CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

Multicast communication for wireless environments has gained importance in recent years. This is mainly due to rapid changes happening in the field of information technology to meet global demands. A detailed analysis of such research work done already is presented and discussed in this chapter. A further discussion of the literature is divided into the following categories

a) Group Key Management for Secure Multicast
b) Wireless Multicast
c) Application of Heuristics and
d) Secure Multicast for Streaming Applications

2.2 GROUP KEY MANAGEMENT FOR SECURE MULTICAST

There are many group key management solutions to implement group re-keying in secure multicast communication. These schemes use a centralized server to generate, store, and distribute the group keys. Whenever there is a membership change in a group, 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. If not managed properly, these “re-key messages” which inform the key change would consume a large amount of network bandwidth and processing overhead (Roberto Di et al 2003).
Multicasting is a scalable solution for group communication. It, however, poses several unique security problems. They use hierarchical sub-grouping to achieve scalability. Third party hosts or members of the multicast group are designated as subgroup managers. They are responsible for secret key distribution and group membership management at the subgroup level. Lakshminath Dondeti et al (1999) proposed a dual encryption protocol for scalable secure multicasting. They showed that unlike the existing secure multicast protocols, this protocol need not trust the subgroup managers with the distribution of data encryption keys. The dual encryption protocol proposed by the authors distributes the encrypted data encryption keys via subgroup managers. They also presented a classification of the existing secure multicast protocols, compared their relative merits and showed the advantages of the proposed protocol.

Wallner et al (1999) proposed an architecture that uses a single GKC (Group Key Controller) to manage all the group members. The GKC generates and encrypts the group key separately for every member of the group. When a member joins/leaves the group, the GKC re-keys the group key. The GKC encrypts and sends this new key to every member separately. This scheme has a hierarchical key tree structure in which the group members are arranged as a logical key tree. Each group member is an external node of the tree and belongs to more than one multicast subgroup. The GKC creates a rooted balanced tree that has as many leaf nodes as there are members. Each leaf node of the key tree is associated with a member of the group. Each internal node represents a logical subgroup. The root node represents the group key.

A Distributed Virtual Reality Environment (DVE) in which many users share virtual space, provides the high level communication and cooperative design facilities. For the large scaled DVE in a wide area network, a reliable and efficient multicast protocol on the Internet is
necessary. Fumiaki Sato et al (1999) developed a reliable multicast protocol based on the sequence server and evaluated it using simulation. From the simulation result, they proved that the protocol was more scalable than the RMP (Reliable Multicast Protocol). However, the protocol has an obvious drawback in that the ordering cost is centralized to the sequence server: Therefore, the scalability and extensibility is limited. Furthermore, security support was not provided. Hence, the authors proposed a method to distribute the workload to some servers to make the protocol scalable and extensible. From the simulation result they showed that the message arrival time to members is extremely reduced.

The development of an IP multicast provides an efficient way for data distribution. Applying this technique to delivering software remotely can save a lot of money. Thus, there is a high demand for such a new service that uses multicast to distribute software securely and reliably. Usually, two phases exist in software delivery, namely, group establishment and data transfer. Lin Han and Nahid Shahmehri (1999) focussed on the multicast group establishment phase. They introduced an agent-based group management system that uses the MFTP (Multicast File Transfer Protocol) as reliable data transfer protocol. The authors have defined a set of application level primitives for MFTP-transparent communication between the sender and the recipients. This system is responsible for authentication and authorization to establish a secure group, which demands that only authorized recipients should join the transmission group.

Wong et al (2000) proposed a scalable key management scheme by constructing a logical tree of KEKs for a given group. In this approach, each member in the key tree is assigned to a unique leaf node, thus fixing the number of leaves to be the group size. Since the number of leaves determines
the height of a tree, the height of the tree is also fixed and so is the total number of tree nodes in this model.

Sudha Varadarajan et al (2000) described two frameworks for secure multicast on active networks. The main security component in the frameworks is the Active Capability (AC) which replaces the passive session key. An Active Capability is an active object that carries out security functions for protecting and controlling access to the object it is associated with. The authors showed that the ACs proposed by this framework can spawn themselves and delegate access. The frameworks exploit the computational power of active networks to provide the security desired for multicast, while removing the drawbacks in traditional approaches. In the proposed security framework, permissions are assigned based on roles. Every AC possesses a delegation count that limits the amount of delegation. An AC also carries the name of the Principal in whom it resides. It was also shown that the proposed framework prevents a malicious eavesdropper from stealing the AC and trying to utilize it for himself.

Patrick McDaniel et al (2001) presented the Antigone 2.0 framework that allows the flexible specification and enforcement of group security policies. Enforcement is achieved through the policy directed composition and configuration of sets of basic security services implementing the group. They summarized the design of the Antigone 2.0 architecture, its use, and the Application Programming Interface (API). The use of the API is illustrated through two applications built on Antigone; a reliable multicast system and a host level multicast security service. They concluded with a description of the current status and plans for future work.

Radha Poovendran and John Baras (2001) presented the issues related to secure multicast communication, in the presence of members who may collaborate to compromise the integrity of the system’s security. They
showed that the ability to compartmentalize the system depends on the availability of trusted intermediate nodes. They also noted that some variations of the recently proposed tree-based schemes do not provide the required level of security and may be compromised if two appropriate members are compromised. They further pointed out that the currently available tree based key distribution schemes are not optimal, and choose the worst case solution for key assignment.

