Sensors **2014**, *14*, 24358-24380; doi:10.3390/s141224358

OPEN ACCESS

sensors

ISSN 1424-8220

www.mdpi.com/journal/sensors

Article

Improved One-Way Hash Chain and Revocation Polynomial-Based Self-Healing Group Key Distribution Schemes in Resource-Constrained Wireless Networks

Huifang Chen [1,2,*] and Lei Xie [1]

[1] Department of Information Science & Electronic Engineering, Zhejiang University, Hangzhou 310027, China; E-Mail: xiel@zju.edu.cn

[2] Zhejiang Provincial Key Laboratory of Information Network Technology, Hangzhou 310027, China

* Author to whom correspondence should be addressed; E-Mail: chenhf@zju.edu.cn; Tel.: +86-571-8795-1820 (ext. 217); Fax: +86-571-8795-2017.

External Editor: Leonhard Reindl

Received: 12 October 2014; in revised form: 9 December 2014 / Accepted: 11 December 2014 / Published: 18 December 2014

Abstract: Self-healing group key distribution (SGKD) aims to deal with the key distribution problem over an unreliable wireless network. In this paper, we investigate the SGKD issue in resource-constrained wireless networks. We propose two improved SGKD schemes using the one-way hash chain (OHC) and the revocation polynomial (RP), the OHC&RP-SGKD schemes. In the proposed OHC&RP-SGKD schemes, by introducing the unique session identifier and binding the joining time with the capability of recovering previous session keys, the problem of the collusion attack between revoked users and new joined users in existing hash chain-based SGKD schemes is resolved. Moreover, novel methods for utilizing the one-way hash chain and constructing the personal secret, the revocation polynomial and the key updating broadcast packet are presented. Hence, the proposed OHC&RP-SGKD schemes eliminate the limitation of the maximum allowed number of revoked users on the maximum allowed number of sessions, increase the maximum allowed number of revoked/colluding users, and reduce the redundancy in the key updating broadcast packet. Performance analysis and simulation results show that the proposed OHC&RP-SGKD schemes are practical for resource-constrained wireless networks in bad environments, where a strong collusion attack resistance is required and many users could be revoked.

Keywords: wireless networks; group communication; group key distribution; self-healing; collusion attack

1. Introduction

Many applications of wireless networks require secure group communications, especially in a hostile environment. In order to protect the sensitive data, group communication keys (also named as group session keys) could be used to encrypt exchanged messages among communicating group members. Therefore, the group key management is critical for providing secure communications.

However, providing efficient key distribution in resource-constrained wireless networks, such as wireless sensor networks, is a challenging issue due to some characteristics of wireless networks.

First, a legitimate group member may not receive the key broadcast message for a particular session due to the unreliable wireless medium, which makes the user request the group manager (GM) to re-transmit the message. When the group size is large, re-transmissions could overwhelm the GM potentially. Furthermore, in some applications with high security requirement, it is important that users only transmit essential messages to avoid making themselves vulnerable. It is desirable to have the self-healing property that enables legitimate group members to recover lost session keys on their own, instead of requesting additional transmissions from the GM.

Second, users may join and/or leave the group frequently. For a large communication group, the group session keys have to be updated due to dynamic group members, which result in the network resource consumption. Hence, an efficient node revocation and join mechanism is important for dynamic communication groups.

Third, wireless devices have limited computation capability, memory and energy. Using energy-consuming techniques, such as the public-key cryptography, to realize the group key management is not applicable for resource-constrained wireless networks. Hence, the energy-efficient property is required.

Three articles [1–3], reviewing self-healing group key distribution (SGKD) schemes have appeared in the literature. Tian *et al.* in [1] provides a survey of available solutions, which is focused on the possible scheme extensions, such as sponsorization or mutual-healing. In [2], the author analyzes the practicality of SGKD schemes in the resource-constrained wireless sensor networks. This review is focused on the scheme performance in terms of the communication overhead and storage overhead. In [3], authors identified three building blocks of the SGKD scheme, selective key distribution mechanism, pre-distributed secret data management and self-healing mechanism, to classify and compare the existing solutions. Based on this three-dimensional classification, a comprehensive review of the development in the area of SGKD schemes is provided.

1.1. Previous Work

Staddon *et al.* first introduced the concept of the self-healing group key distribution (SGKD), and proposed a non-interactive and reliable key distribution scheme in [4]. The basic idea of the SGKD is

to broadcast information that is useful only for legitimate users. In this scheme, users use the secret sharing to bind the capability of recovering lost session keys with the membership. Combined with pre-distributed secrets, legitimate users can recover a session key; otherwise, revoked users cannot infer useful information. However, this scheme has high storage and communication overheads.

Based on the work in [4], several improved SGKD schemes have been proposed [5–29]. In order to increase the efficiency of the scheme in [4], Liu *et al.* proposed some new schemes by combining a personal secret distribution technique with self-healing [5]. Blundo *et al.* analyzed the security model defined in [4,5], and found that it is impossible to satisfy all of the security requirements. Then, based on the self-healing technique with a slightly modified framework in [6] and the self-healing mechanism in [7], a novel SGKD scheme enabling a user to recover all previous session keys from a single key broadcast message was proposed. Hong and Kang proposed a revocation polynomial-based SGKD scheme (RP-SGKD) with low storage and communication overheads [8].

Recent, many hash chain-based SGKD (HC-SGKD) schemes, one-way hash chain (OHC) and dual directional hash chain (DDHC), were proposed in [9–16]. Due to the efficiency of the hash function, these HC-SGKD schemes reduce communication and storage overheads obviously. However, the performance improvement is at the cost of the property of the collusion attack resistance. That is, revoked users colluding with new joined users can recover all session keys, which they are not entitled to get [1].

In [17–19], the pre-arranged life cycle-based SGKD schemes were proposed to make those HC-SGKD schemes resist to the collusion attack. However, these schemes can only apply to the scenario in which the user's life cycle is pre-determined, and the collusion of revoked users within the life cycles and new joined users can recover unauthorized session keys.

In order to resolve the collusion attack resistance problem in existing HC-SGKD schemes, we proposed an SGKD scheme based on the one-way hash chain and revocation polynomial for wireless sensor networks in [20]. However, as using the personal secret structure in Dutta *et al.*'s scheme, the RP-SGKD scheme proposed in [20] inherits the limitation of SGKD schemes in [10,11]. That is, the maximum allowed number of sessions should not be larger than the maximum number of revoked users.

Other techniques, such as subset difference re-keying [21], bilinear pairings [22,23], vector space secret sharing [24,25] and the exponential arithmetic [26], are also used to design SGKD schemes.

Among those existing SGKD schemes, the polynomial secret sharing is the most common cryptographic technique used to implement self-healing key distribution [22]. With regard to the construction method, the polynomial is classified into two types, the revocation polynomial and the access polynomial. Both of them guarantee that only legitimate users can recover the session key(s), while illegitimate users cannot. The SGKD schemes in [5,7–20] are based on the revocation polynomial, and schemes in [27–30] are based on the access polynomial.

Moreover, the hash chain, another cryptographic technique, is used to design the SGKD scheme with other cryptographic techniques. The schemes in [9–20] are hash chain and revocation polynomial-based SGKD (HC&RP-SGKD) schemes, and schemes in [29,30] are hash chain and access polynomial-based SGKD (HC&AP-SGKD) schemes.

1.2. Problems in Existing RP-SGKD Schemes

In this paper, we focus on the SGKD scheme based on the revocation polynomial. After investigating existing RP-SGKD schemes, we find that, except for the collusion attack resistance problem in the HC-SGKD schemes, three other common weaknesses for existing RP-SGKD schemes need to be resolved.

First, the maximum allowed number of revoked/colluding users is limited to be t, where t is the degree of the personal secret polynomial.

Second, the redundancy exists in the key updating broadcast packet, and the communication overhead increases quickly along with the number of sessions.

Third, given the size of the session key updating broadcast packet, the maximum allowed number of sessions and revoked users is too small to use these existing schemes in real resource-constrained wireless networks.

Although the collusion attack resistance problem is partially resolved in [20], the problem, that the maximum allowed number of sessions is limited by the maximum number of revoked users, still exists.

1.3. Our Contributions

Two improved SGKD schemes using the one-way hash chain (OHC) and revocation polynomial in resource-constrained wireless networks are proposed. In the proposed SGKD schemes, by binding the time at which the user joins the group with its capability of recovering group session key(s), some novel methods are presented to utilize one-way hash chain, and to construct the personal secret, the revocation polynomial and the key updating broadcast packet.

To solve the collusion attack resistance problem in existing HC-SGKD schemes and eliminate the limitation of the maximum number of revoked user on the maximum allowed number of sessions, we propose the first SGKD scheme. However, as same as most existing SGKD schemes in [4–12,20], the storage overhead of each user in the first proposed SGKD scheme is high, and determined by the maximum number of revoked user or the maximum allowed number of sessions. To eliminate the impact of the maximum number of revoked user or the maximum allowed number of sessions on the storage overhead, we further propose the second SGKD scheme, a constant storage overhead scheme, to achieve a good tradeoff between the storage overhead and the communication overhead.

