A New Group Key Management Protocol for WSN

Tegshbayar Gerelbayar** · Sang Min Lee** · Jong Sou Park**

ABSTRACT

Sensor networks have a wide spectrum of military and civil applications, particularly with respect to security and secure keys for encryption and authentication. This thesis presents a new centralized approach which focuses on the group key distribution with revocation capability for Wireless Sensor Networks. We propose a new personal key share distribution. When utilized, this approach proves to be secure against k-number of illegitimate colluding nodes. In contrast to related approaches, our scheme can overcome the security shortcomings while keeping the small overhead requirements per node. It will be shown that our scheme is unconditionally secure and achieves both forward secrecy and backward secrecy. The analysis is demonstrated in terms of communication and storage overheads.

Key words : WSN, Key Management

* 이 논문은 2006년도 한국항공대학교 교비지원 연구비에 의하여 지원된 연구의 결과임.
** 한국항공대학교 컴퓨터공학과

1. Introduction

A wireless sensor network (WSN) consists of many sensor nodes that are small and have limited computation and communication capabilities. When sensor networks are deployed in a hostile environment, security becomes extremely important, as they are prone to different types of malicious attacks. For example, an adversary can easily listen to the traffic, impersonate one of the network nodes, or intentionally provide misleading information to other nodes. To provide security, communication should be encrypted and authenticated. The open problem is how to bootstrap secure communications between nodes. In other words, the difficulty lies in how to setup secret keys between communication nodes.

Several key distribution approaches proposed to address WSN security problem appeared in [1]. In most cases, key pre-distribution schemes consider key pre-distribution itself and are focused on handling the pairwise key issue. In LEAP [5], Zhu et al. observed that a WSN requires different types of security mechanisms due to different types of messages exchanged between sensor nodes. Thus, a single key management mechanism is not suitable for meeting different types of security requirements. In LEAP, they use four types of keys – an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with immediate neighboring nodes, and a group key that is shared by all the nodes in the network.

In a WSN, a group key is used for a group header (GH) to encrypt messages to broadcast to the whole group of sensor nodes. For instance, a GH can be used to send queries and issues missions. When compromised nodes are detected, we need to revoke those nodes and update the group key since the group key is shared by all of the member nodes.

Although LEAP is very efficient in terms of communication costs, it is possible to compromise all of the group session keys once the general key K_i is compromised since every node uses K_i and one-way hash function to generate its next session group key.

Zhu et al. proposed GKMPAN, a centralized Group Rekey Scheme [4] that employs probabilistic key predistribution to provide secure channels and $\mu TESLA$ [9] for broadcast authentication. Since it uses probabilistic key predistribution, the coalition of the revoked nodes may possess keys that completely cover the key set of a non-revoked node. Also $\mu TESLA$ requires loosely time synchronization from all the nodes and the key server. Moreover, a legitimate node can be excluded from the network innocently due to the discarding of compromised keys which were used to establish logical paths to other nodes to obtain new group key.

In this paper, we propose a new group key management protocol for Wireless Sensor Networks. Our scheme is derived from a self-healing group key distribution scheme as proposed by Liu et al's work in [6]. The difference between our scheme and Liu's scheme is ① Liu's scheme has additional elements in broadcast message and in scheme for a self-healing property to address group key distribution in highly mobile, volatile and hostile wireless networks such as Mobile Ad-Hoc networks, ② We generate group keys by using the encryption function $K_j = E_C(K_{j-1})$ according to a random number $C \in F_q$. Our scheme

also does not allow k-revoked users to learn current session keys and has the property of being unconditionally secure.

The rest of the paper is organized as follows. Section 2 presents our contributions, notations and model to be used in this paper. In Section 3, we provide the definitions which are used to further clarify that our protocol is information theoretically (unconditionally) secure. Section 4 describes the detailed approach for group key management. We provide the analysis of both security and efficiency and discussions in Section 5. Finally, we conclude in Section 6.

