CHAPTER 9

CONCLUSIONS AND FUTURE ENHANCEMENTS

9.1 SUMMARY

Emerging group communication applications, such as multiparty conferencing, emergency rescue operations etc., have made the design and development of efficient optimized secure multicast protocols in networks a necessity and not just a desire. In this thesis, first the concepts related to multicasting, multicast security and key management, and its various applications are described. Then the analyses and recent advancements in the area of our research are summarized. The main design issues and challenges that multicast key management protocols face are identified, and a brief overview of the existing techniques is provided.

The first step in the literature survey is to list the multicasting key management techniques that are the taxonomy of various group key management protocols. Important protocols in each classification were discussed with their pros and cons. Further a hybrid approach is derived from those algorithms, and its analysis proved that the hybrid approach is better than other algorithms in terms of some parameters which use the clustering concept.

The thesis further analysed parameters like trust in 3rd party, central controlling entity, joining & separation of groups, simple point of failure, security against collusions, scalability, recoverablity, join messages from the GC to the other parts, new member join, leave from messages,
backward secrecy, forward secrecy, keys in control manager, the number of member keys and the processing time for retrieving a group key, and tabulated them.

The thesis further presents the Exclusion Basis System, a combinatorial formulation of the group key management problem that produces optimal results with respect to the parameters $N$, $k$ and $m$, where $N$ is the size of the group, $k$ is the number of keys stored by each member, and $m$ is the number of rekey messages. Further, a general technique for determining the optimal values of $k$ and $m$ as a function $N$ was developed, and the trade-off between $k$ and $m$ described.

For a batch rekeying approach, an algorithm was proposed based on the revised variable length batch rekeying interval and it was compared with the existing batch balanced algorithm. It proves that the proposed work is better than the existing one. The performance evaluation was done for parameters like rekeying costs, update costs, key storage, etc.

The thesis also designed PACK, a highly efficient contributory key agreement scheme, which reduces the overhead associated with key updating in two ways. First, it uses the novel PFMH tree structure that consists of a main tree, which is optimal for user leave, and a join tree, which is optimal for user join. Second, the concept of phantom user location in the PFMH allows cost amortization when handling user leave. Both the theoretical bound analysis and the simulation results have shown that PACK has much lower rekeying costs in terms of communication, computation, and time than the existing schemes.

Another method is proposed in which an attempt has been made to employ secure key management with optimal resource allocation using
multiple edge sharing multicast trees. This provides not only high security but also a faster multicast content delivery with optimal resource utilization.

Finally, a multimedia multicast application scenario PPV system was analyzed with its architectural details, working principles, how it evolved over the years, various level of key hierarchies, and multimedia content distribution were deeply explored and the proposed multi-layered technique along with optimal levels of hierarchy was discussed and a more secure multicast environment was created.

9.2 FUTURE WORK

The solutions mentioned herein can be applied to both wired and wireless networks. Even though the proposed works are applicable to highly secure multicast communication like military applications, proper validation should be needed for applying it against different types of attacks.

Multicasting in MANETs faces many challenges due to the mobility of the nodes, unreliable transmission medium, the lack of dedicated routers and fixed infrastructure, limited transmission range of the devices, and limited available bandwidth. In future, it is possible to extend the proposed protocols to solve some QoS issues, such as power and bandwidth. The mobile devices are equipped with a low power battery, so it is very important to reduce the number of packet transmissions. Moreover, bandwidth consumption is important for supporting real time and multimedia service.

The other performance metrics such as energy-based mobility, link stability, forwarding efficiency and mean delivery latency can be used to evaluate the proposed protocols. Designing a new protocol with different
group mobility models suitable for multicast applications, can also be considered for future work.

This thesis explores the PPV application. The proposed work is also applicable to other major multicast applications like the army, software updates, content distribution, conferencing, etc.

Solutions are merely application specific. In future, generalized solutions for the key management problem can be devised. If possible a rekey-less strategy can be generated.