I.J. Wireless and Microwave Technologies, **2011, 1, 30-37**
Published Online February 2011 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2011.01.05

Available online at http://www.mecs-press.net/ijwmt

A Group-oriented Access Control Scheme for P2P Networks①

Wang Xiaoming[a,*1], Cheng Fan[a,*2]

[a] *Department of Computer Science, Jinan University, Guangzhou 510632, China*

Abstract

A group-oriented access control scheme is proposed for P2P (peer to peer) networks. In the proposed scheme, authentication control, admission control and revocation control are used in order to provide security services for P2P networks. Moreover, the proposed scheme can simply and efficient establish share key between two members without interactions, therefore it can perform secure communications with them. The analysis of security and performance shows that the proposed scheme not only can realize authentication and secure communication, but also can easily and efficiently add new group members and revoke malicious group members. Therefore, it is more efficient, and more practical protocol for P2P networks.

Index Terms: P2P Network; Access Control; Authentication Control; Added and Removed Members

1. Introduction

The need for security services in P2P network makes the research of security mechanisms become very urgency and importance. However, absence of centralized control and dynamic membership exacerbate security problems in P2P networks, and result in that the traditional security mechanisms cannot satisfy the secure need of the dynamic networks, thus requiring very specialized security services such as access control mechanisms etc. Recently, some access control mechanisms for P2P networks and Ad-hoc networks have been proposed [1-10]. But the schemes can only prevent unauthorized member from joining a group, and cannot revoke misbehaving or malicious members from group. However, a secure access control can not only prevent unauthorized members from joining a P2P network, accessing the membership resource, but also revoke the malicious or misbehaving members from P2P network once detected. Otherwise, the security of P2P network will hardly be guaranteed.

This paper addresses the problem of building a generic security services for P2P networks. We divide a P2P network into many group, focus on building admission control, authentication control, and revocation control

① Supported by National Natural Science Foundation of China under Grant (61070164); National Natural Science Foundation of China under Grant (600773083);Natural Science Foundation of Guangdong Province, China (81510632010000022); Science and Technology Planning Project of Guangdong Province, China (2010B010600025)

* Corresponding author:
E-mail address:*1 wxmsq@eyou.com; *2 Cf@eyou.com

for P2P networks. We propose a group-oriented access control scheme in order to provide security services for P2P networks. The proposed scheme can provide admission control, revocation control, authentication control, and secure communication etc. Furthermore, the proposed scheme can simply and efficient establish share key between two members without interactions, therefore it can perform secure communications with them, so it is a more efficient, and more practical scheme in the environments of dynamic membership and no central-trusted authority.

The rest of the paper is organized as follows: Section 2 presents the group-oriented access control scheme for dynamic group. In section 3, the security and properties of the proposed scheme are analyzed. Finally, the concluding remarks are given.

2. Proposed Scheme

The design idea of the proposed scheme is motivated by [1,14]. The proposed scheme employs polynomial function as the basic means of constructing member authentication procedure in order to avoid the need for public key cryptography. The proposed scheme consists of following sections.

2.1. Network model

In order to enhance management, our system model uses group-oriented structure, that is, a P2P network is classed into a number of groups. In each group, exactly one distinguished member, who is called as the group head (GH), is responsible for establishing and organizing the group. Group heads have considerably more trusty, it may be the founding members of P2P network [14]. Group heads can communicate with each other directly and relay data between two groups; Group members can communicate with its group head directly and communicate each other directly in the same group. But the members in two different groups cannot directly communicate in our model.

2.2. Initialization

Let p, q be distinct large primes and $q|(p-1)$, g be a generator which is an element of Z_p^* with an order q (i.e., $g^q = 1 \bmod p$). $h(.)$ is a secure one-way hash function. Assuming also GH_i denotes a group head for group G_i (i= 1,2,…,m); N_n=(n_1,…,n_n) denotes a set of network members in G_i. Each GH_i and n_i have respectively a pair of keys such as (τ_{CH_i}, $y_{CH_i} = g^{\tau_{CH_i}} \bmod p$) and ($\tau_i$, $y_i = g^{\tau_i} \bmod p$). In the initialization phase, let the system have a trusted dealer (TD). After initialization, TD is no longer needed. TD has also a pair of keys such as (τ_{TD}, $y_{TD} = g^{\tau_{TD}} \bmod p$). The initialization includes following several steps:

(1) TD first chooses polynomial

$$c(x,y) = \sum_{\alpha=0}^{t-1} \sum_{\beta=0}^{t-1} c_{\alpha\beta} x^{\alpha} y^{\beta} \bmod q \tag{1}$$

such as $c_{\alpha\beta} = c_{\beta\alpha}$ for each α, β and $c(x,y) = c(y,x)$, and then computes and publishes $e_{\alpha\beta} = g^{c_{\alpha\beta}} \bmod p$ for $\alpha, \beta \in [0,t\text{-}1]$. Where $c_{\alpha\beta}$ -s are the coefficients of $c(x,y)$.

