The Mathematics Behind Key Management in Group Communication

Dr G Padmavathi
Professor, Department of Computer Science
Avinashilingam Institute for Home Science and Higher Education for Women
(Deemed to be University)
Coimbatore-641043

Abstract

Secure Group Communication is a challenging task today because of many threats the Internet is facing. Many group oriented applications are upcoming because of the increased use of Internet for many personal and business applications. Maintaining the secrecy in a group communication is challenging because of group member's dynamism. Cryptographic keys are generated and distributed to the communicating parties for secure communication among group members to maintain the forward and backward secrecy of communication. The important overheads in secure group communication are storage efficiency and communication efficiency. The formulation of minimization of storage and communication overheads is studied and the fundamental structure for the total overheads minimization is a constraint optimization problem. This paper briefly discusses some of the existing group key distribution models. Different Virtual trees for key distribution are also discussed. The constraint optimization problem is presented with the plausible solution.

Keywords

Multicast communication, group key, storage efficiency, communication efficiency, constraint optimization.

I. INTRODUCTION

Secure group communication is a challenging task due to increased personal applications in mobile and cloud. On-line and Credit card transactions, Pay Per View(PPV) programs (like Internet TV, Radio, and Network Video(NV)) and Real Time data distribution (like news updates, VIdeo Conference (VIC),White Board(WB) and stock quotes updates, certain E-commerce applications [8, 15] and distributed applications like Content Based Publish – Subscribe(CBPS) system [18] and On-Line Distance Education(OLDE) system are some of the significant applications of group communication [28]. Here only authorized members can communicate. The authentication and secrecy must be maintained in any communication by exchanging the group keys with the intended users so that the information exchanged cannot be compromised due to intruders. Security is basically defined in terms of Confidentiality, Integrity and Availability.

Cryptographic keys are used to maintain secrecy. Not only that, secure group communication also requires a strong security framework and efficient group key management system to distribute and maintain cryptographic keys to the registered members. Similarly, cryptographic authentication schemes are also necessary to ensure that registered receivers can verify that packets/information come from registered senders only. Generally, the group communication takes place with the help of a common key called the group key. As the group members change, the key must be changed and new keys must be generated and distributed to the current members of the group. When the group members change during communication, absolute secrecy must be maintained so that the past members should not be able to read the future communication and the future members should not be able to read the past communication. This is known as perfect forward secrecy (PFS) and perfect backward secrecy (PBS) respectively. The entire process of changing group key is termed as group rekeying. It is required to perform key updates on every membership change. Virtual key trees are defined to update the keys when group members change. Hence, the key management mechanism recommended must be simple without involving many overheads [37, 38]. The major overheads encountered in the key management solutions are storage overheads and communication overheads. The key generation and distribution is called as the key covering problem [12] and the aim of the paper is to disclose the nature of the problem as the constrained optimization problem and the mathematical method that can solve the key distribution problem. Section 1 brief discussed the introductory concepts. Section 2 discusses the existing key management techniques

followed in group communication. Section 3 describes the key management problem as the constraint optimization problem with the steps involved. Section 4 concludes the paper.

2. EXISTING GROUP KEY MANAGEMENT SCHEMES

The existing multicast or group key management schemes can be broadly classified under the following three categories. Figure 1 depicts the category of group management schemes [14, 19] and some sample protocols following the types.

- Centralized Group Key Management Schemes
- Decentralized Key Management Schemes And
- Distributed Key Management Schemes.

