CHAPTER 1

INTRODUCTION

Multicast communication enables packets to be delivered from a single sender or a number of senders simultaneously, to multiple receivers. In wireless multicast networks high-valued transmissions would need to be encrypted, and only paying users should have the decryption keys. As a result, it is very important to securely distribute the multicast data encryption key to a set of legitimate subscribers. Secure key distribution is one of the significant challenges in secure multicast over wireless networks. This is achieved by changing the group key whenever an existing member leaves the group or a new member joins the group (Bao-Hong Li et al 2004). One problem with the existing single server system serving the whole population is that, its complexity increases as the number of users increases, mainly due to the large number of re-key messages and the size of the key database. Therefore, in order to reduce the complexity and manageability of the system when the multicast group is large, a Multi-server approach is proposed in this thesis.

1.1 MULTICAST COMMUNICATION

The philosophy of secure multicast communication has gained momentum during the last few decades. Now, it is very widely discussed, researched and applied in a variety of environments (Roberto Di Pietro 2003). Its ultimate aim is to achieve secure transmission of packets with considerable savings in bandwidth. By making itself eminently suitable for any type of applications like online audio/video conferencing, collaborative work, transmission of corporate data to selected employees, communication of stock
quotes to brokers, and streaming audio and video, secure multicast communication holds a potential to become, what can be termed as an ‘ideal technology’ for the future. Some recent applications show that multicast is suitable for military applications as well. Secure multicast is indeed a philosophy rather than a technology. By eliminating the bandwidth bottleneck it aims at creating a system that is responsive to the growing need of the applications. Being a philosophy, secure multicast can be applied not only to wired environments but also to wireless networks.

Nowadays, wireless networks have gained prominence and acceptance; it is believed that a large number of services requested by mobile users will be multicast to them from various service-providers. Wireless multicast becomes a challenging task and a topic of great interest among researchers. In many applications, security is as important as performance and low energy consumption. For secure multicasting, we need a cryptographic key management scheme in which cryptographic keys must be used to encrypt and decrypt messages. The cryptographic keys must also be recalculated and redistributed upon certain events, such as a member joining and leaving the group. They must ensure that only authorized participants in the group may access the distributed keys and group data (Baugher and Canetti 2004). Secure key distribution is one of the significant challenges in a wireless environment.

Current trends in wireless applications indicate an increasing demand in future networks for multicast capability. Many multicast applications require not only multicast capability, but also predictable communication performance such as guaranteed multicast latency and bandwidth.
1.2 THE DEVELOPMENT OF MULTICAST COMMUNICATION

Data communication in networks traditionally consists of two types of services – Unicast and broadcast. Unicast (also called point-to-point) communication involves delivering data from one sending node to a one specific receiving node in the network. Broadcast, on the other hand, involves delivering data packets from one specified sending node to all the receivers in the network. In Internet protocol receivers, the address of a receiver is specified in a unicast communication packet, and a unique address is used for specifying a broadcast communication packet.

Unicast and broadcast do not efficiently support many of the present-day applications. Many Internet applications require delivering data from one sender, or from several senders, to multiple but not all the receivers in the network. Examples of such applications include caching and replication of databases and websites in multiple locations. For such applications, unicast is wasteful, in that it generates excessive traffic, while broadcast generates traffic on parts of the network that may not require it.

To address these difficulties, a third technology, Multicast, has emerged in the form of a layer-3 Internet Multicast Protocol Standard as a means of delivering data from one sender to multiple receivers simultaneously over LANs and WANs. While multicast communication is highly demanded in many applications, most of the existing multi computers do not directly support this service; rather it is indirectly supported by multiple one-to-one or broadcast communications, which result in more network traffic and a waste of system resources. The efficiency with which multicast communication can take place is largely determined by the network level support available for such communication. Two factors contribute to the complexity of supporting current multicast applications:
- The lack of reliable multicast transport mechanisms at the network level and
- The lack of network support for large scale multicast communication.

