On the Security of a access polynomial based self-healing key management schemes in wireless sensor networks

Yandong Zheng[1], Hua Guo[1,2*]

[1] State Key Laboratory of Software Development Environment, Beihang University

[2] Beijing Key Laboratory of Network Technology, Beihang University, Beijing 100191, China

Email: hguo@buaa.edu.cn

Abstract

Secure group communication in wireless sensors networks (WSN) is a critical issue. Self-healing mechanism is that nodes in WSN can recover the lost session keys without requiring anything to the group manager (GM). Self-healing can be applied to key management, which can efficiently achieve the secure group communication. In 2015, Sun *et al.* proposed a self-healing group key distribution (SGKD) scheme based on access polynomial and sliding-window in WSN, and they claim that the proposed scheme can achieve any-wise backward secrecy, any-wise forward secrecy and δ collusion resistance. However, we find the scheme can not resist the collusion attack of new joined nodes and revoked nodes, and the legitimate cannot achieve session key recovery in some case.

Keywords: wireless sensors networks, self-healing group key distribution, cryptanalysis

1 Introduction

Recently, wireless sensor networks (WSN) draws more and more attention because of its wide application such as intelligence, rescue missions and military operations. There are large number of sensor nodes, which are powered by batteries and thus, have limited storage and communication capabilities. Besides, the WSN is confronted with some security challenges such as the unreliability, the attack. In order to solve the security challenges, key management is a critical method, which includes key distribution and key updating.

Because of the unreliability of WSN, some group key distribution and key updating messages may not be able to receive the sensors nodes. The direct way is that the node requires GM to retransmit the missing message. The retransmission of large number of nodes will aggravate the communication overhead, which may be a disaster. Staddon [1] proposed a SGKD, which can efficiently reduce the communication overhead of retransmission. The property of self-healing can guarantee that if node misses the key distribution or key updating messages, he can recover the lost group keys just by combining the previous and the subsequent messages.

Staddon [1] first proposed the concept of self-healing and constructed two scheme using lagrange interpolation. The scheme in [1] guarantees that the group nodes can recover the session keys but

*Corresponding author: Hua Guo

the revoked nodes can not, and the lost session key can be recovered by combining the previous and subsequent broadcast message, namely, self-healing. However, Blundo *et al.* [2] found an attack in the construction 1 [1]. Later, Liu *et al.* proposed a novel SGKD scheme based on revocation polynomial, which is more efficient in terms of the storage overhead and communication overhead. More [4] proposed a sliding-window SGKD scheme, which can balance the communication overhead and the self-healing capability. Hong *et al.* simplified the SGKD scheme based on revocation polynomial [3], which communication overhead is further to be reduced. Later, some SGKD schemes based on revocation polynomial are proposed [6]-[20]. Zou *et al.* first proposed the SGKD scheme based on access polynomial, which has constant storage overhead and protects the privacy of nodes' identifies. Later, some SGKD schemes based on access polynomial are proposed [22, 23, 24].

Recently, Sun *et al.* proposed a SGKD scheme based on access polynomial, they claimed that their scheme has δ collusion resistance. However, we find the scheme I and II [25] can not resist collusion attack of the new joined node and the revoked node. Besides, the legitimate user can not recover the session key in some case.

The reminder of the paper is arranged as follows. Section 2 briefly introduces Sun *et al.*'s scheme. The cryptanalysis of Sun *et al.*'s scheme is presented in Section 3. Section 4 concludes the whole paper.

2 Overview of Sun *et al.*'s scheme [25]

In this section, we mainly introduce security model and the proposed scheme I and II in [25]. We take the same notations as Sun *et al.*'s scheme. For readability, some notations are listed in Table 1.

2.1 Security model

The scheme in [25] adopts a modified security model. Next we briefly introduce the security model.

Definition 1 *(Key independence)* $\{GK_t\}_{t\in Z_+} \subset F_q$ *is the set of session keys which are distributed independently and uniformly. The scheme D satisfies session key independence if* $\hbar(GK_t|\{GK_i\}_{i\in Z_+\setminus t} = \hbar(GK_t)$ *for any* $t \in Z_+$.

