EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Two-round contributory group key exchange protocol for wireless network environments

Tsu-Yang Wu, Yuh-Min Tseng* and Ching-Wen Yu

Abstract

With the popularity of group-oriented applications, secure group communication has recently received much attention from cryptographic researchers. A group key exchange (GKE) protocol allows that participants cooperatively establish a group key that is used to encrypt and decrypt transmitted messages. Hence, GKE protocols can be used to provide secure group communication over a public network channel. However, most of the previously proposed GKE protocols deployed in wired networks are not fully suitable for wireless network environments with low-power computing devices. Subsequently, several GKE protocols suitable for mobile or wireless networks have been proposed. In this article, we will propose a more efficient group key exchange protocol with dynamic joining and leaving. Under the decision Diffie-Hellman (DDH), the computation Diffie-Hellman (CDH), and the hash function assumptions, we demonstrate that the proposed protocol is secure against passive attack and provides forward/backward secrecy for dynamic member joining/leaving. As compared with the recently proposed GKE protocols, our protocol provides better performance in terms of computational cost, round number, and communication cost.

Keywords: Group key exchange, Dynamic, Wireless network, Diffie-Hellman assumption

Introduction

Wireless communication technology has widely been applied to many mobile applications and services such as e-commerce applications, mobile access services, and wireless Internet services. Nowadays, people use their cellular phone or PDA (personal digital assistant) to access these mobile services. However, most of such security schemes and protocols deployed in wired networks are not fully applicable to wireless networks (i.e., wireless local area networks [1], mobile ad hoc networks [2], cellular mobile networks [3], and wireless sensor networks [4]) because of the network architecture and the computational complexity of mobile devices. In addition, an intruder is easy to intercept the transmitted messages over a wireless network because wireless communications use radio waves to transmit messages. Meanwhile, most cryptographic algorithms require many expensive computations, thus it will be a nontrivial challenge to design security schemes and protocols for wireless network environments with low-power computing devices [5,6].

With the popularity of group-oriented applications such as collaboration works and electric conferences, secure group communication has received much attention from cryptographic researchers. A group key exchange (GKE) protocol allows that participants establish a group key to encrypt/decrypt the transmitted messages. Thus, GKE protocols can be used to provide secure group communication. In 1982, Ingemaresson et al. [7] proposed the first GKE protocol relied on the two-party Diffie-Hellman scheme [8]. Subsequently, different types of GKE protocols were presented such as constant-round GKE [9-13] and linear-round GKE [14-17]. However, these previously proposed GKE protocols did not deal with the computing capability of mobile devices in wireless mobile networks.

Actually, considering wireless network environments such as wireless local area networks [1] and cellular mobile networks [3], they may be regarded as asymmetric (imbalanced) wireless networks. An imbalanced wireless network consists of mobile clients and a powerful node. Generally, mobile clients may use some mobile

* Correspondence: ymtseng@cc.ncue.edu.tw
Department of Mathematics, National Changhua University of Education, Jin-De Campus, Chang-Hua 500, Taiwan

devices (i.e., cellular phone or PDA) to access mobile applications through the powerful node. If such mobile clients want to perform a secure conference using their mobile devices through cellular mobile networks or wireless local area networks, they must establish a secure group key to encrypt/decrypt the transmitted messages. Considering the computing capability of mobile devices, a flexible approach is to shift the computational burden from the mobile devices to the powerful node. This approach reduces the computational costs on mobile nodes. Consequently, several group key agreement protocols [18-22] for the imbalanced wireless network have been proposed.

In 2003, Boyd and Nieto [18] presented a one-round GKE protocol. Their protocol is efficient for imbalanced wireless networks, but it lacks forward secrecy. Bresson et al. [19] proposed a two-round GKE protocol for imbalanced wireless networks. Unfortunately, their protocol provides only partial forward secrecy [20]. This partial forward secrecy means that leaking the mobile nodes' private keys do not reveal any information about the previous establishment group keys, but leaking the powerful node's private key will enable an adversary to reconstruct the previous group keys. Subsequently, Nam et al. [20] also presented an improvement on the protocol proposed by Bresson et al. In 2007, Tseng [21] demonstrated that the Nam et al.'s protocol has a security weakness. In their protocol, the powerful node can pre-determine the group key. That is, Nam et al.'s protocol is not a contributory GKE protocol. For repairing this weakness, Tseng also proposed a secure group key exchange protocol for imbalanced wireless networks. However, Tseng's GKE protocol does not deal with dynamic member joining/leaving functionality. Note that the dynamic joining/leaving functionality means that other participants need not to re-run the protocol when a participant joins or leaves the group. For a GKE protocol, it is important to provide this dynamic functionality, especially for wireless network environments. For providing dynamic joining/leaving functionality, Chuang and Tseng [22] recently proposed a dynamic group key exchange protocol for imbalanced wireless networks. However, their protocol requires three rounds to establish a group key.

Since the recently proposed GKE protocols [20-22] for wireless network environment are non-authenticated ones. By its very nature, a non-authenticated group key exchange protocol cannot provide participant and message authentication, so it must rely on the authenticated network channel [1,3] or use other schemes [23-25] to provide authentication in advance. Here, as like the recently proposed GKE protocols [20-22], we assume that each mobile client and the powerful node have already authenticated mutually. Here, we focus on the design of a non-authenticated GKE protocol. In this article, we propose a new group key exchange protocol with the dynamic property for wireless network environments. Under several security assumptions, we will prove that the proposed protocol is secure against passive attack and provides forward/backward secrecy for dynamic member joining/leaving. Meanwhile, we demonstrate that the proposed protocol also satisfies the contributiveness property. As compared with the recently proposed GKE protocols, our protocol provides better performance in terms of computational cost, round number, and communication cost.

