CHAPTER 1

INTRODUCTION

1.1 MOBILE AD HOC NETWORKS

This huge world is shrinking because of the rapid development of communication networks. Wireless network technologies have advanced drastically in recent years, including third generation wireless networks, wireless LANs, ad hoc and sensor networks. Among these, the Mobile Ad hoc NETwork (MANET) has an important place for its dynamic and co-operative characteristics. The MANET is a self-configuring network with no permanent infrastructure, which can be quickly formed, on demand, for specific tasks and mission support. Nodes in the MANET are wireless, and may be both routers and terminals. These networks are dynamic in nature; that is, each node is free to join and leave the network in a nondeterministic way. Each node is free to roam about while communicating with others. Nodes can directly communicate with neighbours, which are within direct transmission range but must rely on intermediate nodes to forward packets to distant nodes, which are beyond the direct transmission range. Furthermore, nodes may be highly heterogeneous with respect to processing power, battery life, transmission range, and mobility patterns. Some typical examples of nodes include backpack radios, laptops, handhelds and vehicle computers.

Communication generally happens through wireless links, in which nodes within a radio range communicate and coordinate, to create a virtual and temporary communication infrastructure for data routing and data
transmission. The path between each pair of the users may have multiple links, and the radio links between them can be heterogeneous. Since, each node is a potential part of the virtual support infrastructure, collaborating with others to provide basic communication services to its peers, the individual nodes’ vulnerabilities can directly affect the network’s security state. A typical MANET is shown in Figure 1.1.

![Figure 1.1 MANET](image)

MANETs are autonomous and infrastructure-less networks. They use multi-hop routing and have a dynamic network topology. They have heterogeneous and energy constrained devices. They also have bandwidth constrained variable capacity links. They have limited physical security and network scalability. They are self-created, self-organized and self-administered. These characteristics of MANETs (Hoebeke et al 2004) lead us to the need for the study of security in MANETs.

1.2 SECURITY IN MANET

Despite the design constraints as explained above, MANETs offer numerous advantages also. First of all, this type of network is highly suited for use in situations, where a fixed infrastructure is not available, not trusted, too expensive or unreliable. Because of their self-creating, self-organising and self-administering capabilities, MANETs can be rapidly deployed with minimum user intervention. Their applications include emergency/crisis
management, such as in disaster recovery, where the entire communication infrastructure is destroyed and restoring communication quickly is crucial. Their applications also include the foremost situations, such as the military, healthcare, intelligent buildings, intelligent transportation systems and virtual classrooms, where tactical and confidential data are communicated between the users. In some of these applications, MANETs are hierarchically clustered, where different levels of users have a different hierarchy and different security levels. So, security plays an important role in such hierarchical MANETs, and the necessity of knowing and elucidating the security threats is absolutely essential.

1.2.1 Security Threats in MANETs

As the wireless medium is vulnerable to eavesdropping, and MANET functionality is established through node cooperation, MANETs are intrinsically exposed to numerous security attacks. So message security plays a vital role in data transmission in MANETs. However, because of the absence of an established infrastructure or centralized administration, the implementation of hard-cryptographic algorithms is a challenging prospect.

Wireless MANETs are vulnerable to various attacks (Stallings 2005). Adversaries may attempt passive and active attacks to gain unauthorized access to classified information, and modify, delete or disrupt the information flow. Passive attacks like eavesdropping do not disturb network operation, because the adversary snoops the network traffic to know the information without making any alterations. But active attacks like interfering, impersonation, modification of packets and denial-of-service can significantly affect network operation, because the adversary tampers with the network data and signaling, thus affecting the security of data. Animesh (2009) explained two types of uncooperative nodes in MANETs. They are faulty or malicious nodes, and selfish nodes. Faulty or malicious behavior
refers to the broad class of misbehavior, in which nodes are either faulty, and therefore cannot follow the network protocols, or are intentionally malicious and try to attack the system. Selfishness refers to non cooperation in certain network operations, which may affect the performance of the network severely. In any case, message security is very important because highly strategic information is transferred in most of the applications.