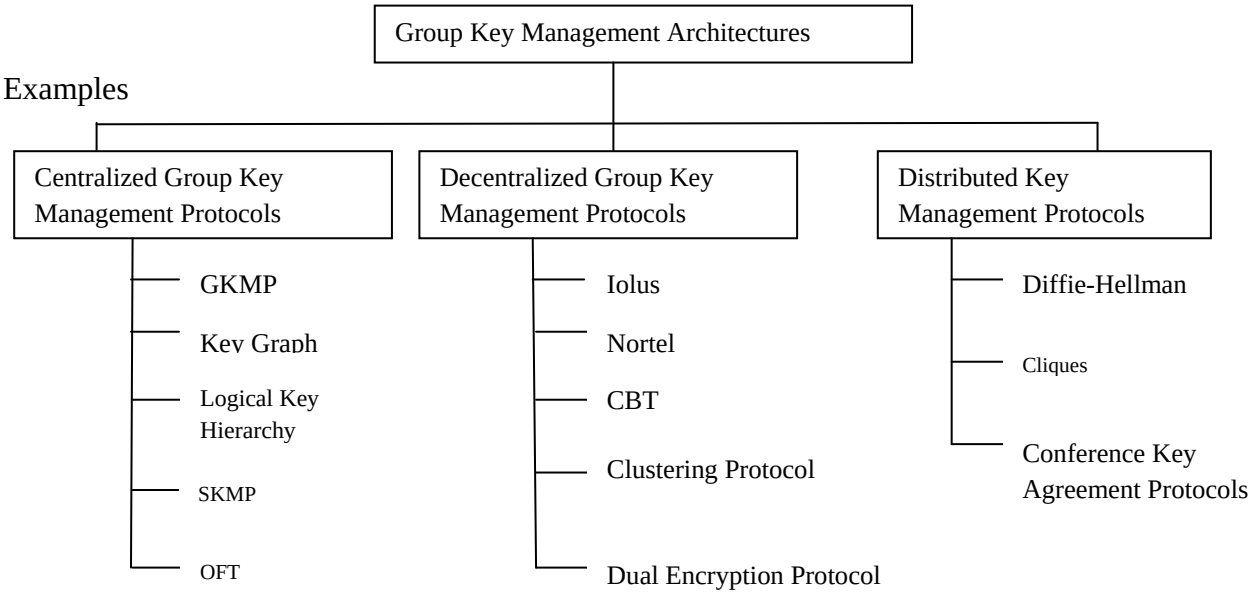

Figure 1. Classifications of Group Key Management Schemes.

In the centralized group key management systems, the single entity called the group controller (GC) or Central Controller(CC) or key server(KS) is employed for controlling the whole group. The KS does not have to rely on any auxiliary entity to perform access control and key distribution. In this case, the central entity is a crucial point of failure. The entire group will be affected if there is a problem with the KS caused by malfunctioning or malicious individual hacks. This may result in the entire disruption of service. Further when the group becomes large, the single party cannot manage the entire group. Some of the popular schemes using this approach are Group Key Management Protocol (GKMP), Scalable Extension To Group Key Management Protocol (SKMP) [3], Logical Key Hierarchy (LKH) by Wallner, Wong's Key Graph (KG) [11], Secure Lock [10], Hierarchical Binary Trees by Caronmi, Hierarchical k-ary tree with clusters and One Way Function Trees(OFT) [1, 20].

In the decentralized approach, the entire group is split into small subgroups. The management of a large group is divided among subgroup controllers minimizing the problem of concentrating the work in the single centralized place. This decentralized control in collaboration with other sub group controllers helps to avoid the central failure allowing more points of failure before the entire group being affected. However, this approach raises the question of trust relations, where the group owner now must trust all the controllers instead of just one. The important models based on decentralized approach [13, 26] are: Iolus [33], Nortel Frameworks, Suman Banerjee's Clustering Protocol, Ballerdie's Core Based Trees [2], Sandro Rafali's Decentralized model and Lakshmi Nath Donetti's Dual Encryption Protocol.

In the third type, the distributed key management approaches [4,5,24, 31, 32], there is no explicit Key Distribution Centre (KDC) or KS for key management. The group members themselves do the key generation. All the members can perform access control and generation of the key is done in a contributory fashion, i.e. the group members contribute for the group key generation. The limitations of this method are: it is meant for small and closed groups, dynamic members cannot be accommodated and the key management is very costly. Some famous models

are Cliques [21], Diffie-Hellman Protocol (DHP) [29] extended to group communication and Conference Key Agreement Protocols [9, 16, 17, 30, 34, 35, 36]. Every Approach has its own advantages and limitations when compared to other approaches.

Virtual key tree structure is the core structure of key distribution. There are three important virtual key tree structures are available in the literature. The efficiency of the virtual key organizations are measured in terms of the two important parameters namely, the storage and the communication costs [6, 7, 25]. Figure 2 shows two logical key hierarchies used for key distribution. The figure Indicates Wallner's rooted binary tree with eight members. The first form is known as logical key tree and the second form is known as star graph. All the members share the root, which is the session key $k_{1-8.}$ Every group member is assigned to a unique leaf node in the key tree. The set of nodes found in between the root node and leaf nodes from the sub-group keys. The members are assigned a set of encryption keys (session key, sub-group keys and individual key) based on their position. The storage efficiency of star is O (N), and the communication efficiency is O (N), whereas the storage efficiency of tree structure is O (N) and communication efficiency is O (log N) where N is the group size.

