An Efficient Group Key Agreement Scheme for Mobile Ad-Hoc Networks

Yang Yang[1, 2], Yupu Hu[2], Chunhui Sun[2], Chao Lv[2], Leyou Zhang[3]
[1]College of Mathematics and Computer Science, Fuzhou University, China
[2] Department of Telecommunication, Xidian University, China
[3]Department of Science, Xidian University, China

Abstract: *Mobile Ad-hoc Networks (MANETs) are considered as the most promising terminal networks in future wireless communications and characterized by flexibility, fast and easy deployment, which make them an interesting technology for various applications. Group communication is one of the main concerns in MANETs. To provide the secure group communication in wireless networks, a group key is required so that efficient symmetric encryption can be performed. In this paper, we propose a constant-round group key agreement scheme to enable secure group communications, which adopts the Identity Based Broadcast Encryption (IBBE) methodology. When a new Ad-hoc network is constructed, the suggested scheme requires no message exchange to establish a group key if the receivers' identities are known to the broadcaster, which is an advantage that outperforms most of the existing key agreement schemes. The proposed scheme can build a new group and establish a new group key with ease when member joins or leaves. In addition, our scheme is efficient in computation and only one bilinear pair computation is required for group members to obtain his/her session key. A highlight property of the scheme is that communication cost remains unchanged as group size grows. Furthermore, we show that the new scheme is proved secure without random oracle. Thus, the scheme can not only meet security demands of larger mobile Ad-hoc networks but also improve executing performance.*

Keywords: *Group key agreement scheme, identity based, broadcast encryption, data security, public key cryptography, standard model.*

Received October 6, 2010; accepted March 1, 2011

1. Introduction

Multi-hop wireless networks, such as Mobile Ad-hoc Networks (MANETs) have received tremendous attention [1, 2] in the past decade due to their rapid deployability and self-organizing configurability as well as broad applications, ranging from tactical communication in a battlefield, disaster rescue after an earth quake, to wildlife monitoring and tracking, last-mile network access, etc. In MANETs the nodes act as mobile IP routers and carry out basic functions such as packets forwarding, routing and network management. When MANETs is constructed in an open network environment, any malicious equipment can eavesdrop on the broadcasted information due to the broadcast nature of radio transmissions. With the growing application of MANETs, there will be much more rampant eavesdropping behavior so that security is increasingly essential and crucial. Therefore, a secure and efficient scheme is required to protect the content of the group communication and ensure that only intended members in this group can obtain the information. Despite all the work conducted over many decades, the implementation of strong protection in a mobile environment is non-trivial. The dynamic character of group changes poses a challenge on group key agreement research for wireless Ad-hoc network. Given a potentially large number of mobile devices, scalability becomes another critical issue. In addition, nodes in wireless Ad-hoc networks are usually low power devices that run on battery power and become unusable after failure or energy depletion. These characteristics of MANETs demand an energy-efficient group key agreement scheme in order to increase the overall network longevity. Constructing group wide keys in a large-scale Ad-hoc network is an important as well as complicate task.

1.1. Related Works

Since the presence of foundational Diffie-Hellman (DH) protocol [12], several other protocols have been proposed for the group case. The original idea of extending the 2-party DH scheme to the multi-party setting dates back to the classical paper of Ingemarsson [16]. Following their work, Steiner *et al*. [22, 23, 24] proposed a family of protocols known as Group Diffie-Hellman (GDH.1, GDH.2, GDH.3). In these protocols, the last group member serves as a controller and performs most of the computation, therefore, it needs more energy compared with other group members. Owning to the limitation of the nodes energy, the GDH protocol family is not suitable for the Ad-hoc networks. Perrig [21] proposed a tree-based key agreement scheme. After that, Kim *et al*. [18] extended the work of [21] to design a Tree-Based Group Diffie-Hellman (TGDH) protocol. Compared with GDH protocols, it scales down the number of exponentiations and received messages required by the last group member to avoid excessive computational and communication costs required by one node. But TGDH protocol still requires each group member to perform large modular exponentiations and transmit/receive long messages. So the TGDH protocol is also inadequate for Ad-hoc networks.

After the work in [4, 9, 25] many other scholars have done abundant related research. However, fairly few research deals with provably-secure group key agreement in a concrete and realistic setting. It is only recently that [20], has presented the first group key agreement scheme proven secure in a well-defined security model. Ng *et al.* [20] incorporated the identity based cryptosystem with bilinear map and broadcast encryption scheme to construct a secure communication scheme for MANETs. In their scheme, the group members do not perform any message exchanges during the generation process of a group key. However, its security relies on the random oracles. It has been shown that when the random oracles are instantiated with concrete hash functions, the resulting scheme may not be secure [3, 10]. Then, Zhang *et al*. [26] designed a new scheme which is proved secure in the standard model rather than the random oracles model. Unfortunately, those schemes suffer from long ciphertexts, i.e., the secret message broadcasted to the users will grow linearly with the number of receivers. With the increment of network scale, the shortcoming mentioned above will lead to even serious problems.

1.2. Our Contribution

In this paper, we propose an efficient key agreement scheme based on Identity-Based Broadcast Encryption (IBBE) approach, aiming at providing a lightweight and fast key agreement solution in MANETs. This scheme not only meets security demands of mobile Ad-hoc networks but also reduces the communication costs. It combines the identity-based cryptosystem [5] with bilinear map to replace the contributory setup of a group key as in the previous protocols [18, 24]. Each group member is conceived as a broadcaster who can select the valid receivers by himself and then transmit the confidential message. The suggested scheme has the following characteris-tics and advantages.