Thomas Hardjono et al (2001) reported the developments in the IETF and described the design of the Group Key Management architecture and Group Security Association (GSA) model within the Secure Multicast Group (SMuG). Through this work they explained the background and context of a Group Security Policy Framework, and described how this fits within the broader Multicast Security Framework developed within the IETF. Finally, the current status of developments within the group security policy in the IETF is discussed. Holeman et al (2002) developed a modified set of rules for multicast groups termed differential security that employ multilevel security. Differential security is a term developed to designate a partial implementation of multilevel security. Multi-level security is the ability to distinguish subjects according to classification levels; it determines to what degree they can access confidential objects. In the case of groups, this means that some members can exchange messages at a higher sensitivity level than others. In multilevel security where confidentiality is of prime concern, a set of rules directs the flow of information. Also, the authors proposed three methods to set up a differentially secure multicast group: (i) the Naïve approach, (ii) the multiple tree differential security (DiffSec) approach, and (iii) the single DiffSec tree approach. In order to evaluate the performances (in terms of the number of links used per packet transmitted) of these approaches, extensive simulation experiments were conducted by varying the network connectivity and group size for both uniform and non-uniform
membership distribution across security levels. Studies showed that the multiple tree and single DiffSec tree approaches performed much better than the Naïve approach. They also discussed the suitability of the schemes taking into account scalability and implementation issues.

Holeman et al (2002) proposed a scheme that attempts to integrate secure multicast with multilevel security by distinguishing subjects according to classification levels, following the Bell-La Padula model rules of multilevel access.

In a secure multicast environment, the distribution of cryptographic keys may be a primary indicator of the system performance. The mathematics of public key cryptography does not scale well especially for large multi-user networks, and a symmetric-key-based system is not feasible over a network spread out geographically. The problems become even more complicated when we begin dealing with multiple levels of security, i.e. different classification levels of traffic as well as group memberships/permissions. Oskar Scheikl et al (2002) presented a new approach to multi-level secure multicast, one that uses the secure lock encryption scheme based on the mathematics of the Chinese Remainder Theorem to distribute keys to various subgroups. The solution could be applied to both one-to-many and many-to-many group communication. Through simulation and analysis the authors proved that the proposed approach presents a viable solution for the distribution of one-time session keys during actual message transmission.

Roberto Di Pietro et al (2003) analyzed the Logical Key Hierarchy (LKH) secure multicast protocol focusing on the reliability of the re-keying authentication process. They showed that key management in the LKH model is subject to attacks. In particular, these attacks can be performed by entities external to the multicast group, as well as from internal users of the multicast group. The spectrum of these attacks is spread from the Denial of Service
(DoS) to the session hijack; that is, the attacker is able to have legitimate
users to commit on a session key that is provided by the attacker. The authors
have shown that the proposed scheme enhances the reliability of security in
multicast communication as far as the authenticity of both encryption keys
and data are concerned.

Fault tolerant secure multicast services have received much
attention among researchers. The fundamental challenge revolves around
developing a selfstabilized, fault tolerant secure multicast model. Elijah
Blessing and Rhymend Uthariaraj (2003) analyzed and evaluated the fault
tolerant nature of different secure multicast models. Also, the recently
proposed LeaSel model was implemented, experimentally tested and analyzed
to determine its fault tolerance behavior. The authors studied that in LeaSel,
the multicast group is divided into subgroups based on administratively
scoped IP multicast and each subgroup has its own multicast group with its
own multicast address. They proved that packets addressed to
administratively scoped multicast addresses do not cross those administrative
boundaries and administrative scoped multicast relies on well-configured
routers to control the boundaries. The results showed that for different
numbers of members in the group, the LeaSel model exhibits the self
stabilization property and proved to be absolutely fault tolerant.

Aldar Chan (2003) introduced the notion of dependence-graphs
which links hash-chained authentication schemes to the well-known graph
theory, and provided an effective analytical model. Based on this model many
important metrics of a hash-chained authentication scheme could be readily
and easily determined from its dependence-graph. He also demonstrated the
design tradeoff of a dependence-graph and provided insights into optimizing
hash-chained schemes.
Goshi and Ladner (2003) proposed the height-balanced 2-3 tree (a B-tree of the order m - 3) and found that it has the best performance among the balancing strategies tested. However, balancing a B-tree after member join involves splitting oversized tree nodes and results in \((m + 2)h\) worst-case re-keying cost, where \(h\) is the tree height. They have also compared the performance of their proposed schemes with other tree-balancing schemes and found that the order-3 B-tree has the best performance. However, rebalancing a B-tree after insertion is achieved by node splitting, which is expensive in terms of the message cost. They propose a scheme in which an NSBHO (Non-Split Balancing High-Order) tree does not use node splitting to balance the tree. The proposed NSBHO tree has the same worst-case re-keying cost incurred by a member removed as a B-tree does. Their experiments showed that the NSBHO tree has a better average case re-keying performance and far superior worst-case re-keying performance than a B-tree.

In multicasting, a message is sent from one party to many recipients or from many recipients to many recipients. Junqi Zhang et al (2003) present a secure multicast scheme based on a novel hybrid key distribution scheme. This approach involves the proposal of a dynamic group key management scheme that enables secure and efficient updating of group members. This is achieved by constructing a public key that is associated with several associated private keys. It provides dynamic group key management services that allow group members to join and leave a group frequently. Furthermore this scheme is able to address data origin authentication and group member authentication without introducing specific additional mechanisms.

