# An Efficient Self-Healing Key Distribution Scheme

Biming Tian, Song Han, and Tharam S. Dillon
DEBI Institute, Curtin University of Technology, Australia
Email: Biming.Tian@cbs.curtin.edu.au

***Abstract*—Self-healing key distribution schemes enable a group user to recover session keys from two broadcast messages it received before and after those sessions, even if broadcast messages for middle sessions are lost due to network failure. These schemes are quite suitable for supporting secure communication over unreliable networks such as sensor networks and ad hoc networks. An efficient self-healing key distribution scheme is proposed in this paper. The scheme based on the concept of access polynomial and self-healing key distribution model constructed by Hong et al. The new scheme reduces communication overhead and computation overhead greatly yet still keeps the constant storage overhead. In addition, we consider the possibility of mutual-healing between neighbor users in wireless networks.**

## I. INTRODUCTION

Self-healing key distribution schemes realize an attractive property: even if during certain sessions some broadcast messages get lost, users are still capable of recovering the session keys simply by using one of broadcast message they have received during previous sessions and one of broadcast messages they will receive in subsequent sessions, without requesting additional transmissions from the group manager. The mechanism enables a large and dynamic group of users to establish session keys for secure communications over an unreliable channel in the manner that is resistant to packet loss and collusion attacks.

Self-healing key distribution scheme appears to be quite useful in several settings where session key is used for a short time-period, due to frequent changes in the group structure. Military-oriented applications as well as Internet application, such as broadcast transmissions and pay-per-view TV, are important examples which can benefit from such approaches. In addition, the self-healing mechanism is quite useful in commercial content distribution applications or electronic services in which communication contents are highly sensitive.

In this paper, we propose an efficient self-healing key distribution scheme for secure group communication in wireless sensor networks. The scheme based on the notion of access polynomial which is introduced in [1] and the security model developed by Hong et al. in [2]. We point out the incorrectness of efficiency analysis in [1]. We show that our scheme reduces communication and computation overheads greatly without weakening the advantage in the storage overhead. In addition, we discuss the possibility of mutual-healing between neighbor users in wireless communications.

The rest of the paper is organized as follows: in Section II, we present an overview of earlier works in the area of self-healing key distribution. In Section III, we introduce concrete construction. In Section IV, we prove the security and analyze the efficiency of the proposed scheme. In Section V, we discuss the possibility of mutual-healing between neighbor users in wireless communications. We conclude the paper in the last section.

## II. RELATED WORKS

The first pioneering work of self-healing key distribution was introduced by Staddon et al. in [3]. Formal definitions, lower bounds on the resources as well as some constructions of self-healing key distribution scheme were proposed in it.

Liu et al. generalized the definitions in [3] and gave some constructions in [4]. The schemes reduced communication overhead and storage overheads by introducing a novel personal key distribution technique. In addition, two techniques that allow trade-off between the broadcast length and the recoverability of lost session keys were proposed. The two methods further reduced the length of broadcast message in situations where there are frequent but short-term disruptions of communication and where there are long-time but infrequent disruptions of communication, respectively.

Blundo et al. in [5] showed an attack that can be applied to the first construction in [3], presented a new mechanism for implementing the self-healing approach, extended the self-healing approach to key distribution, and proposed another key-recovery scheme which enables a user to recover all lost session keys (for sessions in which he belongs to the group) by using only the current broadcast message.

More et al. in [6] introduced sliding window to self-healing key distribution scheme. They addressed the three problems in [3]. The three problems were inconsistent robustness, high overhead and expensive maintenance costs.

Different from the revocation polynomial introduced in [4], Zou et al introduced the notion of access polynomial in [1]. The scheme overcame some shortcomings existing in previous schemes yet still possessed all the advantages of them.

The constructions in [1], [3], [4], [5], and [6] based on Shamir's secret sharing technique and are unconditionally secure.

By introducing an improved secret sharing scheme, Tian et al. proposed a self-healing key scheme with novel properties in [7]. Firstly, the scheme reduced storage overhead of personal key to a constant. Secondly, the scheme concealed the requirement of secure channel in setup phase. In addition, the long-lived scheme was much more efficient than those in [3] and [5]. However, the efficiency improvements are obtained by

978-2-9532443-0-4 

relaxing the security slightly. The scheme is a computationally secure scheme.

To sum up, Shamir's secret sharing is the most common technique used to realize self-healing key distribution. It is performs easily. However, the schemes suffer from high storage and computation overhead. In this paper, we propose an efficient self-healing key distribution scheme for secure group communications in wireless sensor networks. We use access polynomial to substitute common used revocation polynomial. The underlying model is similar to the one given in [2] which is optimized in terms of storage and communication overheads. Our scheme further reduces communication and computation overheads. Fortunately, the storage overhead in our scheme is still a constant.