Compared to existing RP-SGKD schemes, the main advantages of the proposed schemes are four-aspect. First, the collusion attack resistance problem in existing HC-SGKD schemes is solved. Second, a stronger security and more colluding users are to be supported under same conditions. Third, the total communication overhead is reduced without increasing the storage overhead. Fourth, the limitation of the maximum number of revoked user on the maximum allowed number of sessions is eliminated in the proposed SGKD schemes. And the storage overhead is constant in the second SGKD scheme.

The remainder of the paper is organized as follows. In Section 2, the security model on which the proposed schemes are based is defined. In Section 3, two improved SGKD schemes are presented, and the improvements and security performance are analyzed. In Section 4, the performance comparison with some existing schemes is given. Finally, we conclude the paper in Section 5.

2. Security Model

In this section, we briefly define the security model used in the paper. Notations used in the paper and the corresponding denotations are summarized in Appendix (Table A1).

To clarify the performance of the proposed SGKD schemes, the security model used in this paper is defined as follows.

Suppose a communication group in wireless networks with a GM and a set of group users. Each group member is uniquely identified by an ID number i, the group member is denoted as U_i, $i \in \{1, 2, ..., N\}$, and N is the largest ID number. All of the operations perform in a finite field, F_q, where q is a prime, and $q > N$. The lifetime of the SGKD scheme is partitioned into m sessions.

Definition 1: (self-healing group key distribution with *mt*-revocation capability) The scheme is a self-healing group key distribution with *mt*-revocation capability if the following conditions are satisfied.

(a). For a legitimate group member U_i, $U_i \in G_j^{j'}$, $1 \le j' \le j \le m$, the session key for session j, K_j, is determined by the key updating broadcast packet for session j, B_j, and the personal secret, S_i. That is,

$$H(K_j \mid B_j, S_i) = 0 \tag{1}$$

(b). No information about K_j ($1 \le j \le m$) can be obtained from either key updating broadcast packets or personal secrets only. That is,

$$H(K_j \mid S_1, S_2, ..., S_N) = H(K_j \mid B_1, B_2, ..., B_m) = H(K_j) \tag{2}$$

(c). (*mt*-revocation capability) Let $\mathbf{R}_j$ be a set of users be revoked before and in session j, $\mathbf{R}_j = \{R_j^1, R_j^2, \ldots, R_j^j\}$, where $R_j^{j'}$ is the set of users joined the group in session j' and be revoked before or in session j, $|R_j^{j'}| \le t$ and $|\mathbf{R}_j| \le jt$ for $1 \le j \le m$. The scheme has *mt*-revocation capability if for a given $\mathbf{R}_j$, the GM can generate a key updating broadcast packet, B_j, in order that U_i who does not belong to $\mathbf{R}_j$ recovers K_j, whereas the revoked user U_r, $U_r \in \mathbf{R}_j$, cannot recover K_j. That is,

$$H(K_j \mid B_j, S_i) = 0, H(K_j \mid B_j, \{S_r \mid U_r \in \mathbf{R}_j\}) = H(K_j) \tag{3}$$

(d). (Self-healing property) The scheme is self-healing if any user U_i, who joined the group in session j_1 and is still a legitimate group member in session j_2, can recover lost session key for session j, K_j, from the key updating broadcast packet for session j_2, B_{j_2}, and $j_1 < j < j_2$. That is,

$$H(K_j \mid B_{j_2}, \{S_i \mid U_i \in G_j^{j_1}\}) = 0 \tag{4}$$

Definition 2: (*mt*-wise forward secrecy) Let $\mathbf{R}_j$ be a set of users be revoked before and in session j, $\mathbf{R}_j = \{R_j^1, R_j^2, \ldots, R_j^j\}$, where $R_j^{j'}$ is the set of users who joined the group in session j' and are revoked before or in session j, $|R_j^{j'}| \le t$ and $|\mathbf{R}_j| \le jt$ for $1 \le j \le m$. The scheme guarantees *mt*-wise forward secrecy if for any set $\mathbf{R}_j$, all users in $\mathbf{R}_j$ cannot get any information about K_{j+1} even with the knowledge of session keys before session j. That is,

$$H(K_{j+1} \mid B_1, B_2, ..., B_m, \{S_r \mid U_r \in \mathbf{R}_j\}, K_1, K_2, ..., K_j) = H(K_{j+1}) \quad (5)$$

Definition 3: (*any*-wise backward secrecy) Let $\mathbf{D}_j$ be the set of users joined the group after session j, $\mathbf{D}_j = \{D^{j+1}, D^{j+2}, \ldots, D^m\}$, where $D^{j'}$ ($j + 1 \leq j' \leq m$) is the set of users joined the group in session j', and $1 \leq j \leq m$. The scheme guarantees *any*-wise backward secrecy if for any set $\mathbf{D}_j$, all users in $\mathbf{D}_j$ cannot get any information about K_j even with the knowledge of session keys after session j. That is,

$$H(K_j \mid B_1, B_2, ..., B_m, \{S_v \mid U_v \in \mathbf{D}_j\}, K_{j+1}, K_{j+2} ..., K_m) = H(K_j) \quad (6)$$

Definition 4: (*mt*-wise collusion attack resistance capability) Let $\mathbf{R}_{j_1}$ be the set of users be revoked before and in session j_1. Let $\mathbf{D}_{j_2}$ be the set of users joined the group after session j_2. The scheme has *mt*-wise collusion attack resistance capability if given any two disjoint sets $\mathbf{R}_{j_1}$ and $\mathbf{D}_{j_2}$ ($j_1 < j_2$), users in $\mathbf{R}_{j_1}$ colluding with users in $\mathbf{D}_{j_2}$ cannot recover K_j even with the knowledge of $\{B_1, B_2, \ldots, B_m, \{S_r \mid U_r \in \mathbf{R}_{j_1}\}\}$ and $\{B_1, B_2, \ldots, B_m, \{S_v \mid U_v \in \mathbf{D}_{j_2}\}\}$ for $j_1 < j \leq j_2$. That is,

$$H(K_j \mid B_1, B_2, ..., B_m, \{S_i \mid U_i \in \mathbf{R}_{j_1} \cup \mathbf{D}_{j_2}\}) = H(K_j) \quad (7)$$

3. Two Improved Self-Healing Group Key Distribution Schemes

3.1. The OHC&RP-SGKD Scheme 1

In order to resolve the problems mentioned in Section 1.2, we propose two improved SGKD schemes using the one-way hash chain and the revocation polynomial for resource-constrained wireless networks.

To remove the limitation of the maximum number of revoked user t on the maximum allowed number of sessions m, $m < t + 1$, we change the structure of the personal secret used in [20], and propose the first improved SGKD scheme based on the one-way hash chain and the revocation polynomial, named as the OHC&RP-SGKD scheme 1.

In the proposed OHC&RP-SGKD scheme 1, m t-degree polynomials chosen from $F_q[x]$, $s_1(x)$, $s_2(x)$, ..., $s_m(x)$, are used to replace one $2t$-degree polynomial in Dutta *et al.*'s scheme and the RP-SGKD scheme in [20]. When joining the group in session j, U_i stores $S_i = \{\text{å}_j \cdot s_j(i), \text{å}_j \cdot s_{j+1}(i), \ldots, \text{å}_j \cdot s_m(i)\}$ as the personal secret, where å_j is the unique session identifier for session j. Hence, revealing one or more used secret polynomials has no effect on unused personal secret polynomials, and then it has no effect on following group session keys.

3.1.1. The Scheme Detail

The proposed OHC&RP-SGKD scheme 1, including three phases and two cases, is described as follows.

Phase 1: Initialization

The GM independently and randomly chooses m t-degree polynomials from $F_q[x]$, $s_1(x)$, $s_2(x)$, ..., $s_m(x)$, and m numbers from F_q, å_1, å_2, …, å_m.

Each user U_i, $U_i \in \mathbf{G}_1$, receives $S_i = \{å_1 \cdot s_1(i), å_1 \cdot s_2(i), \ldots, å_1 \cdot s_m(i)\}$ as the personal secret from the GM via a secure communication channel, where $\mathbf{G}_1$ denotes the set of group members at the beginning of session 1.

Phase 2: Broadcast in Session *j* ($1 \le j \le m$)

Let $\mathbf{R}_j$ be the set of users be revoked before and in session j, $\mathbf{R}_j = \{R_j^1, R_j^2, \ldots, R_j^j\}$, where $R_j^{j'}$ is the set of users joining the group in session j' and be revoked before or in session j, $R_j^{j'} = \{U_{r_1^{j'}}, U_{r_2^{j'}}, \ldots, U_{r_{w_{j'}}^{j'}}\}$ and $|R_j^{j'}| = w_{j'} \le t$. $r_1^{j'}, r_2^{j'}, \ldots, r_{w_{j'}}^{j'}$ are the IDs of users in $R_j^{j'}$. $R_j^{j'} = \emptyset$ if there are no new joined users in session j'.

