Secured, Authenticated Communication Model for Dynamic Multicast Groups

Prof J.ASHOK [1]
Professor and Head
Department of IT,
GCET, Hyderabad, India.

KOMATI SATHISH [2]
Associate Professor &Head
Department of H&S
NITS, Hyderabad

Y. RAJU [3]
Associate Professor
Department of IT
GCET, Hyderabad, India.

Abstract

Secure Multicast networks forms the backbone for many web and multimedia applications such as Interactive TV, Teleconference etc. The main challenge for secure multicast is scalability, efficiency and authenticity. A communication model is proposed for dynamic multicast groups which is secure and authenticated. In this scheme a group is established and the text messages are transmitted between the users of the group. The proposed scheme is secured, authenticated and supports communication between dynamic multicast groups.

1. Introduction

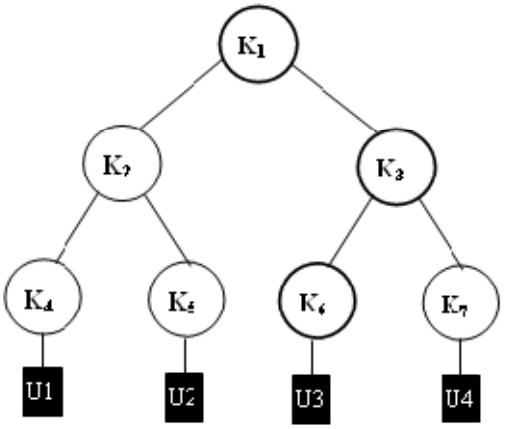
Almost all types of group applications such as interactive TV, Teleconference, Software updates, etc. can benefit from IP multicast, which reduces the server overhead and bandwidth usage by enabling source to send a single copy of message to multiple receivers.

The main problem in secure multicast is access control for making sure that only legitimate members of multicast group have access to the group communication. The security algorithms applicable to unicasting (one to one) environment cannot be applied in multicast groups. The commonly used technique in secure multicast is to maintain a group key that is known to all users in the multicast group, but is unknown to others outside the group. Each time a member either joins or leaves the group, the group key has to be refreshed. The members of the group should be able to compute the new group key efficiently, guaranteeing forward and backward secrecy simultaneously. In a dynamic secure multicast, the group key need to be refreshed very frequently. Once a communication group is formed, the members in a group can send/receive messages from other members of same/different groups. To send a message, a user need to login to the group, compose a message and send to a user/users. The message is generated as a text file and is transmitted to the receiver user/users through an IPC channel. The receiver can view the message, forward to other users or delete it. To transfer text messages between the users socket API can be used. For transmission of messages, each user is provided with a mailbox, which is identified by its user-id.

2. Analysis

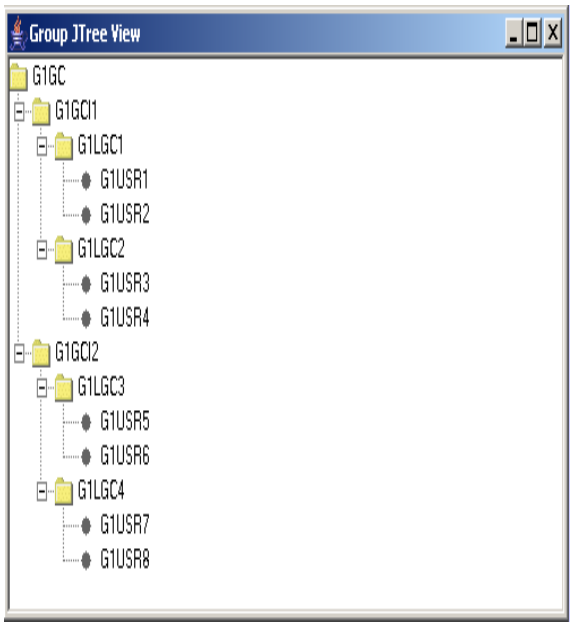
There are several schemes proposed for secure multicast. Iolus approach proposed the notion of hierarchy subgroup for scalable and secure multicast. In this method, a large communication group is divided into smaller subgroups. Each subgroup is treated almost like a separate multicast group and is managed by a trusted group security Intermediary (GSI). GSI connects the subgroup and shares the subgroup key with each of the subgroup members. GSI acts as message relay and key translators between the subgroups by receiving the multicast message from one group, decrypting them and then re-multicast them to the next subgroup. The GSIs are also grouped in a high-level group that is managed by a group security controller (GSC). Although this scheme is scalable but each GSI need to decrypt and encrypt the messages between two subgroups using the respective subgroup keys which degrades the performance of this scheme.

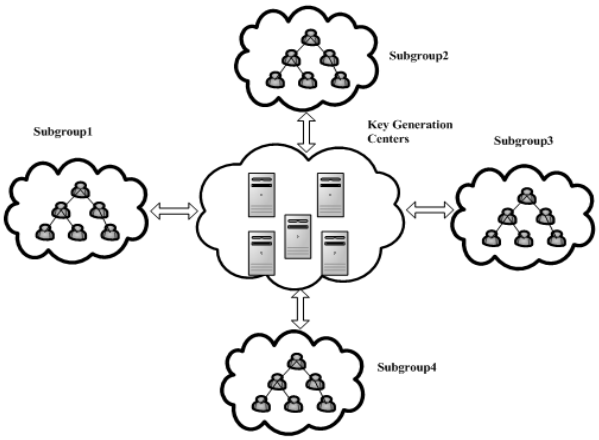
The logical key hierarchy (LKH) is an efficient approach that supports dynamic group membership. This method was proposed by Waller and Wong individually. In this approach, the group controller (GC) maintains a logical key tree where each node represents a key encryption key (KEK). The root of the key tree is the group key used for encrypting data in group communications and it is shared by all users. The leaf node of the key tree is associated with a user in the communication group. Each user secretly maintains the keys related to the nodes in the path from its leaf node to the root. The set of keys that a member knows is known as the key path. When a member leaves the group, all the keys that the member knows, including the group key and its key path is to be refreshed. When a member joins the group, GC authenticates the member and assigns it to a leaf node of the key tree. The GC will send the new member all the keys from its corresponding leaf node to the root (Configures the new member).