Definition 2 *(Session key distribution with any-wise revocation capability) Suppose that* $j \in Z_+$, $l \in \{1, 2, \cdots, n\}$, n *is the total group members,* SK_l^i *is the secret information of* U_l *in session* i. *The scheme D is a session key distribution scheme with any-wise revocation capability if*

(1) For any node U_l *in* G_i, GK_i *is determined by* B_i *and* SK_l^i. *That is* $\hbar(GK_i|B_i, SK_l^i) = 0$.

(2) GK_i *cannot be derived from either* $\{B_t\}_{t\in Z_+}$ *or* $\{SK_l^i\}_{i\in\{1,2,\cdots,n\}}$. *That is*

$$\hbar(GK_i|\{B_t\}_{t\in Z_+}) = \hbar(GK_i|\{SK_l^i\}_{i\in\{1,2,\cdots,n\}}) = \hbar(GK_i).$$

(3) Let $\tilde{R} = R_1 \cup R_2 \cup \cdots \cup R\infty$ *be the set of revoked nodes the lifetime of the group. D has any-wise revocation capability if any nodes belonging to* $\tilde{R}$ *cannot get the secret information* SK_l^i *of node* l *not belonging to* $\tilde{R}$, $i \in Z_+$. *That is*

$$\hbar(\{SK_l^i\}_{i\in Z_+, l:U_l\in G_i}|\{B_t\}_{t\in Z_+}, \{SK_r^k\}_{k\in Z_+, r:U_r\in\tilde{R}}) = \hbar(\{SK_l^i\}_{i\in Z_+, l:U_l\in G_i})$$

D	The proposed scheme
q, F_q	A large primer number, and a finite field of order q
GM	Group manager
G_i	The set of all legitimate group members during session $i, i = 1, 2, \cdots$
U_l	Ordinary sensor nodes in $G_i, l = 1, 2, \cdots, \|G_i\|$
J_i	The set of group members joining the group in session $i, i = 1, 2, \cdots$
R_i	The set of group members revoked in session $i, i = 1, 2, \cdots$
GK_i	Group key in session $i, i = 1, 2, \cdots$
UK_l^i	The pairwise key between U_l and GM in session $i, U_l \in G_i$
SK_l^i	The shared secret information between U_l and GM in session $i, U_l \in G_i$
$H(\cdot), H^k(\cdot)$	One-way hash chain, and continuously hash operation k times
S^F	The seed of the forward key chain
FK_i	The jth element of forward key chain, where $FK_i = H^i(S^F)$
B_i	The broadcast message for key updating in session $i, i = 1, 2, \cdots$
$\phi_i(x)$	Access polynomial generated by GM in session $i, i = 1, 2, \cdots$
δ	The size of the self-healing window
$\hbar(\cdot)$	The entropy function in information theory
$MAC_K(M)$	HMAC operation on M using the key K to ensure message integrity and authentication
S_l^i	The total secret information stored at node l in the group in session i

Table 1: Notations

Definition 3 *(δ-self-healing capability) D has δ-self-healing capability if*

$$\hbar(GK_i|B_{i_1}, B_{i_2}, SK_l^{i_1}, SK_l^{i_2}) = \begin{cases} 0 & if i_2 - i_1 \leq \delta \\ \hbar(GK_i) & if i_2 - i_1 > \delta. \end{cases}$$

where $1 < i_1 \leq i < i_2$ and $U_l \in G_{i_1} \cup G_i \cup G_{i_2}$.

