ISSN:0975-9646

Revocation and Self Healing of keys in Hierarchical Wireless Sensor Network

G.N.Purohit [1], Asmita Singh Rawat[2]

[1]Department of Mathematics,

AIM & ACT, Banasthali University, Banasthali-304022, INDIA

[2] Department of Computer Science,

AIM & ACT, Banasthali University, Banasthali-304022, INDIA

Abstract- In this paper we have discussed a key distribution scheme with revocation and self healing mechanism. Self healing key distribution scheme enables a group of users to establish a group of keys over an unreliable network. In our scheme cluster header distributes session keys to the group nodes for communication. The concept of key distribution scheme with revocation was first mooted by Staddon, since then there have been many improvements in the scheme. We have given a scheme in this paper which removes all the flaws of earlier researches and it is more secure and authenticate.

Keywords- Wireless Sensor Network, Key distribution, Revocation , self- healing**.**

I.INTRODUCTION

Wireless Sensor Networks (WSNs) are solutions for many applications and security requirements. The wireless networks, especially WSNs are ideal for communication in tactical situations such as anti-terrorist operations, rescue missions and battle field, where there is usually no network infrastructures support. A common way to ensure communication security is to encrypt and authenticate the wireless communication. In tactical wireless networks, a sender may broadcast encrypted and authenticated messages to the members and only wireless nodes with valid keys can have access to these messages.

A fundamental service to achieve secure communication is key distribution, where sensor nodes are allotted secret key and these keys are used to encrypt and authenticate message. Among all the security issues for communications in WSNs, key management is a core mechanism to ensure the security of applications and network services in WSNs. Lots of efforts have been dedicated to the study of key distribution in WSNs and these methods are categorized in group key distribution [2],[4],[5],[7], and pair wise distribution [2],[7],[5],[8],[9].

A novel group key distribution schemes that can cope with the highly mobile, volatile and hostile wireless networks in tactical situation (e.g. anti-terrorist operations, rescue missions and battlefields)needs self- healing key distribution with revocation capability concept proposed for the first time by Staddon et.al[11]. First, the proposed techniques are self- healing. We feel that it is more efficient than any other previous schemes. A wireless node can recover lost keys even if it is separated from the network when the key is distributed. Second, the technique does not require heavy computation and wireless nodes can obtain or recover keys by passively listening to broadcast key distribution messages. Reducing the computation and active communication can significially reduce the power consumption and prolong the life time of wireless devices. Thirdly the technique distributes keys via true broadcast, conforming to the broadcast nature of wireless devices. Only select receivers of the messages can recover the key from the broadcast messages. Finally the technique is scalable to very large groups.

The self- healing key distribution technique with the revocation capability reduces the network traffic and workload on the cluster header or group managers. There are some useful military oriented applications of self- healing key distribution schemes with revocation capability, where session keys can be used. There are many such applications of self- healing, naming one of them is , the application of self- healing key distribution with revocation in the broadcast communication over low cost pay TV- channel, the live event transmission can be viewed by the users who have paid for the service.

In this paper we have presented a new self-healing key distribution technique with revocation property that requires constant storage of personal keys for each user proposed key distribution schemes have several advantages including hose inherited from [11] which makes the schemes very attractive for tactical wireless networks.

Organization: The rest of the paper is organized as follows. Section 2 covers the related work; Section 3 covers the notations and terminologies which are used in this paper. Section 4 describes the model; Section 5 covers the working of the model and key distribution. In Section 6 we conclude the paper.

II.RLATED WORK

The process of self healing key distribution with revocation was introduced for the first by Staddon et.al [11]. They have provided relevant definitions and security notions, which were later generalized by Liu et.al[9] and Blundo et.al[2]. Wong and Lam et.al [13] , and Peering et.al[10] considered the problem of reliable group key distribution. Liu et. al [8], proposed a forward error correction to ensure that the group members who missed the broadcast can recover the missed group key. Peering et.al[10], used a hierarchical private key systems of past group keys to achieve reliable group key distribution. Blundo et.al[1] criticized the first construction in Staddon[11] and presented a slightly modified framework. More recently Hong et.al[4] proposed a self healing key distribution having less storage and communication complexity. Presently, Dutta and Mukhopadhyay [4] proposed a new efficient method in the key distribution scheme

III. BASIC TERMINOLOGIES AND NOTATIONS

In this section we introduce the basic terminology used in the paper and the relevant notations used to describe the model.