(1) The GM randomly chooses a number k_j^0 from F_q. And the j-th key chain, $\{k_j^1, k_j^2, \ldots, k_j^j\}$, is calculated with one-way hash function, $h(\cdot)$, and k_j^0 as follows,

$$\begin{aligned} k_j^1 &= h(k_j^0) \\ k_j^2 &= h(k_j^1) = h(h(k_j^0)) = h^2(k_j^0) \\ &\ldots \\ k_j^j &= h(k_j^{j-1}) = h^2(k_j^{j-2}) = \ldots = h^j(k_j^0) \end{aligned} \tag{8}$$

For security, $k_{j_1}^0 \ne k_{j_2}^0$ for $j_1 \ne j_2$.

(2) The GM chooses number sets $R'^{j'}_j$, $R'^{j'}_j = \{r'^{j'}_1, r'^{j'}_2, \ldots, r'^{j'}_{t-w_{j'}}\}$, from F_q for sessions with new joined user(s), where $r'^{j'}_1, r'^{j'}_2, \ldots, r'^{j'}_{t-w_{j'}}$ are random numbers, not used as a user ID and different from each other. The GM constructs the revocation polynomials for the users joined the group in different sessions as,

$$A_j^{j'}(x) = \prod_{z=1}^{|R_j^{j'}|}(x - r_z^{j'}) \prod_{z'=1}^{t-|R_j^{j'}|}(x - r'^{j'}_{z'}),\ j' = 1, 2, \ldots, j \tag{9}$$

The purpose of the padding with the elements in $R'^{j'}_j$ is to make the constructed revocation polynomials be t-degree.

(3) The GM computes

$$\Phi_j^{j'}(x) = A_j^{j'}(x) \cdot k_j^{j'} + \varepsilon_{j'} \cdot s_j(x), j' = 1, 2, \ldots, j \tag{10}$$

where $\varepsilon_{j'} \cdot s_j(x)$ and $k_j^{j'}$ are the masking polynomial and the masking key, respectively.

(4) The GM randomly chooses a session key K_j from F_q.

(5) The GM constructs and broadcasts the message

$$B_j = \mathbf{R}_j \cup \mathbf{R}'_j \cup \{\Phi_j^{j'}(x) \mid j' = 1, 2, \ldots, j\} \cup \{E_{k_j^{j'}}(K_{j'}) \mid j' = 1, 2, \ldots, j\} \tag{11}$$

where $\mathbf{R}'_j = \{R'^1_j, R'^2_j, \ldots, R'^j_j\}$.

Phase 3: Group Session Key Recovery in Session *j* ($1 \le j \le m$)

When a legitimate group member U_i, $U_i \in G_j^{j'}$, receives B_j, it recovers the group session key via following steps.

(1) U_i evaluates $\varepsilon_{j'} \cdot s_j(i)$, $A_j^{j'}(i)$ and $\Phi_j^{j'}(i)$, and computes the masking key as

$$k_j^{j'} = \left[\Phi_j^{j'}(i) - \varepsilon_{j'} \cdot s_j(i) \right] \Big/ A_j^{j'}(i),\ j' = 1, 2, ..., j \tag{12}$$

$A_j^{j'}(i) = 0$ when $U_i \in R_j^{j'}$, which means that revoked users can recover neither $k_j^{j'}$ nor K_j from B_j.

(2) U_i computes all masking keys, $\{k_j^{j''} \mid j' \le j'' \le j\}$, in the j-th key chain with (8).

(3) By decrypting $\{E_{k_j^{j''}}(K_{j''}) \mid j' \le j'' \le j\}$ with $\{k_j^{j''} \mid j' \le j'' \le j\}$, U_i recovers $\{K_{j''} \mid j' \le j'' \le j\}$.

Case 1: Group Member Addition

If a new user, U_v, joins the communication group in session j, a key updating process is launched to ensure the backward secrecy.

The GM allocates $S_v = \{a_j \cdot s_j(v), a_j \cdot s_{j+1}(v), \ldots, a_j \cdot s_m(v)\}$ as the personal secret to U_v via a secure communication channel. Receiving the personal secret, U_v joins $\mathbf{G}_j$.

The GM and users in $\mathbf{G}_j$ launch a key updating process, including Phase 2 and Phase 3, to include U_v.

Case 2: Group Member Revocation

If a user joined the group in session j', U_r, is revoked in session j, a key updating process is launched to ensure the forward secrecy.

The GM includes $(x - r_r^{j'})$ into $A_{j''}^{j'}(x)$ $(j \le j'' \le m)$, which means U_r joins $R_{j''}^{j'}$ and $\mathbf{R}_{j''}$. And then, the GM and users in $\mathbf{G}_j$ launch a key updating process, including Phases 2 and 3, to exclude U_r.

3.1.2. Main Advantages

The proposed OHC&RP-SGKD scheme 1 solves the problems mentioned in Section 1.2, and also has some performance improvements.

(1). With the property of the collusion attack resistance

In the proposed OHC&RP-SGKD scheme 1, the unique identity for each session is introduced. U_v, who joins the communication group in session j, receives $S_v = \{a_j \cdot s_j(v), a_j \cdot s_{j+1}(v), \ldots, a_j \cdot s_m(v)\}$ as the personal secret, where a_j is the joining time identity for session j.

A user U_r, $U_r \in \mathbf{G}_1$, be revoked in session j_1, knows $\{a_1 \cdot s_j(r) \mid 1 \le j \le m\}$. And U_v joined the group in session j_2 $(j_1 < j_2 \le m)$ knows $\{\varepsilon_{j_2} \cdot s_j(v) \mid j_2 \le j \le m\}$. The collusion of U_v and U_r can obtain $\{a_1 \cdot s_j(r) \mid 1 \le j \le m\}$ and $\{\varepsilon_{j_2} \cdot s_j(v) \mid j_2 \le j \le m\}$, but neither $\{a_j \cdot s_j(r) \mid j_1 < j < j_2\}$ nor $\{a_j \cdot s_j(v) \mid j_1 < j < j_2\}$. Hence, they cannot recover $\{K_j \mid j_1 < j < j_2\}$.

Therefore, the proposed OHC&RP-SGKD scheme 1 resolves the collusion attack problem.

(2). Reducing the communication redundancy

Considering that there may have no new joined users in some sessions in real network environments and introducing the unique identity for each session, novel methods are presented to construct the revocation polynomials and the key updating broadcast packet in the proposed OHC&RP-SGKD scheme 1.

In the proposed OHC&RP-SGKD scheme 1, the revocation polynomials for users joined the group in different sessions are constructed in order that a user can be revoked according to its joining time. And if there are no users joined in session j' ($j' \leq j$), $R_j^{j'} = \emptyset$, $A_j^{j'}(x) = \emptyset$, and $\Phi_j^{j'}(x)$ is not included in B_j.

Suppose that during j sessions, the group member addition operation occurs v times. The size of the j-th key updating broadcast packet, B_j, in the proposed OHC&RP-SGKD scheme 1 and Dutta *et al.*'s scheme is $[(t + 1)v + j)]\log_2 q$ bits and $[(t + 1)j]\log_2 q$ bits, respectively. When $v < j$, the size of B_j in the proposed OHC&RP-SGKD scheme 1 is smaller than that of Dutta *et al.*'s scheme.

Hence, with novel structures of the revocation polynomials and the key updating broadcast packet, the communication redundancy reduces.

(3). Updating of personal secrets partially

In existing RP-SGKD schemes, once m sessions expires or t revoked users reaches, these schemes should be reset, and the GM has to update the personal secrets of all legitimate group members because the same personal secret polynomial is shared. In the proposed OHC&RP-SGKD scheme 1, users joined the group in different sessions share different personal secret polynomials, and only the number of revoked users joined the group in the same session reaches t, the scheme will be reset. For example, if $|R_j^{j'}| = t$ in session j, and $j < m$, the GM only needs to update the personal secrets of legitimate users in $G_j^{j'}$.

Hence, the proposed OHC&RP-SGKD scheme 1 can update the personal secrets partially, which in turn prolongs the lifetime of the scheme.

(4). Eliminating the limitation of $m < t + 1$

In the proposed OHC-RP-SGKD scheme 1, users joined the group in different sessions are treated by binding the joining time with the capability of recovering previous session keys, and they are classified according to the joining time. Users joined the group in different sessions are allocated different shares of personal secret polynomials, which makes users joined the group in different sessions be unable to collude together.

The reset of the SGKD scheme is triggered by two conditions as follows.

CON1: The maximum number of sessions expires although the number of revoked users is less than t.

CON2: The number of revoked users reaches t although the maximum number of sessions does not expire.

Considering the CON2 that $|\mathbf{R}_j| = \sum_{j'=1}^{j} |R_j^{j'}| \geq t$ in session j, $j < m$ and $|R_j^{j'}| < t$. In the proposed OHC&RP-SGKD scheme 1, since users joined the group in different sessions cannot coalesce

together, the session key(s) cannot be deduced even if $t + 1$ users joined the group in different sessions are revoked. Hence, the proposed OHC&RP-SGKD scheme 1 does not need to reset.