Definition 4 *(Any-wise forward secrecy) Let $\tilde{R}_i = R_1 \cup R_2 \cup \cdots \cup R_i$ be the set of revoked nodes before and during session i. D guarantees any-wise forward security if every node belonging to $\tilde{R}_i$ cannot get any information about GK_i,$GK_{i+1}, \cdots, GK_\infty$ for any $i \in Z_+$ and $|\tilde{R}_i| \leq \infty$. That is*

$$\hbar(\{GK_t\}_{t\in\{i,i+1,\cdots\}}|\{B_j\}_{j\in Z_+}, \{SK_r^k\}_{k\in Z_+, r:U_r\in\tilde{R}_i}) = \hbar(\{GK_t\}_{t\in\{i,i+1,\cdots\}})$$

Definition 5 *(Any-wise backward secrecy) Let $\tilde{J}_i = J_i \cup J_{i+1} \cup \cdots \cup J_\infty$ be the set of nodes joining the group during and after session i. D guarantees any-wise backward security if all nodes belonging to $\tilde{J}_i$ cannot get any information about $GK_1, GK_2, \cdots, GK_{i-1}$ for any $i \in Z_+$ and $|\tilde{J}_i| \leq \infty$. That is*

$$\hbar(\{GK_t\}_{t\in\{1,2,\cdots,i-1\}}|\{B_j\}_{j\in Z_+}, \{SK_r^k\}_{k\in Z_+, r:U_r\in\tilde{J}_i}) = \hbar(\{GK_t\}_{t\in\{1,2,\cdots,i-1\}})$$

Definition 6 *(λ-collusion resistance) Let $\tilde{R}_r \cup \tilde{J}_s$ be the set of nodes revoked before and during session r and nodes joining the group during and after session s, where $1 < r < s$. D has λ-collusion resistance if the following condition is true. That is*

$$\hbar(\{GK_t\}_{t\in\{r,r+1,\cdots,s-1\}}|\{B_j\}_{j\in Z_+}, \{SK_j^k\}_{k\in Z_+, j:U_j\in\tilde{R}_r\cup\tilde{J}_s}) = \begin{cases} 0 & if s - r \leq \lambda \\ \hbar(\{GK_t\}_{t\in\{r,r+1,\cdots,s-1\}}) & if s - r > \delta. \end{cases}$$

2.2 Sun *et al.* proposed scheme I

In this subsection, we mainly introduce the proposed scheme I in [25]. The scheme I is composed of five parts: **Initialization**, **Broadcast**, **GroupKeyRecoveryandPairwiseKeyUpdating**, **NodeAddition** and **NodeRevocation**.

- **Part1** : **Initialization**

  The offline sever generates a random seek S^F for the forward key chain and a secret $\{SK_l, UK_l^0\}$ only shared between GM and U_l, and send them to GM and U_l, where $l = 1, 2, \cdots, |G_0|$ and G_0 is the initial set of the group. GM keeps the secret information $\{S^F, UK_1^0, SK_1, UK_2^0, SK_2, \cdots, UK_{|G_0|}^0, SK_{|G_0|}\}$, while U_l keeps $\{S^F, UK_l^0, SK_l\}$. As $i \geq \delta$, U_l will store $\{H(GK_{i-\delta}),\ H(GK_{i-\delta+1}) \cdots, H(GK_{i-1}), GK_i\}$,which takes up $(\delta + 1)\log_2 q$ bies. The size of δ meets $\delta \geq MaxSes_{los}$ is the maximum value of consecutive sessions during which group members lost their group keys under unreliable links.

- **Part2** : **Broadcast**

  Key updating and recover will be launched by GM if one of the following cases happens:(a)new nodes want to join the group;(b)malicious nodes are revoked from the group;(c)any intrusion is detected;(d)the current session runs out.

  Consider the process for session i, where $i \in Z_+$.

  (1) GM generates random $\theta_i, \zeta_i, RK_i \in F_q$ and a modified access polynomial

  $$\phi_i(x) = (\theta_i x - \zeta_i)\Pi_{l:U_l \in G_i}(x - UK_l^{i_1}) + RK_i$$

  (2) Group key GK_i is computed as

  $$GK_i = FK_i \oplus RK_i$$

  (3) Using the key RK_i, GM encrypts $RK_{i-1}, RK_{i-2}, \cdots, RK_{i-\delta}$ in Exclusive OR (XOR) cipher using one-way hash operations, and gets $RK_{i-1} \oplus H(RK_i), RK_{i-2} \oplus H(RK_i+1), \cdots, RK_{i-\delta} \oplus H(RK_i + \delta - 1)$. Here, δ is the size of sliding window proposed by More *et al.* in [4], and the length of $H(RK_i + j)$ should be equal to the length of RK_i, where $0 \leq j \leq \delta - 1$.