Brian Zhang et al (2003) described the design and specification of a protocol for scalable and reliable group re-keying together with performance evaluation results. The protocol is based on the use of key trees for secure groups and periodic batch re-keying. At the beginning of each re-key interval,
the key server sends a re-key message to all the users, consisting of encrypted new keys (encryptions, in short) carried in a sequence of packets. They presented a scheme for identifying keys, encryptions, and users, and a key assignment algorithm that ensures that the encryptions needed by a user are in the same packet. Using this protocol they have also made an attempt to deliver new keys to all users with a high probability by the end of the re-key interval. For each re-key message, the protocol runs in two steps: a multicast step followed by a unicast step. Proactive forward error correction (FEC) multicast is used to reduce delivery latency. Experimental results showed that a small FEC block size can be used to reduce the encoding time at the server without increasing server bandwidth overhead. They also proved that early transition to unicast, after at the most two multicast rounds, further reduces the worst-case delivery latency as well as the user bandwidth requirement. Throughout the protocol design, they have striven to minimize the processing and bandwidth requirements for both the key server and users.

Logic key hierarchy is a leading scheme for key distribution in secure multicast. Bao-Hong Li et al (2004) focus on the performance optimizations of LKH, which has the following contributions: First, the LKH scheme is improved using one-way hash function. The improved LKH scheme (denoted as ILKH) can reduce the key server cost by about 1/3. Second, a batch update ILKH algorithm is presented and its performance is evaluated by experiments. Compared with the batch update LKH algorithm proposed, the experiment shows that the proposed algorithm can reduce the key server cost by at least 1/3. Moreover, a batch update ILKH algorithm is also established and its performance evaluated. The experiment shows that this algorithm can also remarkably reduce the key server cost compared with the batch update LKH.
Zhang Jun et al (2004) proposed a new type of key graph the key link-tree scheme for secure group communication, which shows a better performance than the key tree in single re-keying. A new transform algorithm was introduced between the key tree and the key link-tree to get a better re-keying performance. Simulation results proved that the key link-tree scheme has a better performance than the key tree in single re-keying.

Sencun Zhu et al (2004) devised the GKMPAN, an efficient and scalable group re-keying protocol for secure multicast in ad hoc networks. This protocol a probabilistic scheme based on pre-deployed symmetric keys is used for implementing secure channels between members for group key distribution. The GKMPAN also includes a novel distributed scheme for efficiently updating the pre-deployed keys. The GKMPAN is designed to have three attractive properties. First, it is significantly more efficient than group re-keying schemes that were adapted from those proposed for wired networks. Second, the GKMPAN has the property of partial statelessness; that is, a node can decode the current group key even if it has missed a certain number of previous group re-keying operations. This makes it very attractive for ad hoc networks where nodes may lose packets due to transmission link errors or temporary network partitions. Third, in the GKMPAN, the key server does not need any information about the topology of the ad hoc network or the geographic location of the members of the group. The authors studied the security and performance of the GKMPAN through detailed analysis and simulation.

With the rapidly growing importance of multicast in the Internet, several schemes for scalable key distribution have been proposed. These schemes require the broadcast of $O(\log n)$ encrypted messages to update the group key when the nth user joins or leaves the group. Jack Snoeyink et al (2004) have established a matching lower bound, thus showing that $O(\log n)$
encrypted messages are necessary for a general class of key distribution schemes and under different assumptions on user capabilities. While key distribution schemes can exercise some tradeoff between the costs of adding or deleting a user, their main result shows that for any scheme there is a sequence of \(2n\) insertions and deletions whose total cost is \(\Omega(n \log n)\). Thus, any key distribution scheme has a worst case cost of \(\Omega(n \log n)\) either for adding or for deleting a user.

Min-Shiang Hwang et al (2005) proposed an improved flexible tree-based key management framework. When a terminal connects to the designated CDS (content distribution systems), the terminal can efficiently compute its inner node keys from a public bulletin board, and it does not need to have a high computing ability. In other words, it could be used in mostly low powered equipment, such as being used in a wireless environment. Simultaneously, the management center of the CDS can also efficiently structure a public bulletin board with less computation. Through simulation the authors have proved that the proposed scheme is secure against adversary attacks from the external and internal systems.

Along with the widespread deployment of wireless networks, secure key distribution is one of the significant challenges in secure multicast over wireless networks. Win Aye and Mohammad Umar Siddiqi (2005) proposed a new key distribution scheme that offers a novel solution for securely distributing the group key and re-key messages for a mobile host to join and leave a secure multicast group over IPv6 wireless network. This approach uses hybrid key encryption, that is an attempt to optimize the speed of symmetric key encryption while maintaining the security of public key encryption. The proposed scheme also minimizes the number of transmissions required to re-key the multicast group since an efficient re-keying mechanism is provided for membership changes and it imposes minimal storage
requirements mainly required in mobile networks. The authors also showed that the new protocol ensures forward secrecy and backward secrecy.

For richer information services, both network and content providers should ensure the identities of the owners and users, and provide protection of digitized contents from unauthorized access and distribution. Wen-Tsuen Chen et al (2005) proposed a logical key tree based secure multicast protocol, the LKT-SMPCP, to improve the overhead in the SMPCP. The SMPCP is a multicast watermark scheme to protect valued contents from illegal distribution. However, it requires an overhead of O(N) on cryptographic encryptions and message size, where N is the size of group members. Experimental results showed that the LKT-SMPCP reduces the encryption overhead by 30% compared with the original SMPCP.

In a secure multicast environment, the group controller (GC) is in charge of group management, such as subscription and withdrawal of group members and group key management. The GC periodically issues new group keys for a multicast group and delivers them to the group members, which we call the re-key procedure. The GC also re-keys when a member withdraws from the multicast group. The purpose of re-key is to protect the secure multicast communication from group key exposure due to long-time use of group key and from intentional key exposure by withdrawn members. Goo Yeon Lee and Yong Lee (2005) investigated a re-key mechanism and related this mechanism to the amount of disclosed information from group key exposure. They combined the cost of the disclosed information and the cost for group key updates (re-keys) and analyzed the optimum re-key interval on the basis of the number of group members, each member's security level and withdrawal rates.

