I.J. Education and Management Engineering **2012, 3, 7-13**
Published Online March 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2012.03.02

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

An efficient Group Key Management Scheme for Ad Hoc Networks

Wenqi Yu[a,b,*]

[a] *Department of Computer Science and Engineering, Henan Institute of Engineering, Zhengzhou 451191, China*
[b] *School of Journalism and Information Communication, Huazhong University of Science and Technology, Wuhan 430074, China*

Abstract

Ad Hoc networks are characterized by frequently changing network topology. Due to the lack of central authority, forming security association among a group of members in Ad Hoc networks is more challenging than in traditional networks. With the view in mind, group key management plays an important building block of any secure group communication. In this paper, we proposed a group key management based on Identity-based Cryptosystem and Chinese Remainder Theorem. In the proposed scheme, there are no requirements of member serialization and existence of a central entity. Besides this, the scheme the protocol also many highly desirable properties such as contributory and efficient computation of group key, uniform work load for all sensor nodes and efficient support for high dynamics. Compare to other existing group key agreement protocols, the proposed protocol make no assumption about the structure of the underlying wireless network, making it suitable for Ad Hoc networks.

Index Terms: Ad Hoc Networks; Group Key Management; Chinese Remainder Theorem; Identity-based Cryptosystem

1. Introduction

Ad Hoc networks are a collection of autonomous nodes that communicate with each other, in which nodes do not necessarily know each other and come together to form an ad hoc group for some specific purpose. Ad Hoc networks are communicated over wireless channels in the absence of any fixed infrastructure. Moreover, network composition is highly dynamic with devices leaving /joining the network quite frequently. Due to lack of trusted third parities, expensive communication, ease of interception of messages and limited computational capabilities of the device, securing such networks becomes a challenging task.

To secure communication in Ad Hoc networks, messages are often protected by encryption using a chosen cryptographic key, which the scenario of group communication is called group key. Only the members in the group, who know the current group key, are able to recover the original message. Group key management

* Corresponding author:
E-mail address: [*] wqy@163.com

schemes have long attracted intensive research interests from the literature. The most na ïve approach for group key management is the master key approach in which there is one master key pre-deployed in each node. This approach is memory efficient, but has very poor security and key redistribution is difficult. Another approach[1] is the pairwise approach in which the central server or group controller maintains a pairwise key with each node and distributes the group key via unicast to each node, this approach is very secure but communication and memory overhead is intolerable for Ad Hoc networks and scalability is an obstacle difficult to overcome.

Many cryptographic protocols have been developed to provide group key for group communication [2,3,4,5,6], most of which are derived from the two-party Diffie-Hellman (DH) key agreement protocol[7]. While some are secure against passive adversaries only, other dos not have a rigorous security proof. The protocol in [3] first provided provably secure protocols in a well-defined model of security. Yung et al.[4] proposed a scalable "compiler" to transform a group key agreement protocol, into which is secure against an adversary. But one round

Group key management mainly includes activities for the establishment and maintenance of a group key. Secure group communication requires scalable and efficient group membership with appropriate access control measures to protect data and to cope with potential compromise. In the case of communication, when a member joints a group, the group key is re-keyed to ensure that the new member cannot decrypt previous messages. This is a requirement known as backward secrecy. When a member leaves the group, the group key is re-keyed to ensure that future communications cannot be decrypted by the leaving member. This requirement is known as forward secrecy.

In this paper, we propose an efficient group key management scheme based on bivariate polynomial and Chinese Remainder Theorem. In the scheme we use a contributory key agreement protocol for key generation which does not require a centralized key server. The scheme can revoke illegitimate nodes from the group, while being resistant to coalition of *t* compromised nodes. There are only 2 rounds for the initial key formation and join and 1 round for leave. And ever member in the Ad Hoc networks is treated equally and has to perform the same amount of the work to compute the group key. Hence, the communication overheads are saved and the energy consumption overall network is similar.

The remainder of this paper is organized as follows. Section I gives the backgrounds of the proposed scheme in this paper. Section II presents our proposed scheme in detail. Section III deals with the detailed performance analysis and comparisons and section IV conclude this paper.

2. Background

In the following, some basic fact and conclusion the CRT will be summarized.