  (4) GM computes the hash message authentication code (HMAC) with RK_i as $MAC_{RK_i}(\phi_i(x)|\ RK_{i-1} \oplus H(RK_i + 1), \cdots, RK_{i-\delta} \oplus H(RK_i + \delta - 1))$.

  (5) GM updates the secret information as follows.

  (a) Pairwise key UK_l^i between GM and group member U_l:

  $$UK_l^i = \begin{cases} H(i \oplus SK_l) & if 1 \leq i \leq \delta \\ H(H(GK_{i-\delta}) \oplus SK_l) & if i > \delta. \end{cases}$$

  (b) The forward key chain:

  $$FK_{i+1} = \begin{cases} S^F & if i = 0 \\ H(FK_i) & if i \geq 1. \end{cases}$$

(c) The secret information S_0^i is stored in GM as $\{FK_{i+1}, \{UK_l^i, SK_l\}|_{l:U_l \in G_i}, \{RK_t\}|_{1 \le t \le i}, \{H(GK_k)\}|_{i-\delta \le k \le i-1}, GK_i\}$, where $(\delta + 2 + i + 2|G_i|) \log_2 q$ bits space are used.

(6) Finally, GM broadcasts the message B_i,
$B_i = \phi_i(x)|RK_{i-1} \oplus H(RK_i), RK_{i-2} \oplus H(RK_i + 1), \cdots, RK_{i-\delta} \oplus H(RK_i + \delta - 1)|$
$MAC_{RK_i}(\phi_i(x)|RK_{i-1} \oplus H(RK_i), RK_{i-2} \oplus H(RK_i + 1), \cdots, RK_{i-\delta})$

- **Part3** : **GroupKeyRecoveryandPairwiseKeyUpdating**

Suppose that key synchronization for the legitimate node $U_l \in G_i$ gets broken after session i_1, and $0 < i - i_1 \le \delta + 1$ holds, and the information stored in node U_l is $SK_l^{i_1} = \{FK_{i_1+1}, UK_l^{i-1}, SK_l, \{H(GK_k)\}_{i_1-\delta \le k \le i_1-1}, GK_{i_1}\}$. Once node U_l receives B_i, it recovers lost group session keys as follows.

(1) If $i - 1$ is equal to i_1. then execute step(2); otherwise, pairwise key UK_l^{i-1} between GM and U_l is computed as,

$$UK_l^{i-1} = \begin{cases} H((i-1) \oplus SK_l) & if 2 \le i \le \delta + 1 \\ H(H(GK_{i-\delta-1}) \oplus SK_l) & if i > \delta + 1. \end{cases}$$

(2) Compute $RK_i = \phi(UK_l^{i-1})$;

(3) The integrity and broadcast authentication will be checked by using HMAC. First, $MAC_{RK_i}(\phi_i(x)|RK_{i-1} \oplus H(RK_i), RK_{i-2} \oplus H(RK_i + 1), \cdots, RK_{i-\delta} \oplus H(RK_i + \delta - 1))$ is calculated by using RK_i and $\phi_i(x)|RK_{i-1} \oplus H(RK_i), RK_{i-2} \oplus H(RK_i + 1), \cdots, RK_{i-\delta} \oplus H(RK_i + \delta - 1)$; Then, if the computed HMAC and the received HMAC are equal, the message is not tampered by attacks and broadcast authentication get passed; otherwise, discard the message.

(4) Using the key RK_i and one-way hash operations, $RK_{i-1}, RK_{i-2}, \cdots, RK_{i-\delta}$ can be got as $RK_j = H(RK + i - j + 1) \oplus (RK_j \oplus H(RK + i - j + 1))$, where $i - \delta \le j \le i - 1$.

