State-Based Key Management Scheme for Wireless Sensor Networks

Jaemin Park, Zeen Kim, and Kwangjo Kim
International Research center for Information Security (IRIS)
Information and Communications University (ICU),
119, Munjiro, Yuseong-gu, Daejeon, 305-732, Korea
Email: {jaeminpark, zeenkim, kkj}@icu.ac.kr

***Abstract*— In wireless sensor networks, the random key pre-distribution arises as the practical solution for sharing common keys between sensor nodes. Since sensor networks suffer from the resource constraints like limited memory space, key pre-distribution scheme should require less memory space as possible while supporting strong security strength, *i.e.*, high resilience against node capture. However, the existing schemes still require a large number of keys for each sensor to carry. Although location information is facilitated as deployment knowledge for improvement, if two sensor nodes closely located each other have very low probability to be in active-state at the same time, unnecessary key assignments can be happened since keys shared only between them may be hardly used. In this paper, we propose a novel random key pre-distribution scheme that exploits new deployment knowledge, *state of sensors*, to avoid unnecessary key assignments and reduce the number of required keys that each sensor node should carry while supporting higher connectivity and better resilience against node captures. The analysis of our proposed scheme shows the better performance and security strength than the previous schemes.**

I. Introduction

A Wireless Sensor Network (WSN) usually consists of a large number of tiny sensors with limited computation capacity, memory space and power resource. Typically, WSNs are deployed at high density in regions requiring surveillance and monitoring. In military applications, sensors may be deployed in unattended or hostile environments such as battlefields. WSNs are, therefore, vulnerable to various kinds of malicious attacks like eavesdropping, masquerading, traffic-analysis, *etc*. Hence, it is important to protect communications among sensors to maintain message confidentiality and integrity. Recent research shows that secret key pre-distribution for symmetric encryption is one of the practical approaches for establishing secure channels among sensors since the low-power sensors have very limited computational capacity which excludes the applicability of public key cryptosystems.

Recently, many random key pre-distribution schemes [2]–[7] have been proposed. Random key pre-distribution is first proposed by Eschenauer *et al.* [2]. In this scheme, each sensor stores a random subset of keys from a large key pool before deployment. Any of two sensors that can find common keys within their key subsets can use those shared keys for secure communication. Chan *et al.* [3] extended this scheme to enhance the security and resilience of the network using q-compositeness. Du *et al.* [5] and Liu *et al.* [7] further extended random key pre-distribution approach to pairwise key pre-distribution approach in which the shared key between any two sensors is uniquely computed so that the resilience against node capture is significantly improved. However, these schemes still require each sensor to be loaded with a large number of keys for large scale WSNs. Although location information is facilitated as deployment knowledge for improvement [4], [6], if two sensor nodes closely located each other have very low probability to be in active-state at the same time, unnecessary key assignments can be happened since keys shared only between them may be hardly exploited.

To address these problems, we propose a novel approach for random key pre-distribution that exploits new deployment knowledge, *state of sensors*. By facilitating new deployment knowledge, we can reduce the number of required keys that each sensor should carry compared to the previous works [2], [6] while supporting higher connectivity and better security strength.

This paper is organized as follows: In Section 2, we briefly introduce the existing key pre-distribution schemes and their drawbacks. We propose our scheme in Section 3 and analyze our proposed scheme in Section 4. Finally, we conclude our paper in Section 5.

II. Related Works

After Eschenauer *et al.* [2] introduced the first random key pre-distribution scheme, Chan *et al.* [3] proposed the extended scheme which achieves the higher connectivity and better security strength. Du *et al.* [5] and Liu *et al.* [7] further extended random key pre-distribution approach to pairwise key pre-distribution approach to improve the resilience against node capture. However, these schemes still require each sensor node to be loaded with a large number of keys for large scale WSNs. For instance, to implement the random key pre-distribution schemes proposed in [2], [3] for a WSN of size 10,000, at least 200 keys are required for each sensor, which is almost half of the available memory (assume 64-bit keys and less than 4KB data memory [1]).

For improvement, several key pre-distribution schemes [4], [6] that exploits certain deployment knowledge such as location are proposed. Using this deployment knowledge, the

This work was supported by a grant No.R12-2003-004-00015-0 from Ministry of Commerce, Industry and Energy