The remainder of this article is organized as follows. In the next section, we present the security assumptions and the security requirements for a dynamic GKE protocol. In 'A concrete dynamic GKE protocol' section, we propose a concrete dynamic GKE protocol. Security analysis of the proposed protocol is demonstrated in 'Security analysis' section. In 'Performance analysis and discussions' section, we make performance analysis and comparisons. The conclusions are given in 'Conclusions' section.

Preliminaries

In this section, we present the security requirements of dynamic group key exchange protocol, as well as several security assumptions.

Notations

The following notations are used throughout the article:

- p, q: two large primes satisfying $p = 2q + 1$.
- G_q: a subgroup of Z_p^* with the order q.
- g: a generator of the group G_q.
- H: a one-way hash function, H:$\{0, 1\}^* \rightarrow Z_q^*$.
- *SID*: a session identity is public information. Note that each session is assigned a unique *SID*.

Security requirements for dynamic GKE protocol

Here, we define the security requirements of a dynamic GKE protocol as follows:

- *Passive attack*: This attack means that a passive adversary cannot compute the group key by eavesdropping on the transmitted messages over a public channel or efficiently distinguish the group key from a random string.
- *Forward secrecy*: When a new member joins the group, he/she cannot compute the previous established group keys to decrypt the past encrypted messages.

• *Backward secrecy*: When an old member leaves the group, he/she cannot compute the subsequent group keys to decrypt the future encrypted messages.
• *Contributiveness*: In the group, any participants cannot predetermine or predict the resulting group key. In other words, each participant can confirm that her/his contribution has been involved in the group key.

Security of a dynamic GKE protocol

We say that a dynamic group key exchange protocol is secure, if (1) it is secure against *passive attack*; (2) it provides *forward/backward secrecy* for joining/leaving; (3) it satisfies *contributiveness*.

Security assumptions

For the security of our proposed dynamic group key exchange protocol, we need the following hard problems and assumptions [26,27].

• *Decision Diffie-Hellman (DDH) problem*: Given $y_a = g^{x_a} \bmod p$ and $y_b = g^{x_b} \bmod p$ for some $x_a, x_b \in Z_q^*$, the DDH problem is to distinguish two tuples $(y_a, y_b, g^{x_a x_b} \bmod p)$ and $(y_a, y_b, R \in G_q)$.
• *DDH assumption*: There exists no probabilistic polynomial-time algorithm can solve the DDH problem with a non-negligible advantage.
• *Computational Diffie-Hellman (CDH) problem*: Given a tuple $(g, g^{x_a} \bmod p, g^{x_b} \bmod p)$ for some $x_a, x_b \in Z_q^*$, the CDH problem is to compute the value $g^{x_a x_b} \bmod p \in G_q$.
• *CDH assumption*: There exists no probabilistic polynomial-time algorithm can solve the CDH problem with a non-negligible advantage.
• *Hash function assumption*: A secure one-way hash function $H : X = \{0, 1\}^* \rightarrow Y = Z_q^*$ must satisfy following requirements [28]:
(i) For any $y \in Y$, it is hard to find $x \in X$ such that $H(x) = y$.
(ii) For any $x \in X$, it is hard to find $x' \in X$ such that $x' \neq x$ and $H(x') = H(x)$.
(iii) It is hard to find $x, x' \in X$ such that $x \neq x'$ and $H(x) = H(x')$.

A concrete dynamic GKE protocol

In this section, we present a new group key exchange protocol with the member joining/leaving functionality. Without loss of generality, let $\{U_0, U_1, U_2, ..., U_n\}$ be a set of participants who want to generate a group key in an imbalanced wireless network, where U_0 is a powerful node and $U_1, ..., U_n$ are n mobile clients with the limited computing capability. Our proposed dynamic GKE protocol is depicted in Figure 1 and the detailed steps are described as follows.

Step 1: Each client U_i $(1 \leq i \leq n)$ selects a random value $r_i \in Z_q^*$ and computes $z_i = g^{r_i} \bmod p$.. Then, each U_i sends (U_i, z_i) to the powerful node U_0.

Step 2: The powerful node U_0 first selects two random values r_0, $r \in Z_q^*$ and computes $z_0 = g^{r_0} \bmod p$.. Upon receiving n pairs (U_i, z_i) $(1 \leq i \leq n)$, U_0 computes $x_i = z_i^{r_0} \bmod p$ and $y_i = H(x_i||SID) \oplus r$ for $i = 1, 2, ..., n$. Finally, the powerful node U_0 computes $SK = H(r||y_1||y_2||...||y_n||SID)$ and broadcasts $(U_0, y_1, y_2, ..., y_n, z_0, SID)$ to all clients.

Step 3: Upon receiving the messages $(U_0, y_1, y_2, ..., y_n, z_0, SID)$, each client U_i $(1 \leq i \leq n)$ can compute $y_i' = H(x_i||SID') \oplus r'$ and uses r to obtain the group key $SK = H(r||y_1||y_2||...||y_n||SID)$.

Member joining phase. Assume that a new client U_{n+1} want to join the group. This phase is depicted in Figure 2 and the detailed steps are described as follows.

Step 1: Only the client U_{n+1} randomly selects a value $r_{n+1} \in Z_q^*$ and computes $z_{n+1} = g^{r_{n+1}} \bmod p$. Then, U_{n+1} sends (U_{n+1}, z_{n+1}) to the powerful node U_0.

