CHAPTER 3

CANCELABLE MULTIMODAL BIOMETRIC-BASED SECURE AUTHENTICATION SYSTEM

3.1 INTRODUCTION

As the popularity of mobile devices and wireless networks has considerably increased over the past years, wireless MANETs have become one of the most active fields of research, with increasing number of widespread applications. Regardless of the variety of MANET applications there are still some security issues and design challenges that have to be overcome. Most of the hierarchically clustered tactical applications of MANET, such as military networks need different security services at different levels. Depending upon the level of security required, security services can be layered at different levels. Thus, a more secure and critical information system needs to be created. A layered defense that integrates information from various levels can verify with the information stored in databases, and can afford an uncompromised protection with no single point of failure.

The study of different security issues in hierarchical MANET, the different biometric modalities, and multimodal biometric-based security has led to the development of our work. Based on the papers referred to in the literature study, it is understood that the security solutions designed for such
hierarchically clustered high security MANETs should be responsible for providing most of the security services, such as authentication, confidentiality, integrity, authorization, access control, nonrepudiation, anonymity, and availability to the mobile users in a layered manner. In order to achieve these goals, the security solution should deliver a complete protective guard in MANET. Since there is no single mechanism that will offer all the security services in MANETs, our work proposes many security solutions provided by different biometric modalities, that are integrated into one framework, and each part would be accountable for a single security service. For example, the fingerprint-based cryptographic key is generated for encryption to provide data confidentiality. Face-based verification is used for sender authentication. Voice recognition is used to provide receiver authorization. Different services are provided depending upon the level of security.

Moreover, in tactical applications there is a strong need for a secure environment, where all the communicators are expected to interact with each one another in a trusted domain. In such situations, the implementation of a security system which comprises most of the security services becomes very necessary, so that the end users may be provided with better security services. Hence, our work attempts to provide most of the security services discussed in the literature survey, by using different biometric modalities and thus, a trusted environment is ensured. In addition, the level of security increases as the need for security increases, since the environment is expected to have hierarchically segregated users, who may require different levels of security.
Therefore, in our work, the hierarchical security is achieved by exemplifying various security services at various levels. With the intention of solving the issues in MANET security, a biometric-based security system which uses different biometric modalities at different levels is used. Also, to lessen the issues faced by biometrics-based systems, our work makes use of the genetic randomizer for revoking the cryptographic key, the image randomizer for randomizing the facial image, and steganography for biometric privacy. Above all, to prove better performance, our proposed security system is implemented in a MANET environment, and the performance metrics are studied.

Hence, in our work, a system called Cancelable Multimodal Biometric-based Secured Authentication System (CMBSAS) has been suggested, to provide hierarchical, multilevel, multimodal biometric-based security services. In order to handle the issues related to the implementation of CMBSAS, an architecture is designed, as shown in Figure 3.1.
Figure 3.1: Cancelable Multimodal Biometric-based Secure Authentication System
The Cancelable Multimodal Biometric-based Secure Authentication System (CMBSAS) consists of five major components, namely, a hierarchically clustered MANET user environment, security service providers, a multimodal biometric subsystem, a security subsystem and an imaging subsystem.

In the MANET user environment, the nodes are clustered into different groups so that each group has one leader, and the others are considered as end users. The security service providers have three levels, such as low-level, medium-level and high-level. Depending upon the hierarchical level of the communicators, the corresponding security service provider is used. Security service providers are used, as an interface between a hierarchically clustered MANET user environment, and the multimodal biometric security subsystem. This multimodal biometric security subsystem receives the services from the supplementary systems, such as the security subsystem and imaging subsystem. These five components are explained in detail in the following sections.

3.2 HIERARCHICAL HIGH SECURITY MANET ENVIRONMENT

Ad hoc networking can be implemented anywhere, where there is no infrastructure or the existing infrastructure is inconvenient to use. The MANET supports tactical networks and provides support to the network for data communication between mobile devices. Tactical MANETs are specifically used in military scenarios or in disaster areas, in which the existing infrastructure may have been destroyed. Naturally, some kind of hierarchical structure is there in tactical MANETs, which involves at least two types of nodes, such as the supervising nodes and supervised nodes (Elmar et al 2007). Supervising nodes stay in the background, have access to a power source, and therefore, can use more powerful hardware. In contrast to that, the
supervised nodes move frequently, use battery powered mobile devices, and therefore, less powerful hardware. The supervising nodes predestine them to serve as the central authority in securing the network.