## III. CONCRETE CONSTRUCTION

Let $U = \{U_1, \ldots, U_n\}$ be the finite universe of users. A broadcast unreliable channel is available, and time is defined by a global clock. The group manager sets up and manages, by means of joining and revoking operations, a communication group which is a dynamic subset of users of $U$. All of our operations take place in $F_q$, where $q$ is a large prime. $m$ denotes the number of sessions and $t$ denotes the degree of personal key polynomial. Let $G_j \subseteq U$ be the communication group established by the group manager in session $j$. Each user $U_i \in G_j$ holds a personal key $S_i$, which is used to recover the session keys as long as $U_i$ is not removed by the group manager from the group. Let $R_j \subseteq G_{j-1}$ denote the set of revoked group users in session $j$ and $J_j \subset U \setminus G_{j-1}$ denote the set of users who join the group in session $j$ with $R_j \cap J_j = \phi$. Hence, $G_j = (G_{j-1} \cup J_j) \setminus R_j$ for $j \geq 2$ and by definition $G_1 = U$. Moreover, for $j \in \{1, \ldots, m\}$, the session keys $K_j (j = 1, \ldots, m)$ are randomly chosen by the group manager and according to uniform distribution. For each non-revoked user $U_i \in G_j$, the $j$-th session key $K_j$ is determined by broadcast information $B_j$ and personal key $S_i$.

The self-healing key distribution scheme is composed of several procedures. We will introduce them one by one.

*1) Setup:* The group manager randomly chooses a $t$ degree polynomial $S(x)$ from $F_q[x]$ and keeps it secret. Furthermore, it chooses a private unique identity $ID_i \in F_q$ and computes $S(ID_i)$ for each user $U_i$. The tuple $(ID_i, S(ID_i))$ as personal key $S_i$ is transferred to user $U_i$ by the group manager over a secure channel. The group manager chooses $m$ session keys $K_1, \cdots, K_m$ from $F_q$. The session keys are independent to each other and according to uniform distribution.

*2) Broadcast:* For any session $1 \leq j \leq m$, the group manager constructs the access polynomial

$$A_j(x) = (x - VID) \prod_{i=1}^{|G_j|} (x - ID_i) + 1$$

using private identities of users in session group $G_j$. $VID$ is a virtual identity which is randomly chosen by the group manager for each session and different from all users' private identities. $|G_j|$ denotes the number of users in session $j$. Then, the group manager computes

$$P_j(x) = A_j(x) \cdot K_j + S(x)$$

for session $j$. The broadcast message $B_j$ for session $j$ is in the following form:

$$B_j = \{P_1(x), \ldots, P_j(x)\}.$$

*3) Key Recovery:* When a user $U_i \in G_j$ receives the broadcast message $B_j$, it computes $P_j(ID_i)$. Note that $A_j(ID_i) = 1$ for any user $U_i \in G_j$. $U_i$ recovers the session key for session $j$:

$$K_j = P_j(ID_i) - S(ID_i).$$

One should note that $U_i$ can recover the session key if and only if he belongs to the $G_j$. For any user $U_l \notin G_j$, $A_j(ID_l)$ is a value other than 1. $U_l$ gets a value

$$K_j^{'} = \frac{P_j(ID_l) - S(ID_l)}{A_j(ID_l)},$$

which is different from the session key $K_j$.

*4) Self-healing:* Without loss of generality, suppose $U_i$ missed a broadcast message for session $r < j$. As far as it belongs to the session group $G_r$, it picks up the polynomial $P_r(x)$ from broadcast message $B_j$, then computes

$$K_r = P_r(ID_i) - S(ID_i).$$

If more than one broadcast messages get lost, the operation of self-healing is the same as aforementioned.

*5) Add and Revoke user:* If a new user $U_{new}$ applies for joining the session $j$, the group manager checks its legitimacy firstly. If $U_{new}$ is entitled to the session $j$, the group manager chooses a secret and unique identity $ID_{new}$ and computes personal key $S(ID_{new}))$, then the group manager sends personal key $S_i = (ID_{new}, S(ID_{new}))$ to $U_{new}$ over the secure channel between them. In the procedure of broadcast, the group manager constructs new $A_j(x)$ which should include $(x - ID_{new})$.