Step 2: Upon receiving the pair (U_{n+1}, z_{n+1}), the powerful node U_0 computes $x_{n+1} = z_{n+1}^{r_0} \bmod p$ and selects a new value $r' \in_R Z_q^*$. Then, U_0 computes $y_i \oplus H(z_0^{r_i}||SID) = r'$ for $i = 1, 2, ..., n+1$ and $SK' = H(r'||y_1'||y_2'|| \cdots ||y_{n+1}'||SID')$. Finally, the powerful node U_0 broadcasts $(U_0, y_1', y_2', \ldots, y_{n+1}', z_0, SID')$ to all clients.

Step 3: Upon receiving the messages $(U_0, y_1', y_2', \ldots, y_{n+1}', z_0, SID')$, each client U_i $(1 \leq i \leq n)$ can compute $y_i' \oplus H(x_i||SID') = r'$ and uses r' to obtain a new group key $SK' = H(r'||y_1'||y_2'|| \cdots ||y_{n+1}'||SID')$. The client U_{n+1} first computes $x_{n+1} = z_0^{r_{n+1}} \bmod p$ and $y_{n+1}' \oplus H(x_{n+1}||SID') = r'$ to obtain the group key SK'.

Member leaving phase. Without loss generality, we assume that the client U_{n+1} would like to leave the group. This phase is depicted in Figure 3 and the detailed steps are described as follows.

Step 1: The powerful node U_0 first selects a new random value $r'' \in Z_q^*$. Then, U_0 computes $y_i'' = H(x_i||SID'') \oplus r''$ for $i = 1, 2, ..., n$ and $SK'' = H(r''||y_1''||y_2''|| \cdots ||y_n''||SID'')$. Finally, the powerful node U_0 broadcasts $(U_0, y_1'', y_2'', \ldots, y_n'', SID'')$ to all other clients.

Step 2: Upon receiving the message $(U_0, y_1'', y_2'', \ldots, y_n'', SID'')$, each client U_i $(1 \leq i \leq n)$ can compute $y_i'' \oplus H(x_i||SID'') = r''$ and uses r'' to obtain a new group key $SK'' = H(r''||y_1''||y_2''|| \cdots ||y_n''||SID'')$.

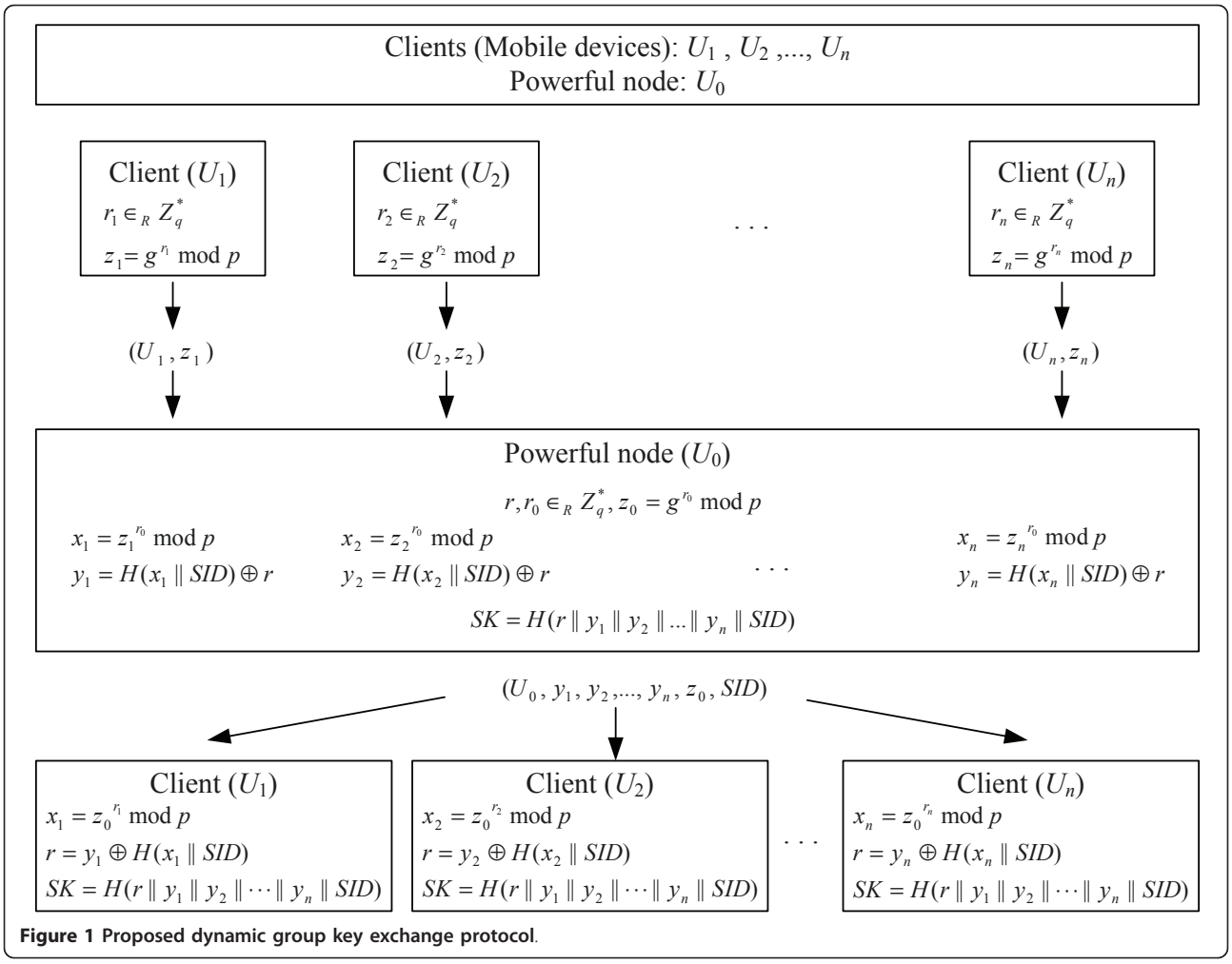

Figure 1 Proposed dynamic group key exchange protocol.