- *Identity Based:* Each group member is assigned a distinguished identity which plays the role of MAC address as in wire network. This is a method that avoids the authentication over digital signatures with certificate issued by a publicly known Certification Authority (CA). Note that though an adversary can disguise himself with a legimate identity, the adversary could not get the private key corresponding to the identity.
- *Dynamic Character:* If a member decides to join or leave the network, a new group key can be easily constructed in our scheme.
- *Scalability:* Given the potentially large number of mobile devices, the communication and computation overhead is almost unchanged due to the elaborative design of the suggested scheme.
- *Average Computation Load:* Each group member is conceived as a broadcaster and the computation load is average for each receiver.
- *Security:* Only the intended receivers can derive the group session key. According to the security reduction theory, the proposed scheme is secure against chosen ciphertext attack and the security of the scheme is proved in the standard model rather than in the random oracle model.
- *Efficiency:* Message exchange is avoided. The suggested scheme only requires the broadcaster to send out an encapsulation of group key to establish the group session key. The receivers can derive the session key using their own private key without any message exchange with other group members. At the same time, merely one bilinear operation is needed to obtain the session key for group member.

1.3. Road Map

The rest of the paper is organized as follows. In section 2, we briefly outline the concept of bilinear map, the hardness assumption, the system model and related security notions. A description of our construction is followed in section 3 and in section 4 we discuss the security and efficiency issues. Finally, our conclusion is drawn in section 4.

2. Preliminary

2.1. Bilinear Map

Let $\mathbb{G}$ and $\mathbb{G}_1$ be two (multiplicative) cyclic groups of prime order p and g is a generator of $\mathbb{G}$. A bilinear map $\hat{e}$ is a map $\hat{e}:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_1$ with the following properties:

1. *Bilinearity:* For all $u, v\in\mathbb{G}$, $a, b\in\mathbb{Z}_P$, we have $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$;
2. *Non-Degeneracy:* $\hat{e}(g, g)\neq 1$;
3. *Computability:* There is an efficiency algorithm to compute $\hat{e}(u, v)$ for all $u, v\in\mathbb{G}$.

The modified Weil pairing and the Tate pairing [5] are admissible bilinear maps. The security of our scheme described here relies on the hardness of the following assumption.

2.2. Hardness Assumption

Security of our scheme will be reduced to the hardness of the q-BDHI problem in the group in which the scheme is constructed. We briefly recall the definition of the q-BDHI problem [6].

- *Definition 1:* (Decisional q-Bilinear Diffie-Hellman Inverse Problem) Given a group $\mathbb{G}$ of prime order p with generator g, $T\in\mathbb{G}_1$ and tuple $Tu=(g, g^{a}, g^{a^2},..., g^{a^q})$ for some uniformly chosen $\alpha\in\mathbb{Z}_p^*$ as input, the decisional q-BDHI problem is to decide whether T equals to $\hat{e}(g, g)^{1/\alpha}$ or to a random element of $\mathbb{G}_1$.
- *Definition 2:* We say that (t, ε) decisional q-BDHI assumption holds in group $\mathbb{G}$ if there is no adversary running in time at most t can solve the q-BDHI problem in $\mathbb{G}$ with an advantage at least ε.

2.3. System Model

Let the set $U=\{ID_1, ID_2, …, ID_N\}$ be the group that contains all the Ad-hoc members. Private Key Generator (PKG) sets up system parameters, authenticates user's identity and generates private keys for each authorized user. We point out that the PKG's role is only to provide the necessary system parameters and distribute each user his private key, hence the PKG is not necessary to keep online after the completion of these procedures and is not required anymore by the users who want to setup a mobile Ad-hoc network. Our scheme consists of four phases: Setup, Extract, Encrypt and Decrypt.

- *Setup Phase:* In this phase, PKG generates the public parameters PK and the master secrete key MK for the system.
- *Extract Phase:* The PKG will verify user's identity ID_i and generate the corresponding private key d_{ID_i} after the successful verification of ID_i.
- *Encrypt Phase:* In this phase, we consider the situation where a group of users $S=\{ID_1, ..., ID_n\}$ are selected to be the receivers using their wireless devices. A session key (group key) K should be established for the group. After knowing the receivers' identities, the broadcaster will generate an encapsulation header Hdr for the group key K, then broadcast (S, Hdr) in the open environment.
- *Decrypt Phase:* After receiving (S, Hdr), the intended users with identity $ID_i\in S$ could derive the group key K with his own private key d_{ID_i}. For the users with identity $ID_i\notin S$, he will get no information about K.

After the session key K is set up for the dynamic Ad-hoc group, the messages M can be encrypted with K to ciphertext C through efficient symmetric encryption algorithm, such as DES or AES. Moreover, the ciphertext C can only be deciphered by the users in this group.

2.4. Security Model

We assume that there exists an adversary $\mathcal{A}$. All messages available in the network are also available to $\mathcal{A}$. This includes all the messages sent by any set S^* of users within the system. The main goal of $\mathcal{A}$ is to attack the scheme by decrypting any messages sent in the network intended to any set of users in S^* but not him. $\mathcal{A}$ is considered to be successful if he wins the following interactive experiment.