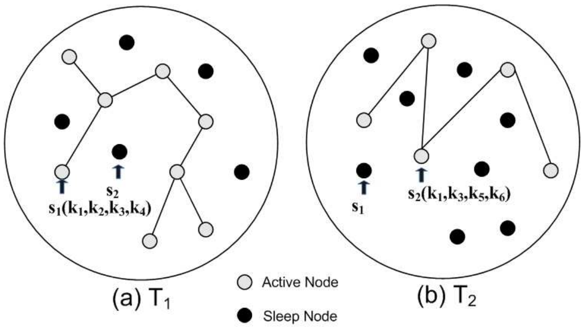

Fig. 1. Example of Unnecessary Key Assignments in WSNs

schemes can improve the connectivity and security strength. However, although a WSN is deployed via random scattering (*e.g.*, from an airplane) in the group-manner [6], actually it's difficult that the schemes know beforehand which nodes will be within communication range of each other after deployment. Even if the nodes are deployed by hand, the large number of nodes involved makes it costly to pre-determine the location of every individual node in each group. What makes it worse, although the location is used as the deployment knowledge for enhancement, unnecessary key assignments can be happened. Since only *active* sensors participate in useful communication, keys only shared between sensors which have low probability to be in *active* at the same time can be unnecessary. Fig. 1 illustrates one example of unnecessary key assignment. Let s_i and k_j (with $i = 1, 2,$ $j = 1, 2, \cdots$)denote the sensor node and its pre-distributed symmetric keys, respectively. Let T_i denote the time-interval when sensor s_i is supposed to be in active-state with high probability. Two sensors, s_1 and s_2, are deployed closely, so they may share more keys as proposed in [6]. Suppose that s_1 and s_2 have key set $\{k_1, k_2, k_3, k_4\}$ and $\{k_1, k_3, k_5, k_6\}$, respectively. During T_1, s_1 are s_2 are in active-state and sleep-state, respectively. Then, as time goes by, s_1 and s_2 transit their states to sleep and active, respectively. If s_1 and s_2 are in *active* state at the same time with very low probability, the shared key only between them, $\{k_1,\ k_3\}$, may be hardly used. Therefore, the key assignments of these keys to s_1 and s_2 are unnecessary.

III. The Proposed Scheme

A. Notations and Terminologies

We utilize the following notations and terminologies for the convenience of description.

- *CDF*: Cumulative Distribution Function
- $F()$: The CDF of 1-D Gaussian function
- $\Phi()$: The CDF of 1-D Gaussian function with mean, $m = 0$ and deviation, $\rho = 1$
- *PDF*: Probability Density Function
- *Q-Function*: 1 - $\Phi()$
- *Global Key Pool*(GlP): A GlP S is a pool of random symmetric keys, from which a group key pool is generated. The cardinality of S equals to $|S|$.

TABLE I

Useful sleep states for WSNs

	StrongARM	Memory	Sensor, A/D	Radio
S_0	active	active	on	tx,rx
S_1	idle	sleep	on	rx
S_2	sleep	sleep	on	rx
S_3	sleep	sleep	on	off
S_4	sleep	sleep	off	off

- *Group Key Pool*(GrP): A GrP S_i is a subset of GlP for $i-$th group, from which a key ring is generated. The cardinality of S_i equals to $|S_G|$.
- *Key Ring*: A *key ring* $R_{i,j}$ is a subset of GrP, which is independently assigned to sensor i classified as the group j.The cardinality of $|R_{i,j}|$ equals to R.
- *Key-Sharing Graph*: Let V represent all the nodes in WSN. A *Key-Sharing GraphG*(V, E) is constructed in the following manner: For any two nodes i and j in V, there exists an edge between them if and only if (1) nodes i and j have at least one common key, and (2) nodes i and j can reach each other within the wireless transmission range, *i.e.*, in a single hop.

B. Modeling of Deployment Knowledge

1) Classification of State: In this paper, new deployment knowledge, *state of sensors*, is exploited for key predistribution. Before modeling of deployment knowledge, we need to classify the states of sensors. In general, several sleep states could be defined as shown in Table I [9].

In this paper, for simplicity, we consider two major operational states: *active* and *sleep*. In the sleep state, the lowest value of the node power is consumed; while being asleep, a sensor cannot interact with the external world like S_3 and S_4 in Table I. On the other hand, the sensors in active-state can interact with the external world with higher node power consumption.

2) Active-State Group: The probability that each sensor node transits to sleep-state can be diverse depending on the MAC(Media Access Control) protocol, sleep scheduling algorithm, events that sensors may receive, and other various unpredictable factors around WSNs. For real application of WSN, it's natural that sensors transit their states periodically with some probability. Especially, in the monitoring and surveillance, implementing sensor nodes to be in active-state at specific time-interval with high probability and sleep at most of other times for prolonging the lifetime of WSNs is efficient since the probability of each sensor's state is unpredictable. Therefore, in this paper, we assume that sensor nodes are implemented to be in active-state at specific time-intervals with high probability and in other time-intervals the probability is relatively low. Then, sensor nodes can be grouped by the time-intervals when they have high probabilities to be in active-state. For instance, if sensor s_1 has high probability to be in active-state at time-interval T_1, it may be grouped as the first group.