Security analysis

In this section, we demonstrate that our proposed GKE protocol can achieve the security requirements defined in 'Security requirements for dynamic GKE protocol' subsection that include withstanding *passive attack*, satisfying *contributiveness* and providing *forward/backward secrecy.*

Passive attacks

Theorem 1. *Under the decision Diffie-Hellman assumption, the proposed group key exchange protocol is secure against passive attacks.*

Proof. Assume that there exists an adversary A who tries to obtain the information about the group key by eavesdropping the transmitted messages over a public channel. Suppose that the adversary A may obtain all transmitted messages (z_0, z_i, y_i, *SID*) for $i = 1, 2,..., n$, where $z_0 = g^{r_0} \bmod p$, $z_i = g^{r_i} \bmod p$, and $y_i = H(x_i||SID) \oplus r = H(z_0^{r_i}||SID) \oplus r$. Here, we want to prove that the adversary A cannot get any information about the group key $SK = H(r||y_1||y_2||...||y_n||SID)$. Under the decision Diffie-Hellman assumption, we prove that two tuples (z_i, y_j, $SK = H(r||y_1||y_2||...||y_n||SID)$) and ($z_i$, y_j, R_1) are computationally indistinguishable for $0 \le i \le n$ and $1 \le j \le n$, where $R_1 \in G_q$.

By contradiction proof, we assume that the adversary A within a polynomial-time can efficiently distinguish (z_i, y_j, $SK = H(r||y_1||y_2||...||y_n||SID)$) and ($z_i$, y_j, R_1) for $0 \le i \le n$ and $1 \le j \le n$. Then, we can construct an algorithm A_1 that can efficiently distinguish a decision Diffie-Hellman (DDH) problem (u_a, u_b, $g^{r_a r_b} \bmod p$) from (u_a, u_b, R_2), where $u_a = g^{r_a} \bmod p$ and $u_b = g^{r_b} \bmod p$ for $r_a, r_b \in Z_q^*$ and $R_2 \in G_q$. Without loss generality, we set $u_a = z_0$ and $u_b = y_1$ as the inputs of the algorithm A_1, A_1 selects n values $t_1, t_2,..., t_n \in_R Z_q^*$ and computes following values:

$$z_1 = z_0^{t_1} \bmod p,\ z_2 = z_0^{t_2} \bmod p, \ldots, z_n = z_0^{t_n} \bmod p$$

and

$$y_2 = y_1^{t_1} \bmod p,\ y_3 = y_1^{t_2} \bmod p, \ldots, y_n = y_1^{t_{n-1}} \bmod p.$$

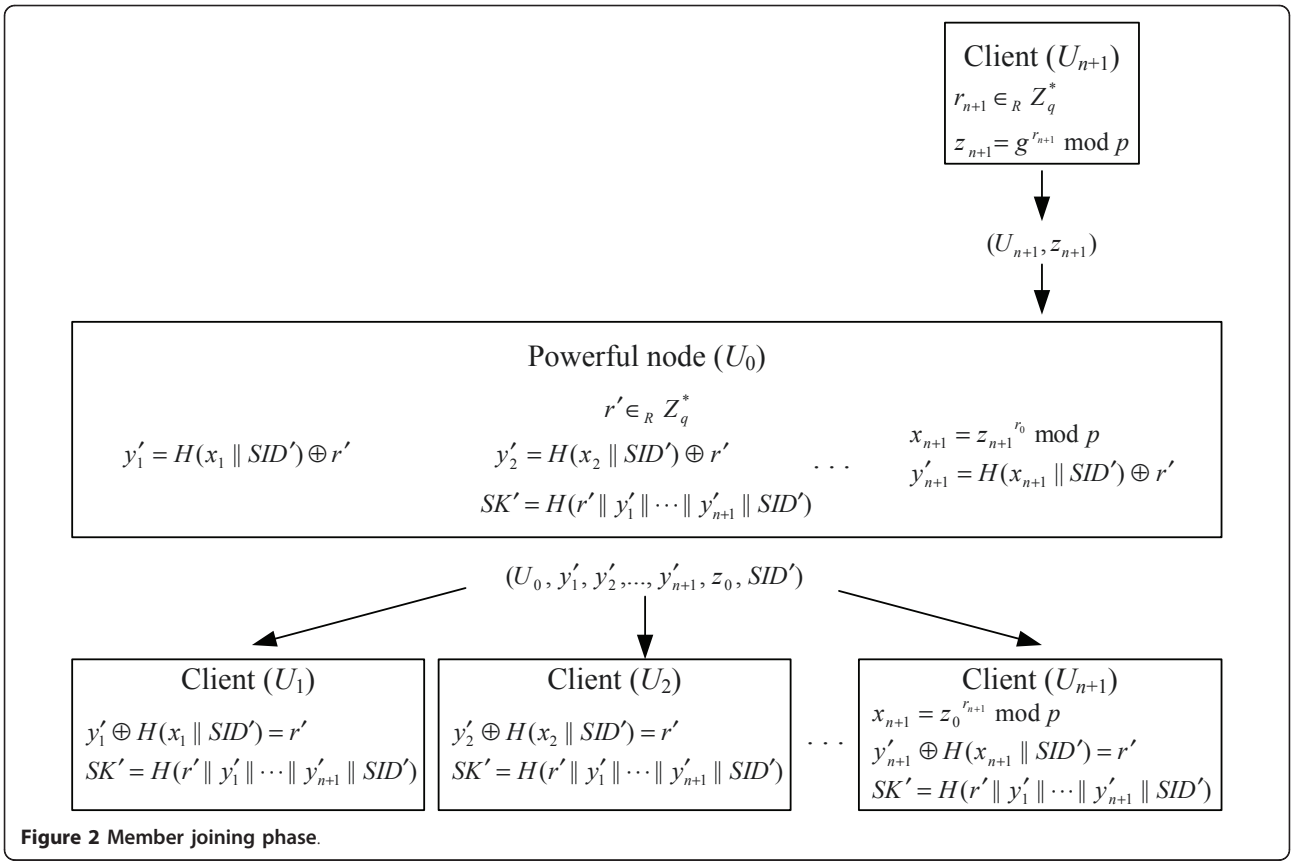

Figure 2 Member joining phase.

