ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Study of Multicast Key Distribution with Reduced Method

Sarita K. Tiwari 1, *Jayant P. Mehare 2*

1,2 Computer Science and Engineering

G H Raisoni College of Engineering and Management

Amravati, India

Abstract— many emerging web and Internet applications are based on a group communications model. Thus, securing group communications is an important Internet design issue. The Key Distribution is major problem of communication and network security. Group communication can benefit from IP multicast to achieve scalable exchange of messages. However, there is a challenge of effectively controlling access to the transmitted data. IP multicast by itself does not provide any mechanisms for preventing no group members to have access to the group communication. In this paper, we present new method for making scheme for efficient computation. In which we include MDS code which is related to the problem of efficient information updates. We also include the efficient re-keying of large groups with dynamic membership: minimizing the overall time it takes for the key server and the group members to process the re-keying message. Specifically, we concentrate on re-keying algorithms and minimize the longest sequence of encryptions and decryptions that need to be done in a re-keying operation, then we provide an optimal schedule of re-keying messages. We propose a new scheme for a scalable multicast key distribution scheme. It focuses explicitly on the issue of snowballing member removal and presents an algorithm that minimizes the number of messages required to distribute new keys to the remaining group members

Index Terms—MDS Algorithm, Rekeying Multicasting, Group Key Management, Key tree, Group Controller, Complexity

I. INTRODUCTION

Multicast is an effective method for distributing information to multiple users in a group communication; it reduces the consumption of network re-sources .Multicast is supported on the internet, or via satellite communication, wireless network, sensors etc., in multicast group communication, all the authorized members share a session key, which will be changed dynamically to ensure forward and backward secrecy referred as "group rekeying".

Traditional networking depends heavily on physical cables or reliable communication channels to pro-vide end-to-end network paths, and with moderate round-trip times and small packet loss probabilities (Zhu et al., 2009). However, with some new emerging networking technologies such as satellite, sensor and vehicle communication networks technology, traditional networks fail to perform well as the new technology has a very long delay network path and possible link distributions (Bhutta et al., 2009)[2].The goal is to actually communicate, i.e. transfer information from one party to another, we also need to keep an eye on practicality. Usually we will assume that any party involved can run polynomial time and space algorithms, no matter whether we are talking about the legitimate parties or an adversary[1].In this paper, the hierarchical key distribution algorithm (or, scheme), which is regard-ed as the most efficient category of key distribution architectures in term of efficiency and scalability is provided.

One of the most efficient approaches to en-sure confidentiality of group communications is employing a symmetric key encryption scheme. But before the sender encrypts and transmits the data over a group communication channel to a group of privileged users, a shared key called group key must be established among them [4]. Group key establishment can be subdivided into group key distribution (GKD) and group key exchange (or group key agreement). Two parallel lines of research, commonly referred to as broadcast encryption (BE) [6] and multicast key distribution (MKD) (multicast encryption), have been established to study the GKD problem. This paper only focuses on multicast key

ISSN: 2321-9653

distribution protocols. To prevent a new member from decoding messages exchanged before it joins a group, a new group key must be distributed to the group when a new member joins. This security requirement is called group backward secrecy [7]. On the other hand, to prevent a departing member from continuing access to the group's communication (if it keeps receiving the messages), the key should be changed as soon as a member leaves. This security requirement is called group forward secrecy [7]. To provide both group back-ward secrecy and group forward secrecy, the group key must be updated upon every membership change and distributed to legitimate members. This process is referred to as immediate group rekeying in literature.

II. MAXIMUM SEPARABLE CODES

Wherever MDS (Maximum Distance Separable) codes are a class of block error control codes that meet the Singleton Bound, i.e., d = n - k + 1 for an (n, k, d) code over GF(q'). A k-symbol message block m = m1 …. mk is expanded to an n-symbol codeword block c = c1……cn [1][10]. Using a proper erasure decoding algorithm, the message block m can be perfectly recovered from any k symbols of the codeword c. We choose the ReedSolomon codes (RS) [9] as the MDS codes, since it isthe most widely used MDS code.For a q-ary (n,M,d)-code, the Singleton bound states that

M £ qn-d+1.This implies that for a linear [n,k]-code we must have qk £ qn-d+1,from which it follows that k £ n - d + 1, or as we prefer to write it,d £ n - k + 1.A linear code which meets this bound is called a Maximum Distance Separable (MDS) code .Since error correcting capability is a function of minimum distance, we see that for given dimensions n and k, the MDS codes are those with the greatest error correcting capability.

2.1Characterizing MDS Codes

There are several useful characterizations of MDS codes. The simplest being;

Proposition 1: A q-ary [n,k] linear code is an MDS code if, and only if, the minimum non-zero weight of any codeword is n - k + 1 the trival example are as follows:

1. For any n and q, V[n,q], a linear [n,n]-code, is an MDS code, since the minimum non-zero weight of any codeword is 1.
2. Another trivial example for any n and q, is the cyclic code generated by the all 1's vector. This is an [n,1]-code with minimum weight n.
3. Yet another trivial MDS code (for any n and q) is obtained by taking all the vectors of even weight in V[n,q]. It is not difficult to see that this is an [n,n-1] code (linear subspace) with minimum distance 2.
4. MDS codes which are not one of these three examples are called nontrivial MDS codes.