- *Init:* $\mathcal{A}$ picks a set of users $S^*=\{ID_1^*,\cdots,ID_n^*\}$ that he wants to attack (with $n\leq N$) and sents S^* to challenger $\mathcal{C}$.
- *Setup:* Challenger $\mathcal{C}$ runs the setup algorithm and sends adversary $\mathcal{A}$ the public parameters PK.
- *Phase 1:* Adversary $\mathcal{A}$ issues private key extract queries and decryption queries.
  1. *Extract Queries*: $\mathcal{A}$ issues private key extract queries for any identity $ID_i\notin S^*$. In response, $\mathcal{C}$ runs Extract algorithm on ID_i and sends the resulting private key d_{ID_i} to adversary $\mathcal{A}$.
  2. *Decryption Queries:* $\mathcal{A}$ issues decryption queries of (ID_i, S, Hdr) with $S\subseteq S^*$ and $ID_i\in S$. Challenger $\mathcal{C}$ responds with $K=Decrypt(S, ID_i, d_{ID_i}, Hdr, PK)$.
- *Challenge:* When $\mathcal{A}$ decides that phase 1 is over, the challenger $\mathcal{C}$ runs *Encrypt* algorithm to obtain (Hdr^*, K). Then challenger $\mathcal{C}$ randomly selects $b\in\{0, 1\}$, sets $K_b=K$ and sets K_{1-b} to a random value in $\mathcal{K}$ which refers to the key pool. The challenger $\mathcal{C}$ returns (Hdr^*, K_0, K_1) to $\mathcal{A}$.
- *Phase 2:* Adversary $\mathcal{A}$ continues to issue private key extract queries and decryption queries as in phase 1 with the constraint that $Hdr\neq Hdr^*$ in decryption queries.
- *Guess:* Finally, the adversary $\mathcal{A}$ outputs a guess $b'\in\{0, 1\}$ and wins the game if $b=b'$.

If $\mathcal{A}$ somehow manages to guess the correct answer in the experiment above, then $\mathcal{A}$ wins the experiment and the scheme is not secure. We say that $\mathcal{A}$ has a guessing advantage ε and the probability of $\mathcal{A}$ winning the experiment is $Pr[b=b']=1/2+\varepsilon$.

- *Definition 3:* We say that a scheme is (t, ε, q_E, q_D) IND-sID-CCA secure if all t time adversaries making at most q_E private key extract queries, q_D decryption queries have advantage at most ε in winning the above game.

3. New Key Agreement Scheme for MANET

Inspired by Boneh's Identity Based Encryption (IBE) scheme [6], we design the efficient group key agreement scheme for MANETs.

3.1. Setup Phase

Given the security parameter k and the maximal size N of all the MANETs members, the PKG chooses a group $\mathbb{G}$ with order p, where $|p|\leq k$.

1. Choose a collision resistant hash function H_1:{0, 1}$^*\rightarrow\mathbb{Z}_P$. H_1 maps arbitrary identity into $\mathbb{Z}_P$.
2. Randomly choose generator g of $\mathbb{G}$ and $\beta, \lambda\in\mathbb{Z}_p^*$, compute $U=g^{\beta}$, $V=g^{\lambda}$.
3. Output the public parameter $PK=(g, U, V)$ while master secret key $MK=(\beta, \lambda)$ is kept secret by PKG.

3.2. Extract Phase

Given user's identity ID_i, PKG will verify user's identity and generate the corresponding private key after the successful verification of ID_i. PKG performs the following steps to generate ID_i 's private key d_{ID_i}.

1. Select random $r_i\in\mathbb{Z}_p^*$. If $H_1(ID_i)+\beta+r_i\lambda=0$ $(mod\ p)$, choose another r_i at random.
2. Calculate ID_i 's private key d_{ID_i} :

$$d_{ID_i}=(d_{i,0},d_{i,1})=(r_i,g^{\frac{1}{H_1(ID_i)+\beta+r_i\lambda}})$$

3.3. Encrypt Phase

Assume that the set of receivers is $S=\{ID_1, ..., ID_n\}$ with $n\leq N$, the broadcaster performs as follows:

1. Randomly select session key $K\in\mathbb{G}_1$.
2. Randomly choose $\tau\in\mathbb{Z}_p^*$ and compute $Hdr=(C_0, C_1, C_2, C_3)$ as follow:
$$C_0=K\cdot\hat{e}(g,g)^{\tau},\ C_1=g^{\tau\cdot\prod_{j=1}^{n}H_1(ID_j)},\ C_2=U^{\tau},\ C_3=V^{\tau}$$
3. Output (S, Hdr) and broadcast it in the system.

3.4. Decrypt Phase

Suppose that the user with identity $ID_i\in S$ has received (S, Hdr), the user compute:

$$K=C_0/\hat{e}(C_1^{1/\prod_{j=1,j\neq i}^{n}H_1(ID_j)}\cdot C_2\cdot C_3^{d_{i,0}},d_{i,1})$$

After the session key K is set up for the dynamic Ad-hoc group, the messages M can be encrypted with K to ciphertext C which can only be deciphered by the users in the group.

