International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Group Key Distribution with Self-healing Property for Unreliable and Communication-constrained Networks

Ting Yuan[1] **Jianqing Ma** **Yiping Zhong** **Shiyong Zhang**

School of Computer Science, Fudan University, Shanghai, 200433, China

Abstract: The most common solution for implementing access control into a dynamic group is to use a group key unknown to all but the users in the group. The group key (i.e., session key) is updated for every session throughout the lifetime of the group with the procedure of group key distribution. In this paper, we propose a group key distribution scheme with self-healing property that enables users in a dynamic group to establish session keys over an unreliable network with constrained bandwidth resources. To achieve this, our scheme also has the limited group membership property that there exists an upper bound on the number of users in the group. Through modeling and analysis, we show that our scheme has a better tradeoff between storage and communication overhead as compared to previous work. In addition, we propose a variant of the scheme which enables key recovery from a single broadcast message.

Keywords: wireless network; network security; key management; group key distribution; self-healing

1. Introduction

Secure group communication requires that all the members in the group share a common cryptographic key (i.e., the group key) distributed by the group manager. Many approaches of secure group communication (e.g., [1, 2, 3, 4, 5, 6, 7]) depend on a reliable channel to distribute keys – an issue which has received much attention thus far. When it comes to an unreliable setting (e.g., a wireless sensor network or WSN [8]), however, a message that contains the group key might never reach some or all of the group members. Requiring that each of such members communicate with the group manager for a retransmission of the lost message would pose a non-negligible burden on the network. In particular, when the group is large and dynamic (i.e., users may join or leave the group periodically), such retransmissions could paralyze the group manager and deplete the communication resources of the network, especially of the resource-constrained WSN. Furthermore, in a hostile environment, redundant messages like the above retransmissions would jeopardize the network with its exposure to adversarial attacks of traffic analysis.

To address secure group communication in unreliable networks, Staddon et al. [9] recently presented a new concept of group key distribution, called self-healing. The core idea of self-healing key distribution is that group members are capable of recovering session keys on their own, without requesting additional transmissions from the group manager. According to [9], for a lost key distribution broadcast which contains the current session key, a user can recover the lost key by combining information from any key distribution broadcast preceding the lost broadcast with information from any key distribution broadcast following it, as long as the user is a group member in the sessions corresponding to these three broadcasts. Since [9],

[1] Corresponding author.
Email address: iamyuanting@hotmail.com

many self-healing key distribution schemes have been proposed in the literature [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20].

The main contribution of this paper is that we propose a novel self-healing key distribution scheme with limited group membership property, which specifies that a secure communication group is restricted to have less than t members, where t is a scheme parameter. Our design motivation is that it is necessary to restrict the maximum number of members in the group whose underlying network is bandwidth-constrained (e.g., a WSN). That is, an excessive number of members would pose a significant communication burden on the network. Furthermore, it is also necessary to limit the group membership when considering quality of service (QoS) in certain applications of such networks (e.g., wireless multimedia sensor networks [21]).

The remainder of the paper is organized as follows. In Section 2, we describe related work on self-healing group key distribution. In Section 3, we define a security model our proposed scheme is based on. In Section 4, we present our self-healing key distribution scheme with specified properties. In Section 5, we give a comparison between our scheme and some previous schemes. In Section 6, we give a slightly modified variant of our scheme with a new property. In Section 7, we conclude this paper and give our future work.

2. Related Work

Broadcast encryption is originated by Berkovits in [22] and then formally defined by Fiat and Naor in [23]. Since then, a number of approaches have been proposed [1, 2, 3, 4, 5, 6, 7]. However, all the above approaches assume that the underlying network is reliable.

Wong and Lam [24] and Perrig et al. [25] have considered a setting which is subject to packet loss. In [24], error correction techniques have been employed to generate information about previous group keys. In [25], short hints for updated group keys are attached to subsequent data packets. Kurnio et al. [26] provides the key recovery property that recovers a session key using the previous and future session keys.