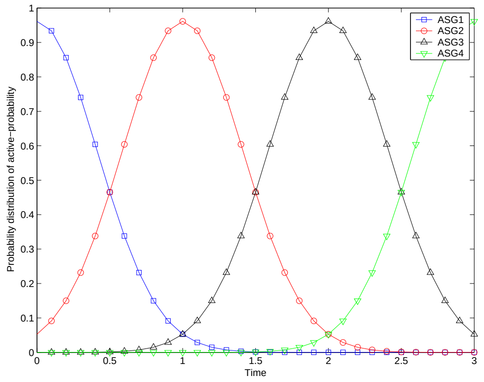

Fig. 2. Probability Distribution of active-probability for each ASG

Based on these assumptions, we define *Active-State Group*(ASG) G_i (i=1,2,3,$\cdots$) is the group of sensor nodes which have high probabilities to be in active-state at the same time-interval. In the actual operation of WSNs, the probability that each ASG is in active-state at given time-interval can be different depending on applications of WSNs, MAC protocols, sleep scheduling algorithms, *etc*. For simplicity, we call this probability as *active-probability* throughout this paper. We model the active-probability as a 1-D Gaussian distribution. Although we only use the Gaussian distribution, our proposed scheme also can be applied to other probability distributions. We denote the time when the active-probability is the highest at t_m^i for each group i. We also assume that $|t_m^i - t_m^{i+1}|$ is constant. Then, if sensor s in G_i has the highest probability to be in active-state around time t_m^i, the PDF of active-probability for sensor s in G_i is as follows:

$$\begin{aligned} f_k^i(t|k \in G_i) &= \frac{1}{\sqrt{2\pi}\rho} e^{-(t-t_m^i)^2/2\rho^2} \\ &= f(t - t_m^i) \end{aligned} \qquad (1)$$

where $f(t) = \frac{1}{\sqrt{2\pi}\rho} e^{-t^2/2\rho^2}$. Without loss of generality, we assume that the PDF for each group is identical except the value of t_m^i, so we use $f_k(t|k \in G_i)$ instead of $f_k^i(t|k \in G_i)$.

Fig. 2 depicts the probability distribution of active-probability of each ASG. We define that two ASGs are *time-neighbors* if their corresponding time-intervals are nearby regardless of their locations. That is, if one ASG is supposed to be in active-state with high probability during one time-interval, the other (time-neighbor) ASG can be in active-state during previous or next time-interval of the former one with high probability. We can find out that if one ASG has the highest active-probability at one time-interval, then it also has moderately high active-probability at nearby time-intervals. Therefore, two time-neighbor ASGs have high probabilities to be in active-state at the same time-interval with the moderate probability.

C. Assumptions and Security Threats

To use the state of sensors as the deployment knowledge, we assume that whole lifetime of WSN can be divided into many small time-intervals and each of them repeats periodically and there is no time-interval when all sensors are in sleep-state.

WSN is vulnerable to several security threats. In this paper, we consider two major security threats; node capture and eavesdropping. First, the attackers can monitor all communications between sensors due to the characteristics of radio broadcast signal. Second, attackers can easily capture node and analyze all information embedded in each sensor node.

D. Key Pre-Distribution Scheme

Using the deployment knowledge modeled in the previous section, we propose a new random key pre-distribution scheme that satisfies all above requirements. Our proposed key pre-distribution scheme consists of three phases: key pre-distribution phase, shared-key discovery, and path-key establishment. Because of adoption of new deployment knowledge, all phases for key pre-distribution are considerably different from Eschenauer *et al.* [2].

1) Key Pre-Distribution Phase: This phase is performed off-line and before the deployment of sensors. We assume that L groups are defined in the modeling of ASG. Key setup server generates a large GlP S, and divides it into L GrPs S_i for each ASG G_i. The purpose of setting up the GrP is to allow the time-neighbor ASGs to share more keys. We will describe the detail GrP setup step later. After completion of GrP setup, for each sensor j in the ASG G_i, randomly selected key ring $R_{j,i}$ from its corresponding GrP S_i is loaded into the memory of the sensors.

2) Shared-Key Discovery Phase: After deployment, the state of each sensor in each ASG transits depending on the sleep scheduling algorithm, events, and other variable unpredictable factors at each time-interval. For secure communication with active-state sensor node at given time-interval, each active-state sensor node first performs key-discovery to find out with which of other active-state sensor nodes they share a key. Such key discovery can be performed by assigning a short identifier to each key prior to deployment, and having each sensor node broadcast its set of identifiers. Sensor nodes which discover that they contain a shared key in their key rings can then verify other active-state sensor node actually holds the key through a challenge-response protocol. For enhancing security in challenge-response, encryption of each identifier on the sender and decryption on the receiver can be utilized. The shared key then becomes the key for that link. After above step, the entire sensor networks forms a key-sharing graph.