U = set of all users in the network

U_i = ith user in the network

C_H = Cluster header which act as a group manager in the model

$n = |U|$ = total number of users in the network

m = Total number of session

t = Total number of compromised users.

F_q = Field of oder q, q is the large integer much greater than n.

S_i = Personal secret of user U_i

SK_j = session key generated by the cluster header in j-th session.

B_j = Broadcast message by cluster header during j-th session.

$P_{i,j}$ = Information collected by U_i through B_j and S_i.

R = set of all revoked users; $|R| < t$

The main concept of self healing key distribution is that users in a large and group communication over an unreliable network can recover lost session keys, even if they have lost some previous broadcast messages without requesting for any repeated transmission from the cluster header C_H. Thus, when self healing key distribution is implemented for a sequence of sessions, it is possible for an user (node) to recover all missed messages but not the first and last key distribution broadcasts.

The idea behind the self healing technique is to use secret sharing to bind the broadcast information that is useful information only to trusted members. In each broadcast the user learns either the actual key or a share of the actual key for each of the sessions. For example in the self healing mechanism, if we suppose $1 \le j_1 < j < j_2 \le m$ where m is the number of sessions. Then for any user U_i who is a member in sessions j_1 and j_2 and missed session *j*, then SK_j can be determined by B_{j1}, B_{j2} and S_i.

As far as revocation of users is concerned, the mechanism of revocation means the removing the compromised node from the users.If a node has been compromised before session *j* , then it is not permitted to receive the broadcast message for all sessions $k \ge j$ and it is revoked in session j. The number of nodes removed during session j are denoted by R_j and $\|R_j\| < t$.

IV.THE MODEL SETUP

In this paper we consider three –tier (layers) hierarchical network model with layers as:

(i)Base station (ii) Cluster headers (iii) Cluster of nodes

The top most layers is the base station and the second layer is the cluster header and finally the lowest layer is the cluster nodes. The key distribution scheme not only provides self healing, but the ability to revoke users from the group. In the model we consider a hierarchical architecture where WSN is partitioned into a number of groups and further in number of sessions. A high end device in placed into each cluster of nodes called Cluster Header C_H. Compared to sensor nodes capability. The high end cluster headers have high computation abilities and larger storage size.

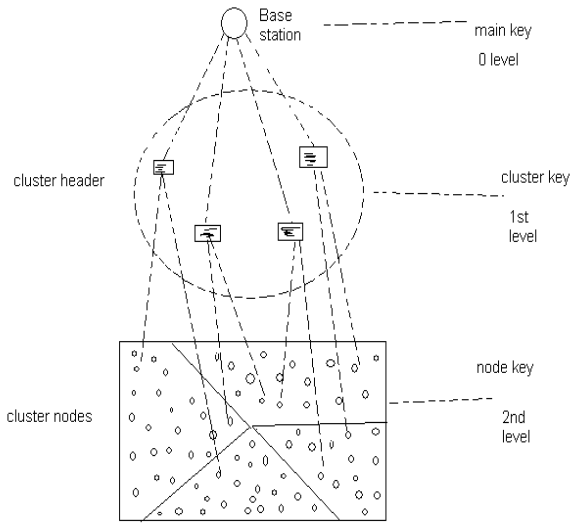

Fig.1.

Base station is very strong as compared to other parts of the model. Base station is responsible for distributing keys to the cluster header and cluster header takes the responsibility of distribution of cluster keys within the cluster nodes. In this model the sensor nodes are partitioned into number of clusters N, and each cluster C_l group has a cluster header . $l \in (1,...,N)$. Each sensor node in a group is uniquely identified by ID number i, where $i \in \{1,...,n\}$, where n is the total number of nodes in all the clusters

The duration of the sessions can be fixed or dynamic depending on the applications. The base station is responsible for the distributing keys to cluster header sensor nodes. We use SK_j to denote the jth session key where $j \in \{1,2,...,m\}$.

In this model we propose two kinds of keys one SK_j the session key and K_{CH} represent the pair wise key or path shared between the cluster header C_H and group nodes. In this model all of the operations take place in a finite field F_q, where q is sufficiently large prime number. Each group node U_i stores a personal secret $S_i \subseteq F_q$, which represents all information of the cluster nodes which may use to recover the session key among the group via a message broadcasting . We use B_j to denote the broadcast message, called session key distribution message.