Motivated by [24] and [25], Staddon et al. introduced the concept of self-healing key distribution, which is quite similar to [26], with formal definitions, lower bounds to the required resources and some constructions. Liu et al. [10] generalized the definitions in [9], developed a novel personal key distribution technique incurring less storage and communication overhead and gave some constructions built upon the technique. Blundo et al. [11] modified previous definitions, gave new lower bounds, showed some problems in previous constructions and proposed some efficient constructions. Also, Blundo et al. [27] analyzed previous definitions and showed that no protocol can achieve some of them. Furthermore, they proposed a new definition, gave lower bounds on it and proposed some constructions under the definition. Saez [12] generalized previous definitions from another perspective, gave some lower bounds and proposed a general construction. Hong and Kang [13] proposed a self-healing scheme which optimizes the storage overhead according to the lower bounds given in [11]. Li et al. [14] proposed a self-healing scheme for local group key management in WSNs, providing group header migration capability. Schemes in [15, 16, 17, 18, 19, 20] all use one-way hash functions on either personal secrets or session keys to further reduce the storage and communication overhead under their respective security models.

3. Security Model

In a group key distribution scheme, a group manager seeks to establish a common key (i.e., the session key) among all the group members, through a broadcast, at the beginning of each session. A session can either be a fixed interval of time or a period during which the group membership (i.e., user join or leave activities) goes unchanged. Hence, when the fixed amount of time elapses or a user joins or leaves the group, the group manager has to initiate a new session by establishing a new session key among the group members. When distributing session keys to the group members, we consider the self-healing property which states that a user in three sequential sessions can recover the session key for the intermediate session when the user only receives broadcasts for the other two sessions from the group manager. Furthermore, the scheme also has the revocation property that any collusion of t users can get no information they are not entitled to, where t is a scheme parameter.

Without loss of generality, we consider a setting where there is a group manager GM and a set of n users, say $U = \{U_1, \ldots, U_n\}$. All of our operations take place in a finite field F_q, where q is a prime larger than n. Each user U_i, stores a personal secret $S_i \subseteq F_q$ (i.e., S_i can be represented as a set of elements of F_q). We assume that the maximum

number of sessions of the group communication is m. For each session j, where $1 \le j \le m$, GM sends the session key K_j, through a broadcast B_j, to the group members. We denote the set of users that are group members in session j by G_j. Thus, for any user $U_i \in G_j$, K_j is determined from B_j and S_i.

In the following, we give our definitions based on those in [10]. We use H to denote the entropy function of information theory [28] in our definitions.

Definition 1 (Session Key Distribution). Let $t, i \in \{1,\ldots,n\}$ and $j \in \{1,\ldots,m\}$.

1. D is a session key distribution scheme if the following are true:
   a) For any user $U_i \in G_j$, K_j is determined from B_j and S_i. That is, $H(K_j \mid B_j, S_i) = 0$.
   b) No information about K_j can be learned from either broadcasts or personal secrets alone. That is, $H(K_j \mid S_1,\ldots,S_n) = H(K_j \mid B_1,\ldots,B_m) = H(K_j)$.
   c) For any set $X \subseteq U$, $|X| \le t$ and $U_i \notin X$, the uncertainty of users in X to determine S_i is at least b bits. That is, $H(S_i \mid \{S_{i'}\}_{U_{i'} \in X}, B_1,\ldots,B_m) \ge b$.
2. D has t-revocation capability if given any set $X \subseteq U$, where $|X| \le t$, the group manager can generate a broadcast B_j, such that for any user $U_i \notin X$, U_i can recover K_j, but the revoked users in X cannot. That is, $H(K_j \mid B_j, S_i) = 0$ and $H(K_j \mid B_j, \{S_{i'}\}_{U_{i'} \in X}) = H(K_j)$.
3. D is self-healing if the following are true for any j, $1 \le j_1 < j < j_2 \le m$:
   a) For any user U_i who is a member in session j_1, j and j_2, the session key K_j is determined from the two sets $\{B_{j_1}, S_i\}$ and $\{B_{j_2}, S_i\}$. That is, $H(K_j \mid B_{j_1}, B_{j_2}, S_i) = 0$.
   b) For any two disjoint sets X and Y, where $|X \cup Y| \le t$, and no users in $X \cup Y$ are members in session j, the set $\{B_1,\ldots,B_{j_1},\{S_{i'}\}_{U_{i'} \in X}\} \cup \{B_{j_2},\ldots,B_m,\{S_{i'}\}_{U_{i'} \in Y}\}$ contains no information about the session key K_j. That is, $H(K_j \mid \{B_1,\ldots,B_{j_1},\{S_i\}_{U_i \in X}\} \cup \{B_{j_2},\ldots,B_m,\{S_i\}_{U_i \in Y}\}) = H(K_j)$.

