A Survey on Key Management Techniques for Wired/Wireless Networks

S. Jabeen Begum
Research Scholar
Velalarcollege Of Engg.& Tech, Erode-12,
Tamilnadu, India.

Dr. T. Purusothaman
Associate Professor,
Dept. Computer Science & Engg.
Governmentcollege Of Tech,
Coimbatore -13, Tamil Nadu, India.

ABSTRACT
Providing key management schemes for large scale multicast groups has become a bottleneck due to many potential commercial applications on Internet such as stock quote and software distribution. For secure multicast communication, all the group members share a common key called as Secret Group Key. Since the member dynamics such as join or leave do not necessarily terminate the multicast session, it is important to update the Group key to all the valid members, so that the non-members do not have access to the future keys. Researchers have proposed several different approaches to the group key management. These approaches can be divided into three main classes: Centralized group key management protocols, Decentralized architectures and Distributed key management protocols. This paper surveys for both Wired and Wireless Networks.

KEYWORDS: Key management, group key, wired/wireless networks

1. INTRODUCTION
Data communication is the engineering discipline concerned with communication between computer systems. A computer network is any set of computers or devices connected with each other to exchange data. Many companies and institutions works have their own collection of workstations connected by Local Area Network (LAN). In case of group communication, that simplifies, building reliable efficient distributed systems. Distributed computer systems or a distributed system consists of hardware and softwarecomponents.The secure group communication abstract provides both point-point and multipoint communication. Applications like file sharing, online gaming, audio/video conferencing, virtual meeting and discussion forums are examples of systems which are organized as a Peer group. Group key management protocol must be secure, efficient and must meet the application needs. Security concerns is the group key which should not be easily known or deducible to an outsider. Group key management protocols must be scalable according to the application needs.The development of secure multicast is becoming more pertinent in wired networks, its implementation in mobile environments (wireless networks) is still in its infancy. Applications and services which are available in wired networks should also be made available in wireless networks and vice versa. There are similar expectations for providing secure and reliable communication in both environments. In case of wireless networks, to make greater utilization of resources in vicinity, it is important for nodes in MANET to be able to discover remote services seamlessly and carry out transactions with the service providers, while security is paramount to the success of the transaction. However all these processes are complicated by the fact that there is no fixed infrastructure and established administration. In MANET [11], each node can be a combination of service user, service provider and service directory, which caches the service providers in vicinity. Therefore a decentralized approach is required for maintaining service and information about service objects. Each node needs a local registry to effectively manage, advertise and discover services.

2. RELATED WORK

Categorization of Key Management Protocols

2.1. Centralized:
A central authority distributes group keys to group members. This central authority can be trusted third party or can be a group authority. Centralized key management [1], [3] is employed for controlling the entire group. Hence centralized key management tries to minimize storage requirements and computational power for both the client and the server. However the problem of single point failure remains existing.Protocols used in Centralized Key Management
The Group Key Management Protocol uses the KDC helped by the first member to join the group creates a Group Key Packet (GKP) that contains a group traffic encryption key (GTEK) and a group key encryption key (GKEK) [4] . The KDC sends a copy of the GKP whenever a new member wants to join the group. As all members know the GKEK, there is no solution for keeping the forward secrecy when a member leaves the group except to recreate an entirely new group without that member.In Logical Key Hierarchy, the KDC [5],[6] maintains a tree of keys. The nodes of the tree hold key encryption keys. The leaves of the tree correspond to group members and each leaf holds a Key Encryption Key associated with that one member. Each member receives and maintains a copy of the KEK associated with its leaf and the KEKs corresponding to each node in the path from its parent leaf to the root. For a balanced tree, each member stores at most (log 2 n)+1 keys, where (log 2 n) is the height of the tree.The One-way Function Tree an improvement in the hierarchical binary tree which reduces the size of the rekeying message from 2.(log2 n) to only (log2 n). The KEKs held by a node's children are blinded using a one-way function and then mixed together using a mixing function. The One-way Function Chain Tree has a different approach that achieves the same communication overhead. This scheme uses a pseudo-random-generator to generate the new KEKs rather than a one-way function and then it is applied only on user

removal. This scheme is known as the one-way function chain tree.

