Chapter 1

Introduction

Information communication has witnessed a phenomenal change in the past few decades. The advent of internet, wireless technology and new portable devices have created a number of new ways of information communication. All these advancements have also opened up a number of new challenges for the researchers. One of the hardest challenge among these is to offer security to information communication over open networks.

A key technology used to achieve security in the emerging information society is cryptography. From e-mail to cellular communications, from secure web access to digital cash, the application of cryptography has become an essential part of today's information systems. With the increasing security requirements, the importance of development, analysis and application of effective cryptographic techniques for establishing secure communication has also increased manifold.

Key establishment and authentication protocols are the part of cryptography concerned with initializing a secure communication. These protocols use different cryptographic primitives such as encryption, signature, and one-way hash functions as their buildings blocks. Using these primitives, the protocol actions are defined for a set of communicating parties to authenticate each other and obtain a common secret key. This common secret, in turn, is used by these parties for encrypting the subsequent communication messages between them.

The design of a key establishment protocol has a number of challenges associated with it. Two major concerns in the design of key establishment protocols are security and efficiency. The security of a protocol, which is of primary concern, can be achieved by ensuring the following two issues. First, the underlying primitives used to build the

protocols need to be secured. Second, the way the primitives have been used to define the actions of the users should also be secured. Ensuring the first part is inherent as the fundamental assumption of any key establishment protocol is that the underlying primitives are secure. Thus the main challenge in providing secure communication is to ensure that the second issue, which defines the actions of the communicating parties, behave in a secure way. However, this has been a tough challenge as evident from the history of designing key establishment protocols. The protocol design has traditionally been extremely error prone, and many protocols proposed in the literature were subsequently shown to be faulty, even years after they were proposed.

The efficiency of the protocols is the second major concern, as they need to be integrated into practical applications. The main efficiency parameters of a protocol are - the number of expensive computations and the communication overhead in terms of messages or rounds. Therefore, in applications where users have constrained resources, ensuring low computational load and constant number of messages/rounds is extremely important. In recent times, different applications requiring secure communication in heterogeneous and resource constrained environment are gaining importance and are expected to be more significant in coming ages.

The focus of this thesis is on the design and analysis of authentication and key establishment protocols for communication between two or more users. In particular, our focus is on designing secure as well as efficient protocols for applications relevant to the new era of information communication involving heterogeneous and resource constrained environments.

In the next section, we give a brief descriptions of some important background works related to authenticated key establishment protocols. In that context, we discuss some of the major challenges or issues in this area from which the motivations of the thesis stem out. In the following section we give the objectives of our work. Finally a description of organization of the thesis is given in the last section.

1.1 Background and Motivation

The key establishment protocol proposed by Needham and Schroeder in 1978 [83] is considered as the starting point of the modern study of key establishment problem. During the same period, another pioneering work was proposed by Diffie and Hellman [98] which in-

troduced the public key system. Since then, a number of protocols were proposed, which formed the foundation of cryptographic key establishment and authenticated protocols. In the past decade, most of the protocols were proposed for communication between two users, using either symmetric or public key systems. Public key cryptography gained popularity due to the ease of key management and its applicability in a number of scenarios. However, public key operations are much more expensive and requires longer keys than symmetric key operations, which make them unsuitable for low power devices. The development of quantum cryptography is also posing a potential threat for the public key systems. Therefore, design of key establishment protocols using comparatively less expensive operations like symmetric key encryption and one-way hash functions are gaining significance particularly in resource constrained environments.

Security in mobile communication is an example where resource constrained users are connected to powerful servers. With the popularity of mobile wireless networks and diversity of applications offered on these, security in mobile communication has become a major concern. The standards for mobile communication also specify authentication and key agreement protocols to be used. However, security standard defined for one generation of mobile communication is not found to be suitable for the next generation of communication scenario where new applications requiring stronger security are being deployed. Also, a good number of security algorithms defined for mobile standards were shown to be faulty by the researchers. Thus, inspecting the security protocols used in the mobile standards has become an interesting area of research.