Definition 2 (t-wise Forward and Backward Secrecy). Let $t, i \in \{1,\ldots,n\}$ and $j \in \{1,\ldots,m\}$. Suppose a key distribution scheme D.

1. D guarantees t-wise forward secrecy if for any set $X \subseteq U$, where $|X| \le t$, and all the users in X are revoked before and in session j, the members in X together can get no information about K_j, even with the knowledge of session keys before session j. That is, $H(K_j \mid B_1,\ldots,B_m,\{S_i\}_{U_i \in X}, K_1,\ldots,K_{j-1}) = H(K_j)$.
2. D guarantees t-wise backward secrecy if for any set $Y \subseteq U$, where $|Y| \le t$, and all the users in Y join the group after session j, the members in Y together can get no information about K_j, even with the knowledge of session keys after session j. That is, $H(K_j \mid B_1,\ldots,B_m,\{S_i\}_{U_i \in Y}, K_{j+1},\ldots,K_m) = H(K_j)$.

4. Self-healing Key Distribution with Revocation

In this section, we present our self-healing key distribution scheme with t-revocation capability based on Definition 1. Our scheme assumes that a secure communication group has a maximum number of $t-1$ group members. Information about the group membership in any session can be known to parties outside the group. For any session j, we use G_j and R_j to denote the set of non-revoked users in session j and the set of revoked users in session j, respectively, where $|G_j| \le t$, $|R_j| \le t$. We assume that our self-healing key distribution is restricted to m sessions. We note that the technique in [9] that extends the lifetime to go beyond m sessions is also applicable to ours, which we do not discuss in this paper.

Construction. Self-healing session key distribution scheme with t-revocation capability.

1. (Setup) Let t be a positive integer. The group manager GM randomly chooses m t-degree polynomials from $F_q[x]$, which are denoted as $\{s_j(x)\}_{j=1,\ldots,m}$. GM also randomly chooses m session keys, $\{K_j\}_{j=1,\ldots,m}$, from F_q and m t-degree polynomials, $\{p_j(x)\}_{j=1,\ldots,m}$, from $F_q[x]$. For each $p_j(x)$, where $1 \le j \le m$, GM computes $q_j(x) = K_j - p_j(x)$. Each user U_i gets its personal secret, $S_i = \{S_j(i), q_j(i)\}_{j=1,\ldots,m}$, from GM through the secure communication

channel between them.