Now, the algorithm A_1 has constructed all (z_i, y_j) and then computes $R_1 = H(y_1 \oplus H(R_2||SID)||y_1||y_2||...||y_n||SID)$ for $0 \le i \le n$ and $1 \le j \le n$. Finally, A_1 sends (z_i, y_j, R_1) to the adversary A.

The adversary A can determine whether SK is equal to R_1. If it is true, then $g^{r_a r_b} \bmod p = R_2$. This means that the algorithm A_1 can run A as a subroutine to efficiently distinguish two tuples (u_a, u_b, $g^{r_a r_b} \bmod p$) from (u_a, u_b, R_2). It is a contradiction for the decision Diffie-Hellman assumption. Thus, the proposed dynamic key exchange protocol is secure against passive attacks.■

Contributiveness

Theorem 2. *By running the proposed group key exchange protocol, an identical group key is established*

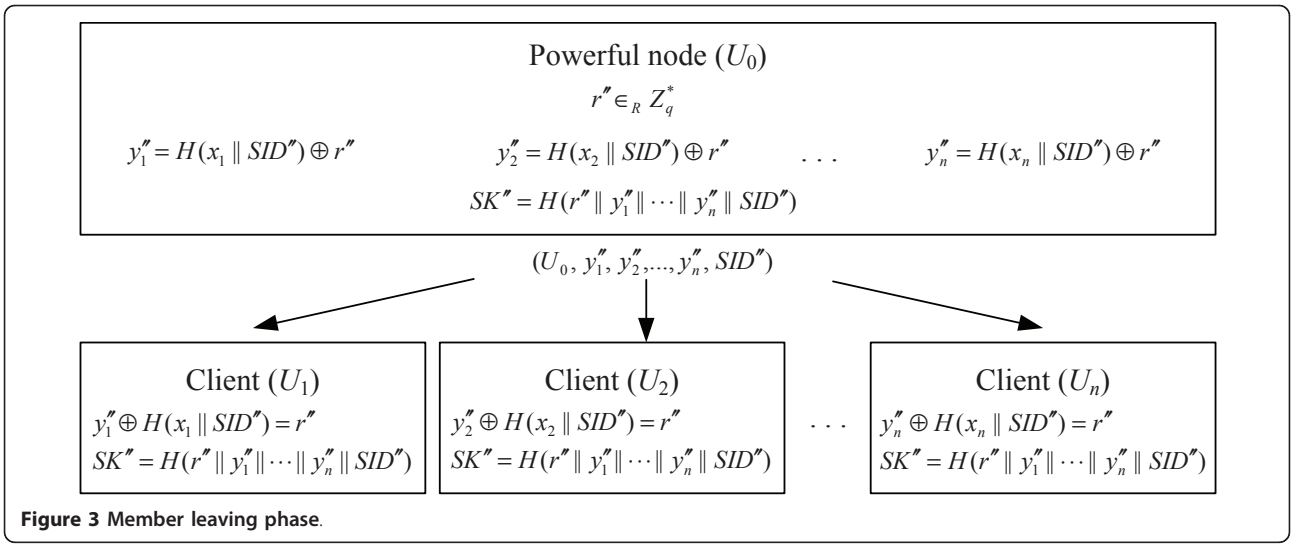

Figure 3 Member leaving phase.

by the group participants. Then, each participant may ensure that her/his contribution has been involved in the group key.

Proof. In the proposed protocol, after the powerful node U_0 broadcasts (U_0, y_1, y_2,..., y_n, z_0, *SID*) to all clients, each client $U_i (1 \le i \le n)$ can use its own secret r_i to compute the value r and then obtains an identical group key *SK*. Thus, this means that the following equations hold:

$$SK = H(r||y_1||y_2||\cdots||y_n||SID) = H(y_1 \oplus H(z_0^{r_1}||SID)||y_1||y_2||\cdots||y_n||SID)$$
$$= H(y_2 \oplus H(z_0^{r_2}||SID)||y_1||y_2||\cdots||y_n||SID)$$
$$= H(y_n \oplus H(z_0{}^{r_n}||SID)||y_1||y_2||\cdots||y_n||SID).$$

Set $V = y_1 \oplus H(z_0^{r_1}||SID) = y_2 \oplus H(z_0^{r_2}||SID) = \cdots = y_n \oplus H(z_0^{r_n}||SID)$. It implies $y_1 = H(z_0{}^{r_1}||SID) \oplus V, y_2 = H(z_0{}^{r_2}||SID) \oplus V, \ldots, y_n = H(z_0{}^{r_n}||SID) \oplus V$. Obviously, each y_i includes the participant U_i's secret value r_i for i = 1, 2,..., n. By the group key $SK = H(r||y_1||y_2||\cdots||y_n||SID) = H(y_i \oplus H(z_0^{r_i}||SID)||y_1||y_2||\cdots||y_n||SID)$, each participant may ensure that her/his contribution has been involved in the group key *SK*. Therefore, our proposed GKE protocol provides contributiveness.■

For convenience to prove the forward/backward secrecy for member joining/leaving, we first prove a lemma as follow.