There are certain definitions which would support the paper:

Definition (i): If D is a key distribution scheme, then

a) For any member U_i, SK_j is determined by B_j and S_i.

b) For any $R \subseteq \{U_1,...,U_n\}$ and $U_i \notin R$, $|R| \le t$ .The user $r \in R$ cannot determine anything about S_i.

c) The information received by $\{U_1,...U_n\}$ from B_j and cannot be determined from the broadcast or personal keys alone.

The cluster header can generate a broadcast message B_j , such that for all $U_i \notin R$, U_i can recover the session key but the revoked members cannot recover any of the keys and thus we call D has a revocation capability.

Definition (ii): For any $R \subseteq \{U_1,...,U_n\}$ with $|R| < t$ the cluster header can generate a broadcast message B_j, such that for all $U_i \notin R$, U_i can recover the session key but the revoked members can't recover any of the of the keys and thus we call D has a revocation capability.

Definition (iii): Suppose $1 \le j_1 < j < j_2 \le m$. Then for any U_i who is member in j_1 and j_2 , SK_j can be determined by B_{j1}, B_{j2} and S_i , and we call this as a self healing.

Definition (iv): In the session key distribution mechanism

Let $t, i \in \{1,...,n\}$ and $j \in \{1,...,m\}$ Then *D* is a session key distribution scheme if following conditions are satisfied:

a) For any member U_i, SK_j is determined by $z_{i,j}$ which in turn is determined by B_j and S_i (i.e. $H(k_j \setminus z_{i,j})$=0 and $H(z_{i,j} \setminus B_j, S_i) = 0$).

b) For any set $R \subseteq \{U_1,...,U_n\}$, $|R| \le t$ and $U_i \notin R$ then the users in *R* cannot determine anything about S_i.

c) Members $\{U_1,...,U_n\}$ learn from B_j that cannot be determined from the broadcast or personal key alone { i.e. $H(\ z_{i,j} \setminus B_1,..., B_m) = H(z_{i,j})$=($H(z_{i,j} \setminus S_1...,S_n)$}.The concept of session key distribution [ ] requires that any coalition of at most *t* valid group members cannot get any information about another members personal secret while in this definition our paper requires that the uncertainity of such coalition to determine another members personal secret.

V. WORKING OF THE MODEL

In this paper we present a technique for self healing key distribution with the revocation capability.

A. Key Distribution Mechanism

The purpose of personal key share distribution is to distribute keys to select cluster nodes so that each of the select (or non-revoked) cluster nodes shares a distinct personal key with the cluster header, but the other (revoked) cluster nodes (as well as the adversary) cannot get any information of the keys. In our approach, the cluster header broadcasts a message, and all the select group members derive their keys from the message.

In this approach a random t-degree polynomial $f(x)$ is chosen from $F_q(x)$, and $f(i)$ is considered to be the personal key share for each cluster node U_i. The cluster header constructs a single broadcast polynomial $w(x)$ such that for a select group member U_i, $f(i)$ can be recovered from the knowledge of $w(x)$ and the personal secret S_i, but for any revoked group member $U_i^{'}$, $f(i')$ cannot be determined from $w(x)$ and $S_i^{'}$.

Specifically, we construct $w(x)$ from $f(x)$ with the help of a *revocation polynomial* $g(x)$ and a *masking polynomial* $h(x)$ by computing $w(x) = g(x)\ f(x) + h(x)$. The revocation polynomial $g(x)$ is constructed in such a way that for any select cluster node U_i, $g(i) \neq 0$, but for any revoked cluster header $U_i^{'}$, $g(i') = 0$. Each cluster header U_v has its own personal secret $Sv = \{h(v)\}$, which may be distributed by the cluster header during setup via the secure communication channel between each cluster header and the cluster node. Thus, for any select group member U_i, new personal key $f(i)$ can be computed by $f(i)$ = (w(i) - h(i))/ $g(i)$, but for any revoked cluster header $U_i^{'}$, no personal key cannot be computed because $g(i)$=0.

The purpose of personal key distribution with t- revocation capability is to distribute the distinct shares of a target t-degree polynomial $f(x)$ to non revoked cluster headers.