2. Contributions, Notations, Model

2.1 Our contributions

In this paper, our contribution considers group key distribution protocol that distributes secure session keys with revocation capability for Wireless Sensor Network.

Through this paper, our main contributions are the following:

① Provide scalable, robust, unconditionally secure, novel framework for group key management that has k-revocation capability and no session limitation.

② Analyze and provide mathematical model of our protocol's performance.

③ Provide a security analysis within an appropriate security framework for group key management system.

2.2 Notations

We concentrate n fixed users$\ U=\{U_1,\cdots,U_n\}$ and each group member is uniquely identified by an ID number i, where $i\in\{1,\cdots,n\}$ and n is the largest ID number. Each group member stores a personal secret $S_i\in F_q$. All of our operations take place in a finite field F_q of size q, where q is a large prime number. We use $H(\bullet)$ to denote the entropy function of information theory [7]. We use K_j to denote the session key that the GH broadcasts to the group members in session j. We use $E_c(\bullet)$ to denote an encryption function over a finite field F_q.

We use M_j to denote the broadcast message by the GH in the session j. We use $Z_{i,j}$ to denote what the member U_i learns through its own personal secret S_i and broadcasted message M_j by the GH. We use the letter k to represent the number of compromised group members that may collude together.

2.3 Our model

- ***Communication model*** : Since Wireless Sensor Networks are often organized as hierarchical cluster architecture, we adopt a simplified group communication model for the communication within one cluster. We assume there are one or several group headers(GH) that are responsible for handling group keys to a large number of legitimate group members. Group headers have both strong computation and communication capabilities, and they also employ tamper resistant techniques. The lifetime of a wireless network is partitioned into time intervals called *sessions*. The duration of sessions may be fixed or dynamic due to the change of network situation. Only legitimate group members that have valid group

keys (session keys) can either access encrypted broadcast messages or broadcast authenticated messages to other group members. Our goal is to ensure that the group header can distribute session keys to members if and only if the group members can get a broadcast message.

- ***Attacker model*** : We assume an attacker may compromise one or more sensor nodes. Also, an attacker can analyze devices and learn stored key materials. Having access to legitimate keys, the attacker can launch attacks without easily being detected. Of course, there is no such attacker have unlimited capabilities. There is some cost associated with capturing, reverse-engineering, and controlling a node. Therefore, we should assume that the adversary can compromise only a limited number of sensor nodes. Under this assumption, our goal is to ensure that once compromised nodes have been detected, such group members will be revoked from the group, and our approach has to tolerate up to k-illegitimate colluding nodes.

3. Definitions for Security Properties

Security properties of a group key management system have been considered in the past [11, 12]. These security properties consist of

① Group key secrecy, which guarantees that it is at least computationally infeasible for an adversary to discover any group key,

② Forward secrecy, which guarantees that a passive adversary who knows a contiguous subset of old group keys cannot discover subsequent group keys,

③ Backward secrecy, which guarantees that a passive adversary who knows a contiguous subset of group keys cannot discover preceding group keys, and

④ Key independence, which is the combination of forward and backward secrecy.

However, they are not sufficient in our framework, since each group member also has access to some secret information (i.e., S_i for U_i), which is used to compute the group keys. In particular, forward secrecy does not imply that the adversary cannot discover the subsequent group keys if he/she further has the secret information only known to some past group members, and backward secrecy does not guarantee that the adversary cannot discover the preceding group keys if he/she is further provided the secret information only known to some new group members. To clarify these requirements, we recall the notions of k-wise forward and backward secrecy} in [6].

Definition : Session Key Distribution with k-wise forward secrecy and k-wise backward secrecy. Let $k, i \in 1, \cdots, \mathrm{n}$ and $j \in 1, \cdots, \mathrm{m}$.