The star architecture is storage efficient but not communication, while the tree organization is communication efficient but not storage efficient. Generally, the preferred storage of efficiency is O (N) and the communication efficiency is O (log N), where N is the group size.

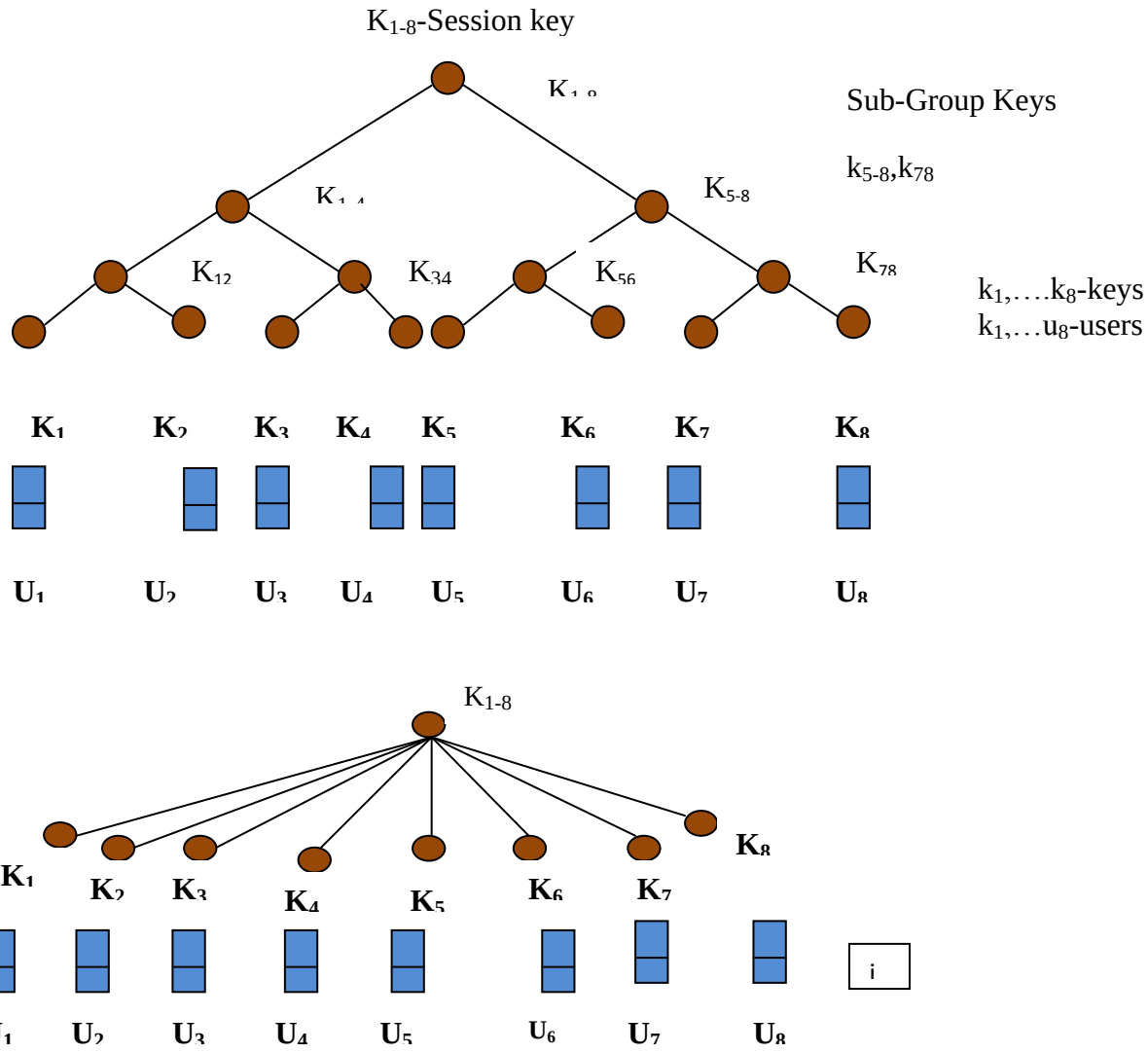

Figure 2. Logical Key Hierarchies : i .Tree , ii. Star

A third type of key tree called hybrid cluster tree is an improved version of logical key tree with the members arranged under each cluster. An example tree is shown in Figure 3.The cluster size is a variable in this tree. Cluster members are the Group members. So each group member has two keys the cluster key and the sub-group key. The hybrid Cluster tree is comparatively storage efficient and the overload is of order O(N/log N).