2.1. Chinese Remainder Theorem (CRT) Overview

Theorem 1 (Chinese Remainder Theorem) Let n_1, n_2, …, n_k be pairwise relative primes, ie. GCD(n_i, n_j)=1, $i \neq j$. Let let r_1, r_2,…r_k be integers. Then the congruent equations

$$\begin{aligned} x &\equiv r_1 \bmod n_1 \\ x &\equiv r_2 \bmod n_2 \\ \ldots &\quad \ldots \\ x &\equiv r_k \bmod n_k \end{aligned}$$

have a unique solution:

$$x = \sum_{i=1}^{k} r_i N_i^{'} N_i (\bmod N)$$

where

$$N = \prod_{i=1}^{k} n_i = n_1 n_2 \cdots n_k$$

$$N_i = \frac{N}{n_i}$$

$$N_i^{'} = N_i^{-1} (\text{mod} n_i)$$

We call n_1, n_2,…,n_k the CRT *moduli* and x the CRT *solution*.

Corollary 1.1 If the integers n_1, n_2,…n_k are pairwise relative prime and N=n_1n_2…n_k, then for all integers a, b it is always valid that $a\equiv b$ mod n if and only if $a\equiv b$ mod n_i for each i=1,2, …,k.

As a consequence of the CRT, any positive integer a<n can be uniquely represent as k-tuple [a_1, a_2, , …a_k] and vice versa, whereby a_i denotes the residue a mod n_i for each i=1,2, , …, k . The conversion of a into the residue system defined by n_1,n_2, , …,n_k is simply done by modular reductions a mod n_i. Conversion back from residue representation to "standard notation" is somewhat more difficult as it requires the calculation stated in the equation.

2.2. Bilinear Pairing

Let G_1 be an additive group of points on an elliptic cure and G_2 be a multiplicative group of a finite field. The order of both groups is q, where q is a large prime and the discrete logarithm problem in Z_q^* is intractable. A bilinear pairing is computable bilinear map between two groups, which could be the modified Weil pairing of the modified Tate Pairing [8,9]. A modified Weil pairing [8] is a bilinear map e: $G_1 \times G_1 \rightarrow G_2$, which satisfies the following conditions:

(1) Bilinear: if P, Q, $R \in G_1$, and $a,b \in Z_q^*$, $e(P+Q, R)=e(P, R)e(P, Q)$, and $e(P, Q)^{ab}=e(aP, bQ)$.

(2) Non-degenerate: There exists P,Q$\in$G1 such that $e(P, Q)\neq 1$.

(3) Computability: There exist efficient algorithms to compute $e(P,Q) \in G_1$.

Definition 1 BDH problem: Given P, aP, bP, $cP \in G_1$, where a, b and c are random numbers from Z_q^*, compute $e(P, P)^{abc} \in G_2$.

Definition 2: CDH problem: Given P, aP, bP,$\in G_1$, where a and b are random numbers from Z_q^*, compute $abP \in G_1$.

BDH problem assumption and CDH problem assumption: There exists no algorithm running polynomial time to solve BDH problem and e CDH problem with non-negligible probability

C. Identity-based Cryptosystem

The Identity-base cryptosystem was first introduced by Shami [10] to simplify the conventional public key cryptosystem (PKCS) and make key management easier. Since then different schemes were suggested in [8,9]. In an identity-based cryptosystem, there is no online trusted authority to verify the validity of their certificate. They are bound to their unique identifier and their private key is obtained for a key generation center (KGC) while their public key is determined with their identity. The center, KGC, can go off-line after the setup of common system parameters and the distribution of keys to users. The basic operations in identity-based consist of "Set Up" and "Private Key Extraction". Let G_1 and G_2 denote two groups of prime order q. q is a prime which is large enough to make solving discrete logarithm problem in G_1 and G_2 infeasible. Let P is a generator of G_1, and the MapToPoint function [4] ,denoted as H_1, encodes the identity of the user to a point in the group G_1. The output point takes the entity's public. That is $Q_A=H_1(ID_A)$ is the public key of user A with identity ID_A. e be a bilinear pairing.

Set Up: The KGC compute his public key $P_{pub}=sP$, where s is the KGC's private key. Then the KGC publishes the system parameters { G_1, G_2, q, P, Ppub, H_1, H_2, e}

Private Key Extraction: For each registered user, the KGC computes the user's public key as $Q_{ID}=H_1(ID)$ and return the private is $S_{ID}=sQ_{ID}$ via a secure channel.

3. The Proposed Scheme

In this section, we will discuss the detail of our proposed group key agreement protocol, Bivariate Polynomial and Chinese Remainder Theorem (BPCRT) based scheme for secure group communications. The different steps of the key establishment process and the join/leave operation are discussed in detail.