(5) Node U_l gets group keys GK_i and $GK_{i-1}, GK_{i-2}, \cdots, GK_{i_1+1}$ as follows:

$$\begin{aligned} GK_{i_1+1} &= FK_{i_1+1} \oplus RK_{i_1+1}, \\ FK_{i_1+2} &= H(FK_{i_1+1}), \\ &\cdots, \\ GK_i &= FK_i \oplus RK_i, \\ FK_{i+1} &= H(FK_i), \end{aligned}$$

(6) Pairwise key UK_l^i is updated as

$$UK_l^i = \begin{cases} H(i \oplus SK_l) & if 1 \le i \le \delta \\ H(H(GK_{i-\delta}) \oplus SK_l) & if i > \delta. \end{cases}$$

The secret information S_l^i is updated as

$$S_l^i = \{FK_{i+1}, UK_l^i, SK_l, \{H(GK_k)\}|_{k=i-\delta, i-\delta+1, \cdots, i-1}, GK_i\},$$

where $(\delta+4)\log_2 q$ bits space are used. It should be noted that when $i-i_1>\delta$ holds, node U_l has lost more than δ session keys consecutively and will request group session keys from GM using SK_l.

- **Part4** : **NodeAddition**

  If node U_w wants to join the group G_i in session i, it is first pre-loaded with secret $\{FK_i, UK_w^{i-1}, SK_w, \{H(GK_k)\}|_{i-1-\delta\le k\le i-1}\}$. Then, a key updating process is launched by GM which has been loaded with $\{UK_w^{i-1}, SK_w\}$ by the sink or offline sever. Once receiving B_i, node U_w computes GK_i and updates UK_w^{i-1} as Part 3 above.

- **Part5** : **NodeRevocation**

  When GM detects that $U_r \in G_{i-1}$ is compromised in session $i-1$, thus GM will revoke U_r in session i by only removing the item $(x-UK_r^{i-1})$ from the polynomial $\Pi_{l:U_l\in G_{i-1}}(x-UK_l^{i-1})$.

2.3 Sun *et al.* proposed scheme II

Scheme II removes the key chain FK_i, but strengthens collusion resistance capability, and becomes more efficient. Similarly, scheme II is also composed of 5 parts. The difference lies in the processes of group keys calculation, recovery and node addition as well.

(A) Group key GK_i is computed as

$$GK_i=\begin{cases} RK_i & if\, i=1\\ H(GK_1)\oplus RK_i & if 1<i\le\delta+1\\ H(GK_{i-\delta-1})\oplus RK_i & if\, i>\delta+1\end{cases}$$

.

(B) Group key recovery Similar to Part 3 in scheme I, only difference exists in step (5). For session i, node $U_l\in G_i$ will calculate current group key GK_i and lost group $GK_{i_1+1},\cdots,GK_{i-1}$, where $0<i-i_1\le\delta+1$. The case $i_1>\delta+1$ is only considered, while other simple cases can be derived easily, and is not given here.

$$\begin{aligned} GK_{i_1} &= H(GK_{i_1-\delta-1})\oplus RK_{i_1},\\ GK_{i_1+1} &= H(GK_{i_1-\delta})\oplus RK_{i_1+1},\\ &\cdots,\\ GK_i &= H(GK_{i-\delta-1})\oplus RK_i,\end{aligned}$$

After session i, GM updates the secret information S_0^i as $\{\{UK_l^i, SK_l\}|_{l:U_l\in G_i}, \{RK_t\}|_{1\le t\le i}, \{H(GK_k)\}|_{i-\delta\le k\le i-1}, GK_i\}$ occupying $(\delta+1+i+2|G_i|)\log_2 q$ bits space, while node $U_l\in G_i$ updates the secret information S_l^i as $\{UK_l^i, SK_l, \{H(GK_k)\}|_{i-\delta\le k\le i-1}, GK_i\}$ occupying $(\delta+3)\log_2 q$ bits space.