2.22.2 Maximum Distance Separable Codes Algorithm

It mainly consist of three parts, they are as follows:

a) Initializing Group controller.

b) Subscribing new members.

c) Applying the procedure of Re-Keying whenever member leaves the group.

Steps for the Algorithm:

Step I : GC Initialization by constructing codeword C using MDS.
Step II : Applying One-Way Hashfunction
Step III : H(x)=y, propoerty of Hashfunction
Step IV : Subscribing new member
Step V : Ji= +ve integer ji!=jk
Step VI : Select Si
Step VII : Applying the procedure of Re-Keying whenever member leaves the group.
Step VIII: Cj=H(Si+r)
Step IX : Member j every 'n' members in the group calculates these own codeword C1 C2.....Cn

Fig.1: *MDS Code Algorithm*

III. PROPOSED WORK

We study how a multicast group can efficiently be distributed in computation. We adopt a common model where session keys are issued and distributed by a 'central group controller'(GC). The resources needed for the GC to distribute session keys to group members include communication, storage and computation resources. We propose a new multicast key distribution scheme whose computation complexity is significantly reduced. Instead of using conventional encryption algorithms, the scheme employs MDS (Maximum Distance Separable) codes, a class of error control codes, to distribute multicast key dynamically. This scheme drastically reduces the computational load of each group member compared to existing schemes employing traditional encryption algorithms. Such a scheme is desirable for many wireless applications where portable devices or sensors need to reduce their computation as much as possible due to battery power limitations. Easily combined with any key-tree based

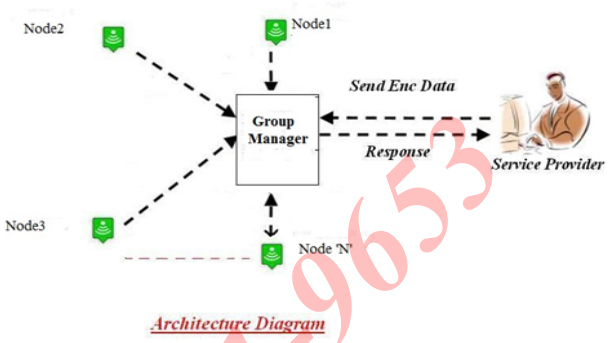
schemes, this scheme provides much lower computational complexity while maintaining low and balanced communication complexity and storage complexity for secure dynamic multicast key distribution. For a dynamic multicast group, a session key is issued by a GC. Using this session key, the GC can establish a secure multicast channel with the authorized group members. Every time group memberships change because of join or leave of some group members, the GC reissues a new session key, which is independent of all the old session keys. This rekeying procedure ensures security of current session and all of the old sessions i.e., the newly joined members cannot recover communications of the old sessions and old members who left the group cannot access the current session. The complexity of the rekeying operation is asymmetric between a new member's join and old member's leave. When a new member joins, the GC can easily multicast the new session key encrypted by the cur-rent session key to all current members, followed by a unicast to the new member to send the new session key encrypted by a predetermined encryption key shared between new member and GC. However when an old member leaves, the current session key cannot be used to convey the new session key in-formation securely, since it is also known to the old member.

For implementing this project here we defined Four Module which are as follows:

1. Data Owner
2. Access Points
3. End User (Nodes)
4. Key Pre distribution

Data Owner

The Data Owner is the service provider which sends data request messages to the nodes via a stationary access node. These data request messages from the service provider will initiate the stationary access node to trigger all nodes, which transmit their data to the requested end user (node). For group communications, the server distributes to each member a group key to be shared by all members of the group, distributing the group key securely to all members requires messages encrypted with individual keys (a computation cost proportional to group size). Each such message may be sent separately via unicast. Alternatively, the messages may be sent as a combined message to all group members via multicast. Either way, there is a communication cost proportional to group size.



Architecture Diagram

Access Points

The Access Points act as authentication access points for the network and trigger r nodes to trans-mit their aggregated data to the End user. A sp sends data request messages to the corresponding nodes via a stationary access node(Group Leader). The end user's data request messages will initiate the stationary access node to trigger all nodes to transmit their aggregated data to the requested end user.

End User (Nodes)

The End Users are one who is authorized the da-ta by the key pair which is generated by the sp while sharing the data. The nodes are connecting to speci-fied group leader in the group manager in router and getting data from the sp via specified router. Whenever a new member is authorized to join the multicast group for the first time, the GC sends it (using a secure unicast) a session key. Once a session key is distributed to the group, any mem-ber can calculate the secret information that other members in the same group hold.The Login Module is used for the Newly joined users to send a request to the Group Controller and it is used for to retrieve the Private keys after the Group Controller assign keys to the new users. The user login the group to enter the user Id and Private Key.

