CHAPTER 7
CONCLUSIONS

7.1 CONCLUSIONS

DKO is developed and it generates random keys and forms group configuration based on factorial methodology. DKO resolves the complication of single common key present in the existing methodologies and thus, deploying a common key for each group. Within a group and between two groups, pairwise key establishment is implemented and mathematically, it is proved by key establishment steps. Also, the number of keys required for deployment is reduced more than 50% than the existing pairwise key predistribution methodologies. Performance metrics such as communication overhead, end-to-end delay, residual energy and memory usage steps towards improved heights. Security is analyzed based on the number of nodes captured and depending on that, the percentage of compromised keys is measured.

As power being the major resource constraint in WSN, power consumption of SNs during pairwise key establishment is analyzed using STEM protocol which employs duty cycling in SNs and results in noteworthy nominal power consumption during key establishment.

Later, to avoid more number of compromised nodes and frequent dis-connectivity in WSN, PTAP is developed to provide balance between trust node and authentication status. Nodes are chosen based on trust threshold value. If any node falls below the threshold value, it is considered as misbehaving node. Key generation is initiated to all the nodes through all the paths by utilizing pairwise key generated from DKO. Packets are encrypted and decrypted with symmetric
encryption model. The following performance metrics such as delivery ratio, end-to-end delay, link reliability rate, network stability rate, network lifetime, control overhead and authentication rate are measured. Finally, fake attack scenarios are created for four types of attacks and the results are obtained by measuring remaining legitimate nodes present in the network. Based on the simulation results, the proposed DKO, PEAK and PTAP achieve better performance than the existing schemes in terms of performance metrics.

As security plays a vital role in military surveillance system, the deployed SNs have great influence of physical attack and other security attacks. To overcome this, the integration of DKO and PTAP is done by designing a prototype TAM. If TAM is applied to military environment, it will result in efficient and secure communication among militants. TAM makes resourceful key predistribution with the generation of less number of using DKO. The SNs of militants are authenticated and the secrecy of data is maintained using PTAP.

7.2 FUTURE WORKS

The real time sensor mote test bed implementation (as discussed in sub section 6.4.1) has been started in the present thesis by generating random keys and by verifying pairwise key establishment. In future work, the optimized performance will be achieved by integrating PTAP to ensure authenticated SN and by including enhanced energy consumption model with PTAP.