The concept of group communication originated from the “Std IP Multicast Model” described by Stephen Deering in 1988. Part of Stephen Deering’s dissertation proposed an architecture and service model sufficient to begin deploying multicast. The evolution of this work led to the creation of the Multicast Backbone (MBone). In 1992, the MBone carried its first worldwide event when 20 sites were connected together to receive the March meeting of the Internet Engineering Task Force (IETF). This first audio conference allowed a few members from all over the world to hear what was being said at the San Diego meeting. The main focus of the evolution of multicast during the early days was on the

- development and refinement of multicast routing and
- development of transport layer protocols to provide additional services like reliability and real-time streaming media support.

Figure 1.1 depicts the evolution of multicast.

![Figure 1.1 The Evolution of Multicast](image-url)
Since 1988, the MBone has grown tremendously. Having achieved a relatively versatile and effective set of routing protocols, the MBone is at a new juncture in its evolution. Commercial interests are increasingly driving the requirement for multicast to evolve beyond a research concept. Pressure is mounting to make multicast a fully deployed, ubiquitous service on par with unicast. It is no longer a simple virtual network sitting on top of the Internet, but is rapidly becoming integrated into the Internet itself. In addition to simple DVMRP tunnels between workstations, the MBone now has native multicast capability provided in the routers themselves. Other multicast routing protocols like Protocol Independent Multicasting (PIM) and Multicast Open Shortest Path First (MOSPF) have been standardized and deployed. Improvements have also been made in transport layer services. The Real-time Transport Protocol (RTP) assists loss and delay sensitive applications in adapting to the Internet's best-effort service model. The trend and eventual goal of the MBone is to facilitate the efficient and effective transmission of real-time multimedia data over the Internet. With the MBone's growth, the demand for new, better, and different applications has also grown. Since the first audio conference in 1992, the MBone has seen the development of new applications based on an increasingly diverse set of media types. Originally, the MBone was considered a research effort and its evolution was overseen by members of the MBone community.

1.3 MULTICAST GROUP CHARACTERISTICS

Multicast enables one-to-one and many-to-many datagram distribution services. It reduces the sender transmission overhead, the network bandwidth requirements, and the latency observed by the receivers (Kin-Ching Chan and Gary Chan 2001). These properties make multicast an ideal technology for communication among a large group of people. A number of parameters describe the characteristics of such groups. These
parameters affect in a crucial way, the security architecture that is used. A few parameters are listed and discussed briefly here.

- Group size
- Membership dynamics
- Lifetime
- Security
- Awareness
- Heterogeneity
- Volume and type of traffic

1.3.1 Group Size

Multicast groups can vary in size from several tens of group members in small discussion groups, through thousands in virtual conferences and classes, and up to several millions in large broadcasts.

1.3.2 Membership Dynamics

Multicast group members can be static or dynamic. Certain applications know the members in advance whereas in some other applications the group members can be dynamic. A dynamic group is difficult to manage and keys need to be refreshed whenever a new member joins the group or an existing member leaves the group. Dynamic membership change affects the performance of a multicast system to a great deal.

1.3.3 Lifetime

As far as lifetime is concerned, a distinction is made between permanent groups and transient groups. The latter exists only as long as a group has members. A permanent group, on the other hand, will continue to exist even if it currently has no active members. A group of all routers in a
sub-network is a typical example of a permanent group. A videoconference is an example of a transient group.

1.3.4 Security

Security requirements can be static for the entire duration of the communication, or they can change dynamically during an established communication (Chaddoud et al 2001). Furthermore, they can vary for the different data streams involved (e.g., audio, video, whiteboard). It is also possible for the meetings of a project team to move through different phases. During certain phases when confidential information is being discussed, there can be no acceptance of anyone listening in on the discussion without detection by the project team. The issue of the extent to which the mechanisms currently being used for point-to-point communication are also suitable for group communication, is likewise raised in the area of security.

