Asian Journal of Information Technology 4 (10): 945-949, 2005

An Improved Efficient Self-healing Group Key Distribution

Sun Haibo, Lin Dongdai and Xue Rui
The State Key Laboratory of Information Security, Institute of Software,
Chinese Academy of Sciences,
The Graduate School of the Chinese Academy of Sciences, Beijing, 100080, China

Abstract: This study presents new group key distribution techniques for large and dynamic groups over unreliable channels. The techniques are based on the self-healing key distribution methods (with revocation capability) By introducing a novel personal key distribution technique, this paper reduces the communication overhead of personal key share distribution and the communication overhead of self-healing key distribution with t-revocation capability where t is the maximum number of colluding group members. Because this technique adopts the polynomial to realize, the degree of these polynomials determine the threshold of the number of colluding group members. And because this scheme is based on ID, so the identity of the excluded member will be open. In this paper, we improved a new scheme based on exponential function to avoid the limitation of threshold and at the same time, our scheme is not based on ID, the identity of member can be protected effectively. All these results are achieved without sacrificing the unconditional security of key distribution and overhead of communication and personal storage. In addition, two techniques proposed to allow trade-off between the broadcast size and the recoverability of lost session keys are also adaptive in present scheme.

Key words: Self-healing, group key distribution, threshold

INTRODUCTION

With the development of wireless networks, how to distribute and update the session key to group members has been one of the hotspot researches. In the wireless, such as military operations and rescue mission where there is usually no network infrastructure support, the adversaries can intercept or tamper the information freely. So it is necessary to encrypt and authenticated the messages in the communication. In recently years, researchers proposed many group key exchange schemes[1,2] to realize the secure communication among group members. These schemes provided a secure method to distribute a session key to valid members and only these members can communicate securely. Though some of these schemes can be used in wireless networks, some unique features of mobile wireless networks introduce new problems that have not been fully considered. For example, the users in wireless networks may move in and out of range frequently, how to distinguish these users and intended attacker and how to recover the lost session key by these valid members. So the schemes used in wireless networks must have the fault tolerant features. In addition, in the wireless networks, the users usually don't have the same power of computation as in the traditional network. Thus, not all of the existing techniques are suitable for large and dynamic wireless networks. In Staddon *et al.*[3], the authors adopt self-healing key distribution that allows group members to recover lost session keys. In liu *et al*[1], the author improved the scheme proposed in by Staddon *et al.*[3] to reduce the communication overhead of personal key share distribution and the self-healing key distribution with t-revocation capability and the storage overhead of each group member where t is the maximum number of colluding group members. But because this scheme adopts the polynomial to realize, it is inevitable to have the limitation of threshold. In addition, this scheme is based on ID, so the identity of these excluded member are leaked. In this scheme, it requires that if a user is excluded once, he can't join the group forever, so it maybe necessary to protect the identity of all members. Our scheme is not based on the ID to avoid the problem and we use exponential function to substitute polynomial to eliminate the limitation of the threshold. Our scheme is achieved without sacrificing the unconditional security of key distribution and the communication and storage overhead. In addition, the two techniques used in by liu *et al*.[4] that allow trade-off between the broadcast size and the recoverability of lost session keys are also adaptive in present.

Corresponding Author: Sun Haibo, The State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, 100080, China,
Tel: 86-10-62654046

Our present has several advantages. First, the scheme is also self-healing; a valid user can recover lost keys even if he is separated from the network when the keys are distributed. Second, this scheme remains the communication overhead and storage overhead as the scheme proposed by liu *et al.*[4] the users could get or recover keys by passively listening to broadcast key distribution messages that is important to wireless devices. Third, the overheads of communication and storage don't depend on the size of the group, the security of our scheme don't depend on the number of compromised group members that may collude together. The organization of this paper is as follow. The first, we introduce the basic definition and the scheme in of liu *et al.*,[4] then we propose the improved scheme and the analysis of the security properties[5,6] of this scheme. In the end, the conclusion and the future directions.

THE BASIC DEFINITION AND SCHEME

In this section, we will introduce some basic definition and the scheme proposed by liu *et al.*[4]. We first assume that there exist a group manager to distribute the personal share and broadcast distribution messages to group member and the manager is reliable. The time interval in wireless called sessions and the duration of sessions may be fixed or dynamic due to the change of group membership. In addition, the attacker may comprise one or more group members, we assume that once detected, such members will be revoked from the group and can't join in the group again. By liu *et al.*[4] it also assume the number of members comprised by attacker is no more that t that is decided by the degree of polynomial. But in our scheme, we don't need this assumption.

