2011 2nd International Conference on Networking and Information Technology
IPCSIT vol.17 (2011) © (2011) IACSIT Press, Singapore

The Application of Proxy Re-Cryptography in Group Key Management for Group Communications System

Wang Qichen

Institute for Interdisciplinary Information Science, Tsinghua University, Beijing, China, 100084
wangqichen@cssci.info

Abstract. This paper presents a group key management mechanism PTGKM based on hierarchical and domain structure in Near-Space Network. The mechanism combines hierarchical and domain structure with the use of proxy re-cryptography algorithms. It has the following characteristics: (1) the core backbone network node cannot obtain the new group key. It only participates in the distribution of the new group key. So the mechanism solves the problem of a single point of failure of group key management based on hierarchical and domain structure; (2) The mechanism restricts the impact of group membership change in its domain, which improves the scalability of group key management scheme; (3) The inter-domain switching algorithm effectively reduces the rekeying overhead of the high mobile nodes' frequent switching between different domains; (4) The mechanism adapts to the characteristics of Near-Space Network and meet the forward security and backward security. The analysis results show that, PTGKM mechanism is applicable to near space environment and has good scalability and reliability.

IndexTerms: Group Key management; Proxy Re-Cryptography; Security

1. Introduction

The Near-Space Network is a new space area which is about 20-100 kilometers and between aviation and spaceflight. There are potential applications for Communication Guarantee, Information Collection and Disaster Quickly Response and it has be a hot research field[1-3]. The size of the Near-Space Network is very large, and resources are very limited. Group communication has been a very important application technology because of its ability to send data to a large number of users in the network in an efficient manner. However, because the Near-Space Network is in high degree of exposure, dynamic topology, heterogeneous networks, large scale and wide range, the network's security was seriously threatened. The safety of the Near-Space Network is at an early stage of which the security mechanisms are not perfect. The existing group key management technologies of secure group communication system are mainly for wired networks, small wireless network, but not suitable for the characteristics of Near-Space Network. And therefore the study of group key management technology in Near-Space Network has great significance and is critical for deployment and application of security group communications system.

2. Description of Proxy Re-Cryptography

The basic idea of proxy re-cryptography algorithm is that a proxy node with proxy key can convert a cipher text encrypted with a pair of keys to another cipher text encrypted with another pair of keys without the need to know the secret decryption key or the plaintext. This paper uses the unidirectional ElGamal proxy cryptography in [7], and its security is equivalent to the original ElGamal public key cryptography, which is based on the intractability of the discrete logarithm problem based on finite fields. It is described as follows:

Definition 1 (Discrete logarithm problem based on finite fields, DL problem) Given a prime number p and a primitive element g On G_p. Given (g, g^x), for a certain x $\in Z^*_P$, to calculate x . There is an algorithm A solving the discrete logarithm problem with the advantage of ε , if and only if

$$\Pr\left[A\left(g, g^{x}\right)=x\right] \geq \varepsilon$$

This probability depends on the random selection of x and the output of A.

Definition 2 (discrete logarithm assumption) Assume ε-DL is right, if and only if there is no probabilistic polynomial time for an attacker with the advantage of ε to solve the DL problem.

3. Proxy-Function Tree Based Group Key Management for Near-Space Network

3.1. Group Key Management Framework

PTGKM mechanism is a group key management mechanism based on the hierarchical and domain structure in the Near-Space Network. The ElGamal proxy re-cryptography algorithm is used in key distribution process to ensure that the rekeying message is transferred to the reliable group members when membership changes. The main idea is that the next group session rekeying message is encrypted by proxy key and group key of group sessions i , which ensures that only the legitimate group members who own these two keys simultaneously can decrypt the rekeying message and get the updated group key. The group key management framework in PTGKM mechanism is designed as follows:

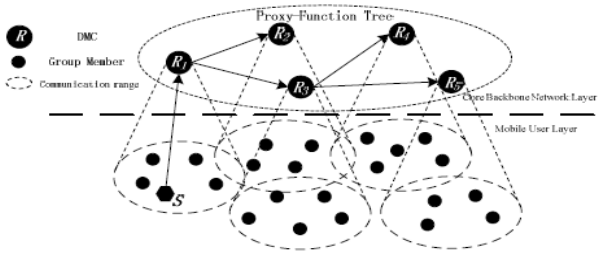

Figure 2. Framework of PTGKM

The ground management and control center in the Near-Space network is as the group management center S in the whole communications system. All the DMCs at the core backbone network compose of a logical proxy-function tree, whose root is the DMC of domain that S is in and the middle proxy nodes are DMCs that participate in group key management. Group Management Centre S is responsible for the group key's generation, distribution and updates. Child proxy nodes get the proxy key from its parent node in a safe way which h achieves hierarchical key distribution tree structure. Group rekeying message is transferred along the path of proxy-function tree. The root proxy node use re-cryptography algorithm encrypts and sends rekeying message to its child proxy node, and then the child proxy node converts the ciphertext from its parent node to another ciphertext that can only be decrypted by members within its domain. In the whole update process, proxy re-cryptography algorithm is used to distribute update message to it child nodes until reaching the leaf proxy node. The sender uses the group key to encrypt communication data and sends encrypted data directly to all legitimate group members. It should be noted that in PTGKM mechanism, the conversion process with proxy cryptographic algorithms is only used in updating the group key, while the security of communication data is guaranteed through encryption with group key.

3.2. Assumptions and Notations

In PTGKM mechanism, we first assume that when the core backbone network initializes, all DMC nodes are verifiable to be legitimate and the adjacent nodes have some basis of trust. Of group key distribution process, DMC nodes in the core backbone network layer is partial trusted, that is to say that the intermediate proxy nodes will use proxy cryptography in an intended way to convert the ciphertext received and forward in a right way. DMC does not participate in group communication. It only has the function of group key management and offers group key distribution services for user nodes in the mobile user layer. And we also assume that all the group rekeying messages can be authenticated. Notations are as follows:

(1) rk_j : Proxy key of a proxy node R_j . It is shared by the proxy node R_j , members in its domain and its child proxy nodes. rk_0 is shared by S and the root proxy node R_0 . The use of proxy key can restrict the impact of group membership change in the domain.

(2) k_i : Group key of session i . It is used to implement group communication among group members. k_i is shared among group members, and $y = g^{k_i} \pmod p$ is the public key. The middle proxy node is not a group member and can not decrypt the ciphertext.

(3) r_j : Random number selected by proxy node R_j . It is a secret parameter selected from Z_q in the process of encryption. r_0 is selected by S .

[7] give a way to use proxy re-cryptography algorithm. But the proxy node needs to know the original group key of session i in the conversion process. So it can not maintain the independence with group session key in the distribution of the new group key, which makes it lost the original meaning to be a proxy. In this paper, PTGKM mechanism improves the use of re-cryptography algorithm. It is shown below:

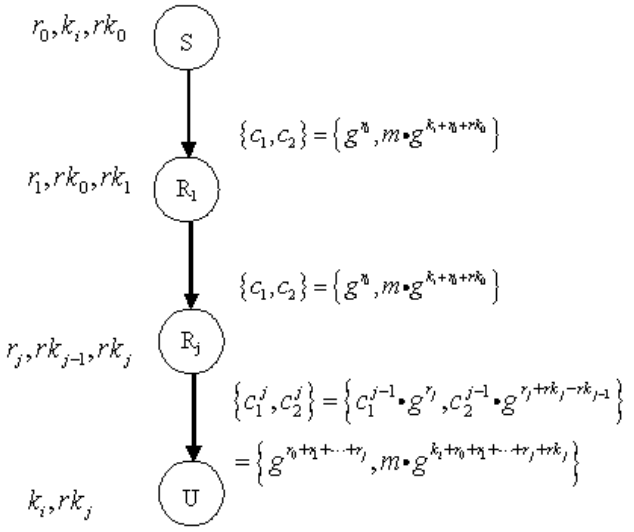

Figure 3. Employment of ElGamal Proxy Re-Cryptograph

3.3. Group Rekeying Algorithm

When the membership of group communication system changes, group management center needs to trigger group rekeying action and form the new group session in order to meet backward security and forward security. Because of high mobility of group members in Near Space network, there are not only group members join in and leave the group communication, but also group members switch between different domains frequently and do not leave the group communication. This paper gives the rekeying algorithm for group members joining in, leaving the group, and stresses in the group rekeying process for members' switching between the domains.

