On the Security of a Self-healing Group Key Distribution Scheme

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

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

Beijing 100191, China

Email: hguo@buaa.edu.cn

Abstract

Recently, in Journal of Security and Communication Networks (5(12):1363-1374, DOI: 10.1002/sec.429), Wang *et al.* proposed a group key distribution scheme with self-healing property for wireless networks in which resource is constrained. They claimed that their key distribution scheme satisfies forward security, backward security and can resist collusion attack. Unfortunately, we found some security flaws in their scheme. In this paper, we present a method to attack this scheme. The attack illustrates that this scheme does not satisfy forward security, which also directly breaks the collusion resistance capability.

Keywords: Cryptanalysis, forward security, collusion resistance, self-healing key distribution.

1 Introduction

In secure group communications, how to manage the key including secure key distribution and key updating is an important problem. It is possible that the key updating messages do not reach a user due to the network's unreliability. A common way is that the users who don't receive the broadcast messages for key's updating ask the Group Manager(GM) to retransmit the missing message, which aggravates the network traffic. A group key distribution scheme with self-healing property can solve this problem satisfactorily. More precisely, a self-healing mechanism enables users to recover the session keys that he could not compute since he didn't receive the broadcast messages because of packet loss. Furthermore, in some security-crucial environments(e.g., military application), users should send as few as messages, lest they expose some important information, i.e., their location position. When the users receive the key updating message, they can compute the session key by combining the broadcast with their own secret. If they lose some broadcast message, they are able to recover the lost session keys by using a previous broadcast and a subsequent one without requesting anything to the group manager.

Staddon *et al.* [1] first proposed a group key distribution scheme with self-healing property. Unfortunately, their first construction was showed insecure by Blundo *et al.* [2]. Later, Blundo *et al.* [3] proposed an efficient self-healing scheme which has less user memory storage. In 2006, a lower bound on the resource of implementing such self-healing schemes was pointed out by Blundo *et al.* [4]. Later,

*Corresponding author: Hua Guo

Liu *et al.*[5] proposed a personal key distribution scheme by using of a broadcast channel, and combined this scheme with the self-healing mechanism in [1]. More *et al.*[6] proposed a novel self-healing group key distribution scheme which is balanced between the self-healing capability and the overhead of the network by using of a sliding window. Later, some key distribution schemes with self-healing property under resource-constrained environment were designed [7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17]. Among them, some schemes are based on the access-polynomial which can be used to keep the group numbers' identity privacy [14, 15, 16, 17].

In 2012, Wang *et al.*[18] presented a novel self-healing group key distribution scheme by using of access-polynomial. In their scheme, self-healing property is achieved by binding the time at which the user joins the communication group with its capability of recovering previous group session keys. They claimed that their scheme satisfies all basic security properties, i.e., backward security, forward security and can resist collusion attack. Unfortunately, we found that some revoked users can recover the current session's session key which should be kept secret from the revoked users. Therefore, Wang *et al.*'s scheme has not forward security, which contributes to the failure of mt-wise collusion resistance.

The structure of the papers is organised as follows. Wang *et al.*'s scheme and the corresponding security model is reviewed in section 2. An attack to Wang *et al.*'s scheme is presented in section 3. We conclude this paper in Section 4. For readability, we list some notations in Table 1.

U_i	the i-th user
m	the maximum sessions
t	the maximum revoked users
F_q	a finite field of order q, and q is a prime
$\mathcal{S}(i)$	the personal secret of U_i
B_j	the j-th broadcast message
$H(\cdot)$	hash function
$E_k(\cdot)/D_k(\cdot)$	a symmetric encryption/decryption function
ε_j	session identifier
k_j^0	the seed of j-th key chain $k_{j_1}^0 \neq k_{j_2}^0$ for $j_1 \neq j_2$
$k_j^{j'}$	the j' key in the j-th key chain
$R_j^{j'}$	users who joined the group in session j' and are revoked before or in session j and $j^{'} \leq j$
$\lvert R_j^{j'}\rvert$	the number of users in $R_j^{j'}$, and $\lvert R_j^{j'}\rvert \leq t$
R_j	users who are revoked before and in session j, and $R_j = \{R_j^1, \cdots, R_j^j\}$
$\lvert R_j\rvert$	the number of users in R_j
$G_j^{j'}$	the users who join the group in session j and are still legitimate in session j and $j' \leq j$
$\lvert G_j^{j'}\rvert$	the number of users in $G_j^{j'}$
G_j	all legitimate group members in session j, and $G_j = \{G_j^1, \cdots, G_j^j\}$
$\lvert G_j\rvert$	the number of users in G_j

Table 1: Notations

2 Brief Introduction of Wang *et. al.*'s Scheme

In this section, we briefly revisit the system model, the security model and Wang *et al.*'s group key distribution scheme with self-healing property.

