CHAPTER 9

CONCLUSION AND FUTURE WORK

The main objective of this thesis is to study the security issues relating to MANETs, and the various security systems designed by researchers. The main challenge in the design of a security system is how to prevent the attacks against data spoofing, and how to authenticate the genuine users in hierarchically clustered high security MANETs. Also, in a hierarchical MANET, each user communication has its own hierarchy, and the security system should be designed in such a way that different security services are available for different levels of users. The biometric system, which is a pattern recognition system that has direct connection with the user identity, is gaining increasing attention as it provides a possible solution to this problem. But, uni-modal biometrics has many problems, and the need for building a multimodal biometrics-based security system has increased. Hence, in this thesis, the focus is on designing a Cancelable Multimodal Biometrics-based Secure Authentication System for hierarchically clustered MANETs, which need high security.

9.1 ROLE OF CANCELABLE MULTIMODAL BIOMETRICS-BASED SECURE AUTHENTICATION SYSTEM

The Cancelable Multimodal Biometric-based Secure Authentication System (CMBSAS) protects the message communicated between different types of users of high security applications of MANETs. In the MANET user environment, the nodes are clustered into different groups, such that each group has one leader, and the others are considered as the end users.
Communication may take place between the users of the same group, or the leader of a group and the users of the same group / the users of a group and its leader, or between the leaders of different groups. Each communication has its own hierarchy of importance as the nodes and no user is allowed to communicate with the users or leaders of other groups.

For user to user communication, one biometric such as the fingerprint is used to encrypt the communication between users. The next type of communication is between the group leader and the users administered by him. The group leader may send instructions to users, or the users may communicate with their group leader, for which two biometric such as the fingerprint and face are used for data security and sender authentication. Since the group leaders play vital role, communication between them is more significant than that between the other users in the group, and hence, three biometric such as the fingerprint, face and voice are used for this communication. In this way, the receiver is authorized by his voice biometric, and sender authentication is done by Eigen face verification and message security is ensured by the fingerprint based cryptographic key. For data integrity, the checksum is used. Privacy and revocability are also ensured by the steganography algorithm, image randomizer and genetic-based cryptographic key generator.

9.2 OUR CONTRIBUTIONS

Our Cancelable Multimodal Biometric-based Secured Authentication System is designed and implemented using the software, MAT LAB, JAVA, and NS-2.

- A multimodal biometric-based security system is designed for a hierarchically clustered MANET environment, which needs high security.
A novel multimodal fusion technique is introduced, which fuses different security services, such as data security, sender authentication and receiver authorization provided by different biometric modalities, such as the fingerprint, face and voice respectively.

Core point detection and feature extraction algorithms are merged to extract the unique features from the fingerprint biometric.

A genetic two-point cross-over operator is used to generate a cancelable / revocable cryptographic key from the fingerprint feature set. A different cross-over operator is used to revoke the key, whenever the user wants to change the cryptographic key.

The cryptographic key is shared with the leader of the group and other users, using the LSB steganography algorithm. In this way, the key distribution is accomplished in secret.

The genetically randomized cryptographic key which is based on the fingerprint biometrics, is used to encrypt the data transferred between the users, using a simple, single round, modified Fiestel algorithm.

The color-based face detection algorithm and Eigen face algorithm are merged for face recognition.

An image randomizer is used for dividing the facial image into different chunks of images, and randomizing the order of the chunks, which ensures the privacy of biometrics.

Voice biometrics is used for authorizing the receiver by matching the Euclidean distances between the average of the
normalized frequency spectrum and the recording of the normalized frequency spectrum of voice.

- The checksum calculator is implemented to find the checksum value, which verifies the integrity of the message transferred.

- Such a Cancelable Multimodal biometric-based Secured Authentication System is implemented in a hierarchically clustered MANET environment where different types of communication take place between different types of users.

- For the user to user communication only fingerprint biometrics is used for providing data security.

- The communication between the user and its leader is secured with fingerprint-based data security and face-based sender authentication.

- For leader to leader communication three biometric such as the fingerprint, face and voice are used for providing data security, sender authentication and receiver authorization.

- The performance of the security system is compared with other algorithms, in terms of time and space complexity. Since, the key size is very less, the space complexity is also less. Since, the key used is strong and unique for each block of data, a simple modified Fiestel algorithm is used as the cryptographic algorithm. This leads to small time complexity for encryption and decryption.

- The performances of the recognition algorithms are compared with other algorithms, in terms of GAR, GRR, FAR and FRR.
True events, such as GAR and GRR are maximized, and false events, such as FAR and FRR are minimized in our system.

- Our CMBSAS is implemented in a MANET environment using NS-2, and performance metrics such as throughput and end-to-end delay are found for the routing protocols AODV, DSR and DSDV; it is proved that our security system does not affect the throughput and delay of the routing protocols much, due to the small overhead present.

- Also, most of the security parameters are provided by our security system, and hence, many attacks on biometrics and MANET security are countered by our security system.

- Our idea of multimodal biometric-based security is implemented in different applications and the performances of such systems are tested.

- In the first application, at the first level, fingerprint biometrics is used in wireless sensor based healthcare systems, to encrypt the communications between doctors and remote patients.

- At a second level, two biometric modalities are used in Automatic Teller Machines, in which the face is used for group authentication and the fingerprint is used for individual authentication.

- In a military scenario, three biometric modalities such as the fingerprint, face and voice are used for three levels of communication, and the performances are verified using various performance metrics with the existing systems.
9.3 FUTURE ENHANCEMENTS

Our system CMBSAS uses three biometric modalities for providing different security services, such as security, authentication and authorization. As a future enhancement, more number of biometric modalities can be used to provide more number of security services. In this thesis, the Eigen face recognition system is used for facial recognition, and the Euclidean distance is used for voice verification. In future, other algorithms can also be tried for this verification, and if possible, GAR may be maximized to 100% and FRR minimized to 0%. Our system CMBSAS is implemented in NS-2, using the routing protocols, such as the AODV, DSR and DSDV. In future, CMBSAS can be implemented using other multicasting routing protocols, such as the Multicast Ad-hoc On-demand Distance Vector (MAODV) and On-demand Multicast Routing Protocol (ODMRP).