(2) TD selects a random number ξ, and computes $\delta_i = y_{CH_i}^{\tau_{TD}} \bmod p$ and a secret share polynomial $s_i = c(x, GH_i)$ for each group head GH_i, and encrypts (ξ, $s_i(x)$) such as $V_i = E_{\delta_i}(\xi \| s_i(x))$ and sends V_i to each cluster head GH_i. Where $E_{\delta_i}\{\cdot\}$ denote encryption operation with a key δ_i using symmetrical encryption algorithm such as AES, || stands for the concatenation operation.

(3) On receiving V_i, GH_i computes $\delta_i = y_{TD}^{\tau_{CH_i}} \bmod p$ and the decrypts V_i, and validates them by checking if

$$g^{s_i(ID_G)} = \prod_{\alpha=0}^{t-1} \prod_{\beta=0}^{t-1} (e_{\alpha\beta})^{(ID_G)^\alpha (GH_i)^\beta} \bmod p \tag{2}$$

If it holds, then each GH_i obtains his secret keys (ξ, $s_i(x)$). Where ID_G is the public identifier of P2P networks. After this, TD is no longer needed.

(4) Each GH_i First chooses polynomials $f_i(x,y)$ and $F_i(x)$

$$f_i(x,y) = \sum_{\alpha=0}^{t-1} \sum_{\beta=0}^{t-1} b_{\alpha\beta} x^\alpha y^\beta \bmod q \tag{3}$$

$$F_i(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1} \bmod q \tag{4}$$

such as $b_{\alpha\beta} = b_{\beta\alpha}$ for each α, β and $f_i(x,y) = f_i(y,x)$. Where $b_{\alpha\beta}$ -s and a_i-s are the coefficients of $f_i(x,y)$)and $F_i(x)$.

(5) GH_i firstly selects a random number ε, and computes $\lambda_i = y_i^{\tau_{CH_i}} \bmod p$ and secret share parameters $F_i(ID_i)$, $k_i(x) = f_i(x, ID_i)$ for each group member, and then encrypts (ε, $k_i(x)$, $F_i(ID_i)$) such as $Q_i = E_{\lambda_i}(\varepsilon \| k_i(x) \| F_i(ID_i))$, and finally sends Q_i to each group member. Where ID_i is the public identifier of the group member.

(6) GH_i computes $z_{\alpha\beta} = g^{b_{\alpha\beta}} \bmod p$ for $\alpha, \beta \in [0, t-1]$ and $\bar{z}_j = g^{a_j} \bmod p$ for $j \in [0, t-1]$, then publishes these as P2P network public information.

(7) On receiving Q_i, each group member computes $\lambda_i = y_{CH_i}^{\tau_i} \bmod p$, and decrypts Q_i and validates ($k_i(x)$, $F_i(ID_i)$) by checking if

$$g^{F_i(ID_i)} = \prod_{j=0}^{t-1} \bar{z}_j^{ID_i^j} \bmod p \quad , \tag{5}$$

$$g^{k_i(ID_G)} = \prod_{\alpha=0}^{t-1} \prod_{\beta=0}^{t-1} (z_{\alpha\beta})^{(ID_i)^\alpha (ID_G)^\beta} \bmod p \tag{6}$$

If they hold, then each group member obtains his partial secret share parameters (ε , $k_i(x)$, $F_i(ID_i)$).

2.3. Authentication control

The processes of mutual authentication and between group members n_i and n_j for the same group and between two group heads are described in the following.

Authentication between group members:

(1) The group member n_i chooses a random number $r_{i,}$ computes $A=h(f(ID_i,ID_j), {}^{\varepsilon,ID_i,ID_j,r_i,GN_i)}$, then sends (A, ID_i,ID_j, GN_i, $r_{i,}$) to n_j. Where GN_i is the public identifier of the group G_i.