Notations: All of our operations take place in a finite field F_q where q is a sufficiently large prime number. Each group member U_i stores a personal secret $S_i \subseteq F_q$ which is the information used by group member to recover the lost key. We use K_j to denote the session key that the group manager distributes to the group members in session j. We use B_j to denote the broadcast message that the group manager uses to distribute the group session key during session j.

Definition 1: D is a key distribution scheme if

- For any member U_i, K_j is determined by B_j and S_i.
- For any $R \subseteq \{U_1,...,U_n\}$ and $U_i \notin R$, the members in R can't determine S_i.
- What members $U_1,...,U_n$ learn from B_j can't be determined from the broadcasts or personal keys alone.

Definition 2: If for any $R \subseteq \{U_1,...,U_n\}$, the group manager can generate a broadcast message B_j such that for all $U_i \notin R$, U_i can recover the session key but the revoked members can't, we call D has revocation capability.

Definition 3: Suppose $1 \le j_1 < j < j_2 \le m$ (m is the number of sessions). If for any U_i who is a member in session j_1 and j_2, K_j can be determined by B_{j1}, B_{j2} and S_i, we call D is self-healing.

Definition 4: If for a key distribution scheme D, in session j, the session key K_j only can be obtained from the broadcast message by valid member, any revoked member can't get it and the personal secret even many such members collude together, we call D satisfy secrecy.

Definition 5: If for any set $R \subseteq \{U_1,...,U_n\}$, and all $r \in R$ are revoked before session j, the member in R together can't get any information about K_j, even with the knowledge of group session keys after session j, we call the scheme D guarantees forward secrecy.

Definition 6: If for any set $R \subseteq \{U_1,...,U_n\}$, and all $r \in R$ join after session j, the member in R together can't get any information about K_j, even with the knowledge of group session keys before session j, we call the scheme D guarantees backward secrecy.

In this study, our security analysis focus on the secrecy , forward secrecy and backward secrecy. The authentication should be complete before the Key distribution, so we don't discuss it here.

Following we will introduce the key distribution proposed by Staddon *et al.*[3]. We first introduce the personal key share distribution because it is the basic idea of the session key distribution. In this approach the manager first chooses a random t-degree polynomial f(x) from $F_q(x)$, and f(i) to be the personal key share for U_i. Then the manager construct broadcast polynomial w(x) such that for any valid U_i, f(i) can be recovered from w(x) and the personal secret S_i. The material scheme is as follow:

Scheme 1. Basic personal key share distribution scheme

- The group manager randomly picks 2t-degree masking polynomials, h(x) from $F_q(x)$. Each group member U_i gets the personal secret $S_i=\{h(i)\}$, via the secure communication channel.
- Given the set of revoked group members $R=\{r_1,r_2,...r_w\}$, here the $r_1,r_2,...r_w$ are the ID of revoked members, $|R| \le t$, the group manager distributes the

Shares of t-degree polynomial f(x) to non-revoked group member by broadcasting message
$B = \{R\} U \{w(x) = g(x)f(x) + h(x)\}$, here
$g(x) = (x- r_1)(x- r_2)...(x-r_w)$.

- For any non-revoked group member U_i, it evaluate the w(x) at point i. Because U_i knows h (i) and g(i)≠, 0 i t can compute the personal share as
$f(i) = \frac{w(i) - h(i)}{g(i)}$.

Obviously, in this scheme, any non-revoked member can effective computer the personal share from the broadcast message and his personal secret. But for revoked member $U_{i'}$,the $g(i') = 0$, so w,(i') =h(i') and he can't get any information of f(x). From the degree of w(x), everyone can know t+w-1 coefficients of h (x). But it is helpless to recover the h (x). At the same time, by conditions, the number of colluding members is no more than t, they can't determine the f(x) from t value. So these revoked member can't get the session key and other valid members' secret S_i.

Liu *et al.*[4] also give a material self-healing key distribution with revocation capability. In session j, when the manager need to distribute K_j to group members, he randomly splits K_j into two t-degree polynomials $p_j(x)$ and $q_j(x)$ such that $K_j = p_j(x)+ q_j(x)$. Then he distribute the $p_j(x)$ and $q_j(x)$ to valid members just as the distribution of f(x) in above scheme. In order to make the members can recover the lost session key, in one session, the manager need to broadcast more distribution messages so that the information obtained in session j by member U_v is $\{p_1(v),...,p_{j-1}(v),K_j,q_{j+1}(v),...q_m(v)\}$.So when some member lost some session key, he can recover it from the value of q(x) obtained from former session and the value of p(x) obtained from latter session. The material scheme is similar to the scheme above, it can be found in liu *et al.*[4] Also, in our scheme, we will adopt the similar technology to realize self-healing, so we don't introduce the details of the scheme here.