2.1 System Model

We adopt the same notations and assumption as those in Zou and Dai's scheme[14]. In the model, the group includes a group manager (GM) and some group members of $U = \{U_1, \cdots, U_n\}$. The GM builds and maintains a group by joining users and revoking operations. Suppose each group user is distributed an unique ID number i, where $0 < i \leq n$. Note that n is chosen by GM and denotes the largest ID number, and i denotes the group member as U_i. The GM sends a personal secret $\mathcal{S}_i$ to U_i by a secure channel when U_i joins the group. Let K_j denote the session key selected by the GM independently and uniformly. For each session, the GM distributes K_j to user $U_i \in G_j$ through a broadcast message B_j during session j, which can be computed by each user U_i using B_j and his personal secret $\mathcal{S}_i$.

2.2 Security Model

Now we briefly introduce the security model of Wang *et al.*'s scheme.

Definition 1 *(self-healing key distribution with mt-revocation capability.) A key distribution scheme has self-healing property and mt-revocation capability if*

(1) For a user $U_i \in G_j$, K_j is determined by S_i and B_j,

(2) Either S_i or B_j alone can not obtain any information about K_j,

(3) mt-revocation capability: given any $R_j \subseteq U$, $|R_j| \leq jt, j \in \{1, 2, \cdots, m\}$, and given a broadcast message B_j which is generated by the GM, for all $U_i \notin R_j$, U_i can recover K_j while revoked users cannot.

(4) Self-healing property: For j and $1 \leq j_1 \leq j \leq j_2 \leq m$, a user U_i, who is a member in session j_1 and j_2, can recover the key K_j from broadcast messages B_{j_1} and B_{j_2}.

Definition 2 *(mt-wise forward secrecy). The scheme achieves mt-wise forward secrecy if:*
Even if any subset of revoked users in R_j collude and learn about session keys before session j, they cannot obtain any information about K_j.

Definition 3 *(any-wise backward secrecy). The scheme achieves any-wise backward secrecy if*
Let D_j denote users who join the communication group after session j, where $D_j = \{D^{j+1}, D^{j+2}, \cdots, D^m\} \subseteq U$, and $D^{j'} (j+1 \leq j' \leq m)$ is users joining the group in session j'. Even if users in D_j collude and learn about session keys after session j, they cannot obtain any information K_j.

Definition 4 *(resistance to mt-wise collusion attack). The scheme is resistant to mt-wise collusion attack if*

Given any two disjoint R_{j_1} and D_{j_2}, users in R_{j_1} colluding with users in D_{j_2} cannot recover $K_j (j_1 \leq j \leq j_2)$ even with the knowledge of $\{B_1, B_2, \cdots, B_m, \{S_i | U_i \in R_{j_1}\}\} \bigcup \{B_1, B_2, \cdots, B_m, \{S_i | U_i \in R_{j_2}\}\}$.

2.3 Wang *et al.*'s Self-Healing Group Key Distribution Scheme

Wang *et al.*'s self-healing group key distribution scheme includes five parts: Setup, Broadcast, Session Key Recovery, Group Member Revocation and Group Member Addition.

- **Setup**

  The GM firstly chooses a t-degree polynomial $\mathbf{S}(\mathbf{x}) = a_0 + a_1 x + \cdots + a_t x^t \in F_q[x]$ at random. Then the GM randomly chooses $\{\varepsilon_i | i = 1, 2, \cdots, m\}$ from F_q independently and uniformly. After that, the GM selects a private and unique secret s_i ($s_i \in F_q$) for each user U_i, $U_i \in G_1$, where G_1 denotes the group members. User U_i receives its personal key $\mathcal{S}_i = \{s_i, \varepsilon_1 \cdot S(s_i)\}$ from the GM through a secure channel between them.

- **Broadcast**

  - For any $1 \leq j \leq m$, let $G_j = \{G_j^1, G_j^2, \cdots, G_j^{j'}, \cdots, G_j^j\}$ be all of the legitimate members in session j. Let $R_j = \{R_j^1, R_j^2, \cdots, R_j^{j'}, \cdots, R_j^j\}$ be all of the revoked users before and in session j. $G_j^{j'} = R_j^{j'} = \varnothing$ if there are not users joining the group in j'-th session.
  - The GM selects $VID_j^{j'}$ and $s_{i'} \in F_q$ at random for each session and $A_j^{j'}(x)$. Note that $VID_j^{j'}$ is unique, and $s_{i'}$ are never used for users' private secret.