(C) Node addition If node U_w wants to join the group G_i in session i, it is first pre-loaded with secret $\{UK_w^{i-1}, SK_w, \{H(GK_k)\}|_{i-1-\delta \le k \le i-1}\}$. Then, a key updating process is launched by GM which has been loaded with $\{UK_w^{i-1}, SK_w\}$ by the sink or offline sever. Once receiving B_i, node U_w computes GK_i and updates UK_w^{i-1} as Part 3 in scheme I [25].

3 Cryptanalysis of Sun *et al.*'s Scheme

In this section, we mainly introduce the two flaws of Sun *et al.*'s scheme I and II.

3.1 Flaws of Scheme I in [25]

3.1.1 Lack of collusion resistance

Let U_l denote the group node who joined the group in session i_1 and revoked in session i_2. Let U_w denote the node who joined the group in session i, where $i_1 < i_2 < i - \delta < i$. When U_l joined the group, he received the secret FK_{i_1}. Thus, he can computes $\{FK_{i_1+1}, \cdots, FK_{i-\delta}, \cdots, FK_i\}$ as

$$\begin{aligned} FK_{i_1+1} &= H(FK_{i_1}), \\ FK_{i_1+2} &= H(FK_{i_1+1}) = H(H(FK_{i_1})) = H^2(FK_{i_1}), \\ &\cdots, \\ FK_i &= H(FK_{i-1}) = \cdots = H^{i-i_1}(FK_{i_1}), \end{aligned}$$

U_w is a legitimate node in session U_w. Thus, he can evaluate RK_i by $\phi_i(UK_w^{i-1})$. The broadcast message composes of $RK_{i-1} \oplus H(RK_i), RK_{i-2} \oplus H(RK_i + 1), \cdots, RK_{i-\delta} \oplus H(RK_i + \delta - 1)$. Then, U_w can compute $\{RK_{i-1}, RK_{i-2}, \cdots, RK_{i-\delta}\}$ as

$$\begin{aligned} RK_{i-1} &= H(RK_i) \oplus (RK_{i-1} \oplus H(RK_i)), \\ RK_{i-2} &= H(RK_i + 1) \oplus (RK_{i-2} \oplus H(RK_i + 1)), \\ &\cdots, \\ RK_{i-\delta} &= H(RK_i + \delta - 1) \oplus (RK_{i-\delta} \oplus H(RK_i + \delta - 1)), \end{aligned}$$

If U_l colludes with U_w, they provide the $\{FK_{i_1+1}, \cdots, FK_{i-\delta}, \cdots, FK_i\}$ by U_l and $\{RK_{i-1}, RK_{i-2}, \cdots, RK_{i-\delta}\}$ by U_w respectively.

Thus, $GK_{i-\delta}, GK_{i-\delta+1, \cdots, GK_{i-1}}$ can be evaluated as

$$\begin{aligned} GK_{i-1} &= FK_{i-1} \oplus RK_{i-1}, \\ GK_{i-2} &= FK_{i-2} \oplus RK_{i-2}, \\ &\cdots, \\ GK_{i-\delta} &= FK_{i-\delta} \oplus RK_{i-\delta}, \end{aligned}$$

The collusion of U_l and U_w can recover the session keys from session $i-\delta$ to $i-1$. However, both of them are not the legitimate node in these sessions. Therefore, the scheme I in [25] can not resist the attack of the new joined node and the revoked node collusion.

3.1.2 Lack of session key recovery capability

In this subsection, we will show the flaw of Sun *et al.*'s Scheme. The flaw makes the scheme cannot achieve session key recovery for a legitimate user. Obviously, it can not be tolerated for a SGKD scheme. We specifically introduce as follows.

