CHAPTER 6
FINDINGS AND DISCUSSIONS

6.1 FINDINGS OF THIS THESIS

The finding of this research is listed below.

- A Mobile Ad hoc Network consists of a set of mobile nodes that have to collaborate, interact and communicate to complete an assigned operation.

- A MANET consists of autonomous, self-organizing and self-operating nodes. It is characterized by links with less bandwidth, nodes with energy constraints, nodes with less memory and processing power and more flat to security intimidation than the fixed networks.

- Secret sharing is an efficient way to distribute a secret among n parties, where each party holds one piece of the secret. A number of key management schemes have been proposed for MANETs.

- From the comparison, the proposed AKM is more realistic because it can handle huge numbers of dynamic nodes in MANET and provide sufficient security requirements.

- In Blakley’s secret sharing scheme there is a delicate distinction between un-qualified groups cannot obtain any
information regarding the key and un-qualified group cannot reconstruct the key.

- Verifiable Secret Sharing schemes based only on the definitional properties of commitments that are almost as good as preceding secret schemes based homomorphic commitments and the computational VSS as a standalone primitive.

6.2 DISCUSSIONS

A general observation is that none of the proposed key-management schemes for MANETs is truly effective for all MANET scenarios. The application must be taken into consideration at the current state of the art. There is a lack of reported attention to the challenges presented by the concrete limitations of communication capacity in MANETs. The necessary values for the computation are distributed to the participating parties using a secret sharing scheme (SSS). Several function sharing schemes have been proposed in the literature, with most of them using Shamir secret sharing as the underlying SSS. Therefore, this research investigated that the modified key management has been conducted with Blakley secret sharing scheme and presented a novel function-sharing scheme for MANET. Next, proposed technique of verifiable secret sharing is presented in this work for a fair reconstruction of the secret. In this verifiable threshold secret sharing scheme, each shareholder verifies that the share comes from an honest dealer and it is not an erroneous piece or a malicious intruder in MANET does not modify it.

The performance evaluations tend to be restricted to computational complexity considerations, whereas the practical constraint of MANETs is more likely the communication capacity rather than the computational power and energy consumption. Both the size and number of messages are
important. Further research on this topic will attempt to simplify the computation complexity of some AKM operations for the workability of ad hoc devices.