    The GM uses the user's private identity to construct the access polynomials $A_j^{j'}(x)$.

    If $|G_j^{j'}| \leq t - 1$,

    $$A_j^{j'}(x) = (x - VID_j^{j'}) \Pi_{i=1}^{|G_j^{j'}|} (x - s_i) \Pi_{i=1}^{t-1-|G_j^{j'}|} (x - s_{i'}), j' = 1, 2, \cdots, j,$$

    Otherwise

    $$A_j^{j'}(x) = (x - VID_j^{j'}) \Pi_{i=1}^{|G_j^{j'}|} (x - s_i), j' = 1, 2, \cdots, j.$$

    It is clear to see that for an active user $U_i \in G_j^{j'}$, $A_j^{j'}(s_i) = 0$. Otherwise, for a non-active user $U_i \notin G_j^{j'}$, $A_j^{j'}(s_i)$ is a random value.
  - The GM randomly chooses a value $k_j^1 \in F_q$ and a one-way hash function $H(\cdot)$. Note that $H^i(\cdot)$ denotes applying i times hash operation. Then GM constructs the j-th key chain for session j: $\{k_j^1, k_j^2, \cdots, k_j^j\}$, where

    $$\begin{aligned} k_j^2 &= H(k_j^1), \\ k_j^3 &= H(k_j^2) = H(H(k_j^1)) = H^2(k_j^1), \\ &\cdots, \\ k_j^j &= H(k_j^{j-1}) = H(H(k_j^{j-2})) = \cdots = H^{j-1}(k_j^1), \end{aligned}$$

    For security, $k_j^1 (1 \leq j \leq m)$ is different from each other.

– The GM randomly chooses a session key K_j from F_q and broadcasts the message

$$B_j = \{P_j^{j'}(x)\}_{j'=1,2,\cdots,j} \cup \{E_{k_j^1}(K_1), E_{k_j^2}(K_2), \cdots, E_{k_j^j}(K_j)\}$$

where $P_j^{j'}(x) = A_j^{j'}(x) + k_j^{j'} + \varepsilon_{j'} \cdot S(x), j' = 1, 2, \cdots, j$ and $E_k(\cdot)$ is a symmetric encryption function.

- **Session Key Recover**

  An active user $U_i \in G_j^{j'}$ can recover the j-th session key when he receives the broadcast message B_j as follows.

  – For a legitimate user, $A_j^{j'}(s_i) = 0$. Therefore U_i compute $k_j^{j'}$ as $k_j^{j'} = P_j^{j'}(s_i) - \varepsilon_{j'} \cdot S(s_i), j' = 1, 2, \cdots, j$.

  For a user $U_i \notin G_j^{j'}$, $A_j^{j'}(s_i)$ is a random value, thus U_i can only get a random value which is different from $k_j^{j'}$.

  – U_i uses the hash function $H(\cdot)$ to compute all $\{k_j^{j''}\}$ for $j' \leq j'' \leq j$ in the j-th key chain.

  – U_i recovers the session keys $\{K_{j''}\}(j' \leq j'' \leq j)$ by decrypting $E_{k_j^{j''}}(K_{j''})$ $(j' \leq j'' \leq j)$ with corresponding keys $\{k_j^{j''}\}(j' \leq j'' \leq j)$.

- **Group Member Revocation**

  If a user U_i who joins the group in session j', is revoked in session j, the GM excludes $(x - s_i)$ from $A_j^{j'}(x)$ and starts a new session.

- **Group Member Addition**

  If, a user U_i joins the group in session $j-1$, the group member chooses a unique identity $s_i \in F_q$ and sends him a personal key $\mathcal{S}_i = \{s_i, \varepsilon_j \cdot S(s_i)\}$ securely. Then the GM reconstructs a access polynomial $A_j^j(x)$ including $(x - s_i)$. For keeping backward secrecy, the GM starts a new session.

3 Attack to Wang *et al.*'s Scheme

We now show how to attack Wang *et al.*'s scheme, and explain why Wang *et al.*'s scheme can not keep the forward security and can not resist to collusion attack.

Let $G_{j_1}^{j'}$ denote users who are legitimate in session j_1 and join the group in session j', where $j' < j_1$, and $G_{j_2}^{j'}$ denote the users who are legitimate in session j_2 and join the group in session j', where $j' < j_1 < j_2$. Suppose that $U_i \in G_{j_1}^{j'}$, $U_r \in G_{j_2}^{j'}$, and U_i is revoked in session j_2. Now we are ready to show how U_i, who is revoked in session j_2, computes the session key K_{j_2} step by step, which breaks the forward security of Wang *et al.*'s scheme.