Hence, the proposed OHC&RP-SGKD scheme 1 can support more sessions under same conditions compared to existing HC-SGKD schemes, and a smaller t can be used to prolong the lifetime of the scheme.

3.1.3. Security Analysis

Based on the security model in Section 2, the proposed OHC&RP-SGKD scheme 1 is secure with following theorems and proofs.

Theorem 1. *The scheme presented in Section 3.1.1 is a secure, self-healing group session key distribution scheme with mt-revocation capability.*

Proof.

(a) A legitimate group member U_i, $U_i \in G_j^{j'}$ and $j' \leq j$, can recover K_j as described in Phase 3. Hence, it follows that $H(K_j|B_j, S_i) = 0$.

(b) Since K_j is independent of S_i, using the personal secret only does not give any information about the session keys. On the other hand, since the masking key and the session key are selected randomly, the key updating broadcast packets cannot give any information about the session keys. Therefore, K_j cannot be determined only with S_j or B_j. Hence, it follows that $H(K_j|S_1, S_2, ..., S_N) = H(K_j|B_1, B_2, ..., B_m) = H(K_j)$.

(c) For $U_r \in R_j^{j'}$, $A_j^{j'}(r) = 0$, which makes $k_j^{j'}$ appears randomly to users in $R_j^{j'}$. Hence, it is impossible for the coalition of users in $\mathbf{R}_j$ to recover K_j because $\mathbf{R}_j$ has no information about $k_j^{j'}$.

Moreover, since only users joined the group in the same session can coalesce together, the coalition of users joined the group in different sessions cannot get information about $\sum_{j''} s_j(x)$. Because $|R_j^{j'}| \leq t$, and the required number of users to determine $\sum_{j''} s_j(x)$ is at least $(t + 1)$, the coalition of users in $\mathbf{R}_j$ cannot recover $\sum_{j''} s_j(x)$, which makes K_j appear randomly to all users in $\mathbf{R}_j$.

Hence, it follows that $H(K_j|B_j, S_i) = 0$, $H(K_j|B_j, \{S_r|U_r \in \mathbf{R}_j\}) = H(K_j)$.

(d) From Phase 3, we observe that the proposed OHC&RP-SGKD scheme 1 makes a user recover lost session keys in previous sessions with current key updating broadcast packet only if the user is not revoked in these sessions.

Specifically, let U_i who joined the group in session j_1 be a legitimate group member in session j_2, and $U_i \in G_{j_2}^{j_1}$. U_i receives B_{j_2}, but not B_j, and $j_1 < j < j_2$. U_i recovers all of the lost session keys as follows.

(1) In Phase 3, U_i, $U_i \in G_{j_2}^{j_1}$ and $j_1 < j_2$, recovers $k_{j_2}^{j_1}$.

(2) With $k_{j_2}^{j_1}$, U_i generates all masking keys, $\{k_{j_2}^{j} | j_1 < j < j_2\}$, in the j_2-th one-way hash key chain.

(3) U_i recovers $\{K_j | j_1 < j < j_2\}$ by decrypting $\{E_{k_{j_2}^{j}}(K_j) | j_1 < j < j_2\}$ with $\{k_{j_2}^{j} | j_1 < j < j_2\}$.

Hence, the proposed OHC-RP-SGKD scheme 1 has the property of self-healing. It follows that

$$H(K_j | B_{j_2}, \{S_i | U_i \in G_j^{j_1}\}) = 0$$ ■

Theorem 2. *The scheme presented in Section 3.1.1 achieves mt-wise forward secrecy.*

Proof. For $U_r \in R_j^{j'}$, $A_{j+1}^{j'}(r) = 0$, which means that U_r cannot recover $k_{j+1}^{j'}$ unless U_r can guess $k_{j+1}^{j'}$ correctly.

Since $|R_j^{j'}| \leq t$, $\sum_{j''} s_{j+1}(x)$ cannot be determined by the coalition of users in $R_j^{j'}$. Moreover, since only users who joined the group in the same session can coalesce together, the coalition of users joined the group in different sessions cannot get information about $\sum_{j''} s_{j+1}(x)$. Hence, although all revoked users in $\mathbf{R}_j$ coalesce together, $\sum_{j''} s_{j+1}(x)$ still cannot be determined, and K_{j+1} cannot be recovered.

Therefore, the proposed OHC-RP-SGKD scheme 1 is *mt*-wise forward secret. It follows that

$$H(K_{j+1}|B_1, B_2, ..., B_m, \{S_r|U_r \in \mathbf{R}_j\}, K_1, K_2, ..., K_j) = H(K_{j+1})$$ ■

Theorem 3. *The scheme presented in Section 3.1.1 achieves any-wise backward secrecy.*

Proof. In order to recover K_j, any user U_i, $U_i \in \mathbf{D}_j$, requires the knowledge of at least $(t + 1)$ distinct points about $\sum_{j''} s_j(x)$, $j'' \leq j$. Suppose that U_i joins the group in session j', the GM gives the personal secret, $S_i = \{\sum_{j''} s_{j1}(i) | j + 1 \leq j' \leq j_1 \leq m\}$ to U_i. Hence, the coalition of user in $\mathbf{D}_j$ cannot compute $\sum_{j''} s_j(x)$ no matter how many users in $\mathbf{D}_j$.

Therefore, the proposed OHC-RP-SGKD scheme 1 is *any*-wise backward secret. It follows that

$$H(K_j|B_1, B_2, ..., B_m, \{S_i|U_i \in \mathbf{D}_j\}, K_{j+1}, K_{j+2}, ..., K_m) = H(K_j)$$ ■

Theorem 4. *The scheme presented in Section 3.1.1 has mt-collusion attack resistance capability.*

Proof. Let $\mathbf{R}_{j_1}$ be a set of users be revoked before and in session j_1, $\mathbf{D}_{j_2}$ be the set of users joined the group after session j_2, and $j_1 < j_2$. We will prove that users in $\mathbf{R}_{j_1}$ colluding with users in $\mathbf{D}_{j_2}$ cannot recover K_j ($j_1 < j \leq j_2$) with B_{j_1} and B_{j_2}.

From Theorem 2, the coalition of users in $\mathbf{R}_{j_1}$ cannot recover K_j for $j > j_1$. Similarly, from Theorem 3, the coalition of users in $\mathbf{D}_{j_2}$ cannot recover K_j for $j \leq j_2$.

On the other hand, any user U_r in $R_{j_1}^{j'}$ only knows $\{\sum_{j'} s_j(r) | j \geq j'\}$, And any user U_i in $D^{j''}$ only knows $\{\sum_{j''} s_j(i) | j > j''\}$. Since only users joined the group in the same session can coalesce together, users in $\mathbf{R}_{j_1}$ colluding with users in $\mathbf{D}_{j_2}$ obtain no information about $\sum_{j'} s_j(x)$ or $\sum_{j''} s_j(x)$, $j_1 < j \leq j_2$. Hence, the collusion of users in $\mathbf{R}_{j_1}$ and $\mathbf{D}_{j_2}$ cannot recover K_j, $j_1 < j \leq j_2$.

Therefore, the proposed OHC-RP-SGKD scheme 1 resists to *mt-wise* collusion attack. It follows that

$$H(K_j | B_1, B_2, ..., B_m, \{S_i | U_i \in \mathbf{R}_{j_1} \cup \mathbf{D}_{j_2}\}) = H(K_j)$$

3.2. The OHC&RP-SGKD Scheme 2

Several parameters have been considered to evaluate the performance of SGKD schemes. With respect to the storage overhead, the proposed OHC-RP-SGKD scheme 1 is not optimal. How to tradeoff among the maximum allowed number of sessions, the maximum allowed number of revoked users, the storage overhead and the communication overhead is still an open issue for the RP-SGKD schemes.

By analyzing the key updating broadcast packet in the proposed OHC-RP-SGKD scheme 1, we observe that each $k_j^{j'}$ is masked by different masking polynomials, $\{\varepsilon_{j'} \cdot s_j(x) \mid j = j', j'+1, \ldots, m\}$. Although using multiple masking polynomials seems to make the attack be more difficult, it does not contribute to the security. Indeed, using one masking polynomial for each $k_j^{j'}$ is sufficient. Hence, the number of masking polynomials and the personal secret stored by each user reduce.

Based on the above discussion, an OHC&RP-SGKD scheme with a constant storage overhead is proposed, name as the OHC&RP-SGKD scheme 2.

The proposed OHC&RP-SGKD scheme 2, including three phases and two cases, is described as follows.

Phase 1': Initialization

The GM randomly chooses a 2*t*-degree polynomial, $s_1(x) = a_0 + a_1x + \ldots + a_{2t}x^{2t}$, a *t*-degree polynomial, $s_2(x) = b_0 + b_1x + \ldots + b_tx^t$, from $F_q[x]$, and a number, α_1, from F_q.

Any user U_i in $\mathbf{G_1}$ receives the personal secret $S_i = \{\alpha_1 \cdot s_1(i), \alpha_1 \cdot s_2(i)\}$ from the GM via a secure communication channel.

Phase 2': Broadcast in Session *j* ($1 \le j \le m$)

The GM randomly chooses a session key K_j and a number k_j^0 from F_q.