2. (Broadcast) In session j, $G_j = \{U_{r_1}, \ldots, U_{r_{w_j}}\}$, where $|G_j| = w_j \le t$, GM chooses $t - w_j$ values, $\{r_i'\}_{i=1,\ldots,t-w_j}$, from the same field that user IDs (i.e., $\{r_i\}_{i=1,\ldots,w_j}$) come from, such that none of these values is used as a user ID. GM then computes a t-degree polynomial, $\Phi_j(x)$, from $F_q[x]$, such that $\Phi_j(x) = p_j(x) + g_j(x) + s_j(x)$, where $g_j(x) = (x - r_1)\cdots(x - r_{w_j})(x - r_1')\cdots(x - r_{t-w_j}')$. Consequently, GM broadcasts the following message: $B_j = \{\Phi_1(x) + \Phi_2(x), \ldots, \Phi_{j-2}(x) + \Phi_{j-1}(x), \Phi_j(x)\}$. Specifically, we have that $B_j = \{\Phi_j(x)\}$, where $j < 3$.
3. (Session Key Recovery) When a non-revoked user, $U_i \in G_j$, receives the broadcast B_j for session j from GM, U_i recovers the polynomial $\Phi_j(x)$, evaluates $\Phi_j(x)$ at point i, recovers the share $p_j(i)$ by the following equation: $p_j(i) = \Phi_j(i) - g_j(i) - s_j(i) = \Phi_j(i) - s_j(i)$, and computes the session key $K_j = p_j(i) + q_j(i)$. U_i then stores K_j to replace $q_j(i)$ since the latter is no longer necessary.
4. (Group Member Addition) When GM wants to add a new user, say U_v, to the group starting from session j, it computes $\{s_i(v), q_i(v)\}_{i=j,\ldots,m}$ and gives $\{s_i(v), q_i(v)\}_{i=j,\ldots,m}$ to U_v as its personal secret, through the secure communication channel between them.

Note that in our scheme, we do not require that the sets of revoked users change monotonically, that is, $R_{j_1} \subseteq R_{j_2}$ for $1 \le j_1 \le j_2 \le m$. Hence, a user that is revoked in session j_1 can rejoin the group in a later session j_2. It is guaranteed that in any session j, where $j_1 \le j < j_2$, the user cannot recover the corresponding session key K_j, if the user is not a member in session j.

5. Analysis

5.1 Security

Our scheme has the properties of unconditional security, self-healing, t-revocation capability, t-wise forward and backward secrecy, as shown in Theorem 1 and 2.

Theorem 1. Our scheme is an unconditionally secure, self-healing key distribution scheme with t-revocation capability.

Proof. We will show that our scheme satisfies all the conditions required by Definition 1.

1. Let us first prove that D is a session key distribution scheme.
   a) A non-revoked user $U_i \in G_j$ recovers the session key K_j during the Session Key Recovery phase in our scheme. Thus, it follows that $H(K_j \mid B_j, S_i) = 0$.
   b) Since the session key K_j and its share $p_j(x)$ (hence, $q_j(x)$) are randomly chosen from F_q and $F_q[x]$, respectively, K_j cannot be determined only by broadcast messages or personal secrets. Thus, it follows that $H(K_j \mid S_1, \ldots, S_n) = H(K_j \mid B_1, \ldots, B_m) = H(K_j)$.
   c) For any set $X \subseteq U$, $|X| \le t$ and $U_v \notin X$, we show that the coalition of X knows nothing about S_v. Assume that U_v joins the group starting from session j. First, after receiving all the broadcast messages $\{B_1, \ldots B_m\}$, we have $\{s_i(v) = \Phi_i(v) - g_i(v) - p_i(v)\}_{i=j,\ldots,m}$. Each $p_i(x)$ is randomly chosen from $F_q[x]$, in order to determine each $p_i(v)$, we must have at least $t+1$ points on each $p_i(x)$ to recover $p_i(x)$ first. Since the coalition of X only has at most t points on each $p_i(x)$, it cannot determine any $p_i(v)$. Second, for the same reason, $\{q_i(v)\}_{i=j,\ldots,m}$ cannot be determined by the coalition of X, either. Thus, we have the following derivation:
   $$\begin{aligned} & H(S_v \mid \{S_{i'}\}_{U_{i'} \in X}, B_1, \ldots, B_m) \\ &= H(\{s_i(v), q_i(v)\}_{i=j,\ldots,m} \mid \{S_{i'}\}_{U_{i'} \in X}, B_1, \ldots, B_m) \\ &= H(\{p_i(v), q_i(v)\}_{i=j,\ldots,m} \mid \{S_{i'}\}_{U_{i'} \in X}, B_1, \ldots, B_m) \\ &= H(\{p_i(v), q_i(v)\}_{i=j,\ldots,m}) \\ &= 2(m - j + 1)\log q. \end{aligned}$$
2. Let $X \subseteq U$, $|X| \le t$, users in X are all revoked in session j. For any non-revoked user $U_i \notin X$, GM can generate a broadcast B_j as described in the Broadcast phase, such that U_i can recover the session key K_j and any