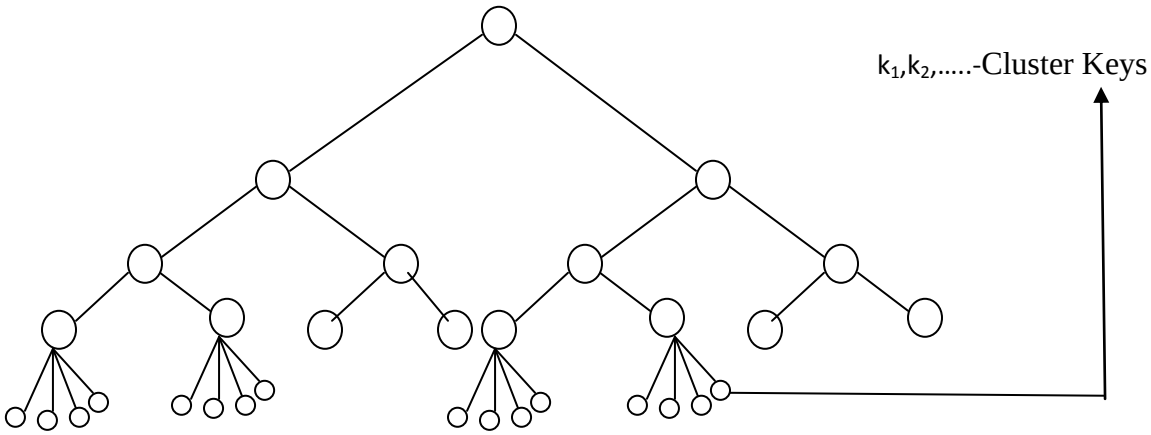

Figure 3.Hybrid Cluster Tree for a group of 32 members

This section briefly discussed the existing logical key tree schemes and their overheads. The next section discusses the formulation of the mathematical model to handle the overhead minimization challenges.

III. MATHEMATICAL FORMULATION OF THE KEY DISTRIBUTION SCHEME

As observed earlier, the storage and communication overheads are two important parameters in the design of the key tree where the simultaneous minimization of both is not possible as there is a tradeoff between the storage and communication overheads [22, 23, 27]. This is an indication of constraint optimization problem or constrained optimization problem.

A) *Constraint Optimization Problem*

Constraint Optimization is one type of Mathematical Optimization problem. Here the objective function is optimized with reference to variables and some constraints. Let us discuss how the constraint optimization is relevant to key management problem. As discussed earlier, the design of the key tree is the challenging one as the traditional binary key tree and star key tree are not performance efficient. Hence there should be a striking balance between the depth of the tree and the number of nodes/ degree of the key tree. The alternative approach, the hybrid cluster tree can handle many users compared to the above two trees and therefore the hybrid key tree is considered as an efficient organization compared to tree and star. So the constraint optimization problem is discussed only with reference to hybrid cluster tree. In the case of hybrid cluster tree, the design of the optimum key tree lies in the two parameters namely, the cluster size and key tree degree. The reason is that as the degree of the tree increases, the storage cost is less and as the depth of the tree contributes for communication efficiency. In case of the hybrid cluster tree, as more group members can be associated with, the hybrid cluster tree is considered efficient.

B) *Optimization of Hybrid Cluster Tree*

In hybrid cluster tree the two parameters are the cluster size (r) and the key degree (n). For a group of size N, the storage cost function S is defined as a function of 'r' and 'n' as,

$S=f_1(r,n)=(n*N/r-1)(n-1)$

The communication update constraint C is defined as,

$C=f_2(r,n)=r-1+(n-1)\log_n(N/r)$

A deterministic approach has been proposed by Mingyan Li.et.al which corresponds to the finding of optimum cluster size. A study revealed that the number of key stored by KS depends on the degree of the tree also. As the degree of the key tree increases, the number of nodes stored in the key tree decreases thus minimizing the central storage. It is found that the relation between Storage and Communication is a Pareto curve. Therefore, the problem is formulated as constraint optimization problem with multiple

parameters. Here the combined cost, which is the total cost function, can be defined as combined storage and communication cost as,

$T=\alpha_1 * S+\alpha_2 * C$, where $\alpha_{1+}\alpha_{2=}1$, where $\alpha_{1,}\alpha_2$ are the design parameters.

