CHAPTER 6

CONCLUSION

As multicasting is predominantly used in many applications, this thesis is indeed instrumental in proposing Energy efficient key management schemes to be adopted for ensuring security.

The main objective of this thesis is to minimize the computation and communication cost involved in multicasting. We have also proposed a trust authority based key management and authentication technique for multicasting in ad-hoc networks.

Initially we constructed an energy efficient topology aware-key tree which mainly aims to reduce the re-keying load by pre-processing the joining members during the idle re-keying interval. The backward and forward secrecies are ensured using temporary key tree and boolean algorithm respectively.

Authentication is performed based upon Diffie-hellman key pair and RSA secret public key pair. This scheme distributes each updated public key to a co-ordinator set. The trust authority uses an RSA secret public key pair and establishes public key certificates for each group member by signing the public key with its secret key. It adopts the proactive secret share update algorithm to periodically update the system secret shares to invalidate compromised secret shares. The nodes joining and leaving the cluster is updated by the subsidizer node. They send valid public key certificate to its co-ordinator set and obtains the public key required for the group key.

6.1 SCOPE FOR FUTURE EXTENSIONS:

1. The proposed algorithms may be enhanced for nodes with mobility.
2. The control messages required for ensuring authentication may optimized.