The same scenario is involved in our CMBSAS, and it protects the message communicated between different types of users of high security applications of MANETs, especially those for which the networks are designed in such a way, that some hierarchy is applied for the users in the network, such as military applications and intelligent buildings. In these types of applications, a group of users are connected in the network, and each group is headed by a group leader. Communication may take place between the users of the same group, or the leader of a group and the users of the same group/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 can communicate with the users or leaders of other groups. These communications are shown in Figure 3.2.
In our proposed CMBSAS, three types of biometric such as the fingerprint, face and voice are used to provide data security, sender authentication and receiver authorization for the communication. At the first level, if the end user of one group wants to communicate with another user of the same group, only one biometrics such as the fingerprint is used. At the second level, users of a group can communicate with their leader or leader of a group can communicate with the users of the same group. For this communication, two biometric such as the fingerprint and face are used. At the third level, leaders of different groups can communicate with each other, and three biometric such as the fingerprint, face and voice are used for this. The following sections describe how these biometric modalities are processed to extract features, and how they are used for providing different security services at different levels.

3.3 MULTIMODAL BIOMETRIC SUBSYSTEM

In order to overcome the disadvantages of uni-modal biometrics, for biometrics to be ultra-secure and to provide more-than-average accuracy, more than one form of biometrics is required, and hence, the need arises for the use of multimodal biometrics (Arun and Anil 2004). Instead of using a single biometrics, a combination of different biometric, can be used for recognizing a human being. Multimodal biometric can be composed in three different fusion methodologies (Anil et al 2006), such as fusion at the feature level (Lakshmi and Fidal 2009), match score level (Sim et al 2007) and decision level (Salil and Anil 2000). As a fourth level a new fusion technique is used in our work, which fuses the security services provided by the system, by adding more biometric modalities as the security level increases.

In the CMBSAS, a multimodal biometric-based security system is implemented in a high security MANET environment, which needs different security services at different levels. The fingerprint-based data security system
is used for providing data confidentiality. Since, the data transferred between the users is important and interception makes it more vulnerable, the data has to be encrypted. In order to encrypt the data, the fingerprint-based cancelable cryptographic key is used with the modified Fiestel algorithm to get the cipher text. The face-based authentication system authenticates the user using his face biometric. It is also essential to verify whether the data originates from a genuine sender in a trusted environment. For authenticating the sender, the Eigen face-based verification algorithm is used, and sender authentication is guaranteed. The voice-based authorization system uses the voice signal of the receiver to provide access for the data received. Euclidean distance is calculated for the recorded voice signal, and is compared with the stored average voice signal. In this way, the receiver is given permission to access the data received by the user.

3.4 SECURITY SERVICE PROVIDERS

There are three levels of security service providers, low, medium and high. These security service providers offer services depending upon the hierarchical level of the communicators. Security service providers are used as an interface between a hierarchically clustered MANET user environment, and the multimodal biometric security subsystem, to provide the corresponding level of multimodal security to the hierarchically clustered MANET.

3.4.1 User to User Communication

The low level security service provider offers service for user to user communication, and for that, only one biometrics is used. As per the diagram 4.2, suppose user-1 of group ‘A’ wants to communicate with user-2 of the same group, the cryptographic key, generated from the fingerprint of user-2 is used to encrypt the actual data by user-1. The receiver, user-2 uses his own
biometric to decrypt the message. In that way, message security is ensured by the fingerprint based cryptographic key.