4. Analysis of the Proposed Scheme

4.1. Correctness

The correctness of the scheme is verified as follow:

$$\begin{aligned}
&C_0/\hat{e}(C_1^{1/\prod_{j=1,j\neq i}^{n}H_1(ID_j)}\cdot C_2\cdot C_3^{d_{i,0}},d_{i,1})\\
&=C_0/\hat{e}(g^{\tau\cdot H_1(ID_i)}\cdot g^{\beta\cdot\tau}\cdot g^{\lambda\cdot r_i\cdot\tau},d_{i,1})\\
&=C_0/\hat{e}(g^{\tau(H_1(ID_i)+\beta+r_i\lambda)},g^{\frac{1}{H_1(ID)+\beta+r_i\lambda}})\\
&=K\cdot\hat{e}(g,g)^{\tau}/\hat{e}(g,g)^{\tau}\\
&=K.
\end{aligned}$$

4.2. Security Analysis

Theorem 1: Suppose the (t',ε) q -BDHI assumption holds in $\mathbb{G}$, then the above scheme is $(t, \varepsilon, q_E, q_D)$ IND-sID-CCA secure, where $t'=t+O(\sigma\cdot q^2)$ and σ is the time for an exponential operation in $\mathbb{G}$.
Proof: Suppose there exists a $(t, \varepsilon, q_E, q_D)$ adversary $\mathcal{A}$ against our scheme, then we construct an algorithm $\mathcal{C}$ that solves the q -BDHI problem with probability at least ε and in time at most t'. The challenger $\mathcal{C}$ is given a tuple $Tu=(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q})$ of the q-BDHI problem. The experiment between $\mathcal{A}$ and $\mathcal{C}$ proceeds as follows.
Preparation:

1. $\mathcal{C}$ randomly chooses $v_1,v_2,\cdots,v_{q-1}\in\mathbb{Z}_p$. Let:
$$f(z)=\prod_{i=1}^{q-1}(z+v_i)=\sum_{i=0}^{q-1}c_iz^i=\sum_{i=1}^{q}c_{i-1}z^{i-1},$$
$$f_i(z)=\frac{f(z)}{z+v_i}=\sum_{j=0}^{q-2}d_jz^j,$$
where $1\leq i\leq q-1$
2. $\mathcal{C}$ computes:
$$\begin{aligned}
h&=\prod_{i=0}^{q-1}(g^{\alpha^i})^{c_i}=g^{\sum_{i=0}^{q-1}c_i\alpha^i}=g^{f(\alpha)},\\
h_i&=\prod_{j=0}^{q-2}(g^{\alpha^j})^{d_j}=g^{\sum_{j=0}^{q-2}d_j\alpha^j}=g^{f_i(\alpha)}=g^{f(\alpha)/(\alpha+v_i)}\\
&=\left(g^{f(\alpha)}\right)^{1/(\alpha+v_i)}=h^{1/(\alpha+v_i)},\\
h_0&=\prod_{i=0}^{q-1}(g^{\alpha^{i-1}})^{c_i}=g^{\frac{1}{\alpha}\sum_{i=0}^{q-1}c_i\alpha^i}=g^{\frac{1}{\alpha}f(\alpha)}=h^{1/\alpha},\\
u&=\prod_{i=1}^{q}(g^{\alpha^i})^{c_{i-1}}=\prod_{i=1}^{q}(g^{\alpha})^{c_{i-1}\alpha^{i-1}}=(g^{\alpha})^{\sum_{i=1}^{q}c_{i-1}\alpha^{i-1}}\\
&=(g^{f(\alpha)})^{\alpha}=h^{\alpha},
\end{aligned}$$
where $1\leq i\leq q-1$
3. Let:
$$T_h=T^{c_0f(\alpha)}\cdot\prod_{i=0}^{q-1}\prod_{j=0}^{q-2}\hat{e}(g^{\alpha^i},g^{\alpha^j})^{c_ic_{j+1}}$$

   a. If $T=\hat{e}(g,g)^{1/\alpha}$, then $T_h=\hat{e}(h,h)^{1/\alpha}$, since
$$\begin{aligned}
f^2(\alpha)&=(\sum_{i=0}^{q-1}c_i\alpha^i)(\sum_{j=0}^{q-1}c_j\alpha^j)\\
&=(\sum_{i=0}^{q-1}c_i\alpha^i)(\sum_{j=1}^{q-1}c_j\alpha^j+c_0)\\
&=(\sum_{i=0}^{q-1}c_i\alpha^i)(\sum_{j=0}^{q-2}c_{j+1}\alpha^{j+1}+c_0)\\
&=(\sum_{i=0}^{q-1}c_i\alpha^i)(\alpha\sum_{j=0}^{q-2}c_{j+1}\alpha^j)+c_0\sum_{i=0}^{q-1}c_i\alpha^i\\
&=\alpha\sum_{i=0}^{q-1}\sum_{j=0}^{q-2}\alpha^i\alpha^jc_ic_{j+1}+c_0f(\alpha)\\
&=\alpha[\sum_{i=0}^{q-1}\sum_{j=0}^{q-2}\alpha^i\alpha^jc_ic_{j+1}+\frac{1}{\alpha}c_0f(\alpha)].
\end{aligned}$$

Then

$$\begin{aligned} T_h &= T^{c_0 f(\alpha)} \cdot \prod_{i=0}^{q-1}\prod_{j=0}^{q-2} \hat{e}(g^{\alpha^i}, g^{\alpha^j})^{c_i c_{j+1}} \\ &= \hat{e}(g,g)^{\frac{1}{\alpha}c_0 f(\alpha)} \cdot \hat{e}(g,g)^{\sum_{i=0}^{q-1}\sum_{j=0}^{q-2}\alpha^i \alpha^j c_i c_{j+1}} \\ &= \hat{e}(g,g)^{\sum_{i=0}^{q-1}\sum_{j=0}^{q-2}\alpha^i \alpha^j c_i c_{j+1} + \frac{1}{\alpha}c_0 f(\alpha)} \\ &= \hat{e}(g,g)^{f^2(\alpha)/\alpha} \\ &= \hat{e}(g^{f(\alpha)}, g^{f(\alpha)})^{1/\alpha} \\ &= \hat{e}(h,h)^{1/\alpha}. \end{aligned}$$

b. If $T \in_R \mathbb{G}_1$, then T_h is a random element in $\mathbb{G}_1$ as well.