In recent times, group oriented applications such as electronic conferences and collaborative works have gained much popularity. Security is very crucial for such applications as these operate in a dynamic environment and communicate over insecure networks. This has catalyzed the demand for secure group communication protocols for various group applications. One way of designing group key establishment protocols is to generalize the two party key establishment protocols to multi-party setting.

A number of researchers concentrated on using group Diffie-Hellman construct for designing group key establishment protocols. However, protocols using group Diffie-Hellman are multi-round in nature, where computation and communication requirements depend on the number of users present. More recently, the advent of low power devices and the heterogeneous, ubiquitous computing environments have necessitated the design of efficient security protocols. These computing environments favor less computation and communication overhead, particularly for the resource constrained users. Therefore the

multi-round, computation-heavy protocols are not suitable here. The protocols designed for peer-to-peer networks requiring equal computing power for all the users are also not applicable in such scenarios. Thus design of group key agreement protocols for heterogeneous environment having resource constrained users is another area of research which needs attention of the researchers.

The design of key establishment protocols for groups also involves a number of issues not faced in two-party key establishment protocols. One such issue is group dynamics where users should be allowed to join and leave a system during a protocol session without affecting the protocol security. This issue of dynamic security has not been addressed in many group key establishment protocols. Another issue arises in a contributory key agreement, where a number of users contribute to the construction of the group key. It is important to ensure that contributions of all the users are considered in the key construction. A number of group key agreement protocols in the literature do not actually ensure this contributive property.

Apart from the computing environments and methods, another major issue with the design of key establishment and authentication protocols is the analysis of their security. In most of the protocols proposed in the literature, the security analysis is performed in a heuristic approach. In this approach, a protocol is claimed to be secure by showing it to withstand a number of existing popular attack scenarios and satisfy a number of desirable properties. However, key establishment protocols have historically been particularly vulnerable to unforeseen attacks, and many of these have taken years before they were demonstrated to have subtle security faults. Moreover, the heuristic approach provides no clear framework to formally describe what it means for a protocol to be “secure”, and what constitutes an “attack”.

Several methods have been proposed to formalize the security analysis of cryptographic protocols. The most well known formal approach among these is the complexity theory based provable security approach pioneered by Bellare and Rogaway in [60]. While these provable models address the two and three party key establishment, the first formal model for group key exchange was proposed by Bresson *et. al* in [32]. The provable security models are gaining importance and gradually becoming a standard for protocol security analysis in the cryptography community. However, most key exchange protocols proposed in the literature are still having an informal heuristic security analysis only.

Based on an extensive study and analysis of the current works related to the above

discussed points, we have identified a number of weaknesses and design issues not addressed adequately in the literature. In particular, we have observed the following issues of key establishment protocol design, that demand immediate attention.

- The current trend of technology is towards designing applications for low power wireless devices. The existing key exchange protocols designed for general networks are not suitable for such scenarios. Therefore design of protocols suitable for resource constrained environment is currently an interesting area of research.

- Design primitives like public key constructs can be expensive for the low power participants. Therefore an attempt to utilize the computationally less extensive primitives like one-way hash functions can be worthwhile.

- Unlike the two and three party protocols, the group based protocols are still less explored. The multi-round group key protocols are not suitable for applications requiring efficiency and scalability. Thus, design of computationally and communication wise efficient and authenticated group key agreement protocols are an important area for investigation.

- Many protocols proposed in the literature were subsequently shown to have weaknesses. Thus, one direction of research in key establishment protocols can always be towards examining the existing systems.

- Along with informal analysis, a more formal approach of analyzing the protocols is essential to gain confidence about their security.

- As new services are being deployed over mobile networks, the requirement of mobile security is one of the highest priorities for the designers. The earlier second generation mobile network security has been extensively analyzed by the researchers. The security flaws found as a result of the analysis have been addressed while designing the next third generation standard. Now, it would be interesting to study whether the new third generation mobile standard is able to address all concerned security issues.