3.4.2 Leader to User / User to Leader Communication

The next type of communication is between the group leader and the users administered by him, and for this communication, the services are offered by the medium level security service provider. At this level, the group leader may send instructions to users, or users may communicate with their group leader; two biometric traits are used for providing data security and authentication. Suppose the leader of group ‘A’ wants to communicate with user-1 of the same group, at first the leader’s facial image is randomized and appended with the actual data. The receiver’s cryptographic key is used to encrypt the actual data and the face, and is transmitted to user-1. At the receiving end, user-1 will use his own fingerprint-based key to decrypt the message and the sender’s face. Then, by using the mean image, the sender’s face is verified. In this way, message security is ensured by the fingerprint based cryptographic key, and sender authentication is done by the Eigen face verification method.

3.4.3 Leader to Leader Communication

Since the group leaders play a vital role, the communication between them is more significant than that between any other users in the group, and thus, a high level security service provider is necessary to offer services. Three biometric modalities such as the fingerprint, face and voice are used for this communication. The receiver’s fingerprint-based cryptographic key is used to encrypt the actual data plus the facial image of the sender, and this encrypted data is concatenated with the normalized frequency spectrum of the average voice signal of the receiver, and then transmitted.
At the receiving end, the reverse process takes place to get the actual data. The receiver’s normalized frequency spectrum of the recorded voice signal is matched with the received average voice signal, and the receiver authorization is verified. Then, the data is decrypted using the receiver’s fingerprint-based cryptographic key, and data confidentiality is ensured. Eigen face verification is done for sender authentication. In this way the receiver is authorized by his voice biometric, and the sender authentication is done by Eigen face verification, and message security is ensured by the fingerprint based cryptographic key.

3.5 IMAGING SUBSYSTEM

The users’ biometric modalities are enrolled, and the biometric features are extracted using the imaging subsystem. It includes three parts, such as the fingerprint processor, face processor and voice processor. The fingerprint processor in turn, has a fingerprint pre-processor, core point detector and feature extractor. The fingerprint biometric is used for providing data confidentiality by means of encryption. In order to generate a cryptographic key from the fingerprint, it has to be pre-processed first. Then, the core point detector finds the position of the core point and the feature extractor extracts the features of the fingerprint. These two algorithms, the core point detection algorithm and the feature extraction algorithm, are fused to find the unique features of the fingerprint, and these features are used as a strong and unique cryptographic key, which can be used for encrypting the messages communicated.

The face processor fuses two algorithms, such as the face detector and the Eigen face generator, for using the face biometrics as the authenticator. A color-based technique is used in the face detector, to separate the facial image from the surroundings, and then the Eigen face verification algorithm is used for authenticating the sender. In the voice processor, initially the voice
input is pre-processed using the voice pre-processor, and then the Euclidean space generator is used to find the Euclidean distance, for authorizing the voice signal.

### 3.6 SECURITY SUBSYSTEM

The security subsystem includes a genetic-based key randomizer, encryptor, checksum calculator, steganographer, and image randomizer. Once the cryptographic keys are generated from the unique features of the fingerprint biometrics, they are randomized, using the genetic two-point cross over operator to generate a cancelable key, which ensures the revocability of the key. That is, if the key is compromised, it can be re-enrolled using another set of cross over points. The generated key is used to encrypt the data by the encryptor, in which the modified, single round Fiestel algorithm is used as the encryption algorithm.

The image randomizer is used to divide the facial image into different parts, and the positions of these parts are randomized, before they are sent to the receiver. As a prerequisite, the order of the facial image is shared between the sender and the receiver. The steganographer implements the Least Significant Bit (LSB) steganography algorithm for covertly sending the fingerprint-based key between the users.

In all these communications, message integrity is verified, by using the checksum calculator. The sender calculates the checksum for the transmitted message, and the receiver does the same for the received message. Checksum matching is done to verify whether the data has been modified during transmission. In this way, data integrity is also ensured. The main objective of our security scheme is to improvise the existing data security approaches for hierarchical MANETs, which need high security, using multimodal biometrics to suit technology enhancements.
Chapter 4 explains how fingerprint biometric pre-processing and feature extraction are done along with the core point detection algorithm, for extracting unique features, and how the genetic cross-over operator is used to generate the revocable cryptographic key. The implementation details of the steganographer for privacy, the checksum calculator for data integrity, and the encryptor using the modified Fiestel algorithm for data confidentiality, are also described.