The resultant function is a convex function and is defined as,

$T=\alpha_1 * f_1(r,n)+\alpha_2 * f_2(r,n)= \alpha_1 * (n*N/r-1)/(n-1)+\alpha_2 *[r-1+(n-1)\log_n(N/r)]$.

C) *Steps involved in Constraint Optimization*

The uniform method followed to handle the constraint optimization is a step by step procedure.

Step 1: Set up the problem in a structured way. Here, it is Minimization of Total Cost (T) represented in terms of S – Storage and C - Communication. Identify the variables. In hybrid cluster tree, the two design variables are r- cluster size and n- key tree degree.

Step 2: Take the partial derivative with respect to the variables used in the objective function.

Step 3: Solve the first order conditions for the variable taken.

Step 4: Set the expressions equal to each other (as there are only two parameters).

Step 5: Use the constraint to solve the variables.

The second challenge is finding of the optimal sub-group size 'r'. Both the cases are addressed in the following presentation.

D) *Solution to Key Tree Design Parameters*

Computing the derivate with respect to 'r' can show the convexity of the total cost function.

$$T = \alpha_1 * S + \alpha_2 * C$$
$$= \alpha_1 * (2n-1) / (n-1) * (N/r) + \alpha_2 * [r + (n-1)* \ln(N/r)/ \ln(n)]$$

Computing the first order and the second order derivatives with respect to the variable 'r' gives,

$$dT/dr = \alpha_1 * (2n-1) / (n-1)*N (-1) (r)^2 + \alpha_2 * [1 + (n-1)/\ln(n) * (r)/N* (-1)*(r)^{-2}].$$
$$= -\alpha_1*(2n-1)/ (n-1)*N*1/(r)^2 + \alpha_2 * [1-(n-1) * 1 / (N*\ln(n)*(r)]$$

With second order differentiation w.r.to 'r',

$$d^2T/dr^2 = -\alpha_1*(2n-1)/(n-1)*N*(-2)/(r)^3 + \alpha_2 * [-(n-1)*(-1)*(r)^2/N*\ln(n)]$$
$$= 2\ \alpha_1 N[2n-1/ (n-1)]*1/(r)^3+ \alpha_2(n-1)/N\ln(n)*(r)^2$$

Since $\alpha_{1,}\ \alpha_2 >0, r>2$ and $n\geq 2$, the second derivative term $d^2T/dr^2>0$. Hence the weighted cost function $\alpha 1 * S + \alpha 2 * C$ is a convex function of r, and has a unique value of 'r' that yields the minimum value for the weighted total cost. The minimum point is computed as the solution to the equation, dT/dr = 0.

$$= -\alpha_1*(2n-1)/ (n-1)*N*1/(r)^2 + \alpha_2 * [1-(n-1) * 1 / (N*\ln(n)*(r)] = 0.$$
$$= \alpha_2 (n-1)\ N\ln(n)r^2 - \alpha_2(n-1)^2r- \alpha_1(2n-1)N^2\ln(n) = 0.$$

The above equation is a quadratic equation in r.

The solution is,

$$r = [1/N\ln(n) \pm {}^1/_2 * [1/N^2\ln^2(n) + 4\ \alpha_1/\ \alpha_2(2n-1)/(n-1)*N^{1/2}]/2$$

Letting $\alpha = \alpha_1/\alpha_2$,

The equation becomes,

$$r = 1/2N\ln(n) \pm {}^1/_2 * [1/N^2\ln^2(n) + 4\alpha(2n-1)/(n-1)*N\ ]^{1/2}$$

Hence, to compute the exact value of 'r', a function can be defined by the triplet (N, n, α). This can also be interpreted by considering T as Pareto Curve of storage Versus Communication for different values of 'r'. Every point on this smooth curve is an optimal point for a given set of triplet (N, n, α). For large values of N, the optimal value of 'r' can be computed by the approximation.

$$r \sim [2\ \alpha\ (2n-1)/(n-1)*N]^{1/2}$$

This section has briefly discussed the feasibility of designing the optimal sub- group size based on the sub-linear approach and using the mathematical theory.