3. Our Scheme

Our scheme is secured & authenticated communication model for dynamic multicast groups. A large communication group is divided into several smaller subgroups. Each subgroup is independently managed by the subgroup controller (SGC). In our scheme, even though a subgroup controller fails, it does not affect its subgroup, because every user in the subgroup can act as the subgroup controller. This is an amazing feature especially for the groups that has a highly dynamic membership change in mobile and ad hoc networks. The keys used in each subgroup of the key generation centers (KGCs) in parallel. All the members in the same subgroup can compute the same subgroup key though the keys for them are generated by different KGCs. This is a desirable feature for large networks as it reduces the workload on a single entity. In this scheme all users in a group are maintained in form of a tree, where each node represents a user, root node represents group controller (GC), for a sub-tree its node represents a sub-group controller (SGC). GC acts like administrator of a group, it accepts requests from users for join/leave group, update users, Re-keying etc. The SGC or SGI also acts like message relay i.e., all messages to/from a sub-group has to be through SGC/GCI. The GC is responsible to maintain a group and the keys of the users of a group. Each user in a group is identified by a user id which is an alphanumeric string, also known as user name.





4. Algorithm

The basic idea of our scheme is the usage of an identity tree, where each node in the tree has an identity. A node in the identity tree is also associated with a key generation key (KGK) which is used for generating a parent key. The root node's KGK is used as the group key.

Each SGC constructs an identity tree and gives it to the KGCs. Given a nodes N_i user id, KGC generates the keys for the nodes by ECC algorithm. The generated key is then encrypted using KGK of the user through DES algorithm and encrypted key is transmitted to the user. The user decrypts the key using its KGK, which provides security to the key and saves it in its key ring. Whenever a new user joins the group a new node is added to the group tree with user name as its identity and GC/SGC requests KGC to refresh the group key and also to generate KGK for the new user. Whenever a user requests to leave the group the GC/SGC removes the node

corresponding to user from group tree and KGC is request to re-key.

Whenever a user wants to send a message to group it generates the message as a text file, it is encrypted using the RSA algorithm and encrypted text file is sent to the SGC/GCI of the subgroup to which it belongs through TCP/IP connection. SGC/GCI of sub tree to which sender belongs establishes a TCP/IP connection with SGC/GCI of sub tree to which receiver belongs and sends the text containing the encrypted message through socket API. The SGC/CGI of receiver establishes a TCP/IP connection with receiver and transmits the text file to it. The encrypted text file is decrypted and is added to the mailbox of user. The user can sign in and view its messages. For a user to sign-in a secret code is generated by GC and provided to the user when it joins the group.

5. Conclusion

This scheme is secured and authenticated. The mechanism is secured by using RSA algorithm for message encryption/decryption, authenticated as each message contains the identity of the user. The KGC supports large and dynamic multicast groups. Maintaining the users in form of a tree makes this scheme scalable and efficient.

6. References

[1] Liming Wang and Chuan –Kun Wu, " Efficient Key Agreement for Dynamic and Large Multicast Groups", International Journal of Network Security, Institute of Software, Chinese Academy of Sciences, Vol.3, No.1, PP.8–17, July 2006

[2] P.S.L.M. Barreto, H Y Kim and Scott "Efficient algorithms for pairing-based cryptosystems" in CRYPTO 2002, LNCS 2442.

[3] D Bonch and M Franklin, "Identity-based encryption fron weil pairing", in CRYPTO 2001, LNCS 2139.

[4] R Canetti, J Garay, G Itkis, K Micciancio, M Naor and B Pinkas, "Multicast security: a taxanomy and some efficient constuctions", in INFOCOM 1999.

[5] R Canetti, S Halevi and J Katz, "A forward secure public key encryption scheme", in Eurocrypt 2003, LNCS 2656.

[6] I Chang, R Engel, D Pendarakis and D Saha, "Key management for secure Internet multicast" using Boolean function minimization techniques", in INFOCOM 1999.

7. Biography

Prof J.Ashok is currently working as Professor and Head of Information Technology at Geethanjali College of Engg. & Technology, Hyderabad, A.P, INDIA. He has received his B.E. Degree from Electronics and Communication Engineering from Osmania University and M.E. with specialization in Computer Technology from SRTMU, Nanded, INDIA. His main research interest includes neural networks, data retrieval process and Artificial Intelligence. He has been involved in the organization of a number of conferences and workshops. He has been published more than 30 papers in national and International journals and conferences. He is currently doing his Ph.D from Anna University and is at the end of submission.

Mr.Komati Sathish is currently working as Associate Professor and Head, department of Humanities & Science at Nagole Institute of Technology and Science Hyderabad, A.P, INDIA. He received his B.Sc.and B.Ed Degrees from kakatiya university,Warangal and Msc(Maths) from Osmania University ,Hyderabad INDIA. His main research interest includes network security, Data mining and ware housing and Database management system. Currently he is doing his M. Tech(CS) from Sri Indu College of Engineering and Technology,JNTUH, Hyderabad.

Mr.Y.Raju is currently working as Associate Professor in the department of IT at Geethanjali College of Engg. & Technology, Hyderabad, A.P, INDIA. He received his M.Tech.(CSE) from JNTU,Hyderabad INDIA. His main research interest includes Information Security, data mining and data ware housing and Bio Informatics.