http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 8 (4): 619-624, 2009
ISSN 1812-5638

Anti-collusive Self-healing Key Distribution Scheme with Revocation Capability

ChunLai Du, MingZeng Hu, HongLi Zhang and WeiZhe Zhang
Research Center of Computer Network and Information Security Technology,
Harbin Institute of Technology, Harbin, 150001, People's Republic of China

Abstract: This study proposes an anti-collusive self-healing group key distribution scheme with revocation using dual directional hash chain. The session key is computed from three parts: forward key, backward key and random session number. The former two parts are built on dual directional hash chain. Users are provided with a set of private secrets according to their legal lifetimes. In terms of communication cost, the proposed scheme is more efficient than the previous schemes not based on one-way hash chain and is slightly increased compared with the previous scheme based on one-way hash chain. According to the security analysis results, the proposed scheme can resist the collusion of revoked users and newly joined users.

Key words: Group key, wireless network, group communication, dual directional hash chain, collusion

INTRODUCTION

Currently, wireless network has more applications in military operations, rescue missions, etc., where there are usually no network infrastructure supports and the adversaries may intercept, tamper even partially interrupt the communication. It is necessary to encrypt and authenticate the messages in the communication. Group key can be used to establish secure communication over an unreliable channel in wireless network.

In mobile wireless networks, users may move in or out of range frequently so that the topology of network dynamically changes with frequent membership changes. Therefore, group key must be re-keyed accordingly. When some legal users lost their keys due to network faults and then requested those keys from the group manager, not only the burden of the group manager was increased but also the wireless network traffic, as well. In order to make legal nodes recover their lost legal keys without asking the group manager, the research on self-healing key distribution started in 2002.

An important concept is session, which is a fixed interval of time. The group manager divides the total lifetime of group communication into certain number of sessions. Each session has a session key. At the beginning of group communication, the group manager sends personal secret information to each of initial group users. The group manager can add users to or remove users from the group at the beginning of each session. The central concept of self-healing key distribution is to broadcast some packets about key so that the legal users can recover their lost session keys due to network failure without requesting help from the group manager. It can decrease the work load on the group manager and reduce the network traffic. The self-healing key distribution scheme must guarantee that only legal users can recover their lost legal session keys but illegal users can not.

Our contributions in this study are as follows; first, we propose an efficient key distribution scheme with self-healing property and revocation capability for secure group communication in wireless network. Present scheme is based on dual directional hash chain so that it has significant improvement in terms of both communication and storage cost compared with those previous schemes which are not based on hash chains. Second, random numbers are used in the process of achieving the important factor for computing session keys. Therefore, our scheme can resist the collusion of revoked users and newly joined users, while the previous schemes based on hash chains can not totally overcome such flaw.

Self-healing key distribution with revocation was first introduced by Staddon *et al.* (2002). In terms of entropy theory, definitions and lower bounds on resources were provided. Liu *et al.* (2003) generalized the definition 2 in the scheme (Staddon *et al.*, 2002) and provided a more efficient construction. Blundo *et al.* (2004) showed an attack applied to the first construction in scheme (Staddon *et al.*, 2002) and presented a new scheme different from those methods (Liu *et al.*, 2003; Staddon *et al.*, 2002). In the scheme (Blundo *et al.*, 2004), a user can recover all the lost legal session keys simply by using the current broadcast messages. Hong and Kang

Corresponding Author: ChunLai Du, Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, Harbin City, 150001, China
Tel: +86-451-86419798 Fax: +86-451-86402573