The *j*-th key chain, $\{k_j^1, k_j^2, \ldots, k_j^j\}$, is computed with (8). And the GM splits $k_j^{j'}$ into two *t*-degree polynomials, $U_j^{j'}(x)$ and $V_j^{j'}(x)$, in order that

$$k_j^{j'} = U_j^{j'}(x) + V_j^{j'}(x), j' = 1, 2, \ldots, j \tag{13}$$

The GM constructs and broadcasts the message

$$B_j = \mathbf{R}_j \cup \mathbf{R'}_j \cup \{M_j^{j'}(x) \mid j' = 1, 2, \ldots, j\} \cup \{N_j^{j'}(x) \mid j' = 1, 2, \ldots, j\} \cup \{E_{k_j^{j'}}(K_{j'}) \mid j' = 1, 2, \ldots, j\} \tag{14}$$

where

$$M_j^{j'}(x) = A_j^{j'}(x) \cdot U_j^{j'}(x) + \varepsilon_{j'} \cdot s_1(x) \tag{15}$$

$$N_j^{j'}(x) = V_j^{j'}(x) + \varepsilon_{j'} \cdot s_2(x) \tag{16}$$

The definitions of $\mathbf{R}_j$, $\mathbf{R'}_j$ and the structure of revoked polynomials, $\{A_j^{j'}(x) \mid j' = 1, 2, \ldots, j\}$, are the same as those in Phase 2 of the proposed OHC&RP-SGKD scheme 1.

Phase 3': Group Session Key Recovery in Session *j* ($1 \le j \le m$)

Any legitimate group member U_i in $G_j^{j'}$ ($j' \le j$) can recover the group session key from B_j through following steps.

(1) U_i computes $U_j^{j'}(i)=[M_j^{j'}(i)-\varepsilon_{j'} \cdot s_1(i)]/A_j^{j'}(i)$ and $V_j^{j'}(i)=N_j^{j'}(i)-\varepsilon_{j'} \cdot s_2(i)$ with (15) and (16), respectively. Thus, $k_j^{j'} = U_j^{j'}(i)+V_j^{j'}(i)$.

(2) U_i computes all of the remaining keys in the j-th key chain, $\{k_j^{j''} \mid j' < j'' \le j\}$.

(3) By decrypting $\{E_{k_j^{j''}}(K_{j''}) \mid j' < j'' \le j\}$ with $\{k_j^{j''} \mid j' < j'' \le j\}$, U_i recovers $\{k_{j''} \mid j' < j'' \le j\}$.

Case 1': Group Member Addition

When a new user, U_v, joins the group in session j, the GM allocates $S_v = \{\text{å}_j \cdot s_1(v), \text{å}_j \cdot s_2(v)\}$ to it via the secure communication channel. Receiving the personal secret, U_v joins $\mathbf{G}_j$.

The GM and users in $\mathbf{G}_j$ launch a key updating process, including Phase 2' and Phase 3', to include U_v.

Case 2': Group Member Revocation

The operation of group member revocation is the same as that described in the Case 2 of the proposed OHC&RP-SGKD scheme 1.

The proposed OHC&RP-SGKD scheme 2 holds all of the advantages described in Section 3.1.2, and also has constant storage overhead for the personal secret of each user.

Along the same lines of the proof of Theorems 1–4, we have the Theorem 5 as follows.

Theorem 5. *The scheme presented in Section 3.2.1 is a secure, self-healing key distribution scheme with mt-revocation capability, and achieves mt-wise forward secrecy, any-wise backward secrecy, and mt-wise collusion attack resistance capability.*

4. Performance Analysis and Comparisons

The performance comparison, in terms of the storage overhead, the communication overhead, the computation overhead, the forward secrecy, the backward secrecy and the collusion attack resistance capability, is listed in Table 1.

4.1. The Storage Overhead for the Personal Secret

The storage overhead for the personal secret of each user comes from the initialization phase. In the proposed OHC&RP-SGKD scheme 1, the storage overhead for the personal secret of each user is $(m - j + 1)\log_2 q$ bits, which is as same as that of schemes in [5,7,8].

In the proposed OHC&RP-SGKD scheme 2, the storage overhead for the personal secret of each user is $2\log_2 q$ bits, which is independent of m and t, and much less than that of the proposed OHC&RP-SGKD scheme 1 and other existing schemes in [4–8,10,11,20].

Table 1. Performance comparison results.

Schemes	**Storage Overhead for Personal Secret (Bits)**	**Communication Overhead for Updating Session Keys (Bits)**	**Computation Overhead (the Number of Multiplication Operations)**	**Forward Secrecy**	**Backward Secrecy**	**Collusion Attack Resistance**
Scheme 3 in [4]	$(m-j+1)^2\log_2 q$	$(mt^2+2mt+m+t)\log_2 q$	$2mt^2+3mt-t$	Yes/t	Yes/t	Yes/t
Scheme 2 in [5]	$(m-j+1)\log_2 q$	$(jt^2+jt)\log_2 q$	$(2t+1)(m+1)$	Yes/t	Yes/t	Yes/t
Scheme 3 in [6]	$2(m-j+1)\log_2 q$	$[(m+j+1)t+(m+1)]\log_2 q$	$mt+t+2tj+j$	Yes/t	Yes/t	Yes/t
Scheme 3 in [7]	$(m-j+1)\log_2 q$	$(2t+1)j\log_2 q$	$2j(t^2+t)$	Yes/t	Yes/t	Yes/t
Scheme 2 in [8]	$(m-j+1)\log_2 q$	$(t+1)j\log_2 q$	$(3t+1)j$	Yes/t	Yes/t	Yes/t
Scheme in [9]	$2\log_2 q$	$(t+j+1)\log_2 q$	$2t+1$	No	No	No
Scheme in [10]	$(t+2)\log_2 q$	$(t+1+j)\log_2 q$	$3t+1$	Yes/t	No	No
Scheme 2 in [11]	$(t+2)\log_2 q$	$(t+1)j\log_2 q$	$(3t+1)j$	Yes/t	Yes/t	No
Scheme in [20]	$(t+2)\log_2 q$	$[(t+1)v+j]\log_2 q$	$3t+1$	Yes/mt	Yes/any	Yes/mt
Proposed OHC&RP-SGKD scheme 1	$(m-j+1)\log_2 q$	$[(t+1)v+j]\log_2 q$	$2t+1$	Yes/mt	Yes/any	Yes/mt
Proposed OHC&RP-SGKD scheme 2	$2\log_2 q$	$[(3t+2)v+j]\log_2 q$	$3t+1$	Yes/mt	Yes/any	Yes/mt

4.2. The Communication Overhead for Updating Session Keys

The communication overhead for updating session keys comes from B_j. In the proposed OHC&RP-SGKD scheme 1, if there are no users joined in session j', $\Phi_j^{j'}(x)$ is not included in B_j. Suppose that the joining operation occurs v times during j sessions, B_j consists of a set of revoked users $\mathbf{R}_j$, $\mathbf{R}'_j$, v t-degree polynomials, $\{\Phi_j^{j'}(x)\}$, and the sequence, $\{E_{k_j^{j'}}(K_{j'}) \mid j'=1,2,...,j\}$. The communication overhead for broadcasting $\mathbf{R}_j$ and $\mathbf{R}'_j$ can be ignored because the IDs can be selected from a small finite field [7]. Hence, the size of B_j is about $[(t+1)v+j]\log_2 q$ bits, which is the same as that of the RP-SGKD scheme in [20], and less than that of existing schemes in [4–8,11],where $v < j \leq m$.

In the proposed OHC&RP-SGKD scheme 2, the size of B_j is $[(3t+2)v+j]\log_2 q$ bits, which is larger than that of the proposed OHC&RP-SGKD scheme 1.

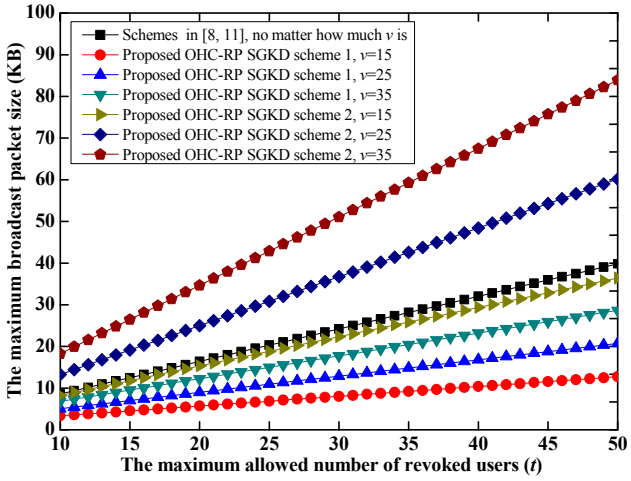
As the assumption in [13], the maximum number of sessions is set to be $m = 50$. Figure 1 shows the comparison of the maximum broadcast packet size when t varies from 10 to 50. Without loss of generality, q is set to be a 128-bit integer.