1.3.5 Awareness

The awareness of the group relates to the awareness of the identity of the other members in a group (Wong et al 2001). In an anonymous group, group members may not be aware of each other at all times during a communication. For example, when a presentation is multicast on the network, some listeners may not identify themselves and, thus, are not known earlier, through the identity of all the members will usually be available to every anonymous one. Note, that in an anonymous group all group members could also be known, but this is not ensured. Group awareness has a major influence on the group services that can be provided. For example, reliability cannot be provided to anonymous groups.
1.3.6 Heterogeneity

Two types of multicast groups are possible: homogeneous and heterogeneous. In a homogeneous group, all the participants at a conference have access to the same resources (Haibin Lu 2005). For example, if one of the group members is on a business trip while the meeting is taking place, he or she may not be able to participate in the meeting over a wireless connection at a lower data rate. The group then needs to be reclassified as a heterogeneous group, because this one member of the group is not able to take advantage of the full quality of the conference.

Members of a heterogeneous group have different capabilities, with respect to their network connections. The reason for heterogeneity can vary from data rate to the type of encoding scheme used. Communication costs can also be a reason for heterogeneity in a group, particularly if one member requests a lower transmission quality in order to save costs related to communication (Hao Yin 2006).

1.3.7 Volume and Type of Traffic

This depends on the type of application. Few applications carry a high volume of real-time data. Some applications send less stringent real-time, low volume data or audio, or real-time, high volume video.

1.4 MULTICAST IN WIRELESS ENVIRONMENTS

The rapid progress in the technologies underlying multicast networking has led to the deployment of many multicast services, such as streaming stock quotes and multimedia services (Paul 1998). Most of the current researches concentrate on providing these real-time multicast applications in wired networks. At the same time, there has been a significant advancement in building a global wireless infrastructure that will free users
from the confines of static communication networks. Users will be able to access the Internet from anywhere at anytime (Mohammad Umar Siddiqi and Win Aye 2005). As wireless connections become ubiquitous, consumers are willing to have multicast applications running on their mobile devices. In order to meet such a demand, increasing research efforts have been made in the area of wireless multicast in recent times (Shin and Suh 2000). Businesses can use wireless multicast to distribute software, news updates, and stock quotes to branch offices. Wireless multicast can be deployed by cellular and service providers to support content distribution services that customers can use.

The following factors are considered crucial while providing multicast services in wireless environments:

- Battery power,
- Bandwidth constraints,
- Host mobility,
- Loss of packets, and
- Wireless security issues.

The multicast protocol used in wired networks, does not perform well in wireless networks, because multicast structures are fragile as the mobile nodes move and connectivity changes (Hwayoung Um and Edward Delp 2003). When a key management scheme is chosen, the structure of the wireless network should be considered very carefully. For example, a wireless cellular network has a unique hierarchy structure and hence, a key management scheme should be easy to deploy.

Researchers focus on two main kinds of wireless multicasts: multicast for infrastructure-based wireless network and multicast for ad hoc networks. Infrastructure-based wireless networks involve base stations and
switches in a fixed topology. On the other hand, ad hoc wireless networks contain no fixed structure; all network components are subject to move without any constraints. In this research, a Multi-server approach focused on an infrastructure-based wireless network is analyzed, and its performance is studied.

1.5 SECURITY REQUIREMENTS IN WIRELESS MULTICAST

In this section, the issues of security requirements in wireless multicast are discussed. The fundamental services of secure multicast for wireless networks are listed and described as follows.

- Authentication
- Confidentiality
- Integrity
- Group key secrecy
- Forward and Backward access control

1.5.1 Authentication

This provides access control to the network by denying access to client stations that cannot authenticate properly. This service addresses the question, “Are only authorized persons allowed to gain access to my network?”

1.5.2 Confidentiality

It was developed to provide “the privacy achieved by a wired/wireless network.” The intent was to prevent information compromise from casual eavesdropping (passive attack). This service, in general,
addresses the question, “Are only authorized persons allowed to view my data?”

1.5.3 Integrity

This service ensures that messages are not modified in transit between the clients and the access point, in an active attack. This service addresses the question, “Is the data coming into or exiting the network trustworthy—has it been tampered with?”

1.5.4 Group Key Secrecy

This property guarantees that it is computationally infeasible for an adversary to discover any group key.

1.5.5 Forward and Backward Access Control

Forward access control ensures that departing members cannot get access to future group data and backward access control ensures that joining members cannot decrypt past group data.