(2005) changed the redundant mode of session key. All the above schemes are based on Shamir's secret sharing technique. Sáez (2005a, b) adopted vector space secret sharing instead of Shamir's secret sharing to realize the self-healing key distribution (Sáez, 2005a) and sponsorization (Sáez, 2005b). More *et al.* (2003) proposed a sliding-window self-healing key distribution scheme. Zou and Dai (2006) adopted a new revocation polynomial to make illegal users get wrong random values. Dutta and Mukhopadhyay (2007a, b) and Dutta *et al.* (2007b, 2008) did not divide session keys into two polynomials but concealed the session keys directly. Jiang *et al.* (2007) proposed a concept of dual directional hash chain. Other schemes (Dutta *et al.*, 2007a; Shi *et al.*, 2007) were also based on hash chain, which could reduce the communication cost and storage cost. However, these schemes (Dutta *et al.*, 2007a; Jiang *et al.*, 2007; Shi *et al.*, 2007) can not resist collusion between revoked users and newly joined users. In order to overcome this drawback, Tian *et al.* (2008) proposed a scheme based on vector space secret sharing and one-way hash chains. However, the scheme was invalid for resisting collusion of newly joined users and revoked users whose lifetimes did not expire. In this study, we devote to totally solve the collusion in self-healing key distribution schemes based on hash function.

PRELIMINARIES

The notations used in the study are defined below:

U	:	Set of all users in the networks
u_i	:	i-th user
GM	:	Group manager
n	:	Total number of users in networks
m	:	Total number of session
t	:	The maximum number of compromised users
F_q	:	A field of order q
S_i	:	Personal secret of user u_i
B_j	:	Broadcast message by the GM in session j
K_j	:	Session key generated by the GM in session j
FS	:	Forward key seed generated by the GM
BS	:	Backward key seed generated by the GM
FK_j	:	i-th forward key in the forward key chain
BK_j	:	i-th backward key in the backward key chain
R	:	Set of all revoked users
R_j	:	Set of revoked users in session j
J_j	:	Set of joined users in session j

A Dual Directional Hash Chain (DDHC) consists of two one-way hash chains with equal length, a Forward Hash Chain (FHC) and a Backward Hash Chain (BHC). First, GM generates two random key seeds, FS and BS, from finite field F_q. Then GM repeatedly applies the same one-way function H on each key seed to produce two hash chains of equal length m. So, the DDHC is denoted by $\{H(FS),\ldots, H^i(FS),\ldots, H^m(FS)\}$ and $\{H(BS),\ldots, H^i(BS),\ldots, H^m(BS)\}$ (Jiang *et al.*, 2007).

We state the following definitions (Dutta *et al.*, 2007a; Tian *et al.*, 2008) that are aimed to computational security for session key distribution, according to the security model in scheme (Liu *et al.*, 2003).

Definition 1: Let $t,i\in\{1,\ldots,n\}$ and $j\in\{1,\ldots,m\}$

- D is a session key distribution with privacy if.
  - For any user u_i, the session K_j is determined by B_j and S_i.
  - It is infeasible to compute session key K_j only from $\{B_1,\ldots, B_m\}$ or $\{S_1,.., S_n\}$.
- D has t-revocation capability if any user $u_i\in R$, where $|R|\leq t$, can't recover K_j from B_j and S_i.
- D is self-healing if any user $u_i\notin R$ who exists from session j_1 to session j_2 can recover $K_{,j}$ where $1\leq j_1<j<j_2\leq m$.

Definition 2: D guarantees t-wise forward secrecy and backward secrecy if:

- For any set R of users revoked before session j, where $|R|\leq t$, it is infeasible for the members in R together to get any information about K_j, even with the knowledge of keys $K_1,\ldots, K_{j-1}$ before session j.
- For the set J of new users joined after session j, where $|J|\leq t$, it is infeasible for the members in J together to get any information about K_j, even with the knowledge of keys $K_{j+1},\ldots, K_m$ after session j.

Definition 3: D resist collusion if for disjoint set B and C, where $B\subset R_v\cup\ldots\cup R_1$, $C\subset J_s\cup\ldots\cup J_m$ and $|B\cup C|\leq t$, it is infeasible for collusion $B\cup C$ to get any information about K_j, where $v<j<s$.

To sum up, definition 1 defines a self-healing key distribution scheme with revocation capability. Definition 2 defines both forward secrecy and backward secrecy. Definition 3 defines resisting collusion property.

PROPOSED SCHEME

The lifetime of group communication is divided into m sessions, where a session is a fixed interval of time. The scheme considers all of operations taking place in a finite field F_q, where q is a large prime number (q>m). The scheme never allows the revoked users to rejoin the group in later sessions. Let H: $F_q\rightarrow F_q$ be a cryptographically secure one-way hash function.