From Figure 1, we observe that, when $v < m$, the size of B_j in the proposed OHC&RP-SGKD scheme 1 is smaller than that of schemes in [8,11] and with the same m and t. For example, when $m = 50$ and $t = 50$, the broadcast packet sizes of the proposed OHC&RP-SGKD scheme 1 are about 12.734 KB, 20.703 KB, and 28.671 KB for $v = 15$, 25 and 35, respectively, while the broadcast packet size of schemes in [8,11] is about 39.844 KB. Moreover, the maximum broadcast packet size in the proposed OHC&RP-SGKD scheme 2 is obviously larger than that of the proposed OHC&RP-SGKD scheme 1, especially is larger than that of schemes in [8,11].

Remark: It is necessary to reduce the communication redundancy as possible. Although the communication overhead in the proposed OHC&RP-SGKD scheme 1 increases with the number of sessions, it grows more slowly than that of schemes in [8,11] under same conditions.

On the other hand, although the broadcast packet size of the proposed OHC&RP-SGKD scheme 2 is larger than that of the proposed OHC&RP-SGKD scheme 1, we will prove later that the total communication overhead for updating group session keys and the personal secrets in the proposed OHC&RP-SGKD scheme 2 is smaller.

Figure 1. The comparison of the maximum broadcast packet size.



4.3. Practicality

Many practical issues should be addressed when an SGKD scheme is implemented in a real-world application.

As we know, ZigBee, a protocol designed for low data rate wireless networks, uses the IEEE 802.15.4 physical and MAC layers to provide data transfer. According to the IEEE 802.15.4 protocol [31], the maximum size of MAC layer payload is from 89 to 119 bytes. When the maximum size of MAC layer payload is 89 bytes, the application layer data larger than 89 bytes will be partitioned into blocks.

Due to the unreliable wireless transmission, the maximum broadcast packet size in the SGKD scheme is also limited. Let the maximum broadcast packet size be 4096 bytes (4 KB), which will be partitioned into 46 packets with 89 bytes/packet. If packets are lost independently and randomly at a rate of 1%, the probability that a 4 KB broadcast packet will not reach the destination is 37.01%. If the packet loss rate is 5% (a fairly high), the probability that a 4 KB broadcast packet reaches the destination is only 9.45%. Hence, m should be larger than 10. However, the maximum broadcast packet size is assumed to be 64 KB in most existing SGKD schemes [4–7], which is not applicable in ZigBee-based wireless networks.

With the limitation of the maximum broadcast packet size, the value of other parameters should be appropriately set for the intended application and compatible with existing network protocols. In SGKD schemes, system parameters affecting the broadcast packet size are the number of sessions (m), the size of the session key ($\log_2 q$), and the degree of the personal polynomial (t). Without loss of generality, it is assumed that q is a 128-bit integer, and session keys are also 128 bits, which are used in a symmetric cipher, such as AES. The maximum broadcast packet size is set to be 4KB. Symbol $[x]$ represents the operation to round x to the integer downward.

(1). The proposed OHC&RP-SGKD scheme 1 *vs.* the scheme in [8]

The performance of the proposed OHC&RP-SGKD scheme 1 is compared to that of the scheme in [5] because the storage overhead of each user in these two schemes is same, both of them are the RP-SGKD schemes, and the scheme in [8] is the best one among existing collusion-attack-resistance schemes in [4–8]. Let $|\mathbf{R}_m|_{\max}$ be the maximum allowed number of revoked users in m sessions.

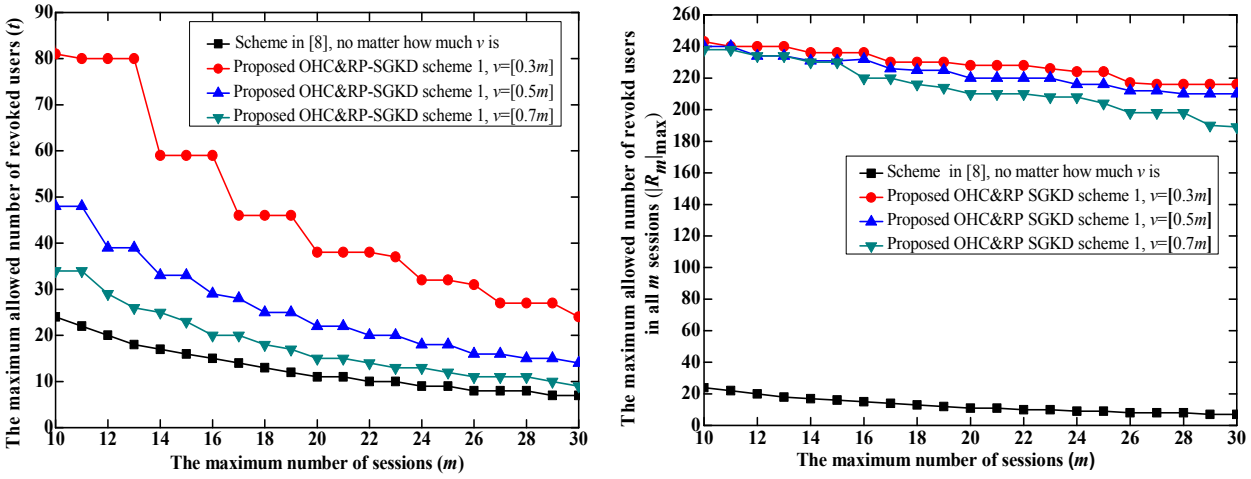
Figure 2 shows performance comparison between the proposed OHC&RP-SGKD scheme 1 and the scheme in [8], where Figure 2a is the tradeoff between m and t, and Figure 2b is the tradeoff between m and $|\mathbf{R}_m|_{\max}$.

From Figure 2a, we observe that the proposed OHC&RP-SGKD scheme 1 can support more sessions than the scheme in [8]. In the proposed OHC&RP-SGKD scheme 1, a smaller t can be used to prolong the lifetime of the scheme because users joined the group in different sessions cannot coalesce together. For example, when t = 15 and m = 16, $|\mathbf{R}_m|_{\max}$ = 15 for the scheme in [8], whereas for the proposed OHC&RP-SGKD scheme 1, when t = 15, m = 44, 28 and 20, $|\mathbf{R}_m|_{\max}$ = 195, 210 and 210 for v = 0.3 m, 0.5 m and 0.7 m, respectively. And when t = 10, m = 59, 39 and 29, $|\mathbf{R}_m|_{\max}$=170, 190 and 200 for v = 0.3 m, 0.5 m and 0.7 m, respectively.

Moreover, the proposed OHC&RP-SGKD scheme 1 can revoke much more users than that of the scheme in [8]. For example, from Figure 2b, when m = 20, $|\mathbf{R}_m|_{\max}$ = 11 for the scheme in [8], whereas

$|\mathbf{R}_m|_{max}$ = 210, 220 and 232 for v = 0.7 m, 0.5 m and 0.3 m, respectively, in the proposed OHC&RP-SGKD scheme 1. Obviously, the proposed OHC&RP-SGKD scheme 1 allows much more revoked users and withstands much more colluding users compared to the scheme in [8].

Figure 2. The performance comparison between the proposed one-way hash chain and revocation polynomial-based self-healing group key distribution (OHC&RP-SGKD) scheme 1 and the scheme in [8]. (**a**) The tradeoff between m and t; (**b**) The tradeoff between m and $|R_m|_{max}$.

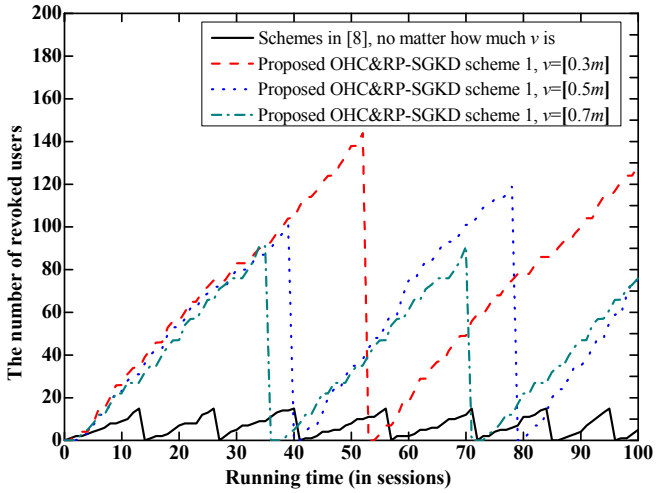


(**a**) (**b**)

In a real-world application, the longer the scheme runs, the more users are revoked. Figure 3 shows the possible lifetime of the proposed OHC&RP-SGKD scheme 1 and the scheme in [8] when two schemes are simulated during 100 sessions.

From Figure 3, we observe that with small values of m and t, the scheme in [8] will be reset frequently, which leads to the energy and bandwidth consumption. However, in the proposed OHC&RP-SGKD scheme 1, more revoked users and more sessions are allowed, and less resetting of the proposed OHC&RP-SGKD scheme 1 contributes to saving the network energy.

Figure 3. The possible lifetime in 100 sessions.