2.2. Decentralized

In the decentralized subgroup approach, the large group is split into small subgroups. Different controllers are used to manage each subgroup, minimizing the problem of concentrating the work on a single place. The Scalable Multicast Key Distribution making use of the trees built by the Core Based Tree (CBT) multicast routing protocol to deliver keys to a multicast group. Any router in the path of a joining member from its location to the primary core can authenticate the member since the router is authenticated with the primary core. Furthermore, there is no solution for forward secrecy other than to recreate an entirely new group without the leaving members.In Intra-Domain Group Key Management, there is a Domain Key Distributor (DKD) [6], [7] and many Area Key Distributors (AKD). Each AKD is responsible for one area. The group key is generated by the DKD and is propagated to the members through the AKDs The key managers (DKD and AKD) are placed in a multicast group, named All-KD-group. The All- KD-group is used by the DKD to transmit the rekey messages to the AKDs. All areas in the domain use the same group key. Therefore, data packets do not need to be translated when passing from one area to another. Moreover, if an AKD is unavailable no members in that area are able to access the group communication, since they will not be able to access AKDs from other areas.In case of wireless networks, existing networks depends on dedicated servers providing centralized basic network services like naming, authentication and timing etc. For instance, conventionally there are DHCP [8] and DNS services in a typical network, while supporting this kind of critical network services is beyond the capability of existing P2P networks. Our approach is to build foundations from P2P system, but take advantages of the hierarchical overlay structure contributed by MANET to provide decentralized network services.

2.3. Distributed

This approach is characterized by having no group controller. The group key can be either generated in a contributory fashion, where all members contribute their own share to computation of the group key, or generated by one member. Although it is fault-tolerant, it may not be safe to leave any member to generate new keys since key generation requires secure mechanisms, such as random number generators, that may not be available to all members. In Distributed Logical Key Hierarchy, the Group controller is completely abolished and the logical key hierarchy is generated among the members, therefore there is no entity that knows all the keys at the same time. This protocol uses the notion of subtrees agreeing on a mutual key. That is, two groups of members namely subtree L and subtree R, agree on a mutual encryption key. Assuming that member ml is to be L's leader and member mr is to be R's leader. Subtree L has subtree key kL and subtree R has subtree key kR. The Diffie–Hellman Logical Key Hierarchy uses a logical key hierarchy to minimize the number of key held by group members. The main difference here is that group members generate the keys in the upper levels using the Diffie–Hellman algorithm rather than using a one-way function. The key of each node is generated from its two children (k=αk1k2 mod p).In Conference Key Agreement protocol, conference key agreement (CKA) [2] where all group members contribute to generate the group key. The group key can be generated with a combining function: K = f (N1, h(N2), .. , h(Nn)), where f is the combining function, h is a one-way function, n is the group size and Ni is the contribution from group member i. The protocol specifies that n - 1members broadcast their contributions (Ni).

2.4. KEY MANAGEMENT PROTOCOLS

2.4.1. Ring Based Approach

In this protocol, members are organized into virtual rings, a member 'M' communicate with the member Mi+1 and member Mn with M1. Group communicates the key with n-1 rounds. Here each member comes up with a random number Ni.

2.4.2. Hierarchal Based Approach

Skinny Tree (STR) is distributed / contributory protocol which is primarily variations of the n-party Diffie- Hellman key exchange. Here, members of groups are organized at leaves of tree. Each leaf holds its secret key and calculates g ki and propagates towards its parent. Now a combined key from children's g ki and g ki +1 is calculated so at end group key is calculated at root. In case of membership change (join/leave) the tree is re-built consequently and hence all the members update the group key which is the root of the tree. Some of the protocols that supports both wired/wireless are Beller et al. [BCY91,92,93] , Beller-Yacobi protocol [BM98] [BY93], Aziz and Diffie protocol [AD94] [BM98] Park's protocol [BP98][P97], ASPeCT Protocol Lee et al. [LHYC98]. Protocols specifically for the group communication are Tree-Based Key Management, Group Key Management Using Key Graphs (KG), Group Key Management using Boolean Function Minimization Techniques (BFMT), HYDRA, DEP, HKT (Hybrid Key Tree), An efficient distributed key management for certification based on hierarchical clustering, Lazos et al.considered a hierarchical key management structure for energy-aware secure multicast group communication in MANETs based on geographic routing.

Key Agreement Protocols

The each group member contributes its share in forming of the new group key while dynamic occur in network. Some of the protocols that supports this concept are A Generic multi-party protocol proposed by Asokan and Ginzboorg [AG00] modified the generic two-party protocol called encrypted key exchange [BM92] and extended it into a multi-party protocol, Burmester and Desmedt's Protocol GDH.2 and extensions, The Hypercube Protocol and extensions.