The self-healing key distribution scheme consists of five procedures, i.e., setup, broadcast, key recovery, adding new members and self-healing, which are defined as follows:

Setup: GM randomly picks two initial key seeds, FS and BS, from F_q. In the pre-processing time, it repeatedly applies the one-way function H on FS and BS to produce DDHC of equal length m. For $1 \le j \le m$, the j-th session key is computed by:

$$K_j = (H(FS)^j + H(BS)^{m-j+1})c_j$$

where c_j is a random number corresponding to session j.

For m sessions, GM chooses, independently and uniformly at random, m t-degree(t<m,n) polynomials $h_1(x), h_2(x), \ldots, h_m(x) \in F_q[x]$ and generates m random numbers $r_1, r_2, \ldots, r_m \in F_q$, respectively corresponding to $h_1(x), h_2(x), \ldots, h_m(x)$.

For $1 \le i \le m$, each user u_i whose lifetime is from session *l* to session v receives the private secrets corresponding to his legal sessions. The private secrets include set $S_i = \{h_l(u_i), h_{l+1}(u_i), \ldots, h_v(u_i)\}$, set $r = \{r_l, r_{l+1}, \ldots, r_v\}$, forward key seed $SFK_i = H(FS)^l$ and backward key seed $SBK_i = H(BS)^{m-v+1}$. GM and u_i communicate through secure channel.

Broadcast: Let R_j be the set of all users revoked in and before sessions j, where $|R_j| = z_j < t$. In the j-th session GM firstly produces random number c_j in the finite field F_q. Secondly, GM produces the revocation polynomial $A_j(x) = \prod_{i=1}^{z_j}(x-u_i)$, where $u \in R_j$ and the broadcast polynomial $W_j(x) = A_j(x)c_j + h_j(x)$, where the polynomial $h_j(x)$ plays the role of masking polynomial. Thirdly, GM produces the set $C_j = \{c_j r_1(c_1+c_2), c_j r_2(c_2+c_3), \ldots, c_j r_{j-2}(c_{j-2}+c_{j-1}), c_j r_{j-1} c_{j-1}\}$. Finally, GM broadcasts the message $B_j = \{W_j(x), C_j, R_j\}$.

Key recovery: When a non-revoked user u_i receives the j-th broadcast message B_j, u_i firstly evaluates $A(\mu)_i$ and subsequently recovers $c_j = (W_j(u_i) - h_j(u_i))/A_j(u_i)$. Secondly, u_i computes the j-th forward key $Fk_j = H(SFK)^{j-l}$ and backward key $BK_j = H(SBS)^{v-j}$. Finally, u_i computes the j-th session key $K_j = (FK_j + BK_j)c_j$.

Adding group member: When a new user u_i expects to join the group and to be active from session *l* to session v, u_i must get in touch with GM. The GM computes u_i's private secrets, i.e., set $S_i = \{h_l(u_i), h_{l+1}(u_i), \ldots, h_v(u_i)\}$, $SFK_i = H(FS)^l$ and $SBK_i = H(BS)^{m-v+1}$. Finally, the GM sends $\{S_i, r = \{r_l, r_{l+1}, \ldots, r_v\}, SFK_i, SBK_i\}$ to u_i via secure channel between GM and u_i.

Self-healing: Suppose user u_i whose lifetime is from session *l* to session v receives broadcast message B_{j1} in session j_1, but not message B_j for session j, where $1 \le l < j < j_1 \le v \le m$ user u_i can recovers the lost session key K_j as follows:

Firstly, u_i repeatedly applies the one-way function H on each of his two key seeds, SFK_i and SBK_i obtained in joining process, until u_i gets the forward key $Fk_j = H(SFK_i)^{j-l}$ and the backward key $Bk_j = H(SBK_i)^{v-j}$ for session j.