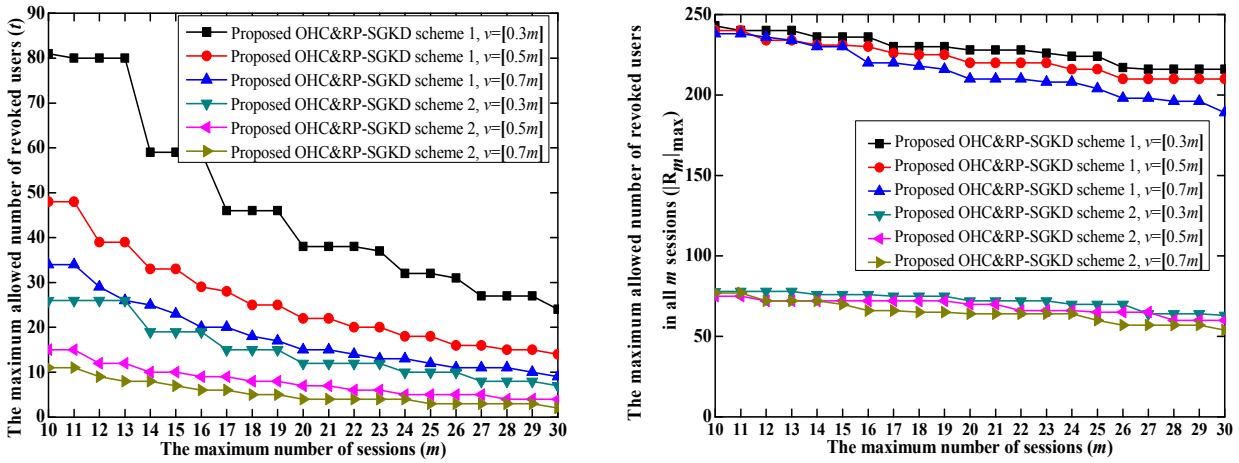
Therefore, the advantage of the proposed OHC&RP-SGKD scheme 1 is obvious for ZigBee-based wireless networks in bad environment where a strong collusion attack resistance is required and many users need to be revoked.

(2). The proposed OHC&RP-SGKD scheme 2 *vs.* the proposed OHC&RP-SGKD scheme 1

In the proposed OHC&RP-SGKD scheme 1 and other existing RP-SGKD schemes, since the storage overhead at each user increases along with the increase of m or t, the power and bandwidth consumption for re-keying personal secrets will be much large. However, the proposed OHC&RP-SGKD scheme 2 has constant storage overhead of $2\log_2 q$ bits.

Figure 4 show the performance comparison of the proposed OHC&RP-SGKD schemes 1 and 2, where Figure 4a is the tradeoff between m and t, and Figure 4b is the tradeoff between m and $|\mathbf{R}_m|_{\max}$.

Figure 4. The performance comparison of the proposed one-way hash chain and revocation polynomial-based self-healing group key distribution (OHC&RP-SGKD) schemes 1 and 2. (**a**) The tradeoff between m and t; (**b**) The tradeoff between m and $|\mathrm{R}_m|_{\max}$.



From Figure 4a,b, we observe that the values of t and m in the proposed OHC&RP-SGKD scheme 2 are smaller than those of the proposed OHC&RP-SGKD scheme 1 under same conditions. However, since the storage overhead for each user in the proposed OHC&RP-SGKD scheme 2 is much less than that of the proposed OHC&RP-SGKD scheme 1, the communication overhead for rekeying the personal secrets in the proposed OHC&RP-SGKD scheme 2 is much less than that in the proposed OHC&RP-SGKD scheme 1.

Wireless devices are usually powered by battery, and most energy is consumed by the communication module. The main concern of the proposed OHC&RP-SGKD scheme 2 is to reduce the total communication overhead for updating the personal secrets and session keys.

Suppose that n users maintain membership during m sessions. For the proposed OHC&RP-SGKD scheme 1, the communication overhead for distributing the personal secrets to n users is $nm\log_2 q$ bits in the initialization phase, and the communication overhead for updating session keys is $[(t+1)v + j]\log_2 q$ bits in the broadcast phase. After running m sessions, the scheme will be reset and new personal secrets should be re-allocated to each group member. Hence, the total communication

overhead for updating session keys and the personal secrets of n users in the proposed OHC&RP-SGKD scheme 1 is

$$E^{(1)} = \left\{ nm^{(1)} + \sum_{j=1}^{m^{(1)}} \left[(t^{(1)} + 1)v + j \right] \right\} \log_2 q \ \text{(bits)} \tag{17}$$

where, $m^{(1)}$ and $t^{(1)}$ denote the session number and the number of revoked users when the proposed OHC&RP-SGKD scheme 1 is reset, respectively.

In the proposed OHC&RP-SGKD scheme 2, the communication overhead for distributing the personal secrets to n users is $2n\log_2 q$ bits, and the communication overhead for updating session keys is $[(3t + 2)v + j]\log_2 q$ bits. Thus, the total communication overhead is

$$E^{(2)} = \left\{ 2n + \sum_{j=1}^{m^{(2)}} \left[(3t^{(2)} + 2)v + j \right] \right\} \log_2 q \ \text{(bits)} \tag{18}$$

where, $m^{(2)}$ and $t^{(2)}$ denote the session number and the number of revoked users when the proposed OHC&RP-SGKD scheme 2 is reset, respectively.

According to the results of Figure 4, when $v = 0.5\ m$, $m^{(1)} = 22$, $t^{(1)} = 20$, $m^{(2)} = 14$, $t^{(2)} = 10$. Hence, after running 154 sessions, the proposed OHC&RP-SGKD scheme 1 is reset seven times and the proposed OHC&RP-SGKD scheme 2 is reset 11 times. Hence, during the 154 sessions, the decrement of the total communication overhead for updating session keys and the personal secrets in the proposed OHC&RP-SGKD schemes 1 and 2 is $\Delta E = E^{(1)} - E^{(2)} = 232.72$ KB when $n = 100$.

Hence, the proposed OHC&RP-SGKD scheme 2 has less storage and total communication overheads, and is therefore quite suitable for resource-constrained wireless networks.

5. Conclusions

To solve the collusion attack problem in existing HC-SGKD schemes, eliminate the limitation of the maximum allowed number of revoked users on the maximum allowed number of sessions, and improve the security and efficiency of existing RP-SGKD schemes, we proposed two improved SGKD schemes using the one-way hash chain and the revocation polynomial for resource-constrained wireless networks in this paper. In the proposed OHC&RP-SGKD schemes, by introducing the unique session identifier and binding the joining time with the capability for recovering previous session keys, the problem of the collusion attack between revoked and new joined users in existing HC-SGKD schemes is resolved. And novel methods for utilizing the one-way hash chain and constructing the personal secret, the revocation polynomial and the key updating broadcast packet are presented to eliminate of the limitation of the maximum allowed number of revoked users on the maximum allowed number of sessions, increase the maximum allowed number of revoked users, and reduce the redundancy in the key updating broadcast packet.

With the security and performance analysis, we concluded the proposed improved OHC&RP-SGKD schemes as follows.

(1) In the proposed OHC&RP-SGKD scheme 1, the impact of t on m is eliminated and the maximum allowed number of sessions is enlarged. In the proposed OHC&RP-SGKD scheme 2,

the storage overhead for the personal secret in each user is constant, $2\log_2 q$ bits, and a better tradeoff between the storage overhead and the total communication overhead is also achieved.

(2) Two proposed improved OHC&RP-SGKD schemes are secure, achieve *mt*-revocation capability, *mt*-wise forward secrecy, *any*-wise backward secrecy, and *mt*-wise collusion attack resistance capability.

(3) The communication overhead of the proposed OHC&RP-SGKD schemes is lower compared to existing RP-SGKD schemes.

(4) Simulation results show that the proposed OHC&RP-SGKD schemes are practical for resource-constrained wireless networks in bad environments where a strong collusion attack resistance is required and many users should be revoked.

For an SGKD scheme, a challenging problem is how to achieve a better tradeoff between the storage overhead and the communication overhead. Since the key updating broadcast packet in the proposed OHC&RP-SGKD scheme 2 is still large, we will focus on reducing the communication overhead in the future work.

Acknowledgments

This work is partly supported by National Natural Science Foundation of China (No. 61071127, No. 61471318), and National High Technology Research and Development Program (863) of China (No. 2012AA090901), and the Fundamental Research Funds for the Central Universities.

Author Conrtibutions

Huifang Chen and Lei Xie proposed two improved OHC&RP-SGKD schemes, analyzed and compared the performance; Lei Xie contributed the simulation results and figures; Huifang Chen wrote the manuscript.

Appendix

Table A1. Notations.