Secure multicast has a variety of applications in e-commerce, e-banking, command and control, video-on-demand, and other internet-based
services. Heydari et al (2006) presented algorithms to improve on the number of re-keying messages (overhead) needed to add to and delete sets of users from a secure multicast group. They presented upper and lower bounds on the number of re-keying bits to add to or delete groups of users from secure multicast groups. A naïve approach was used to handle the simultaneous departure of k users in a sequential manner, as if they were ‘k’ separate individual departures. The authors proved that the proposed approach would take O(n) messages. In addition, the authors have showed how to amortize the cost of group re-keying over time to avoid long periods of system overhead that can potentially block the transmission of desired data at times when large numbers of users simultaneously join or leave multicast sessions.

In order to maintain secure and efficient communication within a dynamic group, it is essential that the generation and management of group key(s) be secure and efficient with real-time response. Typically, a logical key hierarchy is used for the distribution of group keys to users so that whenever users leave or join the group, new keys are generated and distributed using the key hierarchy. Moharrum et al (2006) proposed a Well-Populated Multicast Key Tree (WPMKT), a new efficient technique to handle group dynamics in the key tree and maintain the tree balanced at minimal cost. In WPMKT, sub-trees were swapped in a way that keeps the key tree balanced and well populated. At the same time, re-keying overhead due to reorganization is kept at a minimum. Another advantage of WPMKT was that rebalancing has no effect on the internal key structure of the swapped sub-trees. Results from simulation studies showed that under random user deletion, this approach achieved one order of magnitude in overhead less than the existing approaches. The authors also proved that under clustered sequential user deletion, this approach achieves almost a linear growth with tree size under individual rebalancing.
Loukas Lazos and Radha Poovendran (2006) proposed an energy-aware key distribution scheme, which uses geographical location information. They made the observation that members that are spatially close to each other can potentially be reached with broadcast, or use the same routing paths to receive data. They suggested that group members could be represented as points in the 2-dimensional plane, a clustering algorithm could be used to cluster them into groups and construct a hierarchical key tree structure. Though one can use any suitable clustering algorithm, the authors have developed a variant of the K-means (a popular algorithm in pattern recognition and classification), algorithm for creating appropriate clusters. The K-means algorithm is used due to its ease of implementation and the ability to control the number of steps in which it terminates. The goal of K-means is to create K clusters out of N points (K<N) such that a “loss” cost function is minimized with respect to a dissimilarity measure.

Tzu-Chiang Chiang and Yueh-Min Huang (2006) described how any user in the multicast group can compose the group keys and use the group Diffie Hellman key-exchange protocol (GDH) to securely multicast data from the multicast source to the rest of the multicast group in wireless ad hoc networks. They showed how the GDH allows the multicast source to structure the representation of network topology, and computes a multicast tree according to the measures of GPS units. Through simulation and analysis they proved that the GDH not only provides multicast routing information, but also fits the robustness of wireless networks and reduces the overhead for security management.

Multicast-based applications demand scalable security solutions for group communication infrastructure. Secure key distribution is one such solution that must be addressed in secure multicast sessions. Win Aye and Mohammad Umar Siddiqi (2006) presented an approach named the ESKD,
that offers a novel solution to the hierarchical key distribution problem of large one-to-many group communication. The ESKD is efficiently designed to achieve scalable and secure dynamic group membership. In the ESKD, the intermediate nodes and are not trusted and used as relaying nodes to assist in enforcing the secure multicast group without having any access to the multicast data. In the ESKD, the authors combined the public and secret key systems in order to achieve both the speed advantages of secret key cryptosystems and security advantages of public key cryptosystems. They have also proved that ESKD guarantees group key security and group data secrecy. The authors also provided a comparative analysis of this approach with DEP and showed the efficiency of the ESKD over DEP.

Yuh-Min Tseng (2006) described a conference-key establishment protocol that allows participants to construct a common session key that is used to encrypt/decrypt transmitted messages among the participants over an open channel. A fault-tolerant conference-key agreement protocol with both a constant round number and message size has been proposed in this study. Under the random oracle model, the proposed protocol is demonstrated to be provably secure against impersonator attacks and withstand known-key attacks. Compared to previously proposed protocols with round-efficiency, the proposed protocol proved to have both fault tolerance and forward secrecy, while previously proposed protocols with round-efficiency lack one or both properties.

Alireza Nemaney Pour et al (2007) devised an efficient protocol and associate algorithm for group key management in secure multicast. This protocol is based on a hierarchy approach in which the group is logically divided into subgroups. The group key is organized using member secrets assigned to each member and server secrets assigned to each subgroup, and the inverse value of the member secrets are also used to manage the group key
when a member leaves. Through analysis and simulation they proved that the keys are transmitted to members using multicast with smaller message size at leave.

Guojun Wang et al (2007) proposed an efficient group key management scheme called the ID-based Hierarchical Key Graph Scheme (IDHKGS) for secure multi-privileged group communication. The proposed scheme employs a key graph, on which each node is assigned a unique ID according to the access relations between nodes. When a user joins/leaves the group or changes its access privileges, other users in the group can deduce the new keys using the one-way function by themselves, according to the ID of the joining/leaving/changing node on the graph. Through theoretical analysis and simulation the authors showed that the proposed scheme needs only half the re-keying overhead of the MGKMS Scheme.