Secondly, for broadcast message $B_{j1} = \{W_{j1}(x), C_{j1}, R_{j1}\}$, user u_i computes c_{j1} from $W_{j1}(u_i)$ by his private secret $h_{j1}(u_i)$. By dividing each item of set C_{j1} by c_{j1}, user u_i obtains a new set $C_{j1}' = \{r_1(c_1+c_2), r_2(c_2+c_3), \ldots, r_{j1-2}(c_{j1-2}+c_{j1-1}), r_{j1-1}c_{j1-1}\}$.

Thirdly, user u_i has a private secret set $r' = \{r_l, \ldots, r_j, r_{j+1}, \ldots, r_{j1-1}, \ldots, r_v\}$. Therefore, By using the private secret set $r'' = \{r_j, r_{j+1}, \ldots, r_{j1-1}\}$, where $r'' \subset r'$, user u_i can compute c_j as follows:

- Dividing respectively each item of set $C_{j1}'' = \{r_j(c_j+c_{j+1}), \ldots, r_{j1-2}(c_{j1-2}+c_{j1-1}), r_{j1-1}c_{j1-1}\}$ by corresponding item of set r'', where set C_{j1}'' is a subset composed of the latter j1-j items in C_{j1}', u_i will work out the final set $C_{j1}''' = \{c_j+c_{j+1}, \ldots, c_{j1-3}+c_{j1-2}, c_{j1-2}+c_{j1-1}, c_{j1-1}\}$.
- u_i can work out c_j by a serial of subtraction operations in reverse order as follows: u_i can get c_{j1-2} by the subtraction operation of the last two items, i.e., $(c_{j1-2}+c_{j1-1})-c_{j1-1}$. Therefore, the resultant c_{j1-2} can be used to work with $c_{j1-3}+c_{j1-2}$ to get c_{j1-3} and so on. By this means, u_i finally works c_j out.

Finally, $K_j = (FK_j + BK_j)c_j$.

SECURITY ANALYSIS

Present study shows that proposed scheme realizes a self-healing key distribution with revocation capability and resisting collusion property. Now, we will prove that our scheme satisfies all the conditions required by definition 1, 2 and 3.

Theorem 1: The scheme is secure, self-healing key distribution scheme with t-revocation capability with respect to definition 1.

Proof 1: The scheme is a session key distribution with privacy.

- The process of computing session key K_j by a non-revoked user u_i via broadcast message B_j and his private secrets is described in the third step of proposed scheme.

- The session key K_j for session j is computed from three parts: forward key FK_j, backward key BK_j and random number c_j. A user who does not join the group does not compute the session key K_j due to lacking the information about FK_j and BK_j, even if the user has already gathered all broadcast messages. Similarly, because random number c_j has been concealed in broadcast messages, users holding all private secrets still can not compute K_j before computing c_j from broadcast messages. Therefore, it is infeasible to determine session key only from broadcast messages or personal private secrets.

Proof 2: The scheme has t-revocation capability.

Let $R = R_j \cup \ldots \cup R_1$ ($|R|<t$) be the set of revoked users in and before session j. For user $u_i \in R$, because the revocation polynomial $A_j(u_i)$ is always zero, user u_i can not compute c_j from broadcast polynomial $W(\mu)_i$ Therefore, coalition R must attack the masking polynomial $h_j(x)$ to get c_j. For the size of the coalition R is t at most, the colluding users only have at most t points on the masking polynomial $h_j(x)$. But the degree of the polynomial $h_j(x)$ is t. Hence coalition R can not recover $h_j(x)$. Because there is no information of c_j, it is infeasible for the coalition R to compute session key K_j.

Proof 3: The scheme has self-healing capability, as is described in the fifth step of proposed scheme.

Theorem 2: The scheme achieves t-wise forward security and backward security with respect to definition 2.

Proof 1: Let $R=R_j \cup \ldots \cup R_1$ ($|R|<t$) be a coalition of revoked users colluding in and before session j. In order to attack t-degree polynomial $h_j(x)$, coalition R needs at last t+1 points on $h_j(x)$. But the size of coalition R is t at most. Hence coalition R can not recover $h_j(x)$. Furthermore, because of the one-way property of BHC, it is computationally infeasible to compute $Bk_v = H(BS)^{m-v+1}$ from $Bk_j = H(BS)^{m-j+1}$ for $j<v$. Therefore, the scheme guarantees the t-wise forward security.