revoked user in X cannot. Thus, it follows that $H(K_j \mid B_j, S_i) = 0$. For the coalition of X, it knows at most t points on $q_j(x)$ and nothing on $p_j(x)$ before B_j. After B_j, we have $\{p_j(i') = \Phi_j(i') - g_j(i') - s_j(i')\}_{U_{i'} \in X}$. Since the coalition knows at most t points on $s_j(x)$ and nothing on $\{g_j(i')\}_{U_{i'} \in X}$, it cannot get any information about $p_j(x)$ and in turn the session key K_j. Thus, it follows that $H(K_j \mid B_j, \{S_{i'}\}_{U_{i'} \in X}) = H(K_j)$.

3. Let us prove that D is self-healing.
   a) From the Session Key Recovery phase, any user U_i that is a member in session j_1 and j_2, where $1 \le j_1 < j_2 \le m$, can recover the polynomials $\{\Phi_{j_1}(x), \Phi_{j_1+1}(x), \ldots, \Phi_{j_2-1}(x), \Phi_{j_2}(x)\}$ from the broadcasts B_{j_1} and B_{j_2}. For any session j, where $j_1 < j < j_2$ and $U_i \in G_j$, U_i recovers the session key $K_j = p_j(i) + q_j(i) = \Phi_j(i) - s_j(i) + q_j(i)$. Thus, it follows that $H(K_j \mid B_{j_1}, B_{j_2}, S_i) = 0$.
   b) For any two disjoint sets X and Y, where $|X \cup Y| \le t$ and no users in $X \cup Y$ are members in session j, the set $\{B_1, \ldots, B_{j_1}, \{S_{i'}\}_{U_{i'} \in X}\}$ contains at most $|X|$ points on $s_j(x)$, and the set $\{B_{j_2}, \ldots, B_m, \{S_{i'}\}_{U_{i'} \in Y}\}$ contains at most $|Y|$ points on $s_j(x)$, thus we have at most t points on $s_j(x)$ in $X \cup Y$. After recovering the polynomial $\Phi_j(x)$ from B_{j_1} and B_{j_2}, we have $p_j(x) = \Phi_j(x) - g_j(x) - s_j(x)$. Since $s_j(x)$ cannot be recovered by no more than t points on it and $g_j(x)$ cannot be recovered due to the unknown $\{r_i'\}_{i=1,\ldots,t-w_j}$ in the Broadcast phase, $p_j(x)$ cannot be determined either. Thus, it follows that $H(K_j \mid \{B_1, \ldots, B_{j_1}, \{S_{i'}\}_{U_{i'} \in X}\} \cup \{B_{j_2}, \ldots, B_m, \{S_{i'}\}_{U_{i'} \in Y}\}) = H(K_j)$.

□

Theorem 2. Our scheme achieves t-wise forward and backward secrecy.

Proof. We will show that the scheme satisfies all the conditions required by Definition 2.