If a user $U_{rov}$ is revoked in session $j$, what the group manager should do is excludes $(x - ID_{rov})$ from $A_j(x)$ when it constructs the polynomial $A_j(x)$ in the procedure of *Broadcast*. The group manager makes sure that $U_i$ cannot get the session key $K_j$ by using the broadcast $B_j$ and it private personal key $S_i$. Because of the special construction of access polynomial $A_j(x)$, for any user $U_{rov}$ who is revoked from $G_j$, $A_j(ID_{rov})$ is a value other than 1. If $U_{rov}$ performs the operation of key recovery, it gets a value $K_j^{'} = \frac{P_j(ID_{rov}) - S(ID_{rov})}{A_j(ID_{rov})}$ which is different from the session key $K_j$. For a coalition of less than $t+1$ revoked users, they can collect at most $t$ points on $S(x)$. $S(x)$ is a $t$-degree polynomial so they cannot recover it from $t$ or less point on it. Even they get the unique identity of an authorized user, they cannot recover any personal keys of authorized users. Thus, $K_j$ is completely safe.

The operations of adding and revoking are very efficient in our scheme due to the application of access polynomial. For the condition that more than one user joining or revoking, the operations are the same as aforementioned.

## IV. PERFORMANCE ANALYSIS

In this section, we first prove the security and then analyze the efficiency of the proposed scheme.

### A. Security Analysis

In this section we show that our construction realizes a self-healing key distribution scheme with revocation capability. More precisely, we can prove the following theorem according to the security model in [2].

*Theorem 1.* The construction is a self-healing key distribution scheme with $t$-revocation capability.

*Proof:* (Sketch)

1) The scheme is a session key distribution scheme:
   (a) As described in the procedure of *Key Recovery*, an authorized user can recover session key from the broadcast message by using its personal key.
   (b) On the one hand, since session keys are chosen according to the uniform distribution and independent to the personal keys, it is straightforward to see that the personal keys alone do not give any information about session keys. On the other hand, it is not difficult to see that each $P_j(j = 1, \ldots, m)$ perfectly hides keys $K_j$ by means of $A_j(x)$ and $S(x)$ since $P_j = A_j(x) \cdot K_j + S(x)$. The set of session keys can not be determined by broadcast messages alone.
2) The scheme has $t$-revocation capability:
   Suppose that a coalition $R$ of $t$ revoked group users collude in session $j$. The coalition of $R$ can collect at most $t$ points on $S(x)$. They cannot recover personal key $S(x)$. In addition, the unique identity is kept secret. For the collusion user $R$ cannot construct access polynomial $A_j(x)$. For any guess of user unique identity they can construct a different polynomial $A_j(x)$. Thus, $K_j$ is completely safe.
3) The scheme has self-healing capability:
   (a) For any $U_i$ who is a user in session $r$ and $s$ ($1 \leq r < s \leq m$), the results $A_j(ID_i) = 1(j = r, \ldots, s)$ hold. $U_i$ has personal key $S(ID_i)$. By the method introduced in the procedure of *Key Computation*, $U_i$ can subsequently recover the whole sequences of session keys $K_r, \ldots, K_s$. In fact, in our construction, a qualified user can recover the all the session keys before the session $s$. This is a stronger self-healing scheme.
   (b) Suppose $C \subseteq R_r \cup \ldots \cup R_1$ be a colation of users removed before session $r$ and let $D \subseteq J_s \cup \ldots \cup J_m$ be a colation of users who joins the group from session $s$ and satisfies $C \cup D \leq t$. Because the coalition of $C \cup D$ can collect at most $t$ points on $S_(x)$(for any $r < j \leq s$). Hence, session keys $K_j$ are completely safe with respect to joint coalition of size at most $t$ of new and revoked users.

■

### B. Efficiency Analysis

We take advantage of access polynomial which was introduced by Zou et al. in [1] to design self-healing key distribution scheme. Our scheme reduces communication and computation overheads greatly meanwhile constant storage overhead is kept. Table 1 in [1] shows quantitative comparison of different self-healing schemes in terms of storage, communication and computation overheads. The advantages of [1] can be seen easily from the table. We point out that the communication overhead in [1] comes from broadcast $B_j$ which is composed by $2m$ polynomial. As far as the polynomial $P_j(x)$ is concerned, $P_j(x) = A_j(x) \cdot S_j(x) + H(x)$. Both $S_j(x)$ and $H(x)$ are $t$ degree polynomials, and the degree of $A_j(x)$ amounts to $(|G_j| + 1)$. Generally speaking, $|G_j|$ was larger than $t$. Therefore, the claim that communication overhead is $O(mt)$ is incorrect. A performance comparison between our scheme and the scheme [1] and [2] is showed in table I.