(1) U_i computes $k_{j'}^{j'}$ and $k_{j_1}^{j'}$ with his personal key $\mathcal{S}_i$ and the broadcast messages $P_{j'}^{j'}(x)$ and $P_{j_1}^{j'}(x)$.

(2) In session j' and j_1, U_i receives the broadcast messages $P_{j'}^{j'}(x)$ and $P_{j_1}^{j'}(x)$.

Since

$$P_{j'}^{j'}(x) = A_{j'}^{j'}(x) + k_{j'}^{j'} + \varepsilon_{j'} \cdot S(x), \tag{1}$$

and

$$P_{j_1}^{j'}(x) = A_{j_1}^{j'}(x) + k_{j_1}^{j'} + \varepsilon_{j'} \cdot S(x). \tag{2}$$

Let (1)-(2), and with the values of $k_{j'}^{j'}$ and $k_{j_1}^{j'}$ which are computed from step (1), U_i can obtain

$$A_{j'}^{j'}(x) - A_{j_1}^{j'}(x) = P_{j'}^{j'}(x) - P_{j_1}^{j'}(x) - (k_{j'}^{j'} - k_{j_1}^{j'}).$$

(3) Note that

$$A_{j'}^{j'}(x) = (x - VID_{j'}^{j'})\Pi_{i=1}^{|G_{j'}^{j'}|}(x - s_i)\Pi_{i'=1}^{t-1-|G_{j'}^{j'}|}(x - (s_{i'})_{j'}^{j'}),$$

and

$$A_{j_1}^{j'}(x) = (x - VID_{j_1}^{j'})\Pi_{i=1}^{|G_{j_1}^{j'}|}(x - s_i)\Pi_{i'=1}^{t-1-|G_{j_1}^{j'}|}(x - (s_{i'})_{j_1}^{j'}).$$

where $VID_{j'}^{j'}$ and $(s_{i'})_{j'}^{j'}$ are different from $VID_{j_1}^{j'}$ and $(s_{i'})_{j_1}^{j'}$, respectively, for each session. U_i can factorize

$$A_{j'}^{j'}(x) - A_{j_1}^{j'}(x) = \Pi_{i=1}^{|G_{j_1}^{j'}|}(x - s_i) \cdot R(x),$$

where

$$R(x) = (x - VID_{j'}^{j'})\Pi_{i \in G_{j'}^{j'} - G_{j_1}^{j'}}(x - s_i)\Pi_{i'=1}^{t-1-|G_{j'}^{j'}|}(x - (s_{i'})_{j'}^{j'}) - (x - VID_{j_1}^{j'})\Pi_{i'=1}^{t-1-|G_{j_1}^{j'}|}(x - (s_{i'})_{j_1}^{j'}).$$

Therefore U_i can recover other legitimate users' private identities who join the group in session j' and are still legitimate in session j_1.

(4) Let $P_{j'}^{j'}(x)$ and $P_{j_2}^{j'}(x)$ denote the broadcast messages in session j' and j_2, respectively, where

$$P_{j'}^{j'}(x) = A_{j'}^{j'}(x) + k_{j'}^{j'} + \varepsilon_{j'} \cdot S(x), \tag{3}$$

and

$$P_{j_2}^{j'}(x) = A_{j_2}^{j'}(x) + k_{j_2}^{j'} + \varepsilon_{j'} \cdot S(x). \tag{4}$$

Let (3)-(4), user u_i can obtain

$$k_{j_2}^{j'} = A_{j'}^{j'}(x) - A_{j_2}^{j'}(x) - P_{j'}^{j'}(x) + P_{j_2}^{j'}(x) + k_{j'}^{j'}.$$

Suppose U_r is a legitimate user in session j_2 who joins the group in session j' and is legitimate in session j_1. U_i can obtain U_r's private identity s_r in step (3). Thus U_i is able to compute $P_{j'}^{j'}(s_r)$ and $P_{j_2}^{j'}(s_r)$ using u_r's private identity s_r. U_i can also compute $k_{j'}^{j'}$ since he is legitimate in session j'. In addition, U_r is a legitimate user in session j' and session j_2, hence $A_{j'}^{j'}(s_r) = 0$ and $A_{j_2}^{j'}(s_r) = 0$. Therefore, U_i computes $k_{j_2}^{j'}$ as

$$\begin{aligned} k_{j_2}^{j'} &= A_{j'}^{j'}(s_r) - A_{j_2}^{j'}(s_r) - P_{j'}^{j'}(s_r) + P_{j_2}^{j'}(s_r) + k_{j'}^{j'} \\ &= P_{j_2}^{j'}(s_r) - P_{j'}^{j'}(s_r) + k_{j'}^{j'} \end{aligned}$$

(5) U_i computes all hash chain value $\{k_{j_2}^{j''}\}$ and recovers $\{K_{j''}\}$ by decrypting $E_{k_{j_2}^{j''}}(K_{j''})$ where $(j' \leq j'' \leq j_2)$. Note that K_{j_2} should be kept secret to U_i since he is revoked in session j_2.

