CONCLUSION AND FUTURE WORK

7.1 CONCLUSION

In our work we proposed differentiated key management to provide more robust nodes for secure communication. It actually makes difficult for an adversary to compromise a few nodes and take control over the whole network. This work mainly concentrates on providing more secure paths in comparison with the normal paths. This is essential in WSN because here almost all of the data gets converged at the sink node. An attacker who compromises the node which is closer to the sink can get more crucial data when compared to the one who compromises the nodes at the outer peripheral region. Similarly while sending the data we will have to make sure that the most important data need to be secured. Selection of nodes with more secure keys was done purely on random basis, thus it makes order for the attacker to capture the whole network. Nodes with more keys are more resilient when compared to the normal nodes. when there is two paths we select the apt path calculating the weightage. NRRP algorithm every time chooses different nodes, and hence it prevents looping in the nodes. When a node desires to transmit data to the sink, the next hop is randomly selected from the secured minimum hop neighbors. In the event such as when there is the presence of more than a secure minimum hop links, then weight function is assigned and the best path is elected. This method can prevent smart attacks targeted at the crucial nodes.

A mutual authentication protocol is proposed by allowing sender and recipient to share a common key matrix as an authentication key, and we use random noise matrix in both sender as well as the receiver end, and the verification was done with the help of hamming code. mutual authentication helps to avoid any kind of middle attack in the network. We also proposed a hybrid online and offline signcryption technique is used that satisfy both function of digital signature and public key encryption in a single logical step. The proposed scheme enhances Confidentiality, integrity, authentication and non-
repudiation. In general public key cryptography was not preferred in wireless sensor networks, because of huge amount mathematical calculation required in that process which could drain the processing power, memory, as well as the power supply of WSN. IN our method most of the complex mathematical operations were performed offline and hence we afford the luxury of both digital signature as well encryption in WSN. This method ensures non repudiation an important requirement of wireless sensor networks.

We also proposed group-key management protocol. The group key will be generated from the pre distributed keys of the sensor network. After the distribution of keys, the nodes can be divided into groups by the base station (BS) via gradually varying the antenna angles and transmission power levels. With the ID’s assigned to the each group, the node with the least ID in the group is elected as group leader. Each group leader transmits its encrypted group id and group member list to BS. BS then gathers the information of the member from each group. Finally, BS allots the EBS (Exclusion Basis Systems) group keys to each group. This EBS group key is transmitted to each group leaders and group keying is done. This type of group key management is mainly used in event based sensor networks. The use of exclusion Basis system reduces the number of keys required to control a group, revocation of compromised keys also becomes easier. In event based sensor networks different sets of sensors may capture a similar same event, its necessary to get a clear message out of it. In order preserve the integrity of the message every node is here we are generating a message authentication code, in case of one or two nodes gets compromised, we can still get the data with out issues Shamir’s secret sharing method is used to preserve the integrity with the help these method we can save lot of memory by handling the keys and also by preserving integrity.
7.2 FUTURE WORK

Differential key distribution can be incorporated in MANETS. Though there no centralized sink like structure in MANETS, sometimes we do prefer safer paths then normal .concepts of pre distribution in mobile networks can be a very good future research option.

Confidentiality and integrity are always preferred in all kinds of networks ,so Signcryption and the mutual authentication method using common matrix can be an interesting area of research.

MANETS are known for their cluster formation so group key mangement and preserving the integrity of the data transfer with algorithms like shamir can be a potential idea for future research.

Energy consumption in the networks can be further reduced by making some assumption on the future data by using heuristic data.

Since we have devices with high memory and processing power in MANETS differential key distribution can also be employed along with cache. Usage of cache may save memory.

Improvements can be done on data aggregation which will improve the performance of sensor nodes in great deal.

Multi level layers of trust can be established between different nodes and the complexity of the key management schemes can be varied according to the levels of trust.

Data mining techniques like association rule mining can be combined with key management system for the efficient management of keys.