Observe that the decision that T equals to $\hat{e}(g, g)^{1/\alpha}$ or a random element in $\mathbb{G}_1$ is equivalent to the decision that T_h equals to $\hat{e}(h, h)^{1/\alpha}$ or a random element in $\mathbb{G}_1$.

Init: Adversary $\mathcal{A}$ outputs a challenge set of identities $S^* = (ID_1^*, \cdots, ID_n^*)$ with $n \leq N$.

Setup:

1. Challenger $\mathcal{C}$ chooses $a \in \mathbb{Z}_p^*$ at random and let
   $$b = \prod_{j=1}^{n} H_1(ID_j^*)$$
2. $\mathcal{C}$ Computes $U=u^{a+b}=h^{\alpha(a+b)}$, $V=u=h^{\alpha}$ and lets $\beta=\alpha(a+b)$, $\lambda=\alpha$. Thus, $U=h^{\beta}$, $V=h^{\lambda}$.
3. $\mathcal{C}$ returns $\mathcal{A}$ the public parameters $PK=(h, U, V)$. Note that since α is unknown to $\mathcal{C}$, then β, λ is unknown to $\mathcal{C}$ as well.

- *Phase 1*:
  1. *Extract Queries*. Upon receiving a request on identity ID_i and $ID_i \notin S^*$, the private key $d_{IDi}=(d_{i,0}, d_{i,1})$ is constructed as follows:
     $$d_{i,0} = r_i = \frac{H_1(ID_i)}{v_i} - (a+b),\ d_{i,1} = h_i^{\frac{1}{r_i+a+b}}.$$
     It is obvious that the equation $(r_i+a+b).(\alpha+v_i)= H_1(ID_i)+\beta+r_i\lambda$ holds, since:
     $$\begin{aligned} (r_i+a+b)\cdot(\alpha+v_i) &= H_1(ID_i)+\beta+r_i\lambda \\ (r_i+a+b)\cdot(\alpha+v_i) &= H_1(ID_i)+\alpha(a+b)+r_i\alpha \\ (r_i+a+b)\cdot(\alpha+v_i) &= H_1(ID_i)+\alpha(a+b+r_i) \\ (r_i+a+b)\cdot v_i &= H_1(ID_i) \\ r_i v_i &= H_1(ID_i)-v_i(a+b) \\ r_i &= \frac{H_1(ID_i)}{v_i}-(a+b), \end{aligned}$$
     Then
     $$d_{i,1} = h_i^{\frac{1}{r_i+a+b}} = (h^{\frac{1}{(\alpha+v_i)}})^{\frac{1}{r_i+a+b}} = h^{\frac{1}{H_1(ID_i)+\beta+r_i\lambda}}$$
     Thus, $\mathcal{C}$ has successfully simulated the private key $d_{IDi}=(d_{i,0}, d_{i,1})$.
  2. *Decryption Queries*: To answer the decryption query on (ID_i, S, Hdr) where $S \subseteq S^*$, $ID_i \in S$.
     1. Challenger $\mathcal{C}$ constructs the private key d_{ID_i} for identity $d_{IDi}=(d_{i,0}, d_{i,1})$.
     2. $\mathcal{C}$ computes:
        $$K = C_0 / e(C_1^{1/\prod_{j=1,j\neq i}^{n} H_1(ID_j)} \cdot C_2 \cdot C_3^{d_{i,0}}, d_{i,1}),$$
        and returns to $\mathcal{A}$ the session key K.
- *Challenge*: Adversary $\mathcal{A}$ outputs two keys K_0, $K_1 \in \mathbb{G}_1$ of equal length. $\mathcal{C}$ randomly chooses $b \in \{0, 1\}$ and $w \in \mathbb{Z}_p^*$. Define $\tau = w/\alpha$. The header $Hdr^* = (C_0^*, C_1^*, C_2^*, C_3^*)$ is calculated as follows:
  $$\begin{aligned} C_0^* &= (T_h)^w \cdot K_b, \\ C_1^* &= h_0^{w \cdot b} = (h^{1/\alpha})^{(\alpha\tau)\cdot\prod_{j=1}^{n} H_1(ID_j^*)} = h^{\tau\cdot\prod_{j=1}^{n} H_1(ID_j^*)}, \\ C_2^* &= h^{(a+b)\cdot w} = h^{\alpha(a+b)\cdot\tau} = (h^{\alpha(a+b)})^{\tau} = U^{\tau}, \\ C_3^* &= h^{w} = (h^{\alpha})^{\tau} = V^{\tau}. \end{aligned}$$

1. If $T_h=\hat{e}(h, h)^{1/\alpha}$,
   $$\begin{aligned} C_0^* &= (T_h)^w \cdot K_b = (e(h,h)^{1/\alpha})^w \cdot K_b \\ &= e(h,h)^{w/\alpha} \cdot K_b = e(h,h)^{\tau} \cdot K_b \end{aligned}$$
   It means that Hdr^* is a valid encryption for K_b.
2. If $T_h \in_R \mathbb{G}_1$, then C_0^* is independent of b and Hdr^* is a valid encryption for K_b.