1) Group member join: In the rekeying process for member joining, the member first sends a join request to DMC, and then DMC forwards the request to the Group Management Center S . S Verifies the legitimacy of the members and changes group session and updates group key if it passes. Suppose that in the group session $i - 1$, when a member in the management domain of R_j requests to join a group, after it is validated legitimately S implements the group rekeying algorithm as follows:

a) S generates a new group key k_i independent of k_{i-1} ;

b) S unicasts k_i to the new member securely;

c) R_j unicasts rk_i to the new member securely;

d) S will use a proxy re-cryptography algorithm along the proxy function tree to distribute k_i to all the legitimate members of the group;

In the update algorithm for group member joining, the communication overhead of the update operation is two unicast messages and a broadcast message.

2) Group member leave: The events that group member take the initiative to leave or group management center cancels the member's qualification belong to the leave event. The rekeying process includes proxy key update of DMC and group key update. When the event that member leaving occurs, the group session changes

and DMC R_j performs the update operations. The proxy key update operation is limited to the domain that leaving member located in. Suppose that in the group session i , a group member in R_j leaves group communication system, the implementation of group rekeying algorithm is as follows:

a) R_j first generate a new proxy key rk'_j which is independent of the original proxy key rk_j ;

b) R_j distributes securely rk'_j to all group members in its domain and its child proxy node;

c) S generates a new group key k_{i+1} independent of k_i , and use re-cryptography algorithm to distribute to all group members along proxy-function tree;

In the update algorithm for group member leaving, the communication overhead of the update operation is two broadcast messages.

3) Group member switch inter-domain: In order to reduce group rekeying overhead of group members frequently switch, the paper designs group key delayed update algorithm for member switching between domains. Only after certain conditions are met do we implement the relevant key update operation. Switch user can have multiple proxy keys of multi-domains to ensure that it can reuse these keys when it returns after switch users leaved the original domain for some time.

Group Management Centre S maintains a legitimate user list which contains information of all the legal group members in group communication system. Each DMC maintains a proxy key external owners list (EOL), which contains information of all the legitimate group members who have left this domain and still have the original proxy key. Suppose that in the group session i +1 , there is a member in R_j switches to the adjacent R_{j+1} . Like the process of member join, after verifying the legitimacy of the switch users we implement the related operations, as follows:

a) R_{j+1} generates a new proxy key rk'_{j+1} independent of the original key rk_{j+1} and distributes securely to all group members (including the switch user) and its child proxy node;

b) R_{j+1} adds the information of switch user to EOL, rather than implements proxy key update action;

It does not need to update the current group session key in the whole process. Group communication system must regularly implement update of group key and proxy key, which prevents switch users from getting all proxy keys through inter-domain switch. And when the records of EOL maintained by DMC are more than a certain amount, the DMC must implement its proxy key update operation.

Notation: If the members in this kind leave the group communication, not only we implement member leave rekeying algorithm, but also the DMCs affected implement proxy key updates action

4. Security Analysis

The security of PTGKM mechanism is based on the discrete logarithm assumption and the security of symmetric cryptography. From the aspects of backward security, forward security and framework security, the analysis is as follows:

1) Backward Security:In the group rekeying algorithm for member join, R_j securely unicasts its proxy key rk_j to the new members joined. If group member wants to get k_{i-1} , although it owns rk_j , it do not know k_{j-2} , so it can't decrypt ciphertext $\{c_1, c_2\} = \left\{g^{r_0+r_1+\cdots+r_j}, k_{i-1} \bullet g^{k_{i-2}+r_0+r_1+\cdots+r_j+rk_j}\right\}$, because of the discrete logarithm assumption. So the new member can not get k_{i-1} , even if it intercepted and stored the messages transmited in the network before join. Therefore it can not decrypt the messages, which achieves the backward security of PTGKM.