In this type of scheme each non-revoked group member U_i can only recover its own personal share $f(i)$, since computing the personal key of another non-revoked member Uj requires the knowledge of the personal secret $\{h(j)\}$. The coalition of no more than t revoked members has no way to determine any share on $f(x)$, because no matter what $f(x)$ is, for any evoked cluster header $U_i^{'}$, we have $h(i') = w(i')$, which mplies that any $f(x)$ is possible from the knowledge of the coalition of the revoked cluster nodes.

. Self-Healing Key Distribution with Revocation Capability

Here is an efficient scheme to distribute personal key shares to select cluster nodes for each self healing mechanism. This technique combines the technique with the self-healing method in[11].

Intuitively, the cluster header randomly splits each group session key SK_j into two t-degree polynomials, $p_j(x)$ and $q_j(x)$, such that SK_j = $p_j(x)$ + $q_j(x)$. The cluster header then distributes shares $p_j(i)$ and $q_j(i)$ to each select group member U_i (via broadcast). This allows a cluster header that has both $p_j(i)$ and $q_j(i)$ to recover SK_j by computing SK_j = $p_j(i)$ + $q_j(i)$. Thus, assuming there are m sessions, we can build (m+1) broadcast polynomials in session j to distribute the shares of { $p_1(x)$,..., $p_j(x)$; $q_j(x)$,....., $q_m(x)$ } to all select cluster headers. If any U_i receives the broadcast message, it can recover all {{ $p_1(i)$,..., $p_j(i)$; $q_j(i)$,....., $q_m(i)$ } and compute session key SK_j = $p_j(i)$ + $q_j(i)$. But the revoked cluster headers get nothing from this broadcast message. Furthermore, if a select cluster nodes U_i eceives session key distribution messages in sessions j_1 and j_2, where $j_1 < j_2$, but not the session key distribution

message for session j, where $j_1 < j < j_2$, it can still recover the lost session key SK_j by first recovering $p_j(i)$ and $q_j(i)$ from the broadcast message in sessions j_1 and j_2, respectively and then computing $SK_j = p_j(i) + q_j(i)$.

VI. BASIC SCHEME

Let $h, h_R, h_F : \{0,1\} \rightarrow F_q$ be cryptographic hash function. The base station chooses a root key $r_B = [r_{b1}, r_{b2}]$, where r_{b1} and r_{b2} are random numbers. For each cluster C_k, the base station computes the cluster head key $CB_k = [cb_1^k, cb_2^k]$ where $cb_1^{(k)} = h(c_k, r_{b1})$ and $cb_2^{(k)} = h(c_k, r_{b2})$ and passes the cluster head key to respective clusters. The cluster header sets $cb_1^{(k)}$ to be the seed $S_R^{(k)}$ of the reverse one way hash chain of the length $(m+1)$

$$b_{j,R}^{(k)} = h_R(b_{j-1,R}^{(k)})$$

$$= h_R(h_R(b_{j-2,R}^{(k)}))$$

$$= h_R^j(S_R^{(k)}), 1 \le j \le m-1$$

Where $h_R^{(k)} = h_R$ (j-times) and sets Cb_2^k to be the seed $S_R^{(k)}$ for the forward hash chain of length m.

$$b_{j,F}^{(k)} = h_F(b_{j-1,F}^{(k)})$$

$$= h_F(h_F(b_{j-2,F}^{(k)}))$$

$$= h_F^j(S_F^{(k)}), 1 \le j \le m$$

The cluster key for the session $j \in [1,...m]$ is defined as

$$S_j^{(k)} = b_{m-j+1,R}^{(k)} + h_F^j(S_F^{(k)})$$

$$= h_R^{m-j+1}(S_R^{(k)}) + h_F^j(S_F^{(k)})$$

The cluster header C_k selects m-random t-degree polynomials $f_1^{(k)}(x), f_2^{(k)}(x), ... f_m^{(k)}(x) \in F_q[x]$

The personal secret for the member sensor node $U_i^{(k)}$ is defined to be $S_i^{(k)} = [f_1^k(i), f_2^{)k)}(i), ... f_m^{(k)}(i)$

The cluster header then sends $S_i^{(k)}, b_{m+1,R}^{(k)}$ and $S_F^{(k)}$ to each node U_i in a secure manner.