Let U_l denote a user who joined the group in session i, where $i > \delta$. When U_i joined the group, he will receive the secret $\{FK_i, UK_l^{i-1}, SK_l, \{H(GK_k)\}_{i-1-\delta \le k \le i-1}\}$. If U_l does not receive the broadcast message from session i to session j, where $j - i > \delta$. In session $j+1$, suppose U_l is a legitimate. U_l first computes UK_l^j according to step (1) in the Sch-I's part 3.

$$UK_l^j = H(H(GK_{j-\delta}) \oplus SK_l)$$

Because $j - \delta > i$ and U_l does not receive the broadcast message from session i to session j, U_l can not compute $H(GK_{j-\delta})$. Thus, U_l cannot compute UK_l^j. In this case, even if U_l is a legitimate user, he cannot achieve session key recovery.

3.2 Attack to Scheme II in [25]

3.2.1 Lack of collusion resistance

The scheme II [25] includes the same problem.

Suppose that U_l denotes the node who joined the group in session j_1 and revoked in session j_2, and U_w denotes the node who joins the group in session i, where $i_1 < i - \delta < i_2 < i$. When U_l joined the group, he received the secret $\{H(GK_k)\}|_{i-1-\delta \le k \le i-1}\}$. He is a legitimate node from session i_1 to i_2. He has access to the session keys $\{GK_{j'}\}_{i_1 \le j' \le i_2}$. He can compute $\{H(GK_{j'})\}_{i_1 \le j' \le i_2}$. For u_w, he is a legitimate node in session i. Then, he can obtain $\{RK_{i-1}, RK_{i-2}, \cdots, RK_{i-\delta}\}$ as above.

If U_l colludes with U_w, U_l provide $\{H(GK_{j'})\}_{i_1 \le j' \le i_2}\}$ and U_w provides $\{RK_{i-1}, RK_{i-2}, \cdots, RK_{i-\delta}\}$. Thus, $\{GK_{i-1}, GK_{i-2}, \cdots, GK_{i_2}\}$ can be evaluated as

$$\begin{aligned} GK_{i-1} &= H(GK_{i-\delta-2}) \oplus RK_{i-1}, \\ GK_{i-2} &= H(GK_{i-\delta-3}) \oplus RK_{i-2}, \\ &\cdots, \\ GK_{i_2-1} &= H(GK_{i_2-\delta-2}) \oplus RK_{i_2-1}. \end{aligned}$$

The collusion of U_l and U_w can recover the session keys from session i_2 to $i-1$. However, both of them are not the legitimate node in these sessions. Therefore, the scheme II in [25] can not resist the attack of the new joined node and the revoked node collusion.

The group key is composed of two parts, namely, FK_i, RK_i. For a revoked user, he can compute the FK_i after the session he joined. For a new joined user, he can use RK_i of the current session to obtain $\{RK_{i-1}, \cdots, RK_{i-\delta}\}$ by decrypting $\{RK_{i-1} \oplus H(RK_i), RK_{i-2} \oplus H(RK_i + 1), \cdots, RK_{i-\delta} \oplus$

$H(RK_i + \delta - 1)\}$. Thus, the scheme cannot resist collusion attack. The reason why this attack exists is that the FK_i, RK_i can easily be deduced from the personal secret and broadcast message.

Note that the flaw of Sch-I in 3.1.2 also hold on for the Sch-II.

4 Conclusion

In this paper, we show that two flaws of Sun *et al.*'s scheme. Specially speaking, it can not resist collusion attack of the new joined node and the revoked node. Besides, it can not achieve session key recovery for a legitimate node in some case.

References

[1] 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, Oakland, CA, USA, 12-15 May 2002; pp. 241-257.

[2] Blundo C, D'Arco P, Listo M. A flaw in a self-healing key distribution scheme[C]// Information Theory Workshop, 2003. Proceedings. 2003 IEEE. IEEE, 2003:163-166.

[3] 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(CCS03), Washington, DC, USA, 27-30 October 2003; pp. 27-31.

[4] More S M, Malkin M, Staddon J, et al. Sliding-window self-healing key distribution[J]. Proc. of ACM workshop on Survivable and self-regenerative systems, 2003, 2003.

[5] Hong, D.; Kang, J. An efficient key distribution scheme with self-healing property. IEEE Communications Letters, 2005, 9(8):759-761.

