

A Distributed Multicast Encryption and Management Solutions Based on Security Agent

Ping Zhang^{1#}, Liang Zhou²

1. School of Mathematics and Statistics, Henan University of Science and Technology, 471023, China

2. Airforce Institute of Armament Research, Beijing, 100086, China

#Email: zhangping76@126.com

Abstract

In order to avoid re-key of secure multicast and raise the efficiency of secure multicast, a new method of multicast encryption based on the RSA public key system is put forward. Based on the analysis of the manuscript, the new method has the function that using one key for encryption and many keys for decryption. The method does not need to update private key of everyone in the group when any member changes and satisfies the requirements of secure multicast of forward/backward confidentiality and collusion freedom. By analyzing communication mechanism of the security agent model, simulating performance of network node's sending data packets and applying the multicast encryption method, a distributed security multicast management program based on security agent model is designed, which ensure that the users in the communication group can share the multicast information in the intranet safely.

Keywords: Network Security; Communication Agent; Security Multicast; Key Management

1 INTRODUCTION

With the wide spread of the Internet, the technology based on multicast communication also got fast development. Take the Internet video conference and the applications of information released for example, the mode of multicast communication allows one or more of the managers to send data packets to many more receivers who are the members of the multicast group. The technology has the advantages of improving the efficiency of network communication, reducing network traffic and the server load, etc. However, the problem on reliability and safety of multicast is more complex than unicast. The safety management of key in the multicast is an important research task, which becomes the hotspot of research in this field [1].

The security of IP-multicast includes confidentiality, integrity, availability, and accuracy of the transmission of messages between group members. The multicast packets encrypted transmission is a method to realize the confidentiality. The confidentiality of multicast communication requirements that only authorized members of the group have the encryption/decryption key to encrypt /decrypt the information transmitted. Thus, the issues of multicast key management results, including: the confidentiality of non-group members: the users who are not in the multicast group, cannot use the known information to interpret the data of this group provide by multicast. Forward confidentiality: the nodes quit the multicast initiatively of fiercely (such as malicious nodes) does not continue to participate in multicast, which means they do not use the known key to decrypt the successor multicast packets, and generate a valid encrypted packets; Backward confidentiality: new members of the group may not be able to crack the multicast packets joined before; Anti-complicity crack: any user cleared by the multicast group cannot crack the present multicast key regardless of how they joint.

The traditional scheme of multicast key management is based on symmetric or asymmetric (public key) encryption method. All group members share the encryption and decryption keys. Multicast key managers generate and distribute keys for the members participate in the multicast, in order to protect security requirements as forward confidentiality and backward confidentiality, the key managers need re-generate and distribute group keys regardless

the numbers join or leave, called re-key. The multicast can not be restarted before re-key is completed. Re-key will take up a lot of bandwidth if the group members change frequently. The existing key management schemes, such as centralized key management scheme (GKMP) [2], distributed key management scheme (Clique) [3] and hierarchical and grouping management scheme (Iolus) [4], the focus of the study is how to improve the efficiency of re-key, to reduce the bottlenecks of system.

Symmetric encryption or public key encryption method is primarily designed for unicast communication, thus the problem of re-key emerged when using them for secure multicast. Based on the re-key, the efficiency of security multicast is limited, and is always the bottleneck of the multicast system.

In view of the characteristic that symmetric or public key encryption method is mainly applied to unicast, the idea of multicast encryption method is put forward based on the demand for secure multicast. The basic principle is: each group member, when joining in a multicast group, is assigned with a private key, which is different from other members. For each multicast process, the multicast manager selects users authorized to listen, generate the encryption key using the user's private key and encrypts sent message. Only users authorized to listen can decrypt the message with his private key. Other unauthorized users cannot use their private key to decrypt the data.

Therefore, secure multicast communication encrypts the content of the communication using the group key shared by all members within the group. In order to protect the safety, the key server needs to rekey when membership is changed. Due to the dynamics of the relationship between group members and the high cost of encryption or decryption operations, the performance of the group rekey is main indicator to measure the performance of multicast key management, also an important factor affecting multicast communication.

In order to guarantee the safety of multicast, the key must be updated when the user join in or exit the group. So that, the new members of the group can not access the past communication contents and the exited users can't access the current and future communication contents. Members of the group must be able to effectively calculate the new key, but the any alliance of the exited users can't get it. At the same time, we should also consider the storage costs and communication costs [5]. In order to avoid the update of the secure multicast members' key, strengthen key management and improve the efficiency of security multicast. This paper proposes a new multicast encryption methods and security agent model based on the RSA public-key cryptosystem algorithm. By analysis of multicast demand and network security communication, we get the corresponding distributed secure multicast program.