- *Phase 2:* $\mathcal{A}$ continues to issue queries as in phase 1 with the constraint that $Hdr \neq Hdr^*$ in decryption queries.
- *Guess:* At last, adversary $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$. If $b' = b$ then $\mathcal{C}$ outputs 1 meaning $T=\hat{e}(g, g)^{1/\alpha}$. Otherwise, it outputs 0 meaning $T \neq \hat{e}(g, g)^{1/\alpha}$ but a random element in $\mathbb{G}_1$.

1. If $T \in_R \mathbb{G}_1$, $Pr[c(Tu, T)=0]=1/2$.
2. If $T=\hat{e}(g, g)^{1/\alpha}$,
   $$|\Pr[\mathcal{C}(Tu, T = \hat{e}(g,g)^{1/\alpha}) = 0] - 1/2| \geq \varepsilon$$

Thus

$$\begin{aligned} &\left|\Pr[\mathcal{C}(Tu, T = e(g,g)^{1/\alpha}) = 0] - \Pr[\mathcal{C}(Tu, T) = 0]\right| \\ &\geq \left|\left(\frac{1}{2} \pm \varepsilon\right) - \frac{1}{2}\right| = \varepsilon. \end{aligned}$$

The time complexity of the algorithm $\mathcal{C}$ is dominated by the exponentiations performed in the preparation phase, thus $t' = t + O(\sigma \cdot q^2)$, where σ is the time of one exponentiation in $\mathbb{G}$.

4.3. Comparison with IBBE Schemes

Since the proposed scheme is constructed adopting the Identity Based Broadcast Encryption (IBBE) methodology, we will compare the efficiency of our scheme with the classical IBBE schemes in this subsection. We can see that our scheme achieves excellent efficiency: the sizes of public key, private key and ciphertext are constant. In addition, encryption requires no pairing operations (the value $\hat{e}(g, g)$ can be precomputed and cached) and decryption requires only one pairing operation. We also compare the proposed scheme with other classical IBBE schemes [7, 8, 11, 13, 14, 15, 17] as shown in Table 1.

1. The sizes of public parameters in [7, 8, 11, 14, 15, 17] are linear or sublinear with the number of users in the system, while ours is a constant. Hence, the transmission overhead is reduced in the system initialization phase.
2. The private key of user consists of only two elements in $\mathbb{Z}_p^*$ and thus the storage at the user is decreased.

3. The sizes of ciphertext in [8, 13] grows with the number of users in the system. In a large system, the communication load will be tremendous for the schemes in [8, 13], while the size of ciphertext in our scheme is a constant and the communication overhead remains unchanged. It means that the length of the group key's encapsulation will not grow when the dynamic group is large.
4. The encryption process in [8] is quite complex. And a large amount of matrix operations as well as one bilinear pairing operation are required in [13]. On the contrary, the suggested scheme has succinct encryption process.
5. In the decryption phase, our scheme requires only one bilinear pairing operation which is superior to other schemes [7, 8, 11, 13, 14, 15, 17].
6. On the other hand, the security of IBBE schemes in [11, 13, 14, 15] bases on the random oracle model and the security of the proposed scheme bases on the standard model. As is well known, the schemes based on random oracle may not be secure [3, 10].
7. The security level of q-BDHE [7, 14], q-MBDH [17], q-SDH [15], GDHE [11], q-BDHI assumptions are almost the same and the DM3-partyDH assumption is weaker [8]. The DBDH [13] assumption has the highest security level. However, the security of scheme in [13] is just claimed to be based on the DBDH assumption, but no concrete proof is provided.

To sum up, our scheme achieves higher efficiency compared with the existing IBBE schemes and has the same security level with other schemes. Thus, the communication overhead of the network is greatly decreased and the computation of the users is reduced.

Table 1. Comparison of our scheme with classical IBBE schemes.

IBBE Scheme	Public Parameter Size	Private Key Size	Ciphertext Size	Encrypt (Pairing)	Decrypt (Pairing)	Random Oracle	Hardness Assumption
[7]	$O(n)$	$O(1)$	$O(1)$	0	2	No	q-BDHE
[8]	$O(\sqrt{n})$	$O(\sqrt{n})$	$O(\sqrt{n})$	0	4	No	DM3-partyDH, BSD, DHSD
[11]	$O(n)$	$O(1)$	$O(1)$	0	2	Yes	GDHE
[13]	$O(1)$	$O(1)$	$O(n)$	1	2	Yes	DBDH
[14]	$O(n)$	$O(n)$	$O(1)$	0	2	Yes	q-BDHE
[15]	$O(n)$	$O(1)$	$O(1)$	0	2	Yes	q-SDH
[17]	$O(n)$	$O(1)$	$O(1)$	0	2	No	q-MBDH
Ours	$O(1)$	$O(1)$	$O(1)$	0	1	No	q-BDHI

Note: q-BDHE: Decisional q-Bilinear Diffie-Hellman Exponent Assumption.
q-BDHI: Decisional q-Bilinear Diffie-Hellman Inverse Assumption.
DM3-partyDH: Decision (Modified) 3-party Diffie-Hellman Asssumpti .
DHSD: Diffie-Hellman Subgroup Decision Assumption.
Random Oracle: whether the proof of the scheme is in the random oracle model or not.
q-MBDH: Decisional Modified q-Diffie-Hellman Assumption.
GDHE: General Diffie-Hellman Exponent Assumption.
BSD: Bilinear Subgroup Decision Assumption.
DBDH: Decisional Diffie-Hellman Assumption.