The ultimate goal of the security solution for MANET is to provide security services, such as authentication, authorization, confidentiality, integrity, and availability to the mobile users (Stallings 2005). One distinguishing characteristic of MANETs from the security design perspective is the lack of a clear line of defence. The wireless channel is accessible to both genuine network users and malicious attackers. There is no well-defined place where traffic monitoring or access control mechanisms can be deployed. As a result, the boundary that separates the inside network from the outside world becomes blurred, and that forces the researchers to design a security system which can provide most of the security services needed.

1.2.2 Traditional Security System

The best way to protect data information in the most fine-granular way is providing security at the application specific end-to-end security layer. It is highly desirable to handle data confidentiality and integrity in this layer, since this is the easiest way to protect data from alteration, fabrication and compromise (Shuyao et al 2003). With the rapid evolution of wireless technology, the reliance of MANETs to carry mission critical information is rapidly growing. This is especially important in a scenario where strategic and tactical information is sent. Therefore, the ability to achieve a highly secure authentication is becoming more critical.
Numerous countermeasures, such as strong authentication, encrypting and decrypting the messages using traditional cryptographic algorithms, such as symmetric and asymmetric algorithms and redundant transmission, can be used to tackle the attacks on MANETs. Even though these traditional approaches play an important role in achieving confidentiality, integrity, authentication and non-repudiation, these are not sufficient for more delicate and complex applications, and these techniques can address only a subclass of the threats. The purpose of accurate user authentication and data security, is to allow the legitimate parties to access the database and services, to communicate confidential data from anywhere at any time, while keeping the others out.

Matin et al (2009) evaluated the performance analysis of symmetric encryption in MANET, and concluded that it is more secure, but it slows down the encryption, because it has to do more work for the same amount of input data in a single execution cycle. However, it is challenging to design a key management scheme for symmetric algorithms in mission-critical networks to fulfil the required attributes of secure communications. Also, in symmetric key cryptography, if the attacker finds the key and the algorithm, all data which are exchanged between the two parties are known to the attacker.

To tackle the above said problems, Nai-wei and Kuo-hui (2011) proposed a three-party password-based key exchange protocol in which a client is allowed to share a human-memorable password with a trusted server, such that the two clients can negotiate a session key to communicate with each other secretly. However, it is better suited for resource constrained devices, such as smart cards or mobile units. The distributed and self-organized authentication scheme proposed by Ping et al (2010) for MANETs fulfilled most requirements derived from the special characteristics of
MANETs, including limited physical protection of the broadcast medium, frequent route changes caused by mobility, and lack of structured hierarchy. But the system does not suit hierarchically clustered MANETs, where hierarchical clustering provides a structure for showing the MANET at different levels of detail by superimposing a hierarchy on it. For such hierarchical MANETs, Kyung et al (2004) presented a group key management architecture, and key agreement protocols for secure communication, which used an implicitly certified public key method. Even though it alleviates the certificate overhead and improves computational efficiency, the system has less responsibility in authenticating the users.

Moreover, these traditional mechanisms are costly to implement and MANETs cannot support complex computations or high communication overhead due to the limited memory, computation power and low battery life of mobile nodes (Animesh et al 2009). For these reasons we need to search a different security system, which can overcome all threats faced by MANETs and at the same time the computation overhead should be lessened. A biometric-based security system would be a better solution to alleviate these overheads in which a simple cryptographic algorithm can be used with a small strong biometric key. In order to have a simple cryptographic algorithm, the key used is made stronger.

1.3 BIOMETRIC SECURITY SYSTEM

With the proliferation of large-scale MANETs, the increasing number of applications making use of such networks, and the growing concern for identity theft and data security problems, the design of appropriate secure authentication systems is becoming more and more essential. These systems should have the ability to authenticate persons (i) accurately, (ii) rapidly, (iii) reliably, (iv) without invading privacy rights, (v) cost effectively, (vi) in a user-friendly manner, and (vii) without drastic
changes to the existing infrastructures (Umut 2006). The traditional personal authentication systems that make use of either a piece of knowledge (password) and/or a physical token (identification card) that are assumed to be utilized only by the legitimate users of the system, are not able to meet all of these requirements.