3. CONTRIBUTION TO THIS ARTICLE KEY MANAGEMENT IN WIRED/ WIRELESS NETWORKS

The essential processes identified within a group key management are described as follows:

1. Formation of groups. Formation of a multicast group can be further divided into two processes:

3.1. Creation of multicast groups

At the network level, creation of a multicast group can be done by a host sending a request to a network using the Internet Group Management Protocol (IGMP).In return, the network kernel assigns a specific multicast address for the group . At this point, all the information related to a multicast group such as group membership policy, as well as the

cryptographic keys needed for a group communication, is determined.

3.2. Initial registration of group members

Once the interest to join a particular multicast group is determined, a host instructs the network that he wishes to receive data sent to a specific multicast group (at the application level, this is usually indicated by a host requesting a group service on the Internet). When that happens, it is considered that the host joins the group. From another perspective, any host who wishes to join a multicast group sends a join request to a group manager. Presuming that the host is granted permission to join the group, group related information, in particular the cryptographic keys needed for group communication, is exchanged between the group manager and the group member.

2. Generation and distribution of cryptographic keys.

3. A new member joins / existing member leaves

4. Rekeying

Aspects of Key Management

The main aspects of key management are the provision of the following basic key services:

1. Key generation - The generation of cryptographic keys for a particular cryptographic algorithm..

2. Key registration - The registration of cryptographic keys with entities. Registration of keys is usually done by a trusted registration authority.

3. Key certification - This applies to public key cryptography, to ensure the association of a public key with an entity.

4. Key distribution - The dissemination of cryptographic keys to the communicating entities. Key distribution can be performed using physical (or manual) techniques, or using a trusted third party such as a (KDC) or a key translation centre (KTC), where keys can be delivered to users by using other keys.

5. Key installation - The installation of a key prior to its use.

6. Key update (re-keying) - The ending of the use of one key and beginning of use of another key.

7. Key storage - The secure storage of cryptographic keys prior to use, for short-term use, or for back-up. For security reasons, keys are usually stored physically in a secure environment, for instance using tamper resistant hardware.

8. Key derivation - A special form of key generation, where a key is derived from other keys using some transformation process.

9. Key archiving - The provision of secure long-term storage for keys. Archived keys may be needed at a later time for generation of new keys or to verify certain claims after the key has expired.

10. Key revocation - The revocation of a key after key compromise is suspected, or known, or when it has reached its expiration date.

11. Key de-registration - Part of the key disposal process, a key association with an entity is removed. This is done by a key registration authority.

12.Key disposal - The disposal or destruction of a key that is no longer needed. This process includes all materials both physical and electronic documents associated with a key.

3.3. Key Distribution in Wireless Networks

In communication and network security of mobile ad hoc network, key distribution is one of the major problems. Key distribution refers to methods whereby a center will distribute secret information in such a way that specified privileged subsets of participants will be able to compute certain keys. Even though broadcast encryption could be used to send an encrypted message to a subset of participants, it is prone to security threats; since one participant is corrupted the whole group is corrupted. In this case, threshold broadcast encryption (TBE) becomes a better solution. It allows a center chooses (ad-hoc) a set of n decryption servers and a threshold t, and then broadcast an encrypted session key to a group in such a way that the session key can be recovered only if at least t decryption servers cooperate.

By combining the advantages of both identity-based encryption scheme and some secret sharing techniques, here a new TBE scheme, which is not only proved secure in the random oracle model, but also achieves the shortest ciphertext length. To the best knowledge, it is considered as the best solution but their scheme has the following problems: It is certificate based, so it needs more communication cost for transmitting the certificate for public key; the proposed scheme is robust and secure under chosen-ciphertext attacks based on Decisional Bilinear Diffie-Hellman (DBDH) assumption. Compared with the previously proposed TBE schemes, this scheme needs only one exponentiation computation, which makes it be more efficient than those schemes.

MANETs are expected to evolve as the basis for interpersonal communications with perhaps little or no reliance on centralized infrastructure. Such transient networks may be created on demand to facilitate communication between any two nodes (usually) using multiple hops - the nodes en route acting strictly as routers for this purpose. Mobility imposes restrictions on memory and processor requirements due to limited battery life. The ad hoc nature warrants schemes that could operate for extended periods without referring to a Trusted Authority (TA).

Additionally, any enabling scheme for security should be able to scale well. It introduces a novel key management scheme, RPS - Random Preloaded Subset key distribution - which satisfies all the above requirements. More specifically, RPS is an - secure -conference key pre-distribution scheme. The computational complexity of RPS would depend on the symmetric crypto primitives for one-way functions used to obtain the session keys from the shared keys. No finite field arithmetic is necessary. In an ID-based encryption scheme, a master public key/secret key is generated by private-key generation service (PKG) and the master public key is assumed to be known by everyone. Once this master public key is established, arbitrary identities may be used as public keys for the scheme.