This section discusses some of the theorem that can be applied for the design of the key tree. As discussed earlier, minimization of Key Storage with Communication Constraint is a Constraint Optimization Problem as the Storage Vs Communication is a Pareto Curve**.** Hence, it may be defined as a multi-objective optimization model which can also be solved using heuristics.

IV. CONCLUSION

This paper briefly discussed some significant applications of secured group communication and the challenges in secured group communication. In order to maintain the secrecy of communication the virtual structures are designed and two important overheads are observed namely, storage and communication. The combined overhead minimization is a constraint optimization problem and the possible mathematical approach behind the optimum key tree parameter design is discussed. It is also presented that the problem of on optimum key tree is a multi-objective model which can be solved through heuristic approaches.

REFERENCES

[1] Balenson D., McGrew D., and Sherman A., "Key management for large Dynamic groups: One-way function trees and amortized initialization", IEEE Selected Areas in Communication, Special Issue on Middleware, Vol. 17, pp.1614-1631, August 1999.

[2] Ballardie C., "Scalable Multicast Key Distribution", RFC 1949, May 1996, http://info.internet.isi.edu/in-notes/rfc/files/frc1949.txt.

[3] Banerjee S., and Battarcharjee B., "Scalable Secure Group Communication over IP Multicast", JSAC Special Issue on Network Support for Group Communication", Vol. 20, No. 8, pp. 1511-1527, October 2002.

[4] Boyd C., "On Key Agreement and Conference Key Agreement", In ACISP: Australian Conference on Information Security and Privacy, Springer-Verlag, pp. 294-302, 1997.

[5] Burmester M. V. D., and Desmedt Y., "A Secure and Efficient Conference Key Distribution System", Advances in Cryptography –EURO CRYPT"94, Vol. 950, Lecture Notes in Computer Science, Springer-Verlag, pp.275-286, 1995.

[6] Canetti R., Malkin T., and Nissim K., "Efficient Communication Storage tradeoffs for Multicast Encryption", Conference Proceedings EUROCRYPT 99, PP.456-470, 1999.

[7] Canetti R., Garay J., Itkis G., Micciianancio D., Noar M and Pinkas B., "Multicast Security: a Taxonomy and some efficient constructions", Proceedings of IEEE INFOCOM '99, Vol. 2, pp. 708-716, March 1999.

[8] Celik and A Datta, "A Scalable Approach for Subscription Based Information Commerce", In Proceedings of the 2nd International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems, Milpitas, CA, June 2000.

[9] Chang I., Engal R., Kandlur D., Pendarakis D and Saha D., "Key Management for Secure Internet Multicast using Boolean Minimization Techniques", IEEE INFOCOM, New York, March 1999.

[10] Chiou G. And Chen W., "Secure Broadcasting using Secure Lock", IEEE Transactions on Software Engineering, Vol. 15, No. 8, pp. 929-934, August 1989.

[11] Chung Kei Wong., Mohammed Gouda and Lam S. Simon, "Secure Group Communication using Key Graphs", IEEE/ACM Transactions on Networking, Vol. 8, No. 1, pp. 16-30, February 2000.

[12] Cover T. M. and Thomas J. A., "Elements of Information Theory", Wiley-Interscience, 1991.

[13] Hardjono T., Cain B., and Doraswamy N., "A Framework for Group Key Management for Multicast Security," IETF Internet draft, 1999.

[14] Harney H. And Muckenhirn C., "Group Key Management Protocol (GKMP) Architecture", RFC 2094, July 1997.

[15] Indrakshi Ray and Indrajit Ray, "Using Compatible Keys for Secure Multicasting in E-Commerce", Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS'02), 2002.

[16] Ingemarsson I. And Tang D. T. and Wong C. K., "A Conference Key Distribution System", IEEE Transactions on Information Theory, Vol. 28, No. 5, pp. 714-720, September 1982.

[17] Kim Y., Perrig A. and Tsudik G., "Communication Efficient Group Key Agreement", Proceedings of IFIP SEC 2001, June 2001.

[18] Lukasz Opychal and Atul Prakash., "Secure Distribution of Events in Content-Based Publish- Subscribe Systems", Security 2001 Conference Proceedings, pp. 281-296, 2001.