3.1. Initialization

Initially, the system sets up the parameter (G_1,G_2,P,q) as specified in previous section , where G_1 and G_2 are of the same prime order q, P is the generator for G_1, and e is the bilinear pairing. The system randomly select s as the private key, where $s \in Z_q^*$, then compute the public key $P_{pub}=sP$. Suppose H_1 and H_2 are secure one-way hash function:

$$H_1:\{0,1\}^* \to G_1 ,\ H_2:G_2 \to \{0,1\}^* ,$$

Assume each node U_i with a unique identity ID_i, it public key is given by $Q_i=H_1(ID_i)$ and the private key is $S_i=sQ_i$.

3.2. Group Key Agreement

In order to establish the group key, each node should execute the following steps.

Step 1: Each member M_i choose a random number $r_i \in Z_q^*$ as its ephemeral private key. Then node M_i computes and broadcasts $\{T_i=r_iP,\ R_i=H_2(T_i)S_i\}$ to all other members and keep r_i secret.

Step 2: When member M_i receives the broadcast message from member M_j, member M_i verifies:

$$e(P_{pub}, H_2(T_j)Q_j) = e(P, R_j)$$

If this is true, it computes:

$$M_{ij}=e(T_i, T_j)$$

It obvious that

$$M_{ij} = e(T_i,T_j) = e(r_iP,r_jP) = e(P,P)^{r_ir_j}$$
$$= e(r_jP,r_iP) = e(T_j,T_i) = M_{ji}$$

then member M_i computes the pair key shared with each of member in the group

$$m_{ij}=H_2(M_{ij})$$

where $j=1,\ldots,i-1,i+1,\ n$ and $j\neq i$, here n is the number of members in the group.

Step3: Find the Least Common Multiple (LCM) of the all the pairwise key calculated in Step2 as lcm_i.

Step 4: Select a random k_i, such as $k_i < \min(m_{ij}, \forall j)$, which will be its share of the group key. Also select an arbitrary number r such that $r \neq k_i$ and another number t such the gcd $(t, lcm_i)=1$

Step 5: Solve the CRT

$$crt_i \equiv k_i \bmod lcm_i$$

$$crt_i \equiv r \bmod t$$

Step 6: Receive the *crt* value from all the other members in the group and calculate

$$k_j = crt_i \bmod m_{ij} \text{ for all } j \neq i$$

and then compute the group key

$$\mathrm{GK} = k_1 \oplus k_2 \cdots \oplus k_n$$

As it can be been from the above steps, the Chinese Remainder Theorem is used to send each member's key share to the other entire member in the group. The Identity-base cryptosystem is performed to derive the modulo value in the CRT calculation.

3.3. Join Operation

The operations to be performed when a new member joins a group are explained blow. Let us assume the member M_{n+1} wishes to join an existing group of n members $\{M_1, M_2, \ldots, M_n\}$

Step1: All the current members $\{M_1, M_2, \ldots, M_n\}$ should compute the hash of the current key GK i.e. $h(GK)$. One of the existing members, say member, should transmit this hash value $h(GK)$ and the T_i of all members to the new member n+1.

Step 2: Member n+1 will execute the steps given in the previous section and broadcast the CRT value crt_{n+1} along with its ID.

Step 3: Existing member should compute the pairwise key they share with the member $n+1$ and thereby calculate the key k_{n+1} selected by the member $n+1$. The new group key GK_{new} is computed by XORing the hash

the current key and the key share of the newly jointing smember n+1

$$\mathrm{GK}_{\mathrm{new}} = h(GK) \oplus k_{n+1}$$

From the above steps we can clearly see that only the newly jointing member does the bulk of the work. The existing member only no minimal works in receiving the new key share and XORing with the hash of the old group key.

The hash of the old key is sent to the jointing member since it should receive the shares of the existing member but also not be able to read the messages sent to the group previously.

If there are many members joint the group, all the jointing member should execute the above steps to contribute their share towards the group key. This makes multiple joints very efficient since existing members only perform XOR operations with all the contributed key shares. Also, there are only two rounds of communication in the joint operation.

3.4. Leave Operationse

The leave operation is similar to the joint operation but it needs only one round communication. Let us assume member i is going to leave the group. Then the following operation need to be performed to recomputed the group key.