2 SECURITY AGENT MODEL

Generally the agent with autonomy, flexibility and collaborative features [6], according to its status, can determine what to do next, without the need for artificial or other external intervention. Security agent proposed in the text mainly consists of four modules: security module, communication module, multicast module and knowledge base module. The functional diagram of the security agent model is shown in Figure 1.

2.1 Security Module

Security agent module in your area provides security-related services within the network, and valuable information collected is stored in the knowledge base. Security modules can be divided into several sub-modules, such as anti-virus, intrusion detection, vulnerability scanning, access control, disaster recovery and patch upgrades.

2.2 Communication Module

The main role of communication module is responsible for the information exchange between the hosts and the agents within the network. The sent request information includes demand information, alarm information, as well as safety testing information in the broadcast among agents. Communication module includes communication language and transfer protocol. Communication language is the basis for communication between the agents, and transfer protocol is a communications transport mechanism.

2.3 Multicast Module

Multicast module is the core of the agent to achieve the communication each other within the network or between

intranet users and Internet users. The users are divided into different information groups, as well as to achieve safe and efficient information exchange and share between users in the group. Multicast module consists of creating or deleting group, file encryption or decryption, group key update, key authentication, key generation and key off sub-modules.

2.4 Knowledge Base Module

The data in knowledge base module are provided by the security module. The related security log, status information and alarm information are stored in the knowledge base according to classification. Knowledge base module makes information and knowledge ordering, does a large-scale collection and processing for the original information and knowledge, meanwhile, provide the according means to search [7].

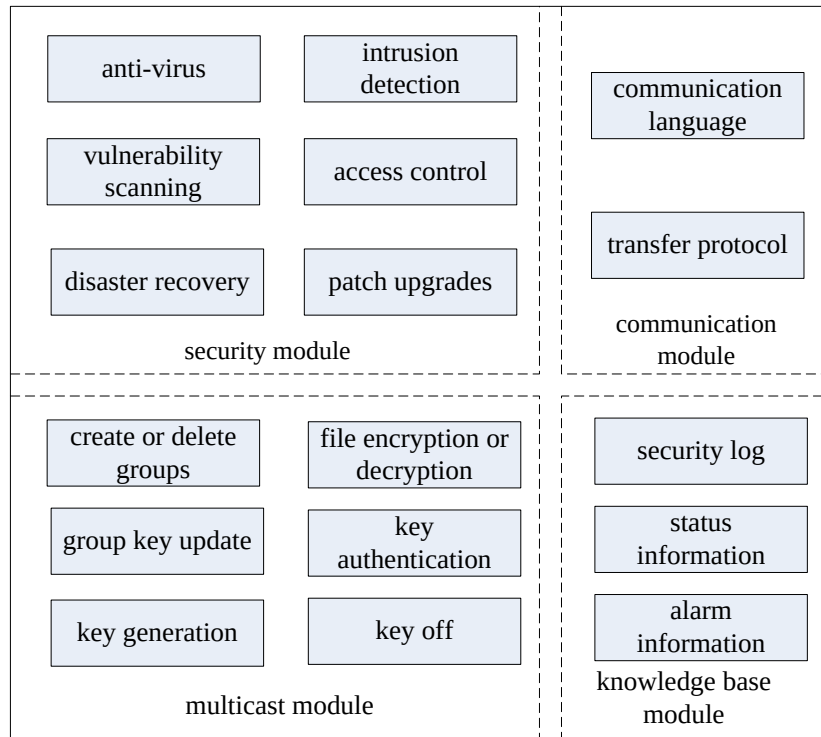


FIG.1 FUNCTIONAL DIAGRAM OF THE SECURITY AGENT MODULE.

3 ENCRYPTION METHOD BASED ON MULTICAST

3.1 RSA Algorithm Description [8]

1) Key generation

- ① Pick two large confidential prime numbers P and Q .
- ② Calculate $n = p \times q$, $\varphi(n) = (p-1)(q-1)$, where $\varphi(n)$ is the Euler function value of n .
- ③ Select an integer e , meet the condition of $1 < e < \varphi(n)$, and $\gcd(\varphi(n), e) = 1$.
- ④ Calculate d , meet $ed \equiv 1 \pmod{\varphi(n)}$, that d is multiplicative inverse of e under the mode $\varphi(n)$. Because e and $\varphi(n)$ are prime mutually, so d should be exist multiplicative, known by the modular arithmetic.
- ⑤ $\{e, n\}$ is public key, $\{d, n\}$ is private key.