In the discussion above, the scheme proposed in liu *et al.*[4] adopt the polynomial to realize the group key distribution and members' self-healing. The overhead of communication and each member's storage is relative small and the users don't need heavy computation. But obviously, there exist a strong limitation in this scheme. The max number of colluding members is decided by the degree of these polynomials chosen by group manager. In another word, the group manager needs to estimate the bound of the number of attackers. But usually in network the change of membership is hard to be forecasted, so this scheme has restriction in actual applications. In next section, based on the same basic idea, we will propose an improved scheme realized by exponential function. our scheme can also realize secure group key distribution and self-healing and remain the overhead of communication and storage as above scheme.

IMPROVED SELF-HEALING GROUP KEY DISTRIBUTION SCHEME

In this section, we will introduce an improved Self-Healing Group Key Distribution scheme based on the same basic idea as liu *et al.*[4] We also will analyse the security of our scheme. The scheme is as follow:

Scheme 2: Improved self-healing session key distribution scheme

- The group manage randomly choose a system parameter α and make each member know it. Then he randomly picks 2m 1-degree masking polynomials $\{h_i(x) = a_i x + b_i\}_{i=1,2,...,m}$ and $\{f_i(x) = a_i' x + b_i'\}_{i=1,2,...,m}$. Each member U_v randomly chooses a nonce r_v and transmits it to the group manager and gets its personal secret $S_v = \{\alpha^{h_i(v)}, \alpha^{f_i(v)}\}_{i=1,2,...,m}$ from the group manager via the secure communication channel. The group manager also picks m random n umber $\{k_i\}_{i=1,2,...,m} \subset F_q$ and set the session keys $K_i = \alpha_{ki}$Then he also picks m random polynomials f $\{p_1(x),...,p_m(x)\}$ From $F_q(x)$, construct $q_i(x) = k_i - p_i(x)$.
- In the j-th session, given the sets of revoked members for sessions in and before session j. $R_i = \{r_1, r_2,..., r_{w_i}\}_{i=1,2,...,j}$, the group manager constructs

$$g_i(x) = \prod_{k=1}^{w_i} (\alpha^{\frac{x}{r_1 r_2 ... r_{w_i}}} - \alpha^{\frac{r_k}{r_1 r_2 ... r_{w_i}}}) \quad 1 \le i \le j$$

Then the group manager broadcasts the following messages:

$$B_j = \{g_i(x)\}_{i=1,...,j} U$$
$$\{P_i(x) = g_i(x)\alpha^{p_i(x)} + \alpha^{h_i(x)}\}_{i=1,...,j}$$
$$U\{Q_i(x) = \alpha^{q_i(x)} + \alpha^{f_i(x)}\}_{i=j,...,m}$$

- When a non-revoked group member U_v receives the B_j, he uses r_v chosen by himself to evaluate $\{P_i(x)\}_{i=1,...,j}$ and $\{Q_i(x)\}_{i=j,...,m}$, recovers the shares $\{\alpha^{p_1(r_v)},...,\alpha^{p_j(r_v)}\}$ and $\{\alpha^{q_j(r_v)},...,\alpha^{q_m(r_v)}\}$, and then computes the current session key $K_j = \alpha^{k_j} = \alpha^{p_j(r_v)+q_j(r_v)} = \alpha^{p_j(r_v)} g\alpha^{q_j(r_v)}$.
The memberalso stores

$$\{\alpha^{p_1(r_v)},...,\alpha^{p_{j-1}(r_v)}, K_j, \alpha^{q_{j+1}(r_v)},..., \alpha^{q_m(r_v)}\}$$

- When a new member (suppose to U_n) wants to join the group starting from session j. He picks a nonce r_n and transmits it to group manager. Then the group manager computes all $\{h_i(n)\}_{i=j,\ldots,m}$ and $\{f_i(n)\}_{i=j,\ldots,m}$ and gives $\{\{\alpha^{h_i(n)}\}_{i=j,\ldots,m}, \{\alpha^{f_i(n)}\}_{i=j,\ldots,m}\}$ to the new member via secure communication channel.