Key Pre-distribution

Many network protocols utilize the existence of disjoint paths (e.g., perfectly secure message trans-mission or multi-path key establishment), but do not address how a node actually determines these paths in the presence on an adversary. The system is investigated what assumptions are

necessary to gather information about the local network topology when adversarial nodes are present and capable of lying about their identity or neighbors in the net-work. These assumptions are practical, and realiza-ble through existing tools such as combinatorial key pre-distribution, localization. The protocols ensure that, except with small probability, if node accepts a path through the network as valid, then each node along that path must be telling the truth about its identity and nodes it can communicate with, so long as a majority of honest nodes are present in the network at each point decisions are made. This module generates the session keys as well as the secured keys used by the members to communicate with the GC(group controller). The private keys are generated using MDS method. The GC (Group Con-troller) sends number of group members to the KGC (Key Generation Center). The keys are generated by the KGC and submitted to the GC. In session key generation, initially sixteen decimal digits are gen-erated by using random number generation method .Then each decimal digit is split and compared with pre determined binary format.

IV. CONCLUSION

We have presented a study on some of the proposed efficient multicasting key distribution with reduced computation for improving the overall efficiency of the key distribution and secure multicasting.In this paper we present the module who help to achieve the goal of computation complexity and MDS Algo-rithm describe for multicasting key distribution By Combing Scheme we can reduce complexity. This schemes were undertaken according to storage re-quirements at both group controller and group members and the number of updates in case of a single leave or multiple leaves.

ACKNOWLEDGMENT

I take this opportunity to thank respected Prof. Jayant P. Mehare Sir, my seminar guide for gener-ous assistance. I am immensely grateful to Hon. HOD Mr. N. R. Chopde Sir, for his encouragement and Guidance. I extend my sincere thanks to our college library staff and the entire staff member for their valuable assistance. I am also thankful to my fellow college us for their help and important sug-gestions.

REFERENCES

[1] Lihao Xu, Cheng Huang, "Computation Effi-cientMulticast Key Distribution," IEEE Trans. Paral-lel And Distributed Systems, Vol 19, No. 5, May 2008.

[2] Deepika Rani K, G. Praveen Babu "Computation-ally effecient group re-keying for time sensitive ap-plications" IJCER Mar-Apr 2012 Vol. 2 Issue No.2 ISSN: 2250–3005

[3] S. Benson Edwin Raj , J. Jeffneil Lalith" A Novel Approach for Computation-Efficient Rekeying for Multicast Key Distribution" IJCSNS VOL.9 No.3, March 2009

[4] S.Sasikala Devi, Dr.Antony Selvadoss Thanama-ni "An optimized approach for Multicast Rekeying using MDS code on PFMH tree" IEEE International Conference on Computational Intelligence and Computing Research 2010

[5] Varalakshmi. R, V. Rhymend Uthaiaraj." Mul-ticast Key Management Using Logic Design" Inter-national Journal Of Multidisciplinary Research Vol.1 Issue 7, November 2011, ISSN 2231 5780

[6] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly Secure Key Dis-tribution in Dynamic Conferences," Advances in Cryptology—Proc. Workshop Theory and Applica-tion of Cryptographic Techniques (EUROCRYPT '93), pp. 471-

[7] C.K. Wong, M. Gouda, and S.S. Lam, "Secure Group Communications Using Key Graphs," Proc. ACM SIGCOMM '98, Sept. 1998.

[8] J. Bloemer, M. Kalfane, M. Karpinski, R. Karp, M. Luby, and D. Zuckerman, "An XOR Based Erasure-Resilient Coding Scheme," Technical Report TR-95-048, Int'l Computer Science Inst., Aug. 1995.

[9] L. Xu and J. Bruck, "X-Code: MDS Array Codes with Optimal Encoding," IEEE Trans. Information Theory, vol. 45, no. 1, pp. 272-276, Jan.1999

[10] M. Abdalla, Y. Shavitt, and A. Wool, "Towards Making BroadcastEncryption Practical," IEEE/ACM Trans. Networking, vol. 8, no. 4,pp. 443-454, Aug. 2000.

[11] M. Blaum, J. Bruck, and A. Vardy, "MDS Array Codes withIndependent Parity Symbols,"IEEE Trans. Information Theory,vol. 42, no. 2, pp. 529-542, Mar. 1996.

[12] R. Blom, "An Optimal Class of Symmetric Key GenerationSystems," Advances in Cryptology—Proc. Workshop Theory andApplication of Crypto-graphic Techniques (EUROCRYPT '84),pp. 335-338, 1984.

[13] R.Canetti,T. Malkin, K. Nissim, "Efficient Communication-Storage Tradeoffs for Multicast Encryption", Advances in Cryptology—Proc. Int'l Conf. Theory and Application of Science, 1989.