① A key distribution scheme D guarantees k-wise forward secrecy if for any set $R \subseteq \mathrm{U}_1, \cdots, U_n$, where $|R| \leq k$, and all $U_r \in R$ are revoked before session j, the members in R together cannot get any information about K_j, even with the knowledge of group keys before session j. i.e.,

$$H(K_j | M_1, \cdots, M_m, \mathrm{S}_{\mathrm{r}\,\mathrm{U}_r \in \mathrm{R}}, \mathrm{K}_1, \cdots, \mathrm{K}_{\mathrm{j}-1}) = \mathrm{H}(\mathrm{K}_\mathrm{j}).$$

② A key distribution scheme D guarantees k-wise backward secrecy if for any set $J \subseteq U_1, \cdots, U_n$, where $|J| \leq k$, and all $U_r \in R$ join after session j, the members in J together cannot get any information about K_j, even with the knowledge of group keys after session j. i.e.,

$$H(K_j | M_1, \cdots, M_m, S_{rU_r \in J}, K_{j+1}, \cdots, K_m) = H(K_j).$$

Note that k-wise forward (backward) secrecy implies forward (backward) secrecy. Thus, ensuring k-wise forward and backward secrecy guarantees forward and backward secrecy, key independence, and group key secrecy. Moreover, it is easy to see that k-wise forward secrecy also implies k-revocation capability.

4. Group Key Management Protocol

- ***Protocol Overview*** : This chapter presents a novel group key distribution techniques for large and dynamic groups. The techniques proposed here are based on the personal key share distribution methods (with revocation capability) proposed by Liu et al. [6]. By applying a keyed permutation and random one-way permutation, out approach overcomes the session limitation in previous work [6]. Moreover, our technique is scalable to very large groups since the storage and communication overhead does not depend on the size of the group, instead they depend on the number of compromised group members that may collude together. All these results are achieved without sacrificing the unconditional security of group key distribution.

4.1 Setup

The GH randomly picks a t-degree bivariate polynomial $g(x, y) = a_{0,0} + a_{1,0}x + a_{0,1}y + \ldots + a_{t,t}x^t y^t$ and a random initial session identifier sid_0 from $F_q[x, y]$. Each group member U_i receives the personal secret, the t-degree polynomial $g(i, y)$ and sid_0 from the GH via the secure communication channel between them. We employ Public Key Cryptography such as TinyECC [10] for establishing secure communication channels rather than probabilistic key-predistribution approaches [4] due to the perfect resiliency of Public Key Cryptography (PKC) and the result of recent studies that the computation overhead of PKC is no longer a significant problem in a WSN [8]. The GH selects randomly a prime key $K_0 \in F_q$ as a group key generating key and keeps it.

4.2 Broadcast

Let $R_j = U_{r_1}, U_{r_2}, \cdots, U_{r_{w_j}}, |R_j| \leq k$ be the set of all revoked members where k is the maximum number of colluding group members for sessions in and before j.

In the j-th ($j > 1$) session key distribution and revocation, the GH computes its j-th session identifier $sid_j = f(sid_{j-1})$ and the next session key $K_j = E_C(K_{j-1})$ according to a randomly chosen number $C_j \in F_q$. Then the GH broadcasts the following message

$$M_j = R_j \bigcup \Gamma_j(x) = \rho_j(x) K_j + g(x, sid_j)$$

where

$$\rho_j(x) = (x - r_1)(x - r_2) \cdots (x - r_{w_j}).$$

Here the polynomial $\rho_j(x)$ is called revocation polynomial and $g(x, sid_j)$ performs the role of masking polynomial. Note that each user $U_i \in U$ knows a single point, namely $g(i, sid_j)$ on the polynomial $g(x, sid_j)$.

4.3 Group Key Recovery

When a non-revoked member U_i receives the j-th session key distribution and revocation message M_j, it first computes the session identifier $sid_j = f(sid_{j-1})$.

Then it evaluates $\Gamma_j(x)$, $\rho_j(x)$, and $g(x, sid_j)$ at point i, and then computes the new session key $K_j = \frac{\Gamma_j(i) - g(i, sid_j)}{\rho_j(i)}$. Revoked members can not recover the new group key since the denominator vanishes when $\rho_j(i') = 0$ for some $U_{i'} \in R_j$.