In the next section, we give the brief description of our works that mainly address the above mentioned concerns.

1.2 Summary of Contributions

The aim of the thesis is to address and investigate the issues of key establishment protocol design mentioned in the previous section. The contributions of the thesis can be subdivided into three parts. Each contribution attempts to address more than one concerns mentioned earlier.

- **One-way hash based key establishment protocol**:
  In this work we have studied the design of symmetric key based protocols using a trusted server. The work is divided into two parts. In the first part of the work, we have identified a class of weakness in the key control property of a set of existing protocols and have given a design principle to avoid it. Then, in the second part, we have proposed a set of key establishment protocols sharing the same basic construction and varying in key control property, to show how the weakness in key control can be avoided in different key control scenarios. We have used computationally inexpensive one way hash functions as the only cryptographic primitive for protocol design. We have also performed a detailed analysis of the variations in communication and computation requirements with changing key control property in the protocols. The protocols impart less computational load on the users and is thus suitable for heterogeneous environment. Finally, we have analyzed the security of the protocol in formal model.

- **Group key agreement for heterogeneous environment**:
  The objective of this work is to analyze and design group key agreement protocols for heterogeneous environment having mostly resource constrained users. First, we have proposed a group key agreement protocol for establishing a contributory group key. The main constructs used to design the protocol is polynomial interpolation and one-way hash function. The protocol addresses efficiency and security issues of existing protocols. The key computation of the protocol is truly contributory and the users are able to verify the utilization of their contribution in the key construction. Then, we present a more efficient variation of the protocol which is suitable for heterogeneous environment. In this protocol, the only on-line computation performed by the resource constrained users is a single XOR computation. A proof of the protocol has been given in the provable security model. To achieve higher scalability, extensions of the protocol has also been proposed for clusters and hierarchies of users. The hierarchical key establishment is also truly contributory and

efficient in terms of computations required.

- **Authentication and key agreement for mobile communication**:
  The objective of this work is to analyze and enhance the authentication and key agreement protocols used in the current mobile network security standard. The analysis reveals some weaknesses and shortcomings. Based on the analysis, we have proposed two improved protocols that address the shortcomings of third generation mobile networks based on GSM and CDMA standards respectively. We further enhance our solution by giving a secure protocol for communication between the home and visited network to ensure end-to-end security.

1.3 Organization of the Thesis

The rest of the thesis is organized as presented next:

- **Chapter 2**: *Background and review*– Explicates the various concepts in key establishment and authentication protocol that are required to prepare the background. Subsequently we discuss the current state of the art in this branch of cryptography.
- **Chapter 3**: *Key establishment protocols using one-way hash functions*– Investigates some of the existing protocols and show their weaknesses to meet the intended key control property. Then, a set of protocols is proposed with varying key control property, using one way hash functions. Finally proof of the main protocol is given in the provable security model.
- **Chapter 4**: *Polynomial interpolation based group key agreement protocol*– Describes an authentication and key agreement protocol using polynomial interpolation property. The protocol allows truly contributory and verifiable key agreement. The chapter also presents auxiliary protocols for dynamic handling of join and leave. The performance efficiency of the protocol is analyzed. Finally the security analysis of the protocol is given in a formal model.
- **Chapter 5**: *Scalable group key agreement protocols in resource constrained environment*– Extends the protocol proposed in the previous chapters to offer more efficiency and scalability for applications in more resource constrained environment. Also, a scalable proposed for applications in hierarchy has been proposed.

- **Chapter 6**: *Authentication and key establishment protocols for secure mobile communication*– Analyzes and proposes enhancements to the two authentication and key agreement protocols for the current mobile security standards.
- **Chapter 7**: *Conclusion*– Concludes the thesis by summarizing the basic findings of the works. It also outlines a few topics of future research interest.