Broadcast. Following **Dutta and Mukhopadhyay[2007],** a similar extended scheme for hierarchical sensor network is proposed. Let $R_j^{(k)} = \{i_1, ...i_w\}$ be the set of revoked sensor nodes in C_k upon the start of session $j \in \{1,..., m\}$ and $\left|R_j^{(k)}\right| = w \le t.$

The cluster head chooses t-w random Ids $R_j^{'(k)} = \{i_t^{'}, i_{t+1}^{'}, ...i_{w+1}^{'}\} \subset \{1,...n\}$ not present in C_k . Then the revocation polynomial $r_j^{(k)}(x)$ is computed as $r_j^{(k)}(x) = (x - i_1)....(x - i_w)(x - i_{w+1}^{'})...(x - i_t^{'})$.

Session Key recovery When a non revoked user $U_i^{(k)}$ receives the j-th session key distribution message $B_j^{(k)}$, it evaluates the polynomial $f_j^{(k)}(i)$ and receives the session key as.

$$b_{m_{j+1},R}^{(k)} = \frac{b_j^{(k)}(i) - f_j^{(k)}(i)}{r_j^{(k)}(i)}$$

Security For security construction of the scheme, we have the following theorem.

Theorem: the above construction is a hierarchical self healing group key distribution scheme

VII.CONCLUSION

In this paper we have proposed a new mechanism for implementing self healing key distribution with the revocation property for wireless sensor network. We have described a secure and efficient construction which improves the communication overhead and complexity. We have developed and analyzed an efficient secure self healing key distribution scheme with the revocation capability enabling very large and dynamic group users to establish a common key for secure communication over an unreliable wireless network. This scheme is highly efficient in terms of storage, communication and computation overhead. For storage, the personal secret together with the authentication accounts for (m+1) $\log q$ bits storage in each sensor node, $\log q$ bits more, compared to the scheme given in **Dutta and Mukhopadhyay[2008],** for the authentication. For communication this scheme generates $t(\log q + \log n) \approx t \log q$ bits key update message.

REFERENCES

[1] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. *Perfectly-secure key distribution for dynamic conferences*, Proc. Crypto 92.

[2] C. Blundo, P. D'Arco, and M. Listo. *A Flaw in A Self-healing Key Distribution Schemes*, Proc. Information Theory Workshop, pp. 163-166, 2003.

[3] C. Blundo, P. D'Arco, A. Santis, and M. Listo. *Deffinitions and Bounds for Self-healing Key Distribution*, Proc. 31st International Colloquium on Automata, Language and Programming, ICALP'04, LNCS 3142, pp. 234-245, 20

[4] R. Dutta, E. C. Change, and S. Mukhopadhyay. *Efficient Self-healing Key Distribution with Revocation for Wireless Sensor Networks Using One Way Key Chains*, Proc. Applied Cryptography and Netwrok Security, ACNS'07, pp. 385-400, 2007.

[5] L. Eschenauer, and V. D. Gligor. *A Key-Management Scheme for Distributed Sensor Networks*, Proc. ACM Conference on Computer and Communication Security, CCS'02.

[6] D. Hong, J. Kang. *An Efficient Key Distribution Scheme with Self healing Property*. IEEE communication Letters'05, Vol. 9, pp. 759-761, 2005.

[7] D. Huang, M. Mehta, D. Medhi, and L. Harn. *Location-aware key management scheme for wireless sensor networks*, Proc. 2nd ACM workshop on Security of Ad Hoc and Sensor Networks.

[8] D. Liu, P. Ning, and W. L. Du. *Group-based Key Pre-distribution in Wireless Sensor Networks*, Proc. ACM Workshop on Wireless Security, 2005.

[9] D. Liu, P. Ning, and K. Sun. *Efficient Self-Healing Group Key Distribution with revocation Capability*, Proc. ACM Conference on Computer and Communication Security, CCS'03, 2003.

[10] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. *SPINS: Security Protocols for Sensor Networks*, Wireless Networks Journal (WINE), September 2002.

[11] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin, D. Dean. *Self-healing Key Distribution with Revocation*, Proc. IEEE Symposium on Security and Privacy, S&P'02, pp. 241-257, 2002.

[12] C. K. Wong, M. G. Gouda, and S. S. Lam. *Secure group communications using key graphs*. In Proceedings of the ACM SIGCOMM '98 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pages 68.79, 1998.

[13] C. K. Wong and S. S. Lam. Keystone: *A group key management service*. In International Conference on Telecommunications, ICT 2000, 2000.