Lemma 3. *Assume that three secret parameters a, b, and c are randomly selected from Z_p*. If a passive adversary knows two values $H(a)\oplus b$ and $H(a)\oplus c$, then the secret b is un-computable under the hash function assumption. Furthermore, the secret a is also un-computable under the same assumption.*

Proof. Note that if the passive adversary can get the secret b from $U = H(a)\oplus b$ and $V = H(a)\oplus c$, then it implies that the adversary can obtain $H(a)$ from U and V. In the following, we want to prove that the passive adversary is unable to get $H(a)$ from U and V under the hash function assumption.

By the contradiction proof, assume that there exists an algorithm A can obtain the value $H(a)$ from $H(a)\oplus b$ and $H(a)\oplus c$ within a polynomial-time. If the algorithm A cannot get a, then it is hard to find $x = a$ such that $H(x) = H(a)$ and $x \neq a$ such that $H(x) = H(a)$ by the hash function assumption (ii). Thus, the algorithm A must get a. That is, there exists an algorithm A which is able to obtain the secret a from $H(a)\oplus b$ and $H(a)\oplus c$ within the polynomial-time.

Based on the algorithm A, we can construct another algorithm A_1 which is able to get x from $H(x)$ within the polynomial-time as follows. Set the value $H(x)$ as input of the algorithm A_1. A_1 executes the following procedures to obtain x:

(1) The algorithm A_1 calls the algorithm A with the input $H(x)\oplus R$, where R is a nonce.
(2) The algorithm A_1 can obtain x from the algorithm A.

According to the above procedures, the algorithm A_1 can get x from $H(x)$ within the polynomial-time. This is a contradiction for the one-way property of the hash function assumption. Therefore, no passive adversary can compute the secret b from $H(a)\oplus b$ and $H(a)\oplus c$ under the hash function assumption. Certainly, the secret a is also un-computable under the same assumption.■

Forward secrecy

Theorem 4. *Under the computation Diffie-Hellman (CDH) and the hash function assumptions, the proposed group key exchange protocol provides forward secrecy for member joining.*

Proof. Assume that a new client U_{n+1} would like to join the group. According to the proposed protocol, U_{n+1} sends $(r_{n+1} \in Z_q^*,\ z_{n+1} = g^{r_{n+1}} \bmod p)$ to the powerful node U_0. Then, U_0 selects $r' \in Z_q^*$ and computes $y_i' \ (1 \le i \le n+1)$ with a new *SID*'. Finally, U_0 broadcasts $(U_0, y_1', y_2', \ldots, y_{n+1}', z_0, SID')$ to all other clients. Hence, all participants can compute a new group key $SK' = H(r'||y_1'||\cdots||y_{n+1}'||SID')$, where $r' = y_i' \oplus H(z_0^{r_i}||SID')$.

Here, we want to prove that the client U_{n+1} cannot compute the previous group key $SK = H(r||y_1||...||y_n||SID)$. We may assume that U_{n+1} has recorded the previous transmitted messages $(z_0 = g^{r_0} \bmod p,\ z_i = g^{r_i} \bmod p,\ y_i = H(x_i||SID) \oplus r, SID)$ for i = 1, 2,..., n. Obviously, if U_{n+1} can get the value r or x_i for some $i \in \{1, 2,..., n\}$, then the key *SK* can be computed. Hence, we want to prove that the following two cases do not occur.

Case I. U_{n+1} can obtain x_i from z_i $(0 \le i \le n)$. Due to $x_i = z_i^{r_0} \bmod p = g^{r_0 r_i} \bmod p$, given a tuple $(g, z_0 = g^{r_0} \bmod p,\ z_i = g^{r_i} \bmod p)$, it is hard to compute $g^{r_0 r_i} \bmod p = x_i$, by the computational Diffie-Hellman (CDH) assumption. Thus, U_{n+1} obtaining x_i from z_i is impossible.

Case II. U_{n+1} can get the value r or x_i from (y_i, y_i', *SID*, *SID*') for i = 1, 2,..., n, where $y_i = H(x_i||SID) \oplus r$ and $y_i' = H(x_i||SID') \oplus r'$. Without loss generality, we set $a = x_i||SID = x_i||SID'$, $b = r$, and c = r' such that $y_i = H(a)\oplus b$ and $y_i' = H(a) \oplus c$. By Lemma 3, we have proven that the values a and b are un-computable under the hash function assumption. Thus, to obtain the value r or x_i is also impossible.

Therefore, the client U_{n+1} cannot compute the previous group key *SK* by Cases I and II. This means that the proposed group key exchange protocol provides forward secrecy.■

Backward secrecy

Theorem 5. *Under the computation Diffie-Hellman (CDH) and the hash function assumptions, the proposed*

dynamic group key exchange protocol provides backward secrecy for member leaving.

Proof. Without loss generality, we assume that an old client U_{n+1} wants to leave the group. According to the proposed protocol, the powerful node U_0 selects a new random value $r'' \in Z_q^*$ and computes $y_i'' \ (1 \leqslant i \leqslant n)$ with a new *SID*". Then, U_0 broadcasts $(U_0, y_1'', y_2'', \ldots, y_n'', SID'')$ to all other participants. Hence, all participants can compute a new group key $SK'' = H(r''||y_1''|| \cdots ||y_n''||SID'')$.