Proof 2: Let $J = J_j \cup \ldots \cup J_m$ ($|J|<t$) be a coalition of joined users colluding from session j. For session key K_{j1}, where $j_1<j$, coalition J requires at least t+1 points on polynomial $h_{j1}(x)$ to attack t-degree polynomial $h_j(x)$. However, the size of coalition J is t at most. Hence coalition J can not recover $h_j(x)$. Furthermore, because of the one-way property of FHC, it is computationally infeasible to compute $Fk_{j1} = H(FS)^{j1}$ from $Fk_j = H(FS)^j$. Therefore, the scheme guarantees the t-wise backward security.

Theorem 3: The scheme resists collusion of revoked users and newly joined users with respect to definition 3.

Proof: Let $B \subset R_v \cup \ldots \cup R_1$ be a set of users revoked from group before session v and let $D \subset J_s \cup \ldots \cup J_m$ be a set of users who joined the group from session s, where $v<s$. Set B and set D are disjointed. Set $L \subset B \cup D$, where $|B \cup D|<t$, is a coalition of users colluding to attempt to get the session key K_j for session j, where $v<j<s$. the coalition L can easily compute forward key FK_j and backward key BK_j for session j via the property of DDHC. Therefore, it is necessary for coalition L to get c_j. Because the size of coalition L is t at most, the coalition L can not have at least t+1 point on t-degree masking polynomial $h_j(x)$. Therefore, it is infeasible for the coalition L to get c_j by attacking masking polynomial $h_j(x)$. Furthermore, in order to get c_j, the coalition L can resort to working on i-th broadcast set C_i for session i, where $i>j$. However, without the knowledge of private secret set $\{r_{v+1}, r_{v+2}, \ldots, r_j, \ldots, r_{s-1}\}$ for session $r_{v+1}, r_{v+2}, \ldots, r_j, \ldots, r_{s-1}$, the coalition L can not get c_j from i-th broadcast set C_i. Therefore, it is infeasible for the coalition L to compute the session key K_j without the knowledge of random number c_j for session j. As a result, the scheme resists the collusion of revoked users and newly joined users.

PERFORMANCE ANALYSIS

In order to evaluate the performance of the proposed method, we will compare the communication complexity and storage cost between our scheme and the previous self-healing session key distribution schemes.

At the j-th session, the broadcast message B_j consists of t-degree broadcast polynomial $W_j(x)$, set C_j and revocation set R_j. The size of set C_j is j-1. The communication cost for the broadcast of revocation set R_j can be ignored because the identity of users can be selected from a small finite field (Hong and Kang, 2005). Therefore, the communication cost of our scheme is $O((t+j)\log q)$ for session j.

In the process of joining group, user u_i who is legal from session j to session v obtains his private secrets, i.e., set S_i, set r, forward key seed SFK_i and backward key seed SBK_i. The size of set S_i and the size of set r are both l-v+1. Therefore, the storage cost of user u_i is a constant, $O((2l-2v+4))\log q)$,corresponding to his lifetime from session l to session v.

We compare the communication complexity and storage cost of our scheme with the previous schemes not based on one-way hash chain. The results are listed in Table 1. The schemes (Dutta and Mukhopadhyay,

Table 1: Comparison between our scheme and previous schemes not based on one-way hash chain