Each secure multicast group maintains a group key which is shared by all group members. However, there are still risks involved with unauthorized users receiving encrypted data such as traffic analysis and possibly cryptanalysis. Furthermore, it is also vulnerable to a denial-of-service attack, in which malicious hosts join a number of multicast groups. In order to control the ability of hosts to join the multicast group Li-Xin et al (2007) devised a Group Access Control (GAC) method. The GAC included sender and the receiver access controls. Routes with the support of the GAC could provide a control mechanism to prevent a malicious host from joining the multicast group. The GAC was also used to verify the capability of a group member, so that only data from authorized senders can be accepted and forwarded to the multicast tree. Though the GAC and the GKM provide different functions, they were often integrated in a system to provide the secure multicast service. The authors showed that it is possible to improve the performance of the GAC and the GKM when both of them are in place.
simultaneously. This architecture substantially reduces the infrastructure requirement by leveraging the existence of the group key management system. Through simulation they also proved that GAC reduces the network and compute overhead by utilizing the group key as an authenticator. Furthermore, it eliminated the propagation of sender access control list among on-tree routers and simulation result showed that it is more efficient than the Gothic.

Multicasting is an efficient communication mechanism to deliver information to a number of recipients. Due to the broadcast nature of wireless communication, multicasting has great potential for commercial and military applications in wireless networks. Yiling Wang et al (2009) proposed a secure and efficient key management scheme called hybrid key management (HKM), for the wireless multicasting. This scheme adjusts to the wireless network topology and applies micro-key management. Compared to the existing multicasting key management approaches, they showed that the proposed approach can achieve operation efficiency.

Secure multicast provides efficient delivery which includes an identical data from a source to multiple receivers. A common solution is to apply a symmetric key that is used to encrypt the transmitted data. However, the heavy cost of the re-keying process is the main problem in large and dynamic multicast groups. The tree-based architecture is widely used to reduce the re-keying cost in terms of storage, transmission and computation. However, it usually requires extra overhead to keep key tree balance which is in order to achieve logarithmic re-keying cost. Iuon-Chang Lin et al (2009) proposed a new RSA-like multicast key management scheme to solve the re-keying problem. This protocol applies a star-based architecture to eliminate the re-keying processes and provide the good performance when the membership changes in a multicast group.
2.3 WIRELESS MULTICAST

More and more applications are relying on the underlying IP multicast facility to disseminate information to several receivers simultaneously with minimum overheads. However, there are serious security concerns that need to be addressed before one can exploit this combined facility. Security issues in multicasting, such as dynamic group management, are further aggravated due to the mobile environment. Shankaran et al (2003) described a secure multicast framework for mobile IP. Based on this framework, they have developed a complete security architecture and secure end-to-end multicast protocols.

The work of Mohit Choudhary et al (2004) tries to capture all secure ad-hoc multicast features and attempts to integrate them with multilevel security. Multilevel security is the ability to distinguish subjects according to classification levels, which determines the degree to which they can access confidential objects. In the case of groups, this means that some members can exchange messages at a higher sensitivity level than others. Their work, also intends to highlight how the two issues of routing and security can be subtly merged into one not affecting each other’s performance, but rather complementing each other to make the protocol more efficient in terms of computation.

Yan Sun et al (2004) presented a method for designing a multicast key management tree for mobile wireless environments. By matching the key management tree to the cellular network topology and localizing the delivery of the re-keying messages, they achieved a significant reduction in the communication burden associated with re-keying, compared to trees that are independent of the topology.
Anindo Mukherjee et al (2004) introduce a novel hierarchical security framework for mobile Ad Hoc Multicast networks in which data encryption is done using a symmetric key and key establishment using symmetric ‘level’ keys and asymmetric node keys. Their primary contention is that the tree formation process should be integrated with the key exchange process and should not be treated as an add-on. The authors have shown that in a mobile environment, mobility factors play an increasingly important role and the scheme effectively handles the impact of mobility on key establishment while minimizing the number of messages to be exchanged.

Yan Sun et al (2004) propose a method for designing a multicast key management tree that matches the network topology. The proposed key management scheme localizes the transmission of keying information and significantly reduces the communication burden of re-keying. Further, in mobile wireless applications, the issue of user handoff between base stations may cause user relocation on the key management tree. To address this, an efficient handoff scheme for the topology-matching key management trees is proposed. The proposed scheme also addresses the heterogeneity of the network. For multicast applications containing several thousands of users, simulations indicate a 55%–80% reduction in the communication cost, compared to key trees that are independent of the network topology. The authors have also shown that the communication cost of the proposed topology-matching key management tree scales better than that of topology-independent trees as the size of the multicast group grows.

Junghyun Nam et al (2004) have proposed an efficient group key agreement protocol well suited for wireless networks consisting of a cluster of mobile devices with limited computational resources and a stationary server with sufficient computational power. The authors have shown that this new constant-round protocol is well suited for a mobile environment and proved
its security under the decisional Diffie–Hellman assumption. The protocol meets simplicity, efficiency, and all the desired security properties.

Yuh-Min Tseng (2006) studied a fault-tolerant conference-key agreement protocol with both a constant round number and message size. The author has proposed a protocol that requires two rounds to establish a conference key. Each participant broadcasts only a constant number of messages. Under the decision Diffie–Hellman problem, the author has demonstrated that the proposed protocol is proved to be secure against passive attacks by active adversaries, and that it can withstand known-key attacks under the random oracle model.