Biometrics-based secure authentication systems that use physiological and/or behavioral traits of individuals, have been the promising candidates for either supplanting or supplementing traditional systems. The different biometric traits such as fingerprint, hand geometry, iris, face, retina, protein structure, signature, DNA, keyboard dynamics, gait, ear, and voice are shown in Figure 1.2.

![Figure 1.2 Different Biometric Traits](image)

These biometric traits are actually bound with the individual, and are very reliable, since biometric information cannot be lost or forgotten, and cannot be forged or guessed easily by the hackers. Since there is nothing to remember or carry, they lead to user convenience too. They improve the authentication accuracy and further, the cost of incorporating biometric
components into a secure authentication system is continually decreasing, whereas the cost of relying on traditional authentication mechanisms is increasing. For these reasons we concentrate on a biometric-based security system rather than traditional security systems for MANETs.

1.4 CANCELABLE MULTIMODAL BIOMETRIC SECURITY SYSTEM

Uni-modal biometric systems recognize individuals based on a single source of biometric information. Such systems are often affected by problems (Anil et al 2004), such as noisy sensor data, non-universality, lack of individuality, lack of invariant representation, susceptibility to circumvention etc. Some of these problems that affect uni-modal biometric systems can be alleviated by using multimodal biometric systems (Nalini et al 2007). Systems that consolidate features obtained from two or more biometric sources for the purpose of person recognition are called multimodal biometric systems. Multimodal biometric systems have several advantages over uni-modal systems. Combining the evidence obtained from different modalities using an effective fusion scheme can significantly improve the overall accuracy of the biometric system. A multimodal biometric system can reduce the False Acceptance Rate (FAR) and provide more resistance against spoofing, because it is difficult to simultaneously spoof multiple biometric sources.

However, multimodal biometric systems have some disadvantages too. They are more expensive and require more resources for computation and storage than uni-modal systems. Multimodal systems generally require more time for enrolment and verification, causing some inconvenience to the users. However, the advantages of multimodal systems far outweigh the limitations, and hence, such systems are being increasingly deployed in security-critical applications. For that reason, many biometric modalities are fused in our security system to improve its accuracy.
Other than the problems discussed above, biometrics also raises several security and privacy concerns, such as ‘biometrics is authentic but not secret’; ‘biometric cannot be revoked or cancelled’; ‘if a biometrics is lost once, it is compromised forever’; ‘cross-matching can be used to track individuals without their consent’ (Hong et al 1999) etc. Hence, if a biometric identifier is compromised, it is lost forever and rendered unusable. Non-invertible or cancelable transforms (Nalini et al 2001) are one of the original solutions to privacy-preserving biometric security, by constructing revocable biometric templates. Instead of using the original biometric, it is transformed using a one-way function, and this method is called as cancelable biometrics. If a biometric is compromised, it can be simply re-enrolled using another transformation function, thus providing revocability. This leads to the generation of a cancelable biometrics-based cryptographic key in this work. For generating a cancelable key, a genetic two-point cross over operator is applied onto the biometric-based key, and if needed, the key can be revoked by changing the positions of the cross over points.

Hence, in this thesis a cancelable multimodal biometric-based security system is presented, which uses different biometric modalities to provide data security and user authentication efficiently. It also solves the privacy and revocability problems that exist in contemporary biometric-based security systems.

