can be done using wireless sensor node which consumes some amount of energy. The devices have the potential to serve as a catalyst for major changes. For this, an energy efficient scheme should be developed. In order to achieve this novel scheme, a Fuzzified Energy Efficient Mechanism (FEEM) can be employed in a clustering-based protocol.