Therefore the scheme cannot satisfy the forward security. When the revoked user U_i obtains the session key $\{K_{j_2}\}$, he of course can give this session key to users who join the group after session j_2 and should not know $\{K_{j_2}\}$. Hence, the scheme can not resist collusion attack.

4 Conclusion

In this paper, we mounted an attack on Wang *et al.*'s self-healing group key distribution scheme, which allows a revoked user to obtain the legitimate group user' identities which should be kept secret from him. Using a legitimate group user' secret identities, the revoked user furthermore can recover a session key which should be kept secret from him since he is already revoked from the group. Therefore, Wang *et al.*'s is insecure since it cannot keep the forward security and has not collusion resistance capability.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 61300172), the Research Fund for the Doctoral Program of Higher Education (No. 20121102120017) and the Fund of the State Key Laboratory of Software Development Environment (No. SKLSDE-2014ZX-14).

References

[1] Staddon, Jessica, et al. "Self-healing key distribution with revocation." Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on IEEE, 2002:241 - 257.

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

[3] Blundo, Carlo, et al. "Design of Self-Healing Key Distribution Schemes." Designs Codes and Cryptography 32.13(2004):15-44.

[4] Blundo, C., P. D'Arco, and A. De Santis. "On Self-Healing Key Distribution Schemes." Information Theory IEEE Transactions on 52.12(2006):5455 - 5467.

[5] Liu, Donggang, P. Ning, and K. Sun. "Efficient Self-Healing Group Key Distribution with Revocation Capability." In Proc. of the 10th ACM Conference on Computer and Communications Security (CCS 03 (2003):231–240.

[6] More, S., et al. "Sliding-window self-healing key distribution, in." Proc. of ACM workshop on Survivable and self-regenerative systems, 2003 (2003).

[7] Hong, Do Won, and J. S. Kang. "An efficient key distribution scheme with self-healing property." Communications Letters IEEE 9.8(2005):759 - 761.

[8] Han, Song, et al. "Efficient threshold self-healing key distribution with sponsorization for infrastructureless wireless networks." IEEE Transactions on Wireless Communications 8.4(2009):1876 - 1887.

[9] Dutta, R., Y. D. Wu, and S. Mukhopadhyay. "Constant Storage Self-Healing Key Distribution with Revocation in Wireless Sensor Network." Communications, 2007. ICC '07. IEEE International Conference on IEEE, 2007:1323 - 1328.

[10] Dutta, R., and S. Mukhopadhyay. "Improved Self-Healing Key Distribution With Revocation In Wireless Sensor Network." Wireless Communications and Networking Conference .wcnc .ieee (2007):2963 - 2968.

[11] Ratna Dutta and Sourav Mukhopadhyay. "Designing Scalable Self-Healing Key Distribution Schemes With Revocation Capability." Parallel and Distributed Processing and Applications (2007):419-430.

[12] Wang, Qiuhua, et al. "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.

[13] Chen, H. "Improved One-Way Hash Chain and Revocation Polynomial-Based Self-Healing Group Key Distribution Schemes in Resource-Constrained Wireless Networks." Sensors 14.12(2014):24358-80.

[14] Zou, Xukai, and Y. S. Dai. "A Robust and Stateless Self-Healing Group Key Management Scheme." International Conference on Communication Technology (2006):1 - 4.

[15] Tian, Biming, S. Han, and T. S. Dillon. "An Efficient Self-Healing Key Distribution Scheme." New Technologies, Mobility and Security, 2008. NTMS '08. IEEE, 2008:1 - 5.

[16] Xu, Qingyu, and M. He. "Improved Constant Storage Self-healing Key Distribution with Revocation in Wireless Sensor Network." Lecture Notes in Computer Science (2009):41-55.

[17] Dutta, Ratna, S. Mukhopadhyay, and T. Dowling. "Enhanced Access Polynomial Based Self-healing Key Distribution.." Lecture Notes of the Institute for Computer Sciences Social Informatics and Telecommunications Engineering (2009):13-24.

[18] Wang, Qiuhua, et al. "Access-polynomial-based self-healing group key distribution scheme for resource-constrained wireless networks." Security and Communication Networks 5.12(2012):1363-1374(12).