Table 2. Performance of the scheme.

Size of Receiver Group	Setup (ms)	Extract (ms)	Encrypt (ms)	Decrypt (ms)
10	27.16561	9.13291	39.69668	27.95358
50	28.08979	9.1751	40.66453	27.83678
100	28.59665	9.38493	39.62374	27.85966
500	27.60003	9.50501	40.17305	28.20485
1000	27.67119	9.35124	40.4944	28.3703
1500	27.61146	9.40652	40.52392	28.52391
2000	27.61858	9.35386	40.70501	29.01165
2500	27.53885	9.74105	41.25094	29.16044
3000	27.56956	9.70953	41.03913	30.4741
3500	27.42004	9.40364	41.48192	29.36541
4000	27.8233	9.68222	42.62817	31.03555
4500	27.34706	9.69421	42.1089	30.57155
5000	27.74195	9.30824	42.34315	30.82534

4.4. Efficiency

This group key agreement scheme has been tested in C language using the Pairing-Based Crypto-graphy (PBC) Library [19]. The type-A elliptic curve parameter is chosen, which provides equivalently 1024bit discrete logarithm security strength and the group order is 160bit. All tests are run on a PC with a 2.0GB of the memory and Pentium Dual core CPU (3.3GHz) running Windows XP system.

We show in Figure 1 and Table 2 the execution time in each process under different n values, where n is the size of receiver group. When n grows from 1 to 5000, the cost of time remains stable in each phase. Thus, the proposed scheme is desirable for large scale MANETs.

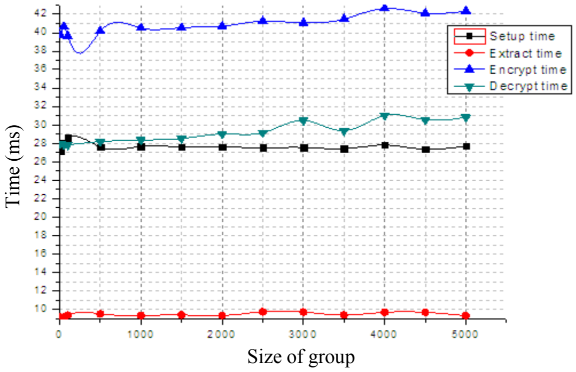

Figure 1. Time efficiency of the scheme.

5. Conclusions

We propose an efficient provably-secure key agreement scheme based on IBBE approach for mobile Ad-hoc networks. Our scheme is computationally efficient. When a new mobile Ad-hoc network is constructed, the proposed scheme only needs to add or exclude that member's ID during the execution of encryption phase to obtain a new group key, which is more efficient than the previous schemes. A desirable property of the suggested scheme is that the encapsulation of group key remains constant so that the communication overhead is unchanged no matter what the network's scalability. Furthermore, under the q -BDHI assumption, the proposed scheme is provably secure without relying on the random oracles. Compared with the existing IBBE schemes, our scheme is more efficient and achieves the same security level with other schemes.

Acknowledgements

This work is supported by the "973" program of China under Grant 2007CB311201 and the National Natural Science Foundation of China under Grants 60970119, 61072067, 61103175, 61100231, 61202350. This work was supported in part by the Technology Innovation Platform Project of Fujian Province under Grant No.2009J1007.

References

[1] Abbas A., "A Hybrid Protocol for Identification of A Maximal Set of Node Disjoint Paths in Mobile Ad-Hoc Networks," *The International Arab Journal of Information Technology*, vol. 6, no. 4, pp. 344-358, 2009.

[2] Ayyadurai V. and Ramasamy R., "Internet Connecti- Vity for Mobile Ad-hoc Networks Using Hybrid Adaptive Mobile Agent Protocol," *The International Arab Journal of Information Technology*, vol. 5, no. 1, pp. 25-33, 2006.

[3] Bellare M., Boldyreva A., and Palacio A., "An Uninstantiable Random-Oracle-Model Scheme for A Hybrid-Encryption Problem," *in Proceedings of International Conference on the Theory and Application of Cryptographic Techniques*, *Advances in Cryptology-EUROCRYPT*, Switzerland, vol. 3027, pp. 171-188, 2004.

[4] Biswas P., "Diffie-Hellman Technique: Extended to Multiple Two-Party Keys and One Multi-Party Key," *Information Security*, vol. 2, no. 1, pp. 12-18, 2008.

[5] Boneh D. and Boyen X., "Efficient Selective-ID Secure Identity-Based Encryption without Random Oracles," *in Proceedings of International Conference on the Theory and Application of Cryptographic Techniques*, *Advances in Cryptology-EUROCRYPT*, Switzerland, vol. 3027, pp. 223-238, 2004.