1.5 ROLE OF SOFT COMPUTING IN BIOMETRICS

Soft computing consists of several computing paradigms including fuzzy logic, neural networks and genetic algorithms, which can be used to create powerful intelligent systems to recognize biometrics. Fingerprint recognition (Mahendra et al 2011, Suliman et al 2002), face biometric recognition (Mayank et al 2010, Meng et al 2002) and voice recognition (Patricia et al 2006, Frankel et al 2000), used a soft computing technique,
named fuzzy neural network, for recognizing the different biometrics such as fingerprint, face and voice. A fuzzy-neural network classifier is used for the classification of the input features, and a genetic algorithm is used for optimizing the number of layers and nodes.

But, in general, genetic algorithms (Fessi et al 2009) are a family of computational models inspired by natural evolution. They belong to the field of evolutionary computation, and are based on three main operators, such as selection, crossover and mutation. Selection selects the fittest individuals, called parents that contribute to the reproduction of the population in the next generation, crossover combines two parents to form children for the next generation, and mutation applies random changes to individual parents to form children. A two-point crossover operator is used in cancelable cryptographic key generation in our system, which has the ability to generate, promote, and juxtapose building blocks to form the optimal and revocable strings.

1.6 OBJECTIVE OF THIS WORK

The main challenge in the design of a security system is, how to prevent data spoofing, and how to authenticate the genuine users in hierarchically clustered high security MANETs. Usually a hierarchical MANET has at least two types of nodes (Elmar et al 2007), such as supervising nodes and supervised nodes. Supervising nodes stay in the background, have access to power supply, 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, and the supervising nodes predestine them to serve as the central authority.

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, is gaining increasing attention as it
provides a possible solution for this, and has a direct connection with the user identity. The objectives of this thesis are explained as follows.

- This thesis aims to design a novel security system, which fuses different security services such as data security, sender authentication and receiver authorization using multimodal biometrics (fingerprint, face and voice) at different levels of hierarchically clustered MANETs, that need high security.

- This thesis analyses the different biometric traits and pre-processes them to extract the necessary features from them. The fingerprint core point detector and feature extractor are fused to extract the unique features from fingerprints. The face detector and Eigen face generator are fused for face recognition, and the voice pre-processor and Euclidean space generator are used for voice biometrics.

- This thesis uses many biometric modalities for providing different security services. As the security level increases, correspondingly the number of security services provided by the system also increases. For example, at the first level fingerprint biometrics is used for data security, at the second level along with fingerprint based security face biometrics is used for sender authentication. Voice biometrics is used for receiver authorization at the third level along with fingerprint-based security and face-based authentication, according to the security requirement.

- An attempt is made in this thesis to override the privacy and revocability problems that exist in most of the biometric-based systems. To maintain the privacy of the biometric, they are not stored as such but their cancelable forms are used. For
revocability, a genetic-based cancelable cryptographic key is generated from the fingerprint biometric. The steganography algorithm and image randomizer are used to ensure privacy.

- This thesis also guarantees that the security system designed has better performance, by implementing it in a hierarchically clustered MANET, and by analyzing the performances of the system, using various measures such as Genuine Acceptance Ratio (GAR), Genuine Rejection Rate (GRR), False Acceptance Ratio (FAR), False Rejection Ratio (FRR), time and space complexity of various algorithms, packet delivery ratio, throughput and end-to-end time delay in NS-2 simulation.

Hence, a Cancelable Multimodal Biometric-based Secured Authentication System (CMBSAS) is developed in this thesis which provides different security services at different levels of hierarchically clustered MANETs that need high security.

1.7 ORGANIZATION OF THE THESIS

The rest of the thesis is organized as follows: Chapter 2 provides an overview of the related work in this area. Chapter 3 describes the various components of our system CMBSAS, with its overall architecture. Data security using fingerprint biometrics is explained in Chapter 4. Chapter 5 provides our contributions towards sender authentication using face biometrics. Chapter 6 explains how the receiver is authorized, using voice biometrics. Chapter 7 details the implementation of our system at different levels of MANETs and in different applications. Chapter 8 analyses the different security services provided, the various security attacks countered by our system, and presents the experimental analysis. Chapter 9 provides the conclusions of our work and suggests possible future enhancements.