2) Forward Security:In the group rekeying algorithm for member leave, after the parent proxy node distributes rk_j' , only the legitimate group members in this domain and the children proxy nodes can update the proxy key from rk_j to rk_j' . Group Management Centre S transfers group rekeying message $\{c_1, c_2\} = \left\{g^{r_0}, k_{i+1} \bullet g^{k_i+r_0+rk_0}\right\}$ along the proxy-function tree. R_j , which is in the transmission path, uses rk_j' to re-encrypt the message, $\{c_1, c_2\} = \left\{g^{r_0+r_1+\cdots+r_j}, k_{i+1} \bullet g^{k_i+r_0+r_1+\cdots+r_j+rk'_j}\right\}$, and transfers to group members in this domain and its child proxy nodes. The legal group members in R_j receive the message and get the new group key k_{i+1} . Because the message is encrypted with k_i and rk_j' , the user who has left group can not get

k_{i+1} without rk_j' . And this user can not continue to participate in group communications too. So the forward security of PTGKM scheme is achieved.

3) Framework Security:According to the basic idea of proxy re-cryptography algorithm, DMC nodes participating in group key distribution only has the message conversion function, and can not get the new group key, which has fundamentally solved the problem of a single point of failure caused by attacking DMC.

5. Performance Analysis

The communication overhead and storage overhead of group rekeying process in PTGKM mechanism is shown in Table 1. N denotes the total number of group members, M denotes the average number of group members in each domain, C denotes the number of proxy child node of a proxy node in the proxy-function tree.

TABLE I. RESULTS OF PERFORMANCE ANALYSIS

Communication overhead	Member join	2+log(M+C)
	Member leave	2log(M+C)
Storage overhead (not including the group key)	DMC	2
	Group member	log M+1

When $N \gg M \gg C$, $\log N \gg \log(M+C) = \log M$ comes into existence. So we can see from Table 1, PTGKM mechanism can not only effectively alleviate the "1-affects-n" problem and improve the scalability of group key management mechanism, but also effectively reduce the network resources overhead of the group key management in Near-Space Network.

6. Conclusion

With the characteristics of near-space self-organizing network model, this paper improved the method in [7] and proposed a new group key management mechanism for the Near-Space Network. The paper takes full advantage of the local characteristics of intra-domain and inter-domain communication to solve the "1-affects-n" problem of group key management. And it also re-designed the proxy re-cryptography algorithm, so that the core backbone network nodes do not require and can not access to the group session key which avoids the problem of a single point of failure fundamentally. And combining the characteristics of the Near-Space Network System, we focused on the group rekeying algorithm for members' inter-domain switching. Finally, the detailed security and performance analysis were given for PTGKM mechanism.

7. References

[1] Wu Youshou. "High Altitude Platform Stations Information System New Generation－Wireless Communications System (part I)," China Radio Management, 2003, pp..3-8

[2] Wu Youshou. "High Altitude Platform Stations Information System New Generation－Wireless Communications System (part II)," China Radio Management, 2003, pp. 14(6):3-8,2003,pp.8-15

[3] Karapantazis S, Pavlidou F, "Broadband communications via high-altitude platforms: a survey," IEEE Communications Surveys & Tutorials, 2005, pp.1-31

[4] Li J H, Renato Levy, Miao Yu, "A Scalable Key Management and Clustering Scheme for Ad Hoc Networks," INFOSCALE'06, 2006, pp.1-10

[5] Zhang Xiaohui, The Research on the Key Management of Ad Hoc Network Clustering Topology, Master Thesis of Beijing University of Posts and Telecommunications,2007

[6] Zhang Xiaoning, Feng Dengguo, "A Cluster Based Security Scheme in Wireless Ad Hoc Networks," Journal of Computer Research and Development,2006, pp.238~243

[7] Jun B H, Young J S, Hyun S Y, "Decentralized Group Key Management for Dynamic Networks Using Proxy Cryptography," Q2SWinet'07,2007