1.6 MULTICAST APPLICATION TYPES

Two general multicast application types have been identified in the effort to provide a common ground for discussing the issues related to multicast security and group key management.

1.6.1 One-to-Many Multicast Applications

The first multicast application type covers cases where the multicast group has one sender and multiple receivers. Transmission is unidirectional, from one sender to many receivers. The receivers are assumed to be passive consumers of the data, while the single sender is the
producer of the data (Junqi Zhang et al 2003). Examples of this multicast application include Pay-Per-View (PPV) programs (e.g., Internet TV, Radio, Video) and other real-time data (e.g., news, stock prices, etc).

Two general cases exist with respect to the data being transmitted. In the first case, the group is concerned more about the authenticity and integrity of the data, and not so much about its confidentiality. An example would be, subscriptions to publicly available data (e.g., Stock market data, government publications). These desired effects can be achieved using public key techniques and message integrity techniques, leaving the data itself readable to non-members. Of more concern here is the second case, where the aim is to prevent non-members from accessing the data. An example would be subscriptions to subscribers-only transmissions (e.g., pay per view Internet TV). Here, encryption techniques can be used for controlling access to the data.

1.6.2 Many-to-Many Multicast Applications

The Many-to-Many multicast application type refers to the case where the relationship between the sender and receiver(s) is equal (democratic) and where the data is of immediate value only to the members of the group (Sandeep Gupta and Sriram Cherukuri 2003). Every member of the multicast group is both a sender and a receiver. An example of this multicast application would be conferencing. The membership of the group may be open or closed. In the Open Many-to-Many multicasts anyone can join the conference provided the identity of the member is known. In the Closed Many-to-Many multicast, only a predefined number of members can join, and the identities of the members are known in advance.

The aim in the Many-to-Many multicast application type is to prevent non-members from accessing the data (Tseng 2007). Hence,
encryption (in addition to message authenticity and integrity techniques) is used for controlling access to the data that is of immediate value only to the members of the group.

1.7 PERFORMANCE PARAMETERS

Several parameters are listed relevant to the performance of group communication and measured against the multicast group size. The relative values of these parameters is measured against the multicast group size.

Member join/leave latency, end-to-end delay, re-keying cost and key update time are some of the important parameters. The highest priority should be the cost of parameters should be minimized. For server optimization problem using heuristic techniques, parameters such as number of destination servers, consolidation efficiency, convergence time, response time, success ratio and work load moved are studied.

1.8 MULTI-SERVER APPROACH FOR SECURE MULTICAST

Traditional data security based on the public key infrastructure (PKI) is applied generally for unicast environments (Wei-Chi Ku and Shuai-Min Chen 2003). Such a point-to-point approach is not suitable for a multicast environment when the group is large and highly dynamic, i.e., the group members join and leave frequently and at random times. In order to securely transmit data in a multicast group, whenever there is a membership change, the data has to be re-encrypted with a different key and the corresponding decryption key has to be made known to all the members in the group (Ariel Orda and Alexander Sprintson 2005). If not managed properly, these “re-key messages” which inform the key change would consume a large amount of network bandwidth and processing overhead (Kin-Ching Chan and Gary Chan 2002). In addition, sometimes the network becomes overloaded and the
network performance reduces sharply. Though, much research has been done, much of the previous work on secure multicast focuses on the key tree scheme. This body of work includes reducing the number of re-key messages and the number of keys stored in the server maintaining the key tree by means of growing and pruning. This work based on the Multi-server network model focuses on reducing the performance parameters, such as member join/leave latency, re-keying cost, delay and key update time.

In a Multi-server system, the group manager sends the message just once to each sub-group manager. The sub-group manager then performs the local distribution of the message to each of the users associated with that message, using locally-available efficient communication channels. Hence such a system uses significantly fewer network transmissions, as compared to that of a single-server system.

Initially, there will be a single server and when the user pool is too large for a single server to handle, the total pool of users is split and served by multiple independent physical servers to minimize member join/leave latency, re-keying cost, delay and key update time. When the underlying traffic changes, each physical server may further split and merge dynamically into multiple logical servers to serve its user traffic to minimize the number of transmissions. In this research an efficient scheme for such splitting and merging is proposed, and its performance based on various parameters under different conditions, is studied.