(2) n_j computes $A'=h(f(ID_j,ID_i), {}^{\varepsilon}$, ID_i, ID_j,r_i, GN_i) and verifies $A=A'$. If it holds, then n_j can make sure that n_i is a legitimate member and has established their share session key $k_{ij}= h({}^{\varepsilon},f(ID_j,ID_i))$. n_j chooses a random number r_j, computes $B= h(f(ID_j,ID_i), {}^{\varepsilon,ID_i,ID_j,r_i,r_j,GN_i)}$, then sends (B, ID_i,ID_j, r_j) to n_i.

(3) n_i computes $B'=h(f(ID_i,ID_j), {}^{\varepsilon,ID_i,ID_j,r_i,r_j,GN_i)}$, and verifies $B'=B$. If it holds, then n_i can make sure that n_i is a legitimate member and has established their share session key $k_{ij}= h({}^{\varepsilon}$, $f(ID_i,ID_i)$). They can securely communicate each other.

Authentication between group heads:

(1) The group head CH_i chooses a random number $t_{i,}$ computes $W=h(CH_i, CH_j, {}^{\xi}, c(CH_i, CH_j), t_{i,})$, and sends (W,CH, t_i) to the group head CH_j.

(2) CH_j computes $W'= h(CH_i,CH_j, {}^{\xi}, c(CH_j, CH_i), t_{i,})$, and verifies $W=W'$. If it holds, then CH_j can make sure that CH_i is a legitimate group head and has established their share session key $K_{ij}= h({}^{\xi}, c(CH_j,CH_i))$. CH_j chooses a random number t_j, computes $E= h(CH_i,CH_j, {}^{\xi}, c(CH_j, CH_i), t_j, t_{i,})$, then sends ($E$, CH_j,t_j, t_i) to CH_i.

(3) CH_i computes $E'= h(CH_i,CH_j, {}^{\xi}, c(CH_j, CH_i), t_j, t_{i,})$, and verifies $E=E'$. If it holds, then CH_i can make sure that CH_j is a legitimate member and has established their share session key $K_{ij}= h({}^{\xi}, c(CH_i,CH_j))$. They can securely communicate each other.

2.4. Admission control

In this section, the admission control is described. If a prospective member wishes to join the group in order to access the network resources, he must obtain the group head approving admission. The admission control involves following steps:

(1) A prospective member n_{new} broadcasts joining request message containing his public key y_{new}, the group name, and timestamps etc. to group head.

(2) The group head GH_i verifies n_{new} the joining request, and computes $\lambda_{new} = y_{new}^{\tau_{CH_i}} \bmod p$ and the secret share parameters $k_{new}(x) = f(x, ID_{new})$, $F_i(ID_{new})$ for the new member, and encrypts (ε , $k_{new}(x)$, $F_i(ID_{new})$) such as, $W_{new} = E_{\lambda_{new}}(\varepsilon \| k_{new}(x) \| F_{new}(ID_{new}))$, and finally sends W_{new} to new member.

(3) On receiving W_{new}, new group member n_{new} computes $\lambda_{new} = y_{CH_i}^{\tau_{new}} \bmod p$, decrypts W_{new}, and validates ($k_{new}(x)$, $F_i(ID_{new})$) by checking if

$$g^{F_i(ID_{new})} = \prod_{j=0}^{t} g^{a_j ID_{new}^j} \bmod p \tag{7}$$

$$g^{k_{new}(ID_G)} = \prod_{\alpha=0}^{t-1} \prod_{\beta=0}^{t-1} (z_{\alpha\beta})^{(ID_{new})^\alpha (ID_G)^\beta} \bmod p \tag{8}$$

If they hold, the new member n_{new} is added into the group and obtains his partial secret share parameters (ε , $k_{new}(x)$, $F_i(ID_{new})$).

2.5. Revokcaiong control

When GH_i detects that some group members have misbehaving and malicious actions such as providing poor service etc., then the malicious members will be revoked from the group as following way. Assuming a group member n_B will be revoked.

(1) GH_i chooses a random number ν , computes $y = h(\nu)$ such as $y \neq F_i(ID_B)$ and constructs a polynomial $\overline{F}_i(x)$ using t-1 non-revoked members' (ID_i, $F_i(ID_i)$) excluding (ID_B , $F_i(ID_B)$) and a point (ν ,y) , that is

$\overline{F}_i(ID_i) = F_i(ID_i)(i = 1,2...,n, i \neq B)$, $\overline{F}_i(ID_B) \neq F_i(ID_B)$

(2) GH_i first chooses random numbers $\bar{\varepsilon}$ and w_j (j=1,2,…, t-1), computes

$$g^{\overline{F}_i(w_j)} \bmod p \ (\ j = 1,2,...,t-1), \tag{9}$$

$$\overline{\sigma} = g^{\bar{f}(0)} \bmod p\ ,\ \varpi = \bar{\varepsilon} + \overline{\sigma} \bmod q\ , \tag{10}$$

and publishes [(λ , w_j , $g^{\overline{F}_i(w_j)}$ (j=1,…,t-1))].