[19] Mathew J. Moyer, Josyula R. Rao and Pankaj Rohtagi, "A Survey of Security Issues in Multicast Communications", IEEE Network, pp. 12-23, November/December 1999.

[20] McGrew d. A., AND Sherman A. T., "Key Establishment in Large Dynamic Groups using One-Way Function Trees", Technical Report No. 0755, TIS Labs at Network Associates, Inc., Glenwood, MD, 1998.

[21] Michael Steiner, Gene Tsudik and Michael Waidner., "Cliques: A New Approach to Group Key Agreement", Proceedings of IEEE International Conference on Distributed Computer Systems, May 1998.

[22] Mingyan Li., Poovendran R., and Berenstein C., "Optimization of Key Storage for Secure Multicast", Proceedings of 2001 Conference on Information Sciences and Systems, 2001.

[23] Mingyan Li., Poovendran R., and Berenstein C., "Design of Secure Multicast Key Management Schemes with Communication Budget Constraint", IEEE Communications Letters, Vol. 6, No. 3, pp. 108-110, 2002.

[24] Oppliger R., and Albenese A., "Distributed Registration and Key Distribution (DiRK)", 12th International Conference on Information Security, 1996.

[25] Perrig A., Song D. and Tygar., "ELK, A New Protocol for Efficient Large Group Key Distribution", Proceedings of IEEE Symposium on Security and Privacy, pp. 247-262, 2001.

[26] Peyravian M., Matyas S. M., Zunic N., "Decentralized Group Key Management for Secure Multicast Communications", Computer Communications, Vol. 22, pp. 1183-1187, 1999.

[27] Radha Poovendran., John S. Baras., "An Information Theoretic Approach for Design and Analysis of Rooted Tree Multicast Key Management Schemes", IEEE Transactions on Information Theory, Vol. 47, No. 7, pp. 2824-2835, November 2001.

[28] Ralph Wittmann., Martina Zitterbart., "Multicast Communication Protocols and Applications", Morgan Kaufman Publishers, 2001.

[29] Stenier M., Tsudik G. And Waidner M., "Diffie-Hellman Key Distribution Extended to Group Communication", Proceedings of the 3rd ACM Conference on Computer and Communications Security, New York, pp. 31-37, 1996.

[30] Stenier M., Tsudik G. And Waidner M., "Key Agreement in Dynamic Peer Groups", IEEE Transactions on Parallel and Distributed Systems, Vol. 11, No. 8, pp. 769-780, August 2000.

[31] Sun B., Trappe W., Sun Y. And Liu K. J. R., "A Time Efficient Contributory Key Agreement Scheme for Secure Group Communications", Proceedings of IEEE International Conference on Communication, Vol. 2, pp. 1159-1163, 2002.

[32] Sun B., Trappe W., Sun Y. And Liu K. J. R., "A Efficient Key Management Scheme for Secure Wireless Multicast", Proceedings of IEEE International Conference on Communication, Vol. 2, pp. 1236-1240, 2002.

[33] Suvo Mittra., "Iolus: A Framework for Scalable Secure Multicasting", Proceedings of ACM SIGCOMM, pp. 277-288, 1997.

[34] Tsudik G., Kim Y., Perrig A., "Simple and Fault Tolerant Key Agreement for Dynamic Collaborative Groups", Proceedings of the 7th ACM Conference on Computer and Communications Security, November 2000.

[35] Wade Trappe., Jie Song., Radha Poovendran., ray Liu K. J., "Key Distribution for Secure Multimedia Multicasts via Data Embedding", Proceedings of IEEE Conference ICASSP'01, pp. 1449-1452, May 2001.

[36] Wade Trappe., Wang Y., and Liu K. J. R., "Establishment of Conference Keys in Heterogeneous Networks", Proceedings of IEEE International Conference on Communications, Vol. 4, pp. 2201-2205, 2002.

[37] Wade Trappe., Jie Song., Radha Poovendran., Ray Liu K. J., "Key Management and Distribution for Secure Multimedia Multicast", IEEE Transactions on Multimedia, Vol. 5, No. 4, pp. 544-557, 2003.

[38] Wallner D. M., Harder E. C., Agee R. C., "Key Management for Multicast: Issues and Architectures", Internet Draft, <draft-wallner-key-arch-01.txt>, 1998.