Venkata Giruka et al (2006) present a multi-party key agreement protocol based on a novel authenticated two-party Elliptic Curve Diffie–Hellman (ECDH) key exchange protocol for dynamic collaborative peer groups. The authors showed that the proposed protocols establish an authenticated, distributed, and contributory group secret key among a group of members, and support group dynamics like member-join, member-leave, group-fusion, and group-fission securely. The authors have also introduced Array-based Binary Key Trees (ABKTs), which are balanced trees that bound the key-computation cost of handling member dynamics to $O(\log n)$, where $n$ is the number of members in the group.

Xukai Zou et al (2006) proposed a Dual Level Key Management scheme and analyzed its security and performance. This scheme utilizes an elegant Dual Level Key Management (DLKM) mechanism using an innovative concept/construction of Access Control Polynomial (ACP) and one-way functions. In this scheme, the first level provides a flexible and secure group communication technology, while the second level offers hierarchical access control. The authors have given a complexity analysis and demonstrated the efficiency and effectiveness of the proposed DLKM in both
the computational grid and data grids. An illustrative example is shown to prove the efficiency and validate the correctness of the proposed DLKM.

Most proposed solutions in the literature do not take fault-tolerance into consideration. Seba (2006) considered the use of failure detectors to enhance the robustness of key establishment. Failure detectors need a periodic exchange of failure information between members. This creates an overhead, which can be a serious drawback for networks with limited bandwidth or heavy traffic. The author has shown that it is possible to reduce considerably this overhead by using an adapted organization of group members. Simulation has been carried out to show that it is a good approach compared to the native protocol used for evaluation.

Yuh-Min Tseng (2006) proposed a new group key agreement protocol for an imbalanced wireless network consisting of many mobile nodes with limited computing capability and a powerful node with less restriction. The author demonstrated that the proposed protocol produces contributory group key agreement and provably secure against passive attacks under the decisional Diffie–Hellman problem assumption. A simulation result on a personal digital assistant (PDA) proved that the proposed protocol is well suited for mobile devices with limited computing capability.

In wireless networks, secure multicast protocols are difficult to implement efficiently due to the dynamic nature of the multicast group and scarcity of bandwidth at the receiving and transmitting ends. Mobility is one of the most distinct features to be considered in a wireless network. Moving users onto the key tree causes extra key management resources even though they are still in service. To take care of frequent handoff between wireless access networks, it is necessary to reduce the number of re-keying messages and the size of the messages. Hwayoung Um and Edward Delp (2006) have proposed a key management tree such that neighbors on the key tree are also
physical neighbors on the cellular network. By tracking the user location, they localize the delivery of the re-keying messages to users who need them. This lessens the amount of traffic in wireless and wired intervals of the network. The group key management scheme uses a pre-positioned secret sharing scheme.

Loukas Lazos and Radha Poovendran (2007) introduced a cross-layer design approach for key management in a wireless multicast, which distributes the cryptographic keys to valid group members in an energy-efficient way. By considering the physical and network layer, they formulated an optimization problem for minimizing the energy required for re-keying. They showed that the optimal solution is not scalable with group size $N$ and developed a simple sub-optimal scheme that exploits the available routing information. They call this scheme, the routing aware key distribution scheme (RAwKey). Simulation studies show that the energy savings achieved by this scheme, and compare its performance with that of routing algorithms.

IEEE 802.11 wireless LAN has become one of the hot topics in the design and development of network access technologies. Jun Lei et al (2007) identified the general requirements used for WLAN authentication and key exchange (AKE) methods, and then classified them into three levels (mandatory, recommended, and additional operational requirements). The authors have presented a review of the issues and proposed solutions for AKE in 802.11 WLANs. Three types of existing methods for addressing AKE issues were identified, namely, the legacy, layered and access control-based AKE methods. Then, a comparative analysis was performed of these methods against the identified requirements. Based on the analysis, a multi-layer AKE framework was proposed, together with a set of design guidelines, which aims at a flexible, extensible and efficient security as well as easy deployment.
Ai Chen et al (2008) leverage the flexibility of associating with different Access-Points (APs), which occurs often due to overlapping coverage of APs, to optimize the network’s objective. Motivated by different revenue functions and network scenarios, three different optimization objectives are considered which are: maximizing the number of admitted users (MNU), balancing the load among APs (BLA), and minimizing the load of APs (MLA). The authors have used centralized approximation algorithms to compute which AP a user should be associated with. Using simulations the authors have evaluated their performance and compared them to a naive approach.

2.4 APPLICATIONS OF HEURISTICS

Shen et al (2001) present heuristic algorithms that may be used for light-path routing and wavelength assignment in optical WDM networks under dynamically varying traffic conditions. They considered both the situations where the wavelength continuity constraint is enforced or not enforced along a light-path. The performance of these algorithms has been studied through simulations. A comparative study of their performance with that of a simpler system that uses a fixed shortest-path routing has been performed. The proposed algorithms provided lower blocking probabilities and are simple enough to be applied for real time network control and management. They have also studied that the heuristic algorithms are computationally simple and efficient to implement and provide good wavelength utilization leading to efficient usage of the network's resources.

T rkay Dereli and Sena Da (2002) studied a hybrid Simulated-Annealing (SA) algorithm for the two-dimensional (2D) packing problem. A recursive procedure has been used in the proposed algorithm to allocate a set of items to a single object. The problem has been handled as a permutation problem and the proposed recursive algorithm is hybridized with the
simulated annealing algorithm. The effectiveness of the algorithm has been tested on a set of benchmark problems. The computational results have shown that the algorithm gives promising results.