(3) A non-revoked group member N_i computes $\overline{\sigma}$ by himself (ID_i, $\overline{F}_i(ID_i)$) and public information (w_j, $g^{\overline{F}_i(w_j)}$ (j=1,…,t)) such as

$$\begin{aligned}\overline{\sigma} &= g^{F_i(ID_i)\prod_{l=1}^{t-1}\frac{-w_l}{ID_i - w_l}} g^{\sum_{j=1}^{t-1}\overline{F}_i(w_j)(\prod_{l=1,l\neq i}^{t-1}\frac{-w_l}{w_j - w_l})\frac{-ID_i}{w_j - ID_i}} \\ &= g^{\overline{F}_i(0)} \bmod p\end{aligned} \tag{11}$$

$$\bar{\varepsilon} = \varpi - \overline{\sigma} \bmod q \tag{12}$$

So a non-revoked group member can recover the secret key $\bar{\varepsilon}$. However, the revoked group member n_B cannot compute $\bar{\sigma} = g^{\bar{F}_i(0)}$ since his (ID_B, $F_i(ID_B)$ is excluded from the polynomial $\bar{F}_i(x)$ and does not satisfy the polynomial $\bar{F}_i(x)$, that is

$$\bar{\sigma} \neq g^{F_i(ID_B)\prod_{l=1}^{t-1}\frac{-w_l}{ID_B-w_l}} g^{\sum_{j=1}^{t-1}\bar{F}_i(w_j)(\prod_{l=1,l\neq i}^{t-1}\frac{-w_l}{w_j-w_l})\frac{-ID_B}{w_j-ID_B}} \bmod p$$

Therefore, the revoked user n_B cannot recover the secret key $\bar{\varepsilon}$, thus he cannot pass authentication with other non-revoked members since using secret key $\bar{\varepsilon}$ in authentication process (see section C). Therefore the group member n_B is revoked from the group.

3. Analysis

3.1. Correctness

Lemma 1. If a polynomial $\bar{F}_i(x)$ is constructed using t-1 non-revoked group member's (ID_i, $F_i(ID_i)$) excluding (ID_B, $F_i(ID_B)$) and a point (ν ,y) such $y \neq F_i(ID_B)$, then $\bar{F}_i(ID_B) \neq F_i(ID_B)$, $\bar{F}_i(ID_i) = F_i(ID_i)(i = 1,2...,n, i \neq B)$.
Proof: According to Lagrange interpolation know:

Given a set of t data points such as (ID_i, $F_i(ID_i)$) and (ν , y), where no two ID_i are the same and $i \neq B$, the interpolation polynomial $\bar{F}_i(x)$ in the Lagrange form is a linear combination as following

$$\bar{F}_i(x) = \sum_{i=1,i\neq B}^{t} F_i(ID_i) \prod_{l=1,l\neq i,l\neq B}^{t} \frac{x-ID_l}{ID_i-ID_l}\frac{x-\nu}{ID_i-\nu} + y\prod_{l=1,l\neq B}^{t}\frac{x-x_l}{\nu-x_l}$$

then $\bar{F}_i(ID_i) = F_i(ID_i)(i = 1,2...,n, i \neq B)$, $\bar{F}_i(ID_B) \neq F_i(ID_B)$.

3.2. Security Analysis

(1) The authentication control can guarantee that only legal group members can access the group resources. Each legal group members have secret keys (ε , $k_i(x)$) and can derive the valid authentication message A or B (see section C). However, an illegal group member will not be able to easily forge a valid authentication messages since they do not obtain secret keys (ε , $k_i(x)$), thus they cannot pass the authentication between group members, therefore the illegal group members cannot access the group resources.