1. Let $X \subseteq U$, $|X| \le t$, all the users in X are revoked before and in session j. Along with all the broadcast messages $\{B_1, \ldots, B_m\}$, the members in X together have at most t points on $s_j(x)$ which requires at least $t+1$ points to determine, so they get no information about the session key K_j. Moreover, since each session key is independently chosen from F_q, the set $\{K_i\}_{i=1,\ldots,j-1}$ contains no information about K_j. Thus, it follows that $H(K_j \mid B_1, \ldots, B_m, \{S_i\}_{U_i \in X}, K_1, \ldots, K_{j-1}) = H(K_j)$.
2. Let $Y \subseteq U$, $|Y| \le t$, all the users in Y join the group after session j. Along with all the broadcast messages $\{B_1, \ldots, B_m\}$, the members in Y together have nothing on $s_j(x)$, so they get no information about the session key K_j. Moreover, since each session key is independently chosen from F_q, the set $\{K_i\}_{i=j+1,\ldots,m}$ contains no information about K_j. Thus, it follows that $H(K_j \mid B_1, \ldots, B_m, \{S_i\}_{U_i \in Y}, K_{j+1}, \ldots, K_m) = H(K_j)$.

□

5.2 Efficiency

Once a new user, say U_v, joins the group starting from session j, U_v stores the personal secret for $m - j + 1$ sessions, $S_i = \{s_i(v), q_i(v)\}_{i=j,\ldots,m}$, which occupies $2(m - j + 1)\log q$ memory space. After receiving the broadcast message $B_{j'}$, where $1 \le j \le j' \le m$ and $U_v \in G_{j'}$, U_v recovers the session key $K_{j'}$ and stores $K_{j'}$ to replace $q_{j'}(v)$. Thus, the total storage overhead in each group member is $2(m - j + 1)\log q$ (at most $2m \log q$).

A broadcast message in the Broadcast phase of our scheme consists of $j-1$ t-degree polynomials, so the broadcast message size is $(t+1)(j-1)\log q$ (at most $(t+1)(m-1)\log q$).

5.3 Comparison

In this subsection, we give a simple comparison of our scheme with four existing self-healing schemes in [9, 10, 11, 13]. Table 1 summarizes the comparison among these five self-healing schemes. We use C3 to denote Construction 3 in [9], and S3 to denote Scheme 3 in [10], etc.

Table 1. Comparison among selected self-healing key distribution schemes in session j.

Schemes	Membership	Member Revocation	Storage Overhead	Communication Overhead
C3 of [9]	unbounded	t	$[(m-j+1)^2+1]\log q$	$[m(t+1)^2+t]\log q$
S3 of [10]	unbounded	t	$2(m-j+1)\log q$	$[(m+j+1)t+m+1]\log q$
S2 of [11]	unbounded	t	$(m-j+1)\log q$	$(2tj+j-1)\log q$
C1 of [13]	unbounded	t	$(m-j+1)\log q$	$(t+1)(j-1)\log q$
Our scheme	$t-1$	unbounded	$2(m-j+1)\log q$	$(t+1)(j-1)\log q$

Our scheme has the unique property of revoking any number of users during the lifetime of the secure group communication, while restricting the group membership to be less than t. As we explained before, by requiring an upper bound of the group membership, our scheme saves limited communication bandwidth and guarantees reasonable QoS by configuring the parameter t according to QoS requirements of the secure group communication.

From Table 1, it is easy to see that our scheme has the least communication overhead among the five schemes. Although C1 of [13] achieves the same least communication overhead, the result does not include the communication overhead for broadcasting the revoked user IDs, due to the reason given in [13]. Hence, our scheme is a bit more efficient than C1 of [13] in terms of broadcast message size. As for storage overhead, our scheme occupies more memory space than S2 of [11] and C1 of [13]. This is mainly because that in order to satisfy the requirement of Definition 1.1c, our scheme divides each session key into two separate shares (i.e., $K_j = p_j(x) + q_j(x)$ for $1 \le j \le m$) to further mask the session key. However, the other two schemes do not satisfy this security requirement. When individually compared with S2 of [11], we can see that our scheme requires twice the memory space and about half the broadcast message size. When considering the trade off between storage and communication overhead, this efficiency difference makes our scheme outperform S2 of [11] in an energy sensitive setting (e.g., a WSN) where communication operations consume more energy than storage ones.