2) Encryption

The plaintext string is divided into blocks firstly when encryption, so that corresponding decimal number of each block are smaller than n , meaning that the length of block is less than $\log_2 n$. Then block of each plaintext m is applied to encryption algorithms:

$$c \equiv m^e \bmod n$$

3) Decryption

Decryption of cipher text block:

$$m \equiv c^d \bmod n$$

3.2 Design of Key and Process of Encryption

Select two large prime numbers P and Q randomly, and P, Q are private. Calculate $n = pq$ and its Euler function $\varphi(n) = (p-1)(q-1)$, n is open, while $\varphi(n)$ is confidential. Randomly selected some distinct primes, $a_1, a_2, a_3, \dots, a_m$, which larger than n . Calculate $d = a_1 a_2 \cdots a_m$. Let $k = \lceil d/n \rceil$, $r = d \bmod n$, where $\lceil x \rceil$ is round symbol, k is open. There are the following results:

$$1. d = kn + r$$

$$2. \text{ For any } a_i \ (i=1, 2, \dots, m),$$

$$\begin{aligned} kn \bmod a_i &= (d - r) \bmod a_i \\ &= ((d \bmod a_i) - (r \bmod a_i)) \bmod a_i \\ &= ((a_i \bmod a_i) - (r \bmod a_i)) \bmod a_i \\ &= (a_i - r) \bmod a_i = a_i - r \end{aligned} \quad (1)$$

If known a_i , n and k , calculate r through equation (1), then calculate d . The other prime numbers instead of a_i , which different from $a_1, a_2, a_3, \dots, a_m$, the equation (1) does not hold. It is difficult to calculate r and d when known p, n, k .

$$3. \text{ By the selection of } a_1, a_2, a_3, \dots, a_m \text{ and the definition of } d, \text{ we can reach a conclusion:}$$

$$\gcd(d, \varphi(n)) = 1$$

Similar to the cryptography of RSA public key, we can calculate e from $ed \equiv 1 \bmod \varphi(n)$ by the extended Euclidean algorithm.

Because the decryption key d is very large, which make the calculations of decryption time-consuming. A research focuses on mode indices algorithm of large integer in decryption calculation of RSA cryptosystem. With more mature and improved Montgomery algorithm or some of efficient function of foreign cryptography algorithm library, it can reduce the calculation. But the above-mentioned algorithm is still far from the actual decryption operations in this article. This will make impossible to decrypt when more multicast members to participate especially and seriously affect the expansion of the group members. To effectively solve this problem, a hash function is introduced. Where the original decryption key d as input to hash function and obtain an output value d' , as follows:

$$d' = \text{Hash}(d) \quad (2)$$

Based on the extended Euclidean algorithm:

$$e'd' \equiv 1 \bmod \varphi(n) \quad (3)$$

Obtain the value of e' , (e', n, k) called the encryption keys should be open, (d', n, k) are decryption keys, and (a_i, n, k) are the private keys of group members, n and k as the secondary key. Hash function $\text{Hash}()$ is open to the public, which satisfy the characteristics of public key cryptosystem.

3.3 Strength Analysis of Multicast Encryption

Multicast encryption method is an improvement of public key cryptography system based on RSA. There are a lot of analyses regarding to strength of RSA public key cryptography. In the improvement part of RSA, known n and k , start from r to calculate d . The range of exhaustive is proportional to n . From the selection of n , we can see the value more than 10^{200} . The crack intensity of exhaustive has more than the DES algorithm, with RSA considerable.

When a_i is few larger than n , it is vulnerable to be attack for brute-force method. To try for all prime numbers greater than n , calculate r according to $r = a_i - kn \bmod a_i$, then obtain decryption key d . So a_i is larger enough

than n .

In some cases, r may be small. It is vulnerable to be attacked by exhaustive method. Therefore, r should be doing some processing to improve the deficiencies. Specific improvement is that according to the formula $r = d \bmod n$, the calculation r is smaller than all of n . According to the formula $d = kn + r = (k-1)n + (n+r) = k'n + r'$, $k' = k-1$, $r' = r + n$, k' and r' are auxiliary keys at this time.

4 SECURITY ANALYSIS

When a new user x join in a multicast group through the Security Agent and obtain the private key a_x , though the user may acquire the previous multicast encrypted data and the corresponding multicast encrypted information, but as the security agents distribute different private key to the members of each group, therefore the private key a_x is not involved in the multiplication of generating decryption key d , so the key d can not be calculated and will not be able to decrypt any previous encrypted data, then this meet the requirements of backward encryption.

If a group member y has exited from the multicast group, but he continued to preserve the private key a_y and also be able to get a new pair of auxiliary key for the multicast and the multicast encrypted data, but because his private key a_y is no longer involved in operation of generating the decryption key d , so it can not recover the new decryption key and can not decrypt the new multicast encrypted data. This meets the feature of forward encryption. So whether it is the new multicast group members to join in or the former members to leave the group, the other members of the group does not need updates the key, and meet the multicast security requirements of forward and backward encryption.

About cracking anti-conspiracy, it is easy to see that the user's private keys are different from each other and there is no relation between them, and the operation of the decryption key d and the auxiliary key n and k is only controlled by security agents. Therefore, no matter how the quitted multicast group members conspiracy, they can not crack the cipher text.