Step 1: Any one the remaining members, say member *j*, finds the Least Common Multiple (LCM) of the all the pairwise key *Lcm* with all other member except the members *i.* Then it selects a new random *K*, such as $K < \min(K_{ij}, \forall j)$, as its new share of the group key. Also it select an arbitrary new number *R* such that $R \neq K$ and another new number *S* such the gcd (*S*, *Lcm*)=1, solve the CRT

$$Crt \equiv K \bmod Lcmj$$

$$Crt \equiv R \bmod S$$

At last, the member j broadcast *Crt* to the members in the group.

It is obvious that when a member leaves the group, only one of the existing members does the major portion of the work.

In case of multiple leaves, all the leaving members should be left out of the computing the LCM as shown above. There is no extra computation is needed since the protocol need not be repeated for each leaving member. Thus the PCRT protocol efficiently supports leave operations and more importantly multiple leave operation is a single round of computation.

4. Performance Analysis

We analyze the proposed scheme to verify that it satisfies the security and performance requirements for secure group communication described in Section Ⅰ.

4.1. Overhead Analysis

The Identity-base cryptosystem and the Chinese Remainder Theorem are not very computationally intensive. And they have been used in the pair key management of Ad Hoc networks. Communication wise the scheme involves only two rounds for initial group key agreement and joint operations and only one round for leave operation.

More importantly for Ad Hoc networks, serialization or ordering of group members and communication is not required for the proper execution of the scheme. Every member in the Ad Hoc network is treated equally and has to perform the same amount of work to compute the group key.

4.2. Security Anslysis

The proposed scheme is effective in defeating attacks on Ad Hoc networks as follows.

First, if an attacker attempt to obtain the group key, he must have the key shares m_i which is selected by each member. To have the key share m_i, he has to get the pairwise key k_{ij} computed by the members. This method depends upon breaking Identity-base cryptosystem.

Second, the proposed scheme ensures backward secrecy and forward secrecy. The compromised members and leaving can be revoked by rekeying the group key. Once new joining members are going to joint the group, a new group key is created. Thus the joining members are denied access to previous communication.

Third，the group key is implicitly authenticated at members. The group key is computed by each member's key share. So the members are assured that no other members except the partners who have the private key can learn the group key.

Last, there is no key control. The group key in the scheme is determined by all members in the group, so that no member alone can control the outcome of the group key.

5. Conclusion

Group key management is one of the most critical technologies in Ad Hoc networks. This paper proposed an efficient group key management using Identity-base cryptosystem and Chinese Remainder Theorem. The proposed scheme does not require member serialization and a central entity, which can enhances the tolerances of Ad Hoc networks to corrupted nodes. It also efficiently support single/multiple members join/leave operation, which is an important factor in Ad Hoc network. The analysis shows the computation cost and communication cost are greatly reduced by our scheme, and the security of the group communication is improved.

References

[1] H.Harey, C.Muckenhirm. “Group key management protocol (gkmp) arthitecture”, IETF Request for comments, RFC 2094, 1997

[2] C.Boyd , J.Nieto. “Round-optimal contributory conference key agreement.” in: the 6th Internagitonal Workshop onTheory and Practice in Public Key Cryptography.2003.pp.161-174

[3] E.Bresson, O.Chevassut, and D.Pointcheval. “Dynamic group Diffie Hellman key exchange under standard assumption.”, in: Proc.of the Int’l Conf. On Theory and Application of Cryptographic Technqiues”. 2002. pp.3210336.

[4] J.Katz and M.Yung. “Scalable protocl for authenticated key exchange”. Journal of Cryptology. Vol.20, 2007, pp.85-113

[5] Y.Kim, A.Perrig, and G.Tsudik. “Simple and fault-tolerant key agreement for dynamic collaboraive groups.” in: Proc.of the 7th ACM Confernece on Computer and Communciations Security. 2000.pp.235-244

[6] M.Steiner, G.Tsudik, and M.Waidner. “Key agreement in dynamic peer groups.”IEEE Transactgions on Parallel and Distributed Systems, vol.11, 2000 pp769-780

[7] W.Diffie and M.E.Hellman, “New directions in cryptography’, IEEE Trans Inform Theory, vol.22, 1976, pp644-654

[8] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology CRYPTP 2001, LNCS vol.2193, 2001, pp.213-229.

[9] H.Y Chien, R.Y Lin, Identity-based key agreement protocol for mobile ad-hoc networks using bilinear pairing, IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Traichung, 2006, pp.8

[10] A. Shamir, Identity based cryptosystems and signature schemes, Advance in Cryptology-Crypto’84, Lecture Notes in Computer Science, 0196: 47-53, 1984