[6] Han S.; Tian B.; He M. Efficient threshold self-healing key distribution with sponsorization for infrastructureless wireless networks. Wireless Communications IEEE Transactions on, 2009, 8(4):1876-1887.

[7] 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.

[8] 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.

[9] Dutta, R.; Mukhopadhyay, S. Designing scalable self-healing key distribution schemes with revocation capability. Parallel and Distributed Processing and Application, LNCS 2007, 4742:419-430.

[10] Chen H.; Xie L. Improved One-Way Hash Chain and Revocation Polynomial-Based Self-Healing Group Key Distribution Schemes in Resource-Constrained Wireless Networks. Sensors, 2014, 14(12):24358-24380.

[11] Xu Q.; He M. Improved constant storage self-healing key distribution with revocation in wireless sensor network. Information Security Applications. Springer Berlin Heidelberg, 2009:41-55.

[12] Dutta, R.; Mukhopadhyay, S.; Emmanuel, S. Low bandwidth self-healing key distribution for broadcast encryption. Pro. 2nd Asia International Conference on Modeling and Simulation (AMS), 2008, pp.867C872.

[13] Dutta, R.; Change, E.C.; Mukhopadhyay, S. Efficient self-healing key distribution with revocation for wireless sensor networks using one way key chains. ACNS 2007, Lecture Notes in Computer Science, vol.4521, pp.385-400, 2007.

[14] Song, H.; Tian, B.; He, M. Efficient threshold self-healing key distribution with sponsorization for infrastructureless wireless networks. Wireless Communications IEEE Transactions on, 2009, 8(4):1876-1887.

[15] Kausar, F.; Hussain, S.; Park, J.H. Secure group communication with self-healing and rekeying in wireless sensor networks. In Mobile Ad-Hoc and Sensor Networks, vol. 4864, pp. 737-748. Springer, Berlin, Heidelberg.

[16] Blundo, C.; DArco, P.; Santis, A. On Self-Healing Key Distribution Schemes. Information Theory IEEE Transactions on, 2006, 52(12):5455-5467.

[17] Yang, Y.; Zhou, J.; Deng, R.; Bao, F. Computationally secure hierarchical self-healing key distribution for heterogeneous wireless sensor networks. Information and Communications Security, Springer Berlin Heidelberg, 2009:135-149.

[18] Wang, Q.; Chen H.; Xie L. One-way hash chain-based self-healing group key distribution scheme with collusion resistance capability in wireless sensor networks. Ad Hoc Networks 11.8(2013):2500C2511.

[19] Dutta R.; Mukhopadhyay S.; Collier M. Computationally secure self-healing key distribution with revocation in wireless ad hoc networks. Ad Hoc Networks, 2010, 8(6):597C613.

[20] Han S.; Tian B.; Zhang Y.; Hu J. An effieient self-healing key distribution scheme with constant-size personal keys for wireless sensor networks. Communications (ICC), 2010 IEEE International Conference on, may 2010:1-5.

[21] Zou X.; Dai YS. A robust and stateless self-healing group key management scheme. Communication Technology, 2006. ICCT '06. International Conference on. IEEE, 2006:1-4.

[22] Dutta R.; Mukhopadhyay S.; Dowling T. Enhanced access polynomial based self-healing key distribution. Security in Emerging Wireless Communication and Networking Systems 2010; 42(1):13C24.

[23] Tian B.; Han S.; Dillon T. An efficient self-healing key distribution scheme. Proc. of the 2nd IFIP International Conference on New Technologies, Mobility and Security, Tangier, Morocco, 2008; 1C5.

[24] Wang, Q.; Chen, H.; Xie, L.; Wang, K. Access-polynomial-based Self-healing Group Key Distribution Scheme for Resource-constrained Wireless Networks. Security and Communication Networks. 2012, 5(12):1363-1374.

[25] Sun X, Wu X, Huang C, et al. Modified access polynomial based self-healing key management schemes with broadcast authentication and enhanced collusion resistance in wireless sensor networks[J]. Ad Hoc Networks, 2015.