1.9 RESEARCH CONTRIBUTIONS

In essence, the thesis analyses the existing multicast key management techniques and the security and protection issues related to them. It introduces a Multi-server approach to handle large multicast groups efficiently by reducing the Member Join Latency, Member Leave Latency, re-
keying cost and Key Update Time. A dynamic split-and-merge scheme is presented to handle frequent user join and leave efficiently. Finally optimizing number of servers during the dynamic split-and-merge operation is studied in order to reduce overall network traffic. The research contributions of the thesis are as follows:

- A comprehensive analysis on the existing multicast key management techniques is performed together with their advantages and drawbacks.

- A simple and yet accurate model validated by extensive simulation of a Multi-servers approach for secure multicast is presented.

- A dynamic split-and-merge scheme to reduce Member join/leave latency, end-to-end delay, re-keying cost and key update time as the underlying user traffic fluctuates, and the conditions under which this can be done efficiently is presented and

- A heuristic approach to find the optimal number of destination servers during dynamic split-and-merge is studied.

- The proposed Multi-servers approach for wireless environment is examined under a realistic scenario.

The result show that the Multi-server approach can achieve a substantial reduction in Member join/leave latency, end-to-end delay, re-keying cost and key update time (more than 80%) as compared with a single server system for secure multicast. This is especially true for some applications characterized by high data rates, and fairly large groups of
concurrent users (e.g., 100000) (such as Internet stock quote applications, and VoD).

1.10 ORGANIZATION OF THE THESIS

The thesis is organized in the form of seven Chapters.

In chapter 1 of the thesis, the required introductory concepts on secure multicast communication for wireless environments are presented. The various applications and characteristics of multicast group are defined. The need for secure multicast in wireless environments is given. The challenges and issues in the implementation of the various multicast protocols in wireless environments are discussed.

In chapter 2, a detailed analysis of research work done already is presented and discussed. The technical milestones and the emerging trends in group communications and QoS oriented applications over wireless environments are studied. This chapter reviews the existing multicast key management techniques and related issues. Also, the literature review on application of heuristics and secure multicast for streaming applications are carried out.

In chapter 3, the concepts related to group key management such as Group Creation, Member Join, Member Leave and Group Destruction are described. Group key management requirements such as security requirements, QoS requirements, Key Server requirements and Group Member requirements are summarized. A detailed analysis on some of the existing multicast key management techniques is also presented.

In chapter 4, the proposed Multi-server approach for key management in wireless environments is studied. Through simulation, a
comparative analysis on the performance of the proposed scheme is performed with the existing single server approach.

In chapter 5, an attempt is made to optimize the number of servers during the dynamic split-and-merge operation under a frequent user join/leave scenario. Two heuristic algorithms FFD bin packing algorithm and the Least Loaded algorithms are applied to get the near optimal solution. A comparison on the performance of these two algorithms is performed. The experimental results show the suitability of these algorithms to the problem under study.

In chapter 6, the performance of proposed Multi-servers approach for wireless environment is examined under a realistic scenario.

In Chapter 7, a summary of the outcomes of the research work is presented. Future research directions that arise from the investigations carried out are also discussed.

1.11 OVERVIEW OF THE RESEARCH

Motivated by the idea of secure multicast communication for wireless environments, this research aims at developing a methodology for large scale multicast using a Multi-server system, where the number of servers in the system is dynamically varied based on the number of current users.

The performance of a Multi-server system is studied based on various parameters such as member join latency, member leave latency, re-keying cost etc. The estimation of these parameters gets complicated due to issues like group dynamics, nature of applications etc. The combinatorial property of such problems warrants the development of some efficient techniques or optimization to obtain a good solution. Hence, this research also
aims at exploring the possibility of applying optimization techniques in the
design of the Multi-server system.

1.12 SUMMARY

The development of a secure multicast system for wireless environments and its issues are discussed in this chapter. Group key management and the basic operations of the group are explained. Finally, an overview of the research carried out is given.