Notations	Denotations
U_i	the *i*-th user
N	the total number of users in a communication group
m	the maximum allowed number of sessions
t	the maximum allowed number of revoked users
j, j', j''	the order of a session
v	the number of sessions with new joined user(s) during m sessions, $v < m$
F_q	a finite field of order q, and q is a prime larger than N
S_i	the personal secret of U_i
B_j	the key updating broadcast packet in session j
K_j	the session key generated by the GM for session j
$H(X)$	the entropy of the random variable X
$H(X\|Y)$	the entropy of X conditioned on Y
$h(\cdot)$	the random one-way function used to compute the one-way key chain

Table A1. *Cont.*

Notations	Denotations
$h^i(\cdot)$	applying hash operation i times
$E_k(.)/D_k(.)$	a symmetric encryption/decryption function
$\mathring{a}_j$	the unique session identifier, a random number selected by the GM for users joined the group in session j, $\mathring{a}_j \in F_q$ and $\varepsilon_{j_1} \neq \varepsilon_{j_2}$ for $j_1 \neq j_2$
k_j^0	the seed of the j-th key chain randomly selected by the GM for session j, $k_j^0 \in F_q$, and $k_{j_1}^0 \neq k_{j_2}^0$ for $j_1 \neq j_2$
$k_j^{j'}$	the j'-th key in the j-th key chain
$A_j^{j'}(x)$	the revoked polynomial constructed by the GM with the IDs of users joined the group in session j' and be revoked before or in session j, and $j' \leqslant j$
$R_j^{j'}$	the set of users joined the group in session j' and be revoked before or in session j, and $j' \leqslant j$
$\lvert R_j^{j'} \rvert$	the number of users in $R_j^{j'}$
$\mathbf{R}_j$	the set of users be revoked before and in session j, and $\mathbf{R}_j = \{ R_j^1, R_j^2, \ldots, R_j^j \}$
$\lvert\mathbf{R}_j\rvert$	the number of users in $\mathbf{R}_j$
D^j	the set of users joined the group in session j
$\mathbf{D}_j$	the set of users joined the group after session j, and $\mathbf{D}_j = \{D^{j+1}, D^{j+2}, \ldots, D^m\}$
$G_j^{j'}$	the set of group members who join the group in session j' and are still legitimate in session j, and $j' \leqslant j$
$\mathbf{G}_j$	the set of all legitimate group members in session j, and $\mathbf{G}_j = \{ G_j^1, G_j^2, \ldots, G_j^j \}$

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Tian, B.; Han, S.; Parvin, S.; Hu, J.; Das, S. Self-healing key distribution schemes for wireless networks: A survey. *Comput. J.* **2011**, *54*, 549–569.
2. Wang, Q. Practically analysis of the self-healing group key distribution schemes for resource-constrained wireless sensor networks. In Proceedings of the 2011 International Conference on Communications and Mobile Computing (CMC 2011), Qingdao, China, 18–20 April 2011; pp. 37–40.
3. Rams, T.; Pacyna, P. A survey of group key distribution schemes with self-healing property. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 820–842.
4. Staddon, J.; Miner, S.; Franklin, M.; Balfanz, D.; Malkin, M.; Dean, D. Self-healing key distribution with revocation. In Proceedings of the 2002 IEEE Symposium on Security and Privacy (SSP 2002), Oakland, CA, USA, 12–15 May 2002; pp. 241–257.
5. Liu, D.; Ning, P.; Sun, K. Efficient self-healing group key distribution with revocation capability. In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS'03), Washington, DC, USA, 27–30 October 2003; pp. 27–31.
6. Blundo, C.; D'Arco, P.; Santis, A. Definitions and bounds for self-healing key distribution. *LNCS* **2004**, *3142*, 234–245.

7. Blundo, C.; D'Arco, P.; Santis, A.; Listo, M. Design of self-healing key distribution schemes. *Des. Codes Cryptogr.* **2004**, *32*, 15–44.
8. Hong, D.; Kang, J. An efficient key distribution scheme with self-healing property. *IEEE Commun. Lett.* **2005**, *9*, 759–761.
9. Dutta, R.; Chang, E.; Mukhopadhyay, S. Constant storage self-healing key distribution with revocation in wireless sensor network. In Proceedings of IEEE International Conference on Communications (ICC 2007), Glasgow, Scotland, 24–28 June 2007; pp. 1323–1332.
10. Dutta, R.; Mukhopadhyay, S. Improved self-healing key distribution with revocation in wireless sensor network. In Proceedings of the 2007 IEEE Wireless Communications and Networking Conference (WCNC 2007), Hong Kong, China, 11–15 March 2007; pp. 2963–2968.
11. Dutta, R.; Mukhopadhyay, S. Designing scalable self-healing key distribution schemes with revocation capability. *LNCS* **2007**, *4742*, 419–430.
12. Dutta, R.; Mukhopadhyay, S.; Emmanuel, S. Low bandwidth self-healing key distribution for broadcast encryption. In Proceedings of the 2nd Asia International Conference on Modeling and Simulation (ICOMS-2008), Kuala Lumpur, Malaysia, 13–15 May 2008; pp. 867–872.
13. Song, H.; Tian, B.; He, M. Efficient threshold self-healing key distribution with sponsorization for infrastructureless wireless networks. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 1876–1887.
14. Kausar, F.; Hussain, S.; Park, J.H. Secure group communication with self-healing and rekeying in wireless sensor networks. *LNCS* **2007**, *4864*, 737–748.
15. Dutta, R.; Change, E.C.; Mukhopadhyay, S.; Efficient self-healing key distribution with revocation for wireless sensor networks using one way key chains. In Proceedings of the 5th International Conference on Applied Cryptography and Network Security (ACNS 2007), Zhuhai, China, 5–8 June 2007; pp. 385–400.
16. Yang, Y.; Zhou, J.; Deng, R.; Bao, F. Computationally secure hierarchical self-healing key distribution for heterogeneous wireless sensor networks. *LNCS* **2009**, *5927*, 135–149.
17. Jiang, Y.; Lin, C.; Shi, M. Self-healing group key distribution with time-limited node revocation for wireless sensor networks. *Ad Hoc Netw.* **2007**, *5*, 14–23.
18. Du, C.; Zhang, H.; Hu, M. Anti-collusive self-healing key distribution scheme with revocation capability. *Inf. Technol. J.* **2009**, *8*, 619–624.
19. Dutta, R.; Mukhopadhyay, S.; Dowling, T. Trade-off between collusion resistance and user life cycle in self-healing key distributions with *t*-revocation. In Proceedings of the 2nd International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2009), London, UK, 4–6 August 2009; pp. 603–608.
20. Wang, Q.; Chen, H.; Xie, L.; Wang, K. One-way hash chain-based self-healing group key distribution scheme with collusion resistance capability in wireless sensor networks. *Ad Hoc Netw.* **2013**, *11*, 2500–2511.
21. Muhammad, J.; Miri, A. Self-healing in group key distribution using subset difference method. In Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications (NCA 2004), Boston, MA, USA, 30 August–1 September 2004; pp. 405–408.

22. Tian, B.; Chang, E.; Dillon, T.S.; Han, S.; Hussain, F.K. An authenticated self-healing key distribution scheme based on bilinear pairings. In Proceedings of the 6th IEEE Consumer Communications and Networking Conference (CCNC 2009), Las Vegas, NV, USA, 10–13 January 2009; pp. 1–5.
23. Tian, B.; Han, S.; Dillon, T.S. A self-healing and mutual-healing key distribution scheme using bilinear pairings for wireless networks. In Proceedings of the 6th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC 2008), Shanghai, China, 17–20 December 2008; pp. 208–215.
24. Tian, B.; Han, S.; Dillon, T.S.; Das, S. A self-healing key distribution scheme based on vector space secret sharing and one way hash chains. In Proceedings of the 9th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM2008), New Port Beach, CA, USA, 23–27 June 2008; pp. 1–6.
25. Wang, Z.; Ma, M. A collusion-resilient self-healing key distribution scheme for wireless sensor networks. In Proceedings of the 2012 IEEE International Conference on Communications (ICC 2012), Ottawa, ON, Canada, 10–15 June 2012; pp. 566–570.
26. Rams, T.; Pacyna, P. Long-lived self-healing group key distribution scheme with backward secrecy. In Proceedings of the 2013 Conference on Networked Systems (NetSys 2013), Stuttgart, Germany, 11–15 March 2013; pp. 59–65.
27. Zou, X.; Dai, Y. A robust and stateless self-healing group key management scheme. In Proceedings of the 2006 IEEE International Conference on Communication and Technology (ICCT 2006), Guilin, China, 27–30 November 2006; pp. 1–4.
28. Tian, B.; Han, S.; Dillon, T.S. An efficient self-healing key distribution scheme. In Proceedings of the 2nd IFIP International Conference on New Technologies, Mobility and Security (NTMS 2008), Tangier, Morocco, 5–7 November 2008; pp. 1–5.
29. Dutta, R.; Wu, Y.; Mukhopadhyay, S.; Dowling, T. Enhanced access polynomial based self-healing key distribution. *Secur. Emerg. Wirel. Commun. Netw. Syst.* **2010**, *42*, 13–24.
30. Wang, Q.; Chen, H.; Xie, L.; Wang, K. Access-polynomial-based self-healing group key distribution scheme for resource-constrained wireless networks. *Secur. Commun. Netw.* **2012**, *5*, 1363–1374.
31. LAN MAN Standards Committee of the IEEE Computer Society. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std 802.15.4–2003 ed.*; IEEE: New York, NY, USA, 2003.