3.4. Key Distribution in Wired Networks

Key distribution system focus on the construction of a scalable key distribution scheme while multicast delivery system focuses on the packet transmission over the multicast bone. Group members can globally share a common group key via the key distribution scheme and then encrypted

packets can be delivered to a group member via multicast data delivery system.Key distribution system operates over a transporting network. In wired network, the root node is a key generator, which is responsible for generating and renewing the common group key. Key generators can be the multicast group creators, one of the group members or a trusted third party. Intermediate nodes members referred as key distributors are the network devices or group members with the capability of assisting the key management operations. Each leaf node represents a subset of group members that attaches to the same key distributors.In the key transporting network, each entity is associated with parameters. The key generator maintains parameters of all the other entities and holds secret information, for generating the common group key. Key distribution establishes a globally shared common group key for secure group communications. Instead of transmitting the determined common group key in the key transporting network only the parameters for deriving the common group key are delivered. Along the path from key generator to legitimate group members, each key distributor performs a transformation on the received data and forwards the result to a next key distributors and sub group members.

4. CONCLUSION

In this article, we presented a survey in the secure group communication area, particularly regarding the secure distribution and refreshment of keying material. We reviewed several proposals, placing them into three main classes: group key management protocols, which try to minimise the requirements of KDC and group members; decentralized architectures, which divide large group in smaller subgroups in order to make the management more scalable; and finally, the distributed key management protocols, which gives all members the same responsibilities. Every class has its particularities, presenting different features, requirements and goals. Our analysis made it clear for both in case of wired or wireless networks; there is no unique solution that can achieve all requirements. While centralized key management schemes are easy to implement, they tend to impose an overhead on a single entity.

5. REFERENCES

[1] Paul Judge and MostafaAmmar, "Security Issues and Solutions in Multicast Content Distribution: A Survey" , Georgia Institute of Technology, 0890-8044/03/$17.00 © 2003 IEEE IEEE Network ¥ January/February 2003

[2] Xiaozhou Steve Li, Yang Richard Yang, Mohamed G. Gouda, Simon S. Lam, "Batch Rekeying for Secure Group Communications", Department of Computer Sciences University of Texas at Austin Austin, TX 78712-1188.

[3] Yongdae Kim, AdrianPerrigy, Gene Tsudik, "Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups" Copyright 2000 ACM 1-58113-203-4/00/0011

[4] Kin-Ching Chan and S.-H. Gary Chan, "Distributed Servers Approach for Large-Scale Secure Multicast", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 20, NO. 8, OCTOBER 2002.

[5] Michael Steiner, Gene Tsudik, Member, "Key Agreement in Dynamic Peer Groups" , IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 11, NO. 8, AUGUST 2000.

[6] Wei-Chi Ku Shuai-Min Chen, Fu JenCatholicUniversity, "An Improved Key Management Scheme for Large Dynamic Groups Using One-Way Function Trees".

[7] RiteshMukherjee ,J.William Atwood, "Proxy Encryption For Secure Multicast Key Management" , Proceedings of the 28th Annual IEEE International Conference on Local Computer Networks (LCN'03) 0742-130/03 $ 17.00 © 2003 IEEE Proceedings.

[8] Yair Amir, John L. Schultz, "Secure Group Communication Using Robust Contributory Key Agreement", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 15, NO. 5, MAY 2004.

[9] Edith C.H. Ngai, Student, and Michael R. Lyu, Professor, Fellow, IEEE, Department of Computer Science & Engineering, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong, "Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks".

[10] Dr. Anil Kapil, Mr. SanjeevRana, "Identity-Based Key Management in MANETs using Public Key Cryptography", International Journal of Security (IJS), Volume (3) : Issue (1).

[11] D.Sivaganesan1 and Dr.R.Venkatesan, "PERFORMANCE ANALYSIS OF BROADCASTING IN MOBILE AD HOC NETWORKS USING CLUSTER APPROACH" , International Journal of Ad hoc, Sensor & Ubiquitous Computing(IJASUC) Vol.1, No.2, June 2010.

[12] PoojaSaini, "Impact of Mobility and Transmission Range on the Performance of Backoff Algorithms for IEEE 802.11-Based Multi-hop Mobile Ad hoc Networks", International Journal of Advancements in Technology (IJoAT) http://ijict.org/ ISSN 0976-4860.