6. Key Recovery from a Single Broadcast

In this section, we give a slightly modified variant of the scheme described in Section 4, which enables a user to recover all the previous session keys for sessions in which it is a member only by the current broadcast message, as apposed to two broadcast messages required in our previous scheme.

The construction of this new scheme is almost the same as that of our previous one, except that we need to modify the broadcast message format in the Broadcast phase in our previous scheme to realize key recovery from a single broadcast message. More specifically, for a specific session j, B_j needs to be modified as follows: $B_j = \{\Phi_1(x), \Phi_2(x), \ldots, \Phi_{j-1}(x), \Phi_j(x)\}$.

From a formal point of view, the self-healing property of the new scheme conforms to the following definition which replaces 1a and 3a in Definition 1:

Definition 3. For any session $1 \le j \le m$, and any user U_i, that is a member in session l, the session key K_l is determined by B_j and S_i. Thus, $H(K_l \mid B_j, S_i) = 0$.

Along the same line of Theorem 1, we have the following theorem:

Theorem 3. The new scheme presented in this section is an unconditionally secure, self-healing key distribution scheme with t-revocation capability.

The storage and communication overhead of the new scheme is the same as that of our previous scheme in Section 4.

7. Conclusion and Future Work

In this paper, we propose an unconditionally secure self-healing key distribution scheme with t-revocation capability for unreliable networks with limited communication resources (e.g., WSNs). Our scheme saves communication bandwidth and guarantees QoS by restricting the group membership to be less than t while allowing for revoking any number of users. Through analysis, we show that our scheme has a better tradeoff between storage and communication overhead than some previous work.

In the future, we will further improve our

proposed scheme in terms of efficiency under the defined security model and compare our improved scheme with other existing schemes. In addition, we try to develop a new security model based on the one in this paper and some new schemes built on it in order to provide better tradeoff between security and efficiency for specific applications.

Acknowledgments

In this paper, we would like to appreciate the support by the Grant No. 60672113 from National Natural Science Foundation of China. We are also very thankful to many colleagues for their helpful comments.

References

[1] H. Harney and C. Muckenhirn, "Group Key Management Protocol Architecture", IETF RFC 2094, 1997.

[2] C. Wong, M. Gouda and S. Lam, "Secure Group Communications Using Key Graphs", In: *Proc. of ACM SIGCOMM '98*, pp. 68-79, 1998.

[3] D. Wallner, E. Harder and R. Agee, "Key Management for Multicast: Issues and Architectures", IETF RFC 2627, 1999.

[4] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor and B. Pinkas, "Multicast Security: A Taxonomy and Some Efficient Constructions", In: *Proc. of IEEE INFOCOM '99*, pp. 708-716, 1999.

[5] R. Canetti, T. Malkin and K. Nissim, "Efficient Communication-storage Tradeoffs for Multicast Encrption", In: *Advances in Cryptology – Eurocrypt '99*, LNCS, 1592: 459-474, 1999.

[6] R. Safavi-Naini and H. Wang, "New Constructions for Multicast Re-keying Schemes Using Perfect Hash Families", In: *Proc. of the 7th ACM Conference on Computer and Communications Security CCS '00*, pp. 228-234, 2000.

[7] D. Naor, M. Naor and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Users", In: *Advances of Cryptology – Crypto '01*, LNCS, 2139: 41-62, 2001.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks", In: *IEEE Communications Magazine*, 40(8): 102-114, 2002.

[9] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin and D. Dean, "Self-Healing Key Distribution with Revocation", In: *Proc. of IEEE Symposium on Security and Privacy '02*, pp. 224-240, 2002.

[10] D. Liu, P. Ning and K. Sun, "Efficient Self-healing Key Distribution with Revocation Capability", In: *Proc. of the 10th ACM Conference on Computer and Communications Security CCS '03*, pp. 82-90, 2003.