Here, we prove that the client U_{n+1} cannot compute the later group key $SK'' = H(r''||y_1''|| \cdots ||y_n''||SID'')$. We may assume that U_{n+1} has recorded all transmitted messages

$(z_0 = g^{r_0} \bmod p, z_i = g^{r_i} \bmod p, y_i = H(x_i||SID) \oplus r, y_i'' = H(x_i||SID'') \oplus r'', SID'')$

for $i = 1, 2,..., n$, where $x_i = z_0^{r_i} \bmod p$. Due to the key $SK'' = H(r''||y_1''|| \cdots ||y_n''||SID'')$ and $r'' = y_i'' \oplus H(x_i||SID'')$, if U_{n+1} can get the value r'' or x_i for some $i \in \{1, 2,..., n\}$ then SK'' can be computed. However, U_{n+1} cannot obtain the values r'' and x_i from $(z_0, z_i, y_i, y_i'', SID'')$ by the similar method in the proof of Theorem 4. Thus, the client U_{n+1} cannot compute the later group key SK''. Finally, the proposed group key exchange protocol provides backward secrecy.■

Performance analysis and discussions

For convenience to analyze the performance of our proposed dynamic GKE protocol, we first define the following notations:

- T_{exp}: The time of executing a modular exponentiation operation.
- T_{inv}: The time of executing a modular inverse operation.
- T_{mul}: The time of executing a modular multiplication operation.
- T_H: The time of executing a one-way hash function operation.
- $|m|$: the bit length of a transmitted message m.

Here, let us discuss the computational cost for each client U_i $(1 \le i \le n)$. In Step 1, the client U_i computes z_i, thus it requires T_{exp}. Upon receiving $(U_0, y_1, y_2,..., y_n, z_0, SID)$, the client U_i computes r and then uses r to obtain the group key SK, thus $T_{\text{exp}}+2T_H$ is required in Step 3. The required computational cost for each client U_i is $2T_{\text{exp}} + 2T_H$. Considering the computational cost of the powerful node, the powerful node might be regarded as a wired gateway with less computing-restriction. In Step 2 of the proposed protocol, the powerful node U_0 computes z_0, x_i and y_i for $i = 1, 2,..., n$. Then the powerful node U_0 computes SK. In total, it requires $(n + 1)T_{\text{exp}} + (n + 1)T_H$. Furthermore, let us discuss the computation cost required for member joining/leaving. The powerful node's computation cost for joining and leaving requires $T_{\text{exp}} + (n + 2)T_H$ and $(n + 1)T_H$, respectively. Each client's computation costs for joining/leaving requires $2T_H$, except for the joining client.

In Table 1, we demonstrate the comparisons between our GKE protocol and the recently proposed GKE protocols [20,22] in terms of the number of rounds, the computational cost and the communication complexity required for each client, the powerful node, and the dynamic member joining/leaving, respectively. It is easy to see that the performance of our GKE protocol is better than Nam et al.'s [20] and the Chuang-Tseng [22] GKE protocols. Meanwhile, our GKE protocol also provides the member dynamic joining/leaving functionality and satisfies contributiveness.

Since Nam et al.'s protocol [20], the Chuang-Tseng protocol [22], and our proposed protocol are non-authenticated GKE ones, they must rely on an authenticated channel or apply other schemes to provide authentication like the Katz-Yung complier [12].

Table 1 Comparisons between our protocol and the recently proposed protocols

	Nam et al.'s protocol [20]	Chuang-Tseng protocol [22]	Our protocol
Number of rounds	2	3	2
Contributiveness property	No	Yes	Yes
Computational cost of each client	$2T_{\text{exp}} + T_{\text{mul}} + T_H$	$2T_{\text{exp}} + 3T_H$	$2T_{\text{exp}}+2T_H$
Uni-casting message size sent by each participant	$\|p\|$	$\|p\| + \|q\|$	$\|p\|$
Computational cost of the powerful node	$(n+2)T_{\text{exp}} + nT_{\text{inv}} + 2nT_{\text{mul}} + T_H$	$(n + 1)T_{\text{exp}} + (2n + 1)T_H$	$(n + 1)T_{\text{exp}} + (n + 1)T_H$
Broadcasting message size sent by the group controller	$(n + 1)\|p\|$	$n(\|p\| + \|q\|)$	$(n + 1)\|p\|$
Providing the member dynamic functionality	No	Yes	Yes
Computational cost for joining (each client)	×	$3T_H$	$2T_H$
Computational cost for leaving (each client)	×	$3T_H$	$2T_H$
Computational cost for joining (powerful server)	×	$T_{\text{exp}} + (2n + 1)T_H$	$T_{\text{exp}} + (n + 2)T_H$
Computational cost for leaving (powerful server)	×	$T_{\text{exp}} + (2n + 1)T_H$	$(n + 1)T_H$

Using their complier into a non-authenticated GKE protocol, the protocol can be transformed into an authenticated GKE. Nevertheless, it will additionally increase a new round, one signature generation, and n - 1 signature verifications for each client. Thus, the computational cost is too expensive for each mobile client. The other option is that each client needs not to authenticate the other clients. It only authenticates the powerful node. Certainly, the powerful node must be trusted. Then, it requires single signature generation and verification for each client. Naturally, the powerful server will additionally add one signature generation and n - 1 signature verifications. Fortunately, some known wireless network environment such as cellular mobile networks [3] and wireless local area networks [1], these clients must be authenticated before they want to connect to their network systems. In addition, the powerful node may apply some existing authentication protocols [23-25] to authenticate the mobile client in advance.

Conclusions

In this article, we have proposed a new dynamic GKE protocol for wireless network environments. Under the decision Diffie-Hellman (DDH), the computation Diffie-Hellman (CDH), and the hash function assumptions, we have proven that the proposed protocol is secure against passive attacks and provides forward/backward secrecy for member joining/leaving. Meanwhile, we have proven that the proposed protocol satisfies contributiveness. As compared with the recently presented GKE protocols, we have demonstrated that our protocol provides better performance in terms of computational cost, round number, and communication cost.