If a group member U_i receives session key distribution messages in sessions j_1 and j_2 but not in session j, where $1 \le j_1 < j < j_2 \le m$, he can recover the lost session key K_j by recovering $\alpha^{p_j(r_i)}$ from the broadcast messages in sessions j_2 and $\alpha^{q_j(r_i)}$ from the broadcast messages in session j_1 and then computing.

$$K_j = \alpha^{p_j(r_i)} g \alpha^{q_j(r_i)}$$

In the following we will analysis the security of scheme 2.

Theorem 1 Scheme 2 is an unconditionally secure, self-healing session key distribution scheme with revocation capability.

PROOF. To prove this theorem is correct, we need to prove scheme 2 satisfies all six definitions.

- From the description of scheme 2, obviously, for any member U_i, he can computer the session key K_j using the broadcast message B_j and his personal secret S_i. For any $R \subset \{U_1,\ldots,U_n\}$, and $U_i \notin R$. They have two ways to determine S_i. The first is from the $\{h_i(x) = a_i x + b_i\}_{i=1,2,\ldots,m}$ or $\{f_i(x) = a_i' x + b_i'\}_{i=1,2,\ldots,m}$ directly. We suppose $|R| = t$, in another word, there are t member collude to determine the personal secret of U_i. In session j, What they have know is $\{r_1,\ldots,r_t, \alpha^{a_j r_1 + b_j},\ldots,\alpha^{a_j r_t + b_j}, \alpha^{a_j' r_1 + b_j'},\ldots,\alpha^{a_j' r_t + b_j'}\}$. If they want to determine S_i in session j, they must determine $h_j(x) = a_j x + b_j$ and $f_j(x) = a_j' x + b_j'$ first and they must hold the nonce r_i. But wo know the r_i is only known by user U_i and the group manager. In addition, determine $h_j(x) = a_j x + b_j A$ and $f_j(x) = a_j' x + b_j'$ from $\alpha^{hj(X)}$ and $\alpha^{fj(x)}$ is equal to solve discrete logarithm. It is computational infeasible. Another way is to determine S_i by the broadcast message, but it also requires there conspirators hold r_i and determine the $p_j(x)$ and $q_j(x)$ first, which is also equal to solve discrete logarithm. So the members in R can't determine S_i. From the third step of scheme 2, the computation of the session key must depend on the broadcast message and the personal key at the same time. So definition 1 can be satisfied.
- In session j, when give the set of revoked members $R \subset \{U_1,\ldots,U_n\}$, the group manager constructs $g_i(x)\ 1 \le i \le j$ the and broadcast relative messages as described in step 2 of scheme 2. Obviously, for any non-revoked member, he can recover the K_j as above. But for any revoked memberU_v, $g_j(r_v) = 0$ and $\{P_j(r_v)\} = h_j(r_v)$. He can't compute the correct K_j. So scheme 2 has revocation capability.
- Suppose $1 \le j_1 < j < j_2 \le m$. If a group member U_i receives session key distribution messages in sessions j_1 and j_2 but not in session j, he can recover the session key K_j. How to recover it we have described in scheme 2.
- Assume a collection R of t revoked group members colludes. In session j, after the group manager broadcast the key distribution messages. What they can know is at most t points on $\alpha^{qj(x)}$ and nothing on $\alpha^{pj(x)}$. Because $\alpha^{fi(x)} = Q_i(x) - \alpha^{qi(x)}$, if they want to get some valid member's secret, they must determine the $\alpha^{qi(x)}$ firstly. But we know, determining $\alpha^{qi(x)}$from arbitrary set of points is equal to solve discrete logarithm, it is computational infeasible. In addition, for any collection of revoked group members, $g_j(x)=0$ and $\{P_j(x)\} = h_j(x)$.They can't get $\alpha^{pj(x)}$ and the session key K_j. So, scheme 2 satisfies secrecy.
- By our basic assumption, the sets of revoked group members must change monotonically. That is, $R_{j_1} \subset R_{j_2}$ for $1 \le j_1 \le j_2 \le m$. Otherwise, if a group member that is revoked in session j_1 rejoins the group in session j_2, he can recover the session key $K^{j1}$by$\alpha^{q_{ji}(x)}$ restored in session before j_1 and $\alpha^{q_{ji}(x)}$ computed from the key distribution messages received in session j_2. So under our basic assumption, once member U_v is revoked in session j, the $g_i(r_v)_{i=j,\ldots,m} = 0$ and he can't compute the $\{\alpha^{p_i(x)}\}_{i=j,\ldots,m}$ sothe forward secrecy can be satisfied. If a new member U_n join the group in session j, according to our scheme, he can get $\{\{\alpha^{h_i(n)}\}_{i=j,\ldots,m}, \{\alpha^{f_i(n)}\}_{i=j,\ldots,m}\}$ and farther compute the $\{\alpha^{p_i(x)}\}_{i=j,\ldots,m}$ and.$\{\alpha^{q_i(x)}\}_{i=1,\ldots,j-1}$ But he can't get and . So he can't get the session key in former sessions. The backward secrecy can be satisfied.