5 DISTRIBUTED MANAGEMENT SCHEME FOR SECURE MULTICAST

This paper presents a distributed management scheme for secure multicast which is suitable for local network to communicate with each other, as the figure 2 shown. GSA (Global Security Agent) is a node which analyzes and processes the data from multiple LSA (Local Security Agent). LSA is a node of network packet collection, preliminary analysis and the management of the subnet which achieves key security and data transfer between agents, it can be elected a member as LSA in each subnet.

If some members of the subnet need to communicate with each other between different subnets, you can create temporary LSA groups and use multicast encryption skills to achieve the safety communication between the group members. Meanwhile, the security sub-module in LSA real-time monitors the security situation in the each subnet, and sends the alarm information and host status information to GSA. GSA will write the related information in the database. For the administrators, it is easier to manage and monitor whether the state of each host within the network suffered attacks. Therefore, based on ensuring the safety of the intranet, the program can make the multicast group members to share information safely.

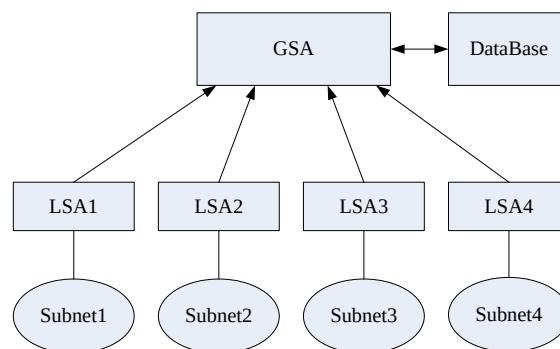


FIG.2 THE DISTRIBUTED SECURITY MULTICAST MANAGEMENT SCHEMATIC DIAGRAM

6 CONCLUSIONS

The security agent module is a kind of new technology, and has distinctive advantages in the large scale networks, distributed system and cross-platform application. If the technology of security agent module is introduced in the communication systems, the advantages as follows: clear system architecture, good scalability and good portability. At the same time, the security agent module has the advantage of low occupancy of network system and host resource.

By the analysis of security agent model, this paper proposes a new multicast encryption method based on RSA, and then gives a scheme suitable for distributed secure multicast on the Internet. By analyzing the security of the scheme, the function that one key encrypt and more key to decrypt is achieved in the multicast group. When some group members get changed, there is no need to reset other members' key, which can achieve the encryption of the multicast information and satisfy the important requirements that forward encryption, backward encryption and cracking anti-conspiracy in secure multicast.

ACKNOWLEDGMENT

This topic of research is supported by Henan University of Science and Technology Foundation for young scholars (No: 2009QN0033), Henan University of Science and Technology Foundation for the cultivation of innovative ability (No: 2012ZCX015), the project development plan of science and technology of Luoyang City (No: 1301042A), Basic and frontier research projects of the Henan Provincial Department of Science and Technology (No: 142300410014) and Scientific and technological research projects of the Henan Provincial Department of Education (No: 2011A520012, 14A510021).

REFERENCES

- [1] Cao Guo-liang, Zhou Jie, "A secure multicast encryption algorithm and key management model", Journal on Communications, Vol.26, No.1A, 2005, pp.100-105
- [2] H. Harney, C. Muckenhirn, "Group key Management Protocol (GKMP) Architecture", RFC 2094 (Experimental), 1997
- [3] Hardjono, T., B. Cain, "Simple key management protocol for PIM", Internet Engineering Task Force, Vol.20, No.1, 2000, pp.15-30
- [4] Dai Weihui, Zhu Qi, and Wang Chunshi, "Risk Management Model of Information Security in IC Manufacturing Industry", Journal of Computers, vol.7, pp.317-324, 2012
- [5] Deering S, "Host Extensions for IP Multicasting", RFC1112, 1989, pp.56-62
- [6] Li Yuan-zheng, "A Security Multicast Scheme with the Hierarchical Group Key Management", Journal of Electronics and Information Technology, Vol.26, No.7, 2004, pp.1053-1056
- [7] Zhao Qian, "Research on family and shops real-time status of 3G Wireless Remote Monitoring System", Journal of Software, vol.6, pp.814-818, 2011
- [8] Yang Yi-xian, Niu Xin-xin, Applied Cryptography Tutorial, Beijing: Electronic Industry Press, 2005
- [9] Cheng Xiangguo, Yang Chen, and Yu Jia, "A new approach to group signature schemes", Journal of Computers, vol.6, pp.812-817, April 2011

AUTHORS



¹**Ping Zhang** was born in Mudanjiang City, Heilongjiang Province, China in December 1976, Associate Professor, Ph.D., is mainly engaged in cryptography and information security.

²**Liang Zhou**, Ph.D., is principally engaged in the study of information security protective equipment.