List of Abbreviations

CDH: computation Diffie-Hellman; DDH: decision Diffie-Hellman; GKE: group key exchange; PDA: personal digital assistant.

Acknowledgements

This research was partially supported by National Science Council, Taiwan, ROC, under contract no. NSC97-2221-E-018-010-MY3.

Competing interests

The authors declare that they have no competing interests.

Received: 1 December 2010 Accepted: 14 June 2011
Published: 14 June 2011

References

1. ANSI/IEEE. Wireless LAN media access control (MAC) and physical layer (PHY) specifications. ANSI/IEEE Std, (1999) 802.11: 1999 (E) Part 11, ISO/IEC 8802-11
2. C Perkins, *Ad Hoc Networking*. (Addison-Wesley, MA, 2001)
3. GPRS, General packet radio services (GPRS) service description (stage 2). (2002) TS 122 060, ETSI
4. I Akyildiz, W Su, Y Sankarasubramaniam, E Cayirci, A survey on sensor networks. IEEE Commun, Mag. **40**(8):102–114 (2002). doi:10.1109/MCOM.2002.1024422
5. T Phan, L Huang, C Dulan, Challenge: integrating mobile wireless devices into the computational grid. Proceedings of MOBICOM' 02. 271–278 (2002)
6. H Yang, H Luo, F Ye, S Lu, L Zhang, Security in mobile ad hoc networks: challenges and solutions. IEEE Wireless Commun. **11**(1):38–47 (2004). doi:10.1109/MWC.2004.1269716
7. I Ingemaresson, TD Tang, CK Wong, A conference key distribution system. IEEE Trans Inform Theory. **28**(5):714–720 (1982). doi:10.1109/TIT.1982.1056542
8. W Diffie, ME Hellman, New directions in cryptography. IEEE Trans. Inform. Theory. **22**(6):644–654 (1976)
9. E Bresson, M Manulis, Contributory group key exchange in the presence of malicious participants. IET Inform Security. **2**(3):85–93 (2008). doi:10.1049/iet-ifs:20070113
10. M Burmester, Y Desmedt, A secure and efficient conference key distribution system.Inform. Process. Lett. **94**(3):137–143 (2005)
11. J Katz, JS Shin, Modeling insider attacks on group key exchange protocols. Proceedings of CCS' 05. 180–189 (2005)
12. J Katz, M Yung, Scalable protocols for authenticated group key exchange. J Crypt. **20**, 85–113 (2007). doi:10.1007/s00145-006-0361-5
13. YM Tseng, A robust multi-party key agreement protocol resistant to malicious participants. Comput J. **48**(4):480–487 (2005). doi:10.1093/comjnl/bxh111
14. G Ateniese, M Steiner, G Tsudik, New multiparty authentication services and key agreement protocols. IEEE J Select Areas Commun. **18**(4):628–639 (2000). doi:10.1109/49.839937
15. E Bresson, O Chevassut, D Pointcheval, Dynamic group Diffie-Hellman key exchange under standard assumptions. Proceedings of EUROCRYPT' 02 321–336 (2002). LNCS 2332
16. M Steiner, G Tsudik, M Waidner, Diffie-Hellman key distribution extended to group communication. Proceedings of CCS' 96. 31–37 (1996)
17. M Steiner, G Tsudik, M Waidner, Key agreement in dynamic peer groups. IEEE Trans. Parallel Distribut. Syst. **11**(8):769–780 (2000)
18. C Boyd, G Nieto, Round-optimal contributory conference key agreement. Proceedings of PKC' 03 161–174 (2003). LNCS 2567
19. E Bresson, O Chevassut, A Essiari, D Pointcheval, Multual authentication and group key agreement for low-power mobile devices. Comput. Commun. **27**(7):1730–1737 (2004)
20. J Nam, J Lee, S Kim, D Won, DDH-based group key agreement in a mobile environment. J Syst Softw. **78**(1):73–83 (2005)
21. YM Tseng, A resource-constrained group key agreement protocol for imbalanced wireless networks. Comput Security. **26**(4):331–337 (2007). doi:10.1016/j.cose.2006.12.001
22. YH Chuang, YM Tseng, An efficient dynamic group key agreement protocol for imbalanced wireless networks. Int J Netw Manage. **20**(4):167–180 (2010)
23. J Arkko, H Haverinen, EAP AKA authentication. Draft-Arkko-Pppext-Eap-Aka-11, IETF. (2003)
24. YM Tseng, GPRS/UMTS-aided authentication protocol for wireless LANs. IEE Proc Commun. **153**(6):810–817 (2006). doi:10.1049/ip-com:20050366
25. YM Tseng, USIM-based EAP-TLS authentication protocol for wireless local area networks. Comput Stand Interfaces. **31**(1):128–136 (2009). doi:10.1016/j.csi.2007.11.014
26. D Boneh, The decision Diffie-Hellman problem. Proceedings of 3rd Algorithmic Number Theory Symposium. 48–63 (1998)
27. V Shoup, Lower bounds for discrete logarithms and related problems. Proceedings of Advances in Cryptology - Eurocrypt' 97. 256–266 (1997)
28. NIST/NSA FIPS 180-2, *Secure Hash Standard (SHS)*. (NIST/NSA, Gaithersburg, MD, 2005)

doi:10.1186/1687-1499-2011-12
Cite this article as: Wu *et al.*: Two-round contributory group key exchange protocol for wireless network environments. *EURASIP Journal on Wireless Communications and Networking* 2011 **2011**:12.