Scheme	Communication complexity	Storage cost	Collusion resistance
Construction 3 (Staddon *et al*., 2002)	$(mt^2+2mt+m+t)\log q$	$(m-j+1)^2\log q$	Y
Scheme 3 (Liu *et al*., 2003)	$[(m+j+1)t+(m+1)]\log q$	$2(m-j+1)\log q$	Y
Scheme 2 (Blundo *et al*., 2004)	$(2tj+j)\log q$	$(m-j+1)\log q$	Y
Construction 1(Hong and Kang, 2005)	$(tj+j-t-1)\log q$	$(m-j+1)\log q$	Y
Scheme (Sáez, 2005a)	$[1+(t+1)(m-1-t/2)]\log q$	$(m-j+1)\log q$	Y
Scheme (Sáez, 2005b)	$[[t(m^2-m+2)]/2]\log q$	$t(m-j+1)\log q$	Y
Construction 1 (More *et al*., 2003)	$(t^2+tm)\log q$	$m\log q$	Y
Scheme (Zou and Dai, 2006)	$[2j(t+1)]\log q$	$2\log q$	Y
Scheme (Dutta and Mukhopadhyay, 2007a)	$(tj+j-t-1)\log q$	$(t+1)\log q$	N
Scheme (Dutta and Mukhopadhyay, 2007b)	$(t+j+1)\log q$	$(t+1)\log q$	N
Scheme (Dutta *et al*., 2007b)	$(t+j+1)\log q$	$3\log q$	N
Proposed scheme	$(t+j)\log q$	$(2l-2v+4))\log q$	Y

Table 2: Comparison between our scheme and previous schemes based on one-way hash chain

Scheme	Communication complexity	Storage cost	Revocation capability	Collusion resistance
Scheme (Jiang *et al*., 2007)	$1\log q$	$2\log q$	N	N
Scheme (Shi *et al*., 2007)	$1\log q$	$2\log q$	N	N
Scheme (Dutta *et al*., 2007a)	$(t+1)\log q$	$(m-j+1)\log q$	Y	N
Scheme (Tian *et al*., 2008)	$(2t+1)\log q$	$(2m+1)\log q$	Y	Partial
Proposed scheme	$(t+j)\log q$	$(2l-2v+4))\log q$	Y	Y

2007a, b; Dutta *et al*., 2007b) do not have the capability of resisting collusion. The communication complexity of our scheme is $O((t+j)\log q)$ while those of the other schemes are more than or equal to $O((t+j+1)\log q)$. Furthermore, the storage cost of a user in our scheme is $(2l-2v+4))\log q$ which corresponds to his lifetime. Although the two schemes (Zou and Dai, 2006; Dutta *et al*., 2007b) are more efficient than ours in terms of storage cost, proposed scheme is more efficient than theirs in terms of the communication complexity. According to the comparison results in Table 1, we conclude that our scheme is more efficient than the previous schemes not based on one-way hash chain.

We compare the communication complexity and storage cost of our scheme with previous schemes based on one-way hash chain. The results are shown in Table 2. Although the two schemes (Jiang *et al*., 2007; Shi *et al*., 2007) are better than our scheme in term of communication complexity and storage cost, the users in the schemes (Jiang *et al*., 2007; Shi *et al*., 2007) can not be revoked by GM and will exit only with their lifetimes expiring. Furthermore, these two schemes can not resist the collusion of newly users and detached users. Although the scheme (Dutta *et al*., 2007a) has the revocation capability, it can not resist the collusion of newly joined users and revoked users. The scheme (Tian *et al*., 2008) can resist the collusion of newly joined users and revoked users whose lifetimes have expired. However, the scheme (Tian *et al*., 2008) can not resist the collusion of newly joined user and revoked users whose lifetimes do not expire. From the comparison in Table 2, although the communication cost and storage cost of proposed scheme are slightly increased, only our scheme can resist collusion of newly joined user and revoked users no matter whether their lifetimes expire or not.

CONCLUSION

In this study, an anti-collusive self-healing group key distribution scheme with revocation is proposed. A user is provided with a set of legal private secrets according to his lifetime. Forward key and backward key are built on DDHC. The communication cost of the proposed scheme is more efficient than those of the previous schemes not based on one-way hash chain, while the communication cost is slightly increased compared with those of the previous schemes based on one-way hash chain. By adopting random number set r corresponding to sessions, our scheme overcomes the vital drawback in previous schemes based on one-way hash chains. In a word, our scheme can resist the collusion of revoked users and newly joined users. The proposed scheme is secure and will find more applications in unreliable wireless network.

ACKNOWLEDGMENTS

This study is supported by National High Technology Research and Development Program of China under Grant No. 2007AA01Z446 and National Natural Science Foundation of China under Grant No. 60703014. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers and editors, which have improved the presentation.