4.4 Add group members

When the GH adds a group member starting from session j, it distributes the personal secret $g(v, y)$ and sid_j to the new user U_v via the secure communication channel between them.

5. Analysis

5.1 Security Analysis

The security property of the our protocol can be stated by Theorem 1.

Theorem 1 : *The protocol presented in Chapter 4 is an unconditionally secure, session key distribution scheme with k-revocation capability and $\log q$-bit privacy.*

Proof :

① ⓐ j-th session key recovery in member U_i is described in step 3 in our protocol. Thus

$$H(K_j | M_j, S_i) = H(K_j | Z_{i,j}) = 0.$$

ⓑ Let's assume a collection R of k-revoked users collude in session j. The coalition of R only has at most k-points on $g(x, sid_j)$. Since legitimate user U_i's personal secret $S_i = g(i, sid_j)$ is a point over a t-degree polynomial, it is impossible for coalition R to learn $g(i, sid_j)$. Thus,

$$H(S_i | \mathrm{S}_{\mathrm{r}U_r \in \mathrm{R}}, \mathrm{M}_1, \cdots, \mathrm{M}_{\mathrm{m}}) = H(g(i, sid_j) | \mathrm{g}(\mathrm{r}, \mathrm{sid}_{\mathrm{j}})_{U_r \in \mathrm{R}}, \mathrm{M}_1, \cdots, \mathrm{M}_{\mathrm{m}})$$

Since U_i's personal secret is an element of F_q, we have $H(g(i, sid_j)) = \log q$. Thus,

$$\begin{aligned} H(S_i | \mathrm{S}_{\mathrm{r}U_r \in \mathrm{R}}, \mathrm{M}_1, \cdots, \mathrm{M}_{\mathrm{m}}) &= H(g(i, sid_j) | \mathrm{g}(\mathrm{r}, \mathrm{sid}_{\mathrm{j}})_{U_r \in \mathrm{R}}, \mathrm{M}_1, \cdots, \mathrm{M}_{\mathrm{m}}) \\ &= H(g(i, sid_j)) \\ &= \log q. \end{aligned}$$

ⓒ Since the K_j is generated by the previous session key K_{j-1} and random number C, $Z_{i,j} = \mathrm{K_j}$ cannot be determined by either a broadcast message M_j or personal key S_i. It follows that

$$\begin{aligned} H(Z_{i,j} | M_1, \cdots, M_m) &= H(Z_{i,j}) \\ &= H(Z_{i,j} | S_1, \cdots, S_n). \end{aligned}$$

② (k-revocation property). Let's assume that a collection R if k-revoked users collude in session j. The colluding members only have at most k-points on the polynomial $g(x, sid_j)$. Hence the coalition R cannot recover the t-degree polynomial $g(x, sid_j)$. Also K_j is generated by the previous session key K_{j-1} and random number $C \in F_q$, the j-th session key K_j is completely safe. Hence,

$$H(K_j | C_j, S_j) = 0$$
$$H(K_j | M_1, \cdots, M_j, \mathrm{S}_{\mathrm{r}\mathrm{U}_r \in \mathrm{R}}) = \mathrm{H}(\mathrm{K}_\mathrm{j}).$$

Theorem 2 : *The protocol presented in Chapter 4 has the properties of k-wise forward secrecy and k-wise backward secrecy.*

Proof :

① (k-wise forward secrecy) Let's assume a coalition R, where $|R| \leq k$ users were revoked before the current session j.
Since at least $k+1$ points are needed on the polynomial $g(x, sid_j)$ to recover the current session key K_{j} for any user $U_r \in R$ and R has no information about K_j by Theorem 1.c, the session key K_j still appears to be random for the coalition R. Hence,

$$H(K_j | M_1, \cdots, M_m, \mathrm{S}_{\mathrm{r}\mathrm{U}_r \in \mathrm{R}}, \mathrm{K}_1, \cdots, \mathrm{K}_\mathrm{j}) = \mathrm{H}(\mathrm{K}_\mathrm{j}).$$