From discuss above, scheme 2 satisfies all definitions described.

In the scheme proposed in By liu *et al.*[4] all the functions are polynomial functions. Suppose in scheme 1 $W(x) = g(x) f(x) + h(x)$, the degree of f (x) is t, h (x) is 2t. Then if the number of colluding group members exceed t, from the known point of these member, the f (x) can be uniquely determined and also because this scheme is

based on ID, these colluding members can get any other member's personal secret. So the scheme proposed By staddon *et al.*[3] has the limitation of the number of colluding group members. But in our scheme, we use exponential functions to substitute polynomial functions. To determine a exponential function by finite point is impossible, so our scheme don't have the threshold limitation.

Following, we attempt to give the overhead of communication and personal storage in our scheme.

The storage requirement in scheme 2 comes from two parts. First, in the first step, each group member is required to store the personal secret, which occupies 2 m log q memory space. Moreover, in order to recover from message loss, each member needs to store one share of each session key or the session key itself if it has both shares, which totally require m log q memory space. So the overall storage overhead in each member is at most 3m log q. It is the same to the scheme in 2. The broadcast message in session j consists of j+m+1exponential functions. Because α is public, the degree of $f_i(x)$, $h_i(x)$is 1, the degree of $p_i(x)$ and $q_i(x)$ is not required too high, so the overhead of communication mainly focus on the $g_i(x)$ which depend on the number of revoked members. Because of the indetermination of degree of $p_i(x)$,$q_i(x)$ and the number of revoked members. The overhead of communication is hard to determine, but compare to the scheme in of liu *et al.*[4] in the scope of the threshold, the overhead of communication is similar. In addition, our scheme doesn't have the limitation of the number of collude members. So in some actual wireless network where the number of attacker can't be estimated, our scheme is much more adaptive. Also in liu *et al.*[4], suggest two techniques that allow trade-offs between the broadcast message size and the recover ability of lost session keys. These two techniques are also available in our scheme. Because of the limitation of space, we don't describe these two techniques in detail.

CONCLUSIONS

In this study, we presented an improved efficient self-healing group key distribution scheme for large and dynamic groups over unreliable channels. By introducing exponential function to substitute polynomials, we avoid the limitation of the number of colluding members and presented scheme 2 is an unconditionally secure and self-healing group key distribution scheme without sacrificing the unconditional security of key distribution and the overhead of communication and personal storage. Of course the exponential computation is more complex than the polynomial computation. So our scheme need the wireless nodes have more powerful device. But in some wireless network, where the users have enough computational ability, such as military operations or scientific explorations, our scheme is more adaptive.

REFERENCES

1. Wallner, D., E. Harder and R. Agee, 1999. Key management for multicast: Issues and architectures. IETF Request for Comments, RFC 2627,
2. Wong, C.K., M.G. Gouda and S.S. Lam, 1998. Secure group communications using key graphs. In ACM SIGCOMM 98, pp: 68-79.
3. Staddon, J., S. Miner, M. Franklin, D. Balfanz, M. Malkin and D. Dean, 2002. Self-healing key distribution with revocation. In Proc. 2002 IEEE Symp. Security and Privacy, pp : 224-240.
4. Liu, D., P. Ning and K. Sun, 2003. Efficient self-healing group key distribution with revocation capability. In: Proc. 10th ACM Conf. Computer and Communications Security, (CCS '03),
5. Perrig, A., D. Song and J.D. Tygar. 2001. ELK. A new protocol for efficient large-group key distribution. In: Proc. IEEE Symp. Security and Privacy, pp: 247-262.
6. Steiner, M., G. Tsudik and M.Waidner, 2000. Key agreement in dynamic peer groups. IEEE Trans. on Parallel and Distributed Systems, 11:769-780.