Thorsten Aurisch (2005) introduced the Multicast Internet Key Exchange (MIKE) and discussed the issues related to it. In this work they adapted tree-based key management for military usage. They described that the hybrid system concept of MIKE provides separate operation modes for tactical and strategic networks. The concept is based on key trees and combines a key distribution with a key agreement algorithm. The key management quality depends on the scalable group key update mechanism by handling dynamic groups. They showed that using key trees increases the efficiency of the management. They have also presented two optimization techniques utilizing the information about the characteristics of the military groups to increase the group key update efficiency. The performance of these techniques is evaluated by two benchmark programs.

Yao Zhao and Fangchun Yang (2006) proposed an accumulated k-subset algorithm (AK algorithm) to balance the load in distributed SLEE. Based on a model of resource heterogeneity and load vector, they have found that the AK algorithm improves the k-subset algorithm by accumulating load information within every update interval. Experiments on different update intervals and request arrival rates suggested, that the AK further reduces the herd effect due to stale load information, and outperforms the k-subset algorithm by 5%-10%. Clautiaux et al (2007) proposed a new exact method for the well-known two-dimensional bin-packing problem. It is based on an iterative decomposition of the set of items into two disjoint subsets. They have tested the efficiency of this method against the benchmarks of the literature.
Liansheng Tan et al (2007) designed an efficient algorithm for the calculation of the solution to the placement of proxies for performance optimization in hierarchical reliable multicast (HRM). Proxy is introduced to localize feedback and retransmission, and thus significantly depress traffic redundancy and reduce latency. The placement of proxies is a key issue in HRM. The authors have theoretically analyzed the performance improvement made by the placement of proxies and presented a new approach to the optimal partition of a sub tree for performance optimization in the placement of a single proxy. Based on this approach, a new greedy algorithm was designed experimentally compared with several existing heuristic algorithms. The results proved that, the new algorithm outperforms in the tradeoff between performance and complexity.

Latency reduction in distributed interactive applications has been studied intensively. Such applications may have stringent latency requirements and dynamic user groups. Knut-Helge Vik et al (2008) focus on application-layer multicast with a centralized approach to the group management. The groups are organized in overlay networks that are created using graph algorithms that create a tree structure for the group. A tree has no cycles and uses a small routing table, as opposed to a connected overlay mesh. The authors have investigated a group of spanning tree problems that are referred to as Steiner-tree problems, and they have a particular focus on reducing the diameter of a tree, which is the maximum pair wise latency in a tree. The authors have also devised a new Steiner-tree heuristics that reduced the diameter, and also proposed new edge-pruning algorithms to make the tree construction faster. These heuristics and algorithms were implemented and analyzed experimentally along with several spanning-tree and core-selection heuristics found in the literature. The authors found that a full-mesh of shortest paths makes it difficult for Steiner-tree heuristics to find better trees than spanning tree algorithms.
2.5 SECURE MULTICAST FOR STREAMING APPLICATIONS

In an on-demand video system, the video repository generally has limited streaming capacities, and may be far from the users. In order to achieve higher user capacity and lower network transmission cost, many schemes have been proposed in the past. For example, Gary Chan and Fouad Tobagi (2001) studied a number of caching schemes to store multicast movie contents on to the local servers, and devised a new caching scheme that keeps a circular buffer of data for the movie requested, and hence movies are partially cached. By adjusting the size of the buffer, they were able to achieve better tradeoff between network channels and local storage, as compared to the traditional caching in which a movie is treated as an entity, and proved that the proposed approach was able to achieve a much lower system cost to offer on-demand video services.

Poon and Lo (2001) developed an efficient disk scheduling scheme to provide a starvation-free storage system for the multicast VoD system using double-rate batching. Through simulation they showed that when the request rate is 0.1 arrival/s, only 22 disks are sufficient to reduce the waiting time to less than 0.5s. In addition, the memory requirement of the scheduling algorithm in the server was also evaluated. It was shown that the proposed scheme requires less memory than the traditional VoD system for popular movies.

Jack Lee (2002) proposed a novel architecture called the Unified VoD (UVoD) that can be configured to achieve cost-performance tradeoff anywhere between the two extremes (i.e., TVoD and NVoD). Assuming that a video client can concurrently receive two video channels and has local buffers for caching a portion of the video data, the proposed UVoD architecture can
achieve significant performance gains (e.g., 400% more capacity for a 500-channel system) over TVoD under the same latency constraint. Based on the numerical and simulation results the authors studied the performance of the UVoD.

Tarik Taleb et al (2003) proposed a novel method for video-on-demand services. The basic idea in this method is to repeatedly transmit popular movies on staggered channels. If a request comes in between staggered start times, the user joins the most recently started multicast session and then requests the missing part from a neighbor. Therefore, a user must have enough buffer space to buffer the data between staggered transmissions. This scheme was referred to as Neighbors-Buffering Based Video-on-Demand (NBB-VoD) architecture. Through analytical results and simulation, the authors proved that the proposed architecture achieves a better performance than the already existing systems (True-VoD, Near-VoD, and Unified-VoD) in terms of both scalability and disk-bandwidth requirements.

Cyrus Choi and Mounir Hamdi (2003) analyzed the performance degradation problems using recently proposed VoD systems, namely, batched and centralized-buffer VoD systems that occur during the handling of interactions. Then a new system called the Multi-Batch Buffer (MBB) system, which attempts to solve these problems, was proposed. The proposed system handles a majority of interaction requests by scalable buffering techniques, employed in the buffer of the local servers and the set-top boxes (STBs). They have performed extensive simulation for the analysis and performance evaluation of the proposed VoD system. The simulation results demonstrated that the proposed VoD system proved to be very scalable and outperformed related state-of-the-art VoD systems.