[6] Boneh D. and Franklin M., "Identity-Based Encryption from the Weil Pairing," *Society for Industrial and Applied Mathematics Journal on Computing*, vol. 32, no. 3, pp. 586-615, 2003.

[7] Boneh D. and Waters B., "A Fully Collusion Resistant Broadcast, Trace, and Revoke System," *in Proceedings of the 13th ACM Conference on Computer and Communications Security*, USA, pp. 211-220, 2006.

[8] Boneh D., Gentry C., and Waters B., "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys," *in Proceedings of the 25th annual international conference on Advances in Cryptology*, Heidelberg, vol. 3621, pp. 258-275, 2005.

[9] Brecher T., Bresson E., and Manulis M., "Fully Robust Tree-Diffie-Hellman Group Key Exchange," *in Proceedings of the 8th International Conference on Cryptology and Network Security*, Heidelberg, vol. 5888, pp. 478-497, 2009.

[10] Canetti R., Goldreich O., and Halevi S., "The Random Oracle Methodology," *Journal of the Association for Computing Machinery*, vol. 51, no. 4, pp. 557-594, 2004.

[11] Delerablee C., "Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys," *in Proceedings of the 13th International Conference on Theory and Application of Cryptology and Information Security, Advances in Crypotology-ASIACRYPT*, vol. 4833, Heidelberg, pp. 200-215, 2007.

[12] Diffie W. and Hellman M., "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[13] Du X., Wang Y., Ge J., and Wang Y., "An ID-Based Broadcast Encryption Scheme for Key Distribution," *IEEE Transactions on Broadcasting,* vol. 51, no. 2, pp. 264-266, 2005.

[14] Gentry C. and Waters B., "Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts)," *in Proceedings of the 28th Annual International Conference on Advances in Cryptology: the Theory and Applications of Cryptographic Techniques-EUROCRYPT*, Heidelberg, vol. 5479, pp. 171-188, 2009.

[15] Guo S. and Zhang C., "Identity-Based Broadcast Encryption Scheme with Untrusted PKG," *in Proceedings of the 9th International Conference for Young Computer Scientists*, Hunan, pp. 1613-1618, 2008.

[16] Ingemarsson I., Tang D., and Wong C., "A Conference Key Distribution System," *IEEE*

Transactions on Information Theory, vol. 28, no. 5, pp. 714-719, 1982.

[17] Jong P., Hee K., Sung H., and Dong L., "Public Key Broadcast Encryption Schemes with Shorter Transmissions," *IEEE Transactions on Broadcasting*, vol. 54, no. 3, pp. 401-411, 2008.

[18] Kim Y., Perrig A., and Tsudik G., "Tree-Based Group Key Agreement," *ACM Transactions on Information and System Security*, vol. 7, no. 1, pp. 60-96, 2004.

[19] Lynn B., The PBC library, available at: http://crypto.stanford. edu/pbc/.

[20] Ng Y., Mu Y., and Susilo W., "An Identity-Based Broadcast Encryption Scheme for Mobile Ad-Hoc Networks," *Journal of Telecommunications and Information Technology*, vol. 1, pp. 24-29, 2006.

[21] Perrig A., "Efficient Collaborative Key Management Protocols for Secure Autonomous Group Communication," *in Proceedings of the International Workshop on Cryptographic Techniques and E-Commerce*, China, pp. 192-202, 1999.

[22] Steiner M., Tsudik G., and Waidner M., "CLIQUES: A New Approach to Group Key Agreement," *in Proceedings of IEEE, the 18th International Conference on Distributed Computing Systems*, Netherlands, pp. 380-387, 1998.

[23] Steiner M., Tsudik G., and Waidner M., "Diffie-Hellman Key Distribution Extended to Group Communication," *in Proceedings of the 3rd ACM Conference on Computer and Communications Security*, USA, pp. 31-37, 1996.

[24] Steiner M., Tsudik G., and Waidner M., "Key Agreement in Dynamic Peer Groups," *IEEE Transactions on Parallel and Distributed Systems*, vol. 11, no. 8, pp. 769-780, 2002.

[25] Tseng Y. and Wu T., "Analysis and Improvement on A Contributory Group Key Exchange Protocol Based on the Diffie-Hellman Technique," *Informatica*, vol. 21, no. 2, pp. 247-258, 2010.

[26] Zhang L., Hu Y., and Mu N., "An Identity-based Broadcast Encryption Protocol for Ad-hoc Networks," *in Proceedings of The 9th International Conference for Young Computer Scientists*, USA, pp. 1619-1623, 2008.

Yang Yang received her PhD degree in School of Communication Engineering from Xidian University of China in 2011. Now she is a lecturer in School of Math. And Computer Science of Fuzhou University. Her main research interests include network security and security protocol.

Yupu Hu received his PhD degree in School of Communication Engineering from Xidian University of China in 2008. Now he is a professor in School of Telecommunication Engineering of Xidian University. His main research interests include information security and cryptography.

Chunhui Sun is a PhD student in School of Communication Engineering of Xidian University. His main research interests include side channel attack and network security.

Chao Lv is a PhD student in School of Communication Engineering of Xidian University. His main research interests include security protocol, RFID protocol and formal verification.

Leyou Zhang received his PhD degrees in applied mathematics from Xidian University of China in 2009. Now he is an associate professor in the Department of Mathematical Sciences of Xidian University. His main research interests include security protocol and public key cryptography.