TABLE I
PERFORMANCE COMPARISON

| Schemes | User storage | Communication | Computation |
|---|---|---|---|
| Hong | $(m-j+1)logq$ | $(tj+j+t)logq$ | $(3t+1)logq$ |
| Zou | $2logq$ | $(t+\|G_j\|+3)logq$ | $(t+\|G_j\|+1)logq$ |
| New one | $2logq$ | $(\|G_j\|+2)logq$ | $(\|G_j\|+1)logq$ |

Although the proposed scheme reduces the communication overhead greatly, the communication overhead increases with the number of users in a group. It is meaningful to explore new way to further reduce the communication overhead due to limited communication capability of wireless nodes.

## V. THE POSSIBILITY OF MUTUAL-HEALING

We consider the possibility of mutual-healing between neighbor users in wireless networks. It is meaningful to detect counterpart measures. In this section, we just discuss the notions of it without exploring technical details.

More et al. in [6] pointed out that the protocol in [3] suffered from inconsistent robustness. Subsequently, they used a sliding window to make error recovery consistently robust: after an initial *Setup* procedure, any lost key can be recovered as long as two sufficiently close broadcast messages–one before it and one after it–are received. Similar technique was taken in [1]. The minimum size of the window can be dynamic adjusted according to network condition. Both [6] and [1] guaranteed that user can recover window size session keys for previous sessions if it receive a broadcast message. However, the problem of how to recover the session key if the last broadcast message gets lost has never been taken into consideration. In addition, some applications, such as live and pay-per-view TV, have strictly requirement of freshness. They would better lost only a limit number of broadcast messages.

It is virtually impossible to make users completely self-healing. We considerate the idea of mutual-healing, which was also discussed in [8]. That is, if a user has missed more than a fixed number broadcast message or the last broadcast message, it can get assistance from its neighboring nodes. The users in the same session group cooperate with each other forwarding broadcast messages which its neighbor users missed. Thus robust performance is achieved.

Bohio et al. in [8] claimed that there are two requirements for multi-healing: the authentication on requesting user and the authentication on requested session key. If a user does not receive the broadcast message from the group manager, it will contact its neighboring user to get the missed session key. The neighboring node needs to perform authenticate operation. They suggested using an identity-based pair-wise shared secret proposed in [9], as which requires less communication and is non-interactive if identities are public.

As messages are broadcasted in the form of plain-text, anyone can receive them. We argue that the authentication of requested session key is needless. Instead, user only needs to forward the broadcast message corresponding to the requested session key. If the requesting user is entitled for the session, it will be able to recover the session key, otherwise not. Nevertheless, in order to avoid attacks on their limited resource, effective countermeasures must be developed.

## VI. CONCLUSION

We proposed an efficient self-healing key distribution scheme for secure group communications in wireless sensor networks. The scheme was based on the notion of access polynomial introduced in [1] and self-healing key distribution model developed in [2]. We analyzed the performance of the scheme proposed in [1] and [2]. We pointed out the incorrectness in the analysis of communication overheads in [1] and showed that communication and computation overheads in our scheme reduces to the half of the ones in [1] without weakening the advantage in storage overhead.

## REFERENCES


[1] X. Zou and Y. Dai, *A Robust and Stateless Self-Healing Group Key Management Scheme*, Communication Technology, 2006. ICCT '06. International Conference on, pp.1-4, Nov 2006.

[2] D. Hong and J. S. Kang, *An Efficient Key Distribution Scheme with Self-healing Property*, IEEE Communication Letters, Vol.9, No.8, August, 2005.

[3] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin and D. Dean, *Self-healing Key Distribution with Revocation*, proceedings of IEEE Symposium on Security and Privacy, pp. 224-240, 2002.

[4] D. Liu, P. Ning and K. Sun, *Efficient Self-healing Group Key Distribution with Revocation Capability*, Proceeding of the 10th ACM CCS, 2003.

[5] C. Blundo, P. D'Arco, A. Santis and M. Listo, *Design of Self-healing Key Distribution Schemes*, Design Codes and Cryptography, No.32, pp.15-44, 2004.

[6] S. M. More, M. Malkin, J. Staddon and D. Balfanz, *Sliding Window Self-healing Key Distribution with Revocation*, ACM Workshop on Survivable and Self-Regenerative Systems, pp.82-90, 2003.

[7] B. Tian and M. He, *Self-Healing Key Distribution Scheme with Novel Properties*, International Journal of Network Security, Vol.7, No.2, pp.147-152, 2008.

[8] M. J. Bohio and A. Miri, *Self-Healing Group Key Distribution*, International Journal of Network Security, Vol.1, No 2, pp.110-117, 2005.

[9] B. Pinkas, *Efficient State Updates for Key Management*, Proceedings of the IEEE, Special Issue on Enabling Technologies for Digital Rights Management, Vol.92, No.6, pp. 910-917, 2004.