② (k-wise backward secrecy) Let's assume a coalition J, where $|J| \leq k$ and all users $U_r \in J$ join after the current session j. The coalition J can not get any information about any previous session key K_{j1} for $j_1 \leq j$ even with the knowledge of group keys after session j. This is because of the fact that in order to know K_{j1}, $U_l \in J$ requires the knowledge of at least $k+1$ points on the polynomial $g(x, sid_j)$ and also the knowledge of the session identifier sid_{j1}. Now when a new member U_v joins the group starting from session $j+1$, the GH gives the new member a new t-degree polynomial $g(v, y)$ as its personal secret and the $j+1$-th session identifier sid_{j+1}. Note that $sid_{j+1} = f(sid_j)$, where f is a random one-way permutation. Hence the newly joint member can not trace back for previous session identifiers sid_{j1} for $j1 \leq j$ because of the one-way property of the function f. Also the coalition J knows only k points on $g(x, sid_j)$ and thus can not compute $g(x, sid_j)$. Hence our protocol is k-wise backward secure and we have

$$H(K_j | M_1, \cdots, M_m, \mathrm{S}_{\mathrm{r}\mathrm{U}_r \in \mathrm{J}}, \mathrm{K}_{\mathrm{j}+1}, \cdots, \mathrm{K}_\mathrm{m}) = \mathrm{H}(\mathrm{K}_\mathrm{j}).$$

5.2 Cost Analysis

- ***Storage overhead*** : The storage requirement in our scheme comes from Setup phase and after receiving the session key distribution message. Each member needs to store a session identifier sid_j and a t-degree polynomial as its personal secret. In the Setup phase, each user stores the initial session identifier sid_0 and a t-degree polynomial as its personal secret key (e.g. $g(i, y)$ for user U_i). After receiving the

broadcast message M_j, each user stores the j-th session identifier sid_j. Each of these elements belongs to F_q. Thus, the total overhead of storage should be $(t+1)\log q$. Moreover, the personal key is reused to next m sessions without any alteration and the maximum session number (m) is no longer needed to be determined in Setup phase.

Consequently, our scheme eliminates the limitations of m sessions in previous work [6].

- ***Communication overhead :*** In each session, the broadcast message consists of a set of ID(s) of revoked users R_j, and coefficients of one t-degree polynomial $\Gamma_j(x)$. Thus, the size of the broadcast M_j in session j is $(k+t)\log q$.

5.3 Comparison with Related works

Following Table presents a comparative summary of our proposed scheme with the related approaches by comparing their storage overhead and communication complexity.

〈Table 1〉 Comparison of Cost

Schemes	Communication	Storage
Liu et al.'s work	$((2m+1)t+m+k)$ $*\log q$	$3m\log q$
GKMPSN	$(k+2)\log q$	$(l+2)\log q$
Our work	$(k+t)\log q$	$(t+1)\log q$

Liu et al. [6] generalized the definition for self-healing group key distribution scheme and provided some constructions by introducing a novel personal key distribution technique. However their scheme could not be efficient in resource-limited sensor network due to its higher cost and self-healing feature that undesirable in sensor network.

Zhu et al. proposed GKMPSN [4] that employs probabilistic key predistribution to provide secure channels. Thus, before deployment, we need to store l distinct keys for delivering group key in GKMPSN. Storage and communication overhead of such scheme looks pretty good, however, the coalition of the revoked nodes may possess keys that completely cover the key set of a non-revoked node since it uses probabilistic key predistribution. That means within the number of compromised nodes, this scheme could not offer the desired security level for sensor network.

Group rekeying in LEAP proposed by Zhu et al. [5] is extremely efficient because, on average, every node only transmits one key. Besides, due to its too simple design of protocol, it is easy to attack such networks for intruders.