[11] C. Blundo, P. D'Arco, A. Santis and M. Listo, "Design of Self-healing Key Distribution Schemes", In: *Design Codes and Cryptology*, 32: 15-44, 2004.

[12] G. Saez, "On Threshold Self-healing Key Distribution Schemes", In: *N. P. Smart: Cryptography and Coding 2005*, LNCS, 3796: 759-761, 2005.

[13] D. Hong and J. Kang, "An Efficient Key Distribution Scheme with Self-healing Property", In: *IEEE Communications Letter*, Vol. 9, pp. 759-761, 2005.

[14] H. Li, K. Chen, Y. Zheng and M. Wen, "A Locally Group Key Management with Revocation and Self-healing Capability for Sensor Networks", In: *Proc. of the International Conference on Systems and Networks Communication ICSNC '06*, pp. 29-33, 2006.

[15] R. Dutta, E. C. Chang and S. Mukhopadhyay, "Efficient Self-healing Key Distribution with Revocation for Wireless Sensor Networks Using One Way Key Chains", In: *Proc. of the 5th International Conference on Applied Cryptography and Network Security*, LNCS, 4521: 385-400, 2007.

[16] R. Dutta and S. Mukhopadhyay, "Improved Self-Healing Key Distribution with Revocation in Wireless Sensor Network", In: *Proc. of Wireless Communications and Networking Conference WCNC '07*, pp. 2963-2968, 2007.

[17] R. Dutta and S. Mukhopadhyay, "Designing Scalable Self-healing Key Distribution Schemes with Revocation Capability", In: *Parallel and Distributed Processing and Applications*, LNCS, 4742: 419-430, 2007.

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

[19] Y. Jiang, C. Lin, M. Shi and X. Shen, "Self-healing Group Key Distribution with Time-limited Node Revocation for Wireless Sensor Networks", In: *Ad Hoc Networks*, 5(1): 14-23, 2007.

[20] F. Kausar, S. Hussain, J. H. Park and A. Masood, "Secure Group Communication with Self-healing and Rekeying in Wireless Sensor Networks", In: *Mobile Ad-Hoc and Sensor Networks*, LNCS, 4864: 737-748, 2007.

[21] I. F. Akyildiz, T. Melodia and K. R. Chowdhury, "A Survey on Wireless Multimedia Sensor Networks", In: *Computer Networks: The International Journal of Computer and Telecommunications Networking*, 51(4): 921-960, 2007.

[22] S. Berkovits, "How to Broadcast a Secret", In: *Advances in Cryptology – Eurocrypt '91*, LNCS, 547: 536-541, 1991.

[23] A. Fiat and M. Naor, "Broadcast Encryption", In: *Advances in Cryptology – Crypto '93*, LNCS, 773: 480-491, 1994.

[24] C. Wong and S. Lam, "Keystone: A Group Key Management Service", In: *International Conference on Telecommunications ICT 2000*, 2000.

[25] A. Perrig, D. Song and J. D. Tygar, "ELK, a New Protocol for Efficient Large-Group key Distribution", In: *Proc. of IEEE Symposium on Security and Privacy*, pp. 247-262, 2001.

[26] H. Kurnio, R. Safani-Naini and H. Wang, "A Secure

Re-keying Scheme with Key Recovery Property", In: *Proc. of the 7th Australian Conference on Information Security and Privacy ACISP '02*, LNCS, 2384: 40-55, 2002.

[27] C. Blundo, P. D'Arco, A. Santis and M. Listo, "Definitions and Bounds for Self-healing Key Distribution", In: *Fuzzy Sets and Systems, 31st International Colloquium on Automata, Languages and Programming ICALP '04*, LNCS, 3142: 234-245, 2004.

[28] T. Cover and J. Thomas, "Elements of Information Theory", John Wiley and Sons, Inc., 1991.