(2) The proposed scheme can withstand a forgery attack. Because ε and $k_i(x)$ are generated by GH_i, and encrypted and transferred to each legal group member, so an illegal group member cannot obtain the secret keys (ε ,$k_i(x)$), thus they cannot generate valid authenticated messages to pass authentication. If a legal group member leaks secret key ε to an illegal group member, then the illegal group member cannot also pass authentication since he does not know secret key $k_i(x)$. If a legal group member n_i leaks secret keys ε and $k_i(x)$ to an illegal group member, the illegal group member must masquerade the legal member n_i in order to pass authentication since the authentication message includes the two authenticated member's identifier ID_i

or ID_j and secret key $k_i(ID_i)$ or $k_i(ID_j)$ (see section C). If the illegal member generates the authentication message using his identifier, the authentication message is easily detected since $k_i(ID_j) \neq k_j(ID_i)$. So he only can masquerade the legal member n_i in order to pass authentication. However, any legal member does not want other member to fake himself, therefore any legal group member cannot leak their secret keys ε and $k_i(x)$ to any illegal group member.

(3) The proposed scheme can resist the reply attack. In our scheme, a random number r_i or r_j is used one time when the group members mutually authenticate, so it can resist the reply attack.

(4) The proposed scheme can safely communicate. When a group member passes the authentication procedure with other member, a shared key $k_{ij}= h(\varepsilon, f(ID_j,ID_i))$has already established between them. The shared key between the two members is pair-wise, so it is used to safely communicate between the two members since the shared key is only know to two members. Moreover, because each shared key is only know to two members who established it, even if an attacker compromised member knows, he can only know what the compromised member knows, but not the shared keys between other non-compromised members. Hence, the security of the entire P2P network is not compromised.

(5) Security of the scheme is based on the discrete logarithm assumption and polynomials as long as the attacker is no allowed to corrupt more than (t-1) group members in a group. This is because an a attacker who corrupts at most (t-1) group members can only obtain at most (t-1) share polynomials that are less than a threshold t.

In other hand, obtaining the secret share of group members from public information ($z_{\alpha\beta}$, $\bar{z}_j$) are as difficult as solving the discrete logarithm problem.

3.3. Performance Analysis

(1) The proposed scheme has features with authenticating group members, adding new group members and revoking malicious group members (see sections C,D,E).

(2) The proposed scheme only needs to store two keys and a polynomial in each group member no matter how large the network size is.

(3) The scheme doesn't require any interaction between group head and group member when a new member is added and a malicious member is revoked. Three interactions are needed when two group members accomplish authentication each other.

(4) The computation cost for authentication phase is 4 hash function computations and 2 polynomial computations. The computation cost for adding a new member phase is 4 hash function computations and 2 polynomial computations; The computation cost for revoking group member phase is t modular exponent computations for a group head and a modular exponent computation for each group member.

4. Conclusion

This paper proposed a group-oriented access control scheme for P2P networks. The proposed scheme provides an efficient authentication and secure communication for group members. Member joining or removal is also simple and quick. Moreover, the proposed scheme also analyzes security and performances and shows that the scheme is secure and practical for P2P networks.

References

[1] N. Saxena, G. Tsudik, and J.H.Yi. Efficient Node Admission for Short-lived Mobile Ad Hoc Networks. 13th IEEE International Conference on Network Protocols, November 6-9, 2005, Boston, Massachusetts, USA.

[2] X,M.Wang. Decentralized Access Control Scheme for Dynamic Group. International Conference on Information Technology and Environmental Systems Sciences, 2008.

[3] Y.Zhou, Y.Zhang,Y.Fang, Access control in wireless sensor networks, Ad Hoc Networks 5 ,2007: 3–13.

[4] H.F.Huang. A novel access control protocol for secure sensor networks. Computer Standards & Interfaces 31,2009: 272–276.

[5] H.S.Kim, S.W. Lee. Enhanced Novel Access Control Protocol over Wireless Sensor Networks .IEEE Transactions on Consumer Electronics, Vol. 55, No. 2, MAY 2009.

[6] C. Blundo, A.D.Santis, A.Herzberg, S.Kutten, U.VaccaroU, and M. Yung. Perfectly-Secure Key Distribution for Dynamic Conferences. In CRYPTO'92, number 740 in LNCS, 1992:48-52

[7] M.Naor, B.Pinkas, and O.Reingold. Distibuted Pseudo -Random Functions and KDCs. In EUROCRYPT'99, number 1592 in LNCS, 1999: 327-346.

[8] D. Liu, P.Ning. Establishing Pairwise Keys in Distributed Sensor Networks. In ACM Conference on Computers and Communication Security, Oct. 2003: 52-61.

[9] G.F. Gu, B.B.Zhu etc. PLI: A New Framework to Protect Digital Content for P2P Networks.In: The International conference application and network security. Kunming, china, 2003:206-216.