REFERENCES

Blundo, C., P. D'Arco, A. de Santis and M. Listo, 2004. Design of self-healing key distribution schemes. Des. Codes Cryptogr., 32: 15-44.

Dutta, R. and S. Mukhopadhyay, 2007a. Designing scalable self-healing key distribution schemes with revocation capability. Proceedings of 5th International Symposium on Parallel and Distributed Processing and Applications, Niagara Falls, Canada, Aug. 29-31, Springer Berlin/Heidelberg, pp: 419-430.

Dutta, R. and S. Mukhopadhyay, 2007b. Improved self-healing key distribution with revocation in wireless sensor network. Proceedings of IEEE Wireless Communications and Networking Conference, Kowloon, China, Mar. 11-15, IEEE Press, pp: 2963-2968.

Dutta, R., E.C. Chang and S. Mukhopadhyay, 2007a. Efficient self-healing key distribution with revocation for wireless sensor networks using one way key chains. Proceedings of 5th International Conference on Applied Cryptography and Network Security, Zhuhai, China, LNCS 4521, Jun. 5-8, Springer Berlin/Heidelberg, pp: 385-400.

Dutta, R., Y.D. Wu and S. Mukhopadhyay, 2007b. Constant storage self-healing key distribution with revocation in wireless sensor network. Proceedings of IEEE International Conference on Communications, Glasgow, Jun. 24-28, IEEE Press, Scotland, UK., pp: 1323-1328.

Dutta, R., S. Mukhopadhyay and S. Ennanuel, 2008. Low band with self-healing key distribution for broadcast encryption. Proceedings of 2nd Asia International Conference on Modeling and Simulation, May 13-15, IEEE CS Press, pp: 867-872.

Hong, D. and J.S. Kang, 2005. An efficient key distribution scheme with self-healing property. IEEE Commun. Lett., 9, 8: 759-761.

Jiang, Y.X., C. Lin, M.H. Shi and X.M. Shen, 2007. Self-healing group key distribution with time-limited node revocation for wireless sensor networks. Ad Hoc Netw., 5,1: 14-23.

Liu, D.G., P. Ning and K. Sun, 2003..Efficient self-healing group key distribution with revocation capability. Proceedings of the 10th ACM Conference on Computer and Communications Security, Oct. 27-31, ACM Press, Washington, DC. USA., pp: 231-240.

More, S.M., M. Malkin, J. Staddon and D. Balfanz, 2003. Sliding-window self-healing key distribution. Proceedings of the ACM Workshop on Survivable and Self-Regenerative Systems (In Association with 10th ACM Conference on Computer Communications Security). Fairfax, Oct. 31, ACM Press, VA, United States, pp: 82-90.

Sáez, G., 2005a. On threshold self-healing key distribution schemes. Proceedings of 10th IMA International Conference on Cryptography and Coding, Dec. 19-21, Springer Verlag, Cirencester, UK., pp: 340-354.

Sáez, G., 2005b. Self-healing key distribution schemes with sponsorization. Proceedings 9th IFIP TC-6 TC-11International Conference on Communications and Multimedia Security, Salzburg, Austria, Sept. 19-21, Springer Verlag, pp: 22-31.

Shi, M.H., X.M. Shen, Y.X. Jiang and C. Lin, 2007. Self-healing group-wise key distribution schemes with time-limited node revocation for wireless sensor networks. IEEE Wirel. Commun., 14,5: 38-46.

Staddon, J., S. Miner, M. Franklin, D. Balfanz, M. Malkin and D. Dean, 2002. Self-healing key distribution with revocation. Proceedings of the IEEE Symposium on Research in Security and Privacy, May 12-15, IEEE CS Press, pp: 241-257.

Tian, B., S. Han, T.S. Dillon and S. Das, 2008. A self-healing key distribution scheme based on vector space sharing and one way hash chains. Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks, Jun. 23-26, IEEE CS Press, USA., pp: 1-6.

Zou, X.K. and Y.S. Dai, 2006. A robust and stateless self-healing group key management scheme. Proceedings of International Conference on Communication Technology, Guilin, China, Nov. 27-30, IEEE Press, pp: 1-4.