Melek Önen and Refik Molva (2004) first classified secure multicast applications with regard to customer expectations, and suggested a
new approach that defines different recipient categories based on their “loyalty” and treats each category differently by offering better service to more loyal recipients. They proposed to restructure the Logical Key Hierarchy (LKH) scheme by separately regrouping members, based on their membership duration aiming at preserving members with long duration membership from the impact of re-keying operations caused by the arrivals or departures of short-lived members. Through extensive simulation they then computed system parameters like re-keying intervals based on the customer satisfaction criteria.

The secure distribution and maintenance of key information are essential for controlling access to video multicast systems. Hao Yin et al (2006) devised a novel SMDE (Statistical Modulation Data Embedding) scheme using a dedicated channel independent of the video stream. The authors used the embedded data to convey key information and were able to achieve added security and reduce bandwidth resource consumption. Through extensive simulation they have demonstrated that the proposed SMDE scheme can provide error resilience, transparency for adaptation mechanisms, high accuracy of detecting the embedded data and real-time processing capability for video applications.

Sencun Zhu et al (2006) studied the security issues that arise in an overlay multicast architecture, where service providers distribute content such as web pages, static and streaming multimedia data, real time stock quotes, or security updates to a large number of users. In particular, two major security problems of overlay multicast, network access control and group key management, are addressed. First, the bandwidth-efficient scheme, called the CRBR that seamlessly integrates network access control and group key management was presented. Through extensive performance analysis and simulation the authors proved that the proposed scheme incurs much smaller
communication overhead than the existing schemes when they are directly applied in overlay multicast. A DoS-resilient key distribution scheme, called the k-RIP, that delivers updated keys to a large fraction of nodes with high probability even if an attacker can selectively compromise nodes in the multicast data delivery hierarchy and command these compromised nodes to drop keying packets, was also proposed.

Hao Yin et al (2006) proposed a novel Content-Aware Secure Multicast (CASM) protocol for video distribution that seamlessly integrates three important modules: 1) a scalable light-weight algorithm for group key management 2) a content-aware key embedding algorithm that can make video quality distortion imperceptible, and is reliable for clients to detect embedded keys and 3) a smart two-level video encryption algorithm that can selectively encrypt a small set of video data only, and yet ensure the video as well as the embedded keys unrecognizable without a genuine key. Performance evaluation studies built upon a CASM prototype have demonstrated that the CASM is highly robust and scalable in dynamic multicast environments. Experimental results have also validated that the CASM enables secure key and video content distribution with minimized bandwidth overheads. Its content-aware key embedding and encryption algorithms are fast enough to support real-time video multicasting.

Siddhartha Annapureddy et al (2007) addressed the issues of providing a Video-on-Demand (VoD) using P2P mesh-based networks. They showed that providing high quality VoD using P2P is feasible using a combination of techniques including (a) network coding, (b) optimized resource allocation across different parts of the video, and (c) overlay topology management algorithms. Through simulations and a prototype implementation, they showed that systems that do not optimize in all these
dimensions could significantly under-utilize the network resources resulting in poor VoD performance.

Providing video-on-demand (VoD) services for mobile devices in next generation networks, such as the worldwide interoperability for microwave access (WiMAX), is an important trend. Jenhui Chen and Jui-Hsiang Sun (2007) proposed a proactive scheme, named remainder arrangement broadcasting (RAB) to lower the required buffer size. Then, to shorten the start time of video playing, the reactive method was added to the RAB scheme, named the hybrid RAB (HRAB). Simulation results showed that the RAB could achieve a lower buffer size, which is under 10%, without requiring a large bandwidth and HRAB could shorten the waiting time as well.

Dakshayini and Manjunath (2008) proposed a unique VoD architecture and On-line dynamic buffer allocation algorithm for efficient buffer and bandwidth management. This scheme reduced the bandwidth requirement between the main multimedia server and the Proxy servers by allocating and then reallocating the buffer at the Proxy server (PS) dynamically based on the current frame size. Through simulation they showed a considerable reduction of load on the main multimedia server by storing more number of frequently used videos at the PS.

Unlike those on Internet, the media providers on P2P networks are ordinary nodes with limited shared resources such as bandwidth. Multi-sender methods are the best existing solutions to video streaming on P2P networks. Mohammad Hamed Firooz et al (2008) have proposed the use of a multicast method on the top of an arbitrary multi-sender method so that all requesting peers receive almost the same expected bit-rate. Experimental results, derived from implementation of the proposed algorithm on Pastry P2P network
confirm the authors’ claim. Another advantage of the proposed method over the existing methods is its scalability with the number of receivers.

2.6 STATE OF THE ART

The literature review indicates that several researchers have attempted to improve the scalability and security of multicast communication in wireless environments. Parameters such as latency, the number of keys, re-keying cost, and bandwidth have been considered. On careful analysis of the literature the following conclusions are arrived at:

1) The majority of the literature discussed so far dealt with the group key management in wired environments, where the nodes are stationary and issues like node mobility and handoff do not arise.

2) A few authors have dealt with group key management for wireless environments. In these systems parameters such as communication cost for join/leave operations, and bandwidth savings have been considered.

3) Single server approaches using the LKH for group key management have the drawback of a single point of failure.

4) No author has dealt with the Multi-server approach for large scale multicast.

5) Not much work is reported on the usage of heuristic techniques for server consolidation problem.
2.7 SUMMARY

A comprehensive review of the literature in the area of multicast communication has been presented in this chapter. The drawbacks and limitations in the current state of art are identified and the direction of the current research is indicated.