6. Conclusion

We have introduced a novel centralized group key distribution and revocation protocol for Wireless Sensor Networks that consists of scalable large groups of resource-constrained sensor nodes deployed in unattended and harsh areas. In contrast to related studies, our proposed approach can overcome security problems by its unconditional security property and can tolerate k-colluding illegitimate nodes since it achieves both forward secrecy and backward secrecy. Moreover, our group key management mechanism is

scalable since communication and storage overheads do not depend on the number of members of the group. In contrast to the previous constructions, the personal key of a user can be reused to next m sessions without any alteration in our proposed scheme, thus eliminating the limitations of m sessions in the Setup phase. The protocol is properly analyzed in an appropriate security model to prove that it is unconditionally secure and achieves both forward secrecy and backward secrecy. We believe our approach can improve the practicality of group key distribution and revocation schemes for wireless sensor networks.

References

[1] S. A. Camtepe and B. Yener, Key Distribution Mechanisms for Wireless Sensor Networks : a Survey, RPI Technical Report TR-05-07, March 2005.

[2] A. Shamir, How to share a secret. Communications of the ACM, Vol. 22, pp. 612-613, 1979

[3] S. Zhu, S. Setia, S. Xu, and S. Jajodia, GK MPAN : An Efficient Group Key Management Protocol for Secure Multicast in Ad-Hoc Networks, In Proceedings of the 1st International Conference on Mobile and Ubiquitous Systems(Mobiquitous 2004), Boston, MA, 2004.

[4] S. Zhu and W. Zhang, Group Key management in Sensor network, Security in sensor network, Auerbach Publications, pp. 91-102, 2007.

[5] S. Zhu, S. Setia, and S. Jajodia, LEAP : Efficient security mechanisms for large-scale distributed sensor networks,. In 10-th ACM Conference on Computer and Communications Security (CCS 2003), 2003.

[6] D. Liu, P. Ning, and K. Sun, Efficient self-healing group key distribution with revocation capability, ACM CCS, pp. 231-240, 2003.

[7] R. Douglas, Stinson : Cryptography-Theory and Practice, Shannon's Theory, (Chapman and Hall/CRC, 2006), pp. 45-70, 2006.

[8] David Wagner, The Conventional Wisdom About Sensor Network Security, http://www.cs.berkeley.edu/daw/talks/sens-oak05.pdf, Accessed Dec. 2007.

[9] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar : SPINS : Security protocol for Sensor Networks, ACM-MobiCom, 2001.

[10] D. J. Malan, A. Welsh, and M. D. Smith, A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Crypt., IEEE SECON, pp. 71-80, 2004.

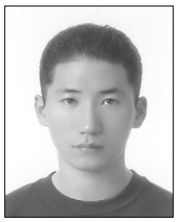
[11] A. Perrig, D. Song, and, J. D. Tygar, ELK, a new protocol for efficient large-group key distribution, In Proc. of IEEE Symp. on Security and Privacy, pp. 247-262, 2001.

[12] M. Steiner, G. Tsudik, and M. Waidner, Key agreement in dynamic peer groups, IEEE Trans. on Parallel and Distributed Systems, Vol. 11, No. 8, pp. 769-780, August 2000.

Tegshbayar Gerelbayar

2002년 한국항공대학교 컴퓨터공학과 (공학사)

2008년 한국항공대학교 컴퓨터공학과 (공학석사)



이 상 민

2005년 한국항공대학교 항공통신정보공공학과 (공학사)
2007년 한국항공대학교 컴퓨터 공학과 (공학석사)
2007년～현재 한국항공대학교 컴퓨터공학 박사과정

박 종 서

1983년 한국항공대학교 항공통신학과 (공학사)
1986년 노스캐롤라이나대학 전기컴퓨터공학과 (공학석사)
1994년 펜실베니아주립대학교 컴퓨터공학부 (공학박사)
1994년～1996년 펜실베니아주립대학교 컴퓨터공학과 조교수
1996년～현재 한국항공대학교 컴퓨터공학과 교수