3) Path-Key Establishment Phase: Sensor nodes can set up path keys with sensor nodes in their vicinity that they did not happen to share keys with in their key rings. If the key-sharing graph is connected, a path can be found from a source sensor node to other active-state sensor nodes. The source node can then generate a path key and send it securely via a path to the target sensor node.

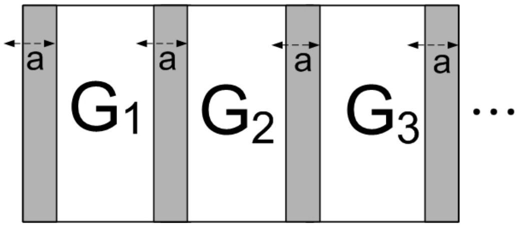

Fig. 3. Shared keys between nearby GrPs

E. Setting up GrPs

Since key assignments are determined by the active-probability, in some cases sensors may be in active-state even though they are not assumed to be. Therefore, sensors in one group should share some keys with sensors not only in same group but also in other groups. For this, some portion of each GrP should be overlapped with other GrPs. Since the active-probability of each group follows the Gaussian distribution, sensor nodes have moderately high probabilities to be in active-state at the previous and next time-interval. Therefore, to set up the GrPs, some keys are from the previous and next GrPs.

We will show how to assign keys to each GrP S_i such that GrPs of nearby time-intervals have a certain number of common keys. We assume that a, *overlapping factor*, determines the certain number of common keys between two nearby time-interval groups. In our scheme, one GrP shares exactly $a|S_G|$ with the previous and next time-interval GrPs($0 \leq a < 1$). To achieve this property, we divide the keys in each GrP into three partitions like illustrated in Fig. 3. Keys in each partition are those keys that are shared between corresponding nearby time-interval GrPs. For instance, in Fig. 3, the left partition of G_2 consists of $a|S_G|$ keys shared between G_1 and G_2.

Given the GlP S and overlapping factor a, we now describe how to select keys for each GrP. Since we use similar methodology used in [6], here we briefly describe the way to set up GrPs. First, keys for S_1 are selected from S; then remove selected $|S_G|$ keys from S. Then, for each S_i, select $a|S_G|$ keys from GrP S_{i-1}; then select $k = (1-a)|S_G|$ keys from S, and remove the selected k keys from S. After G_1 selects $a|S_G|$ keys from G_2, no other group can select any one of these keys. These procedures repeat until all GrPs are set up.

Now we calculate the number of keys in each GrP. Since keys selected from the other groups are all distinct, the sum of all the number of keys should be equal to the $|S|$. Therefore, we have the following equation:

$$|S_G| = \frac{|S|}{L - aL + a}$$

where L is the number of groups.

F. Sensor Deployment

After key pre-distributions has established, all sensor nodes are deployed in the real sensing field. Fig. 4 illustrates one example of sensor deployment. Sensor nodes from two ASGs are deployed to be able to cover all the area of real sensing field according to the existing coverage-concerned sensor-deployment strategies. Here, r indicates the radio coverage range of each sensor node. Since sensors are grouped based on the time-interval when they have high probability to be in active-state regardless of their locations, the coverage-problems in WSNs solely depend on the sensor-deployment strategies.

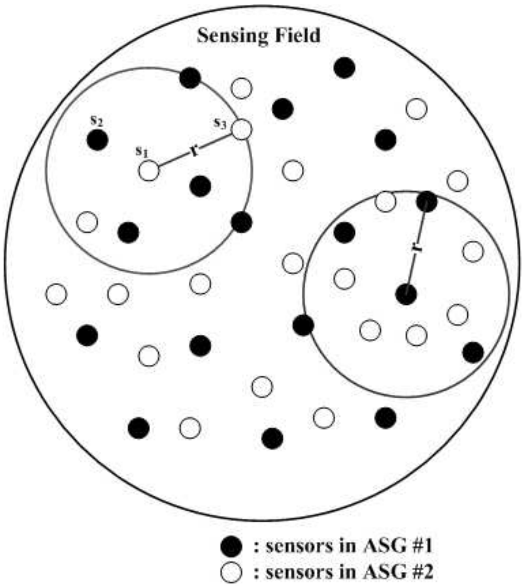

Fig. 4. Example of Sensor Deployment

IV. Performance Evaluation and Simulation

In this section, we analyze our proposed scheme in detail. For analysis, we adopt similar methods used in [6]. However, since we adopt new deployment knowledge different from [6], some parts are slightly different.

A. Evaluation Metrics

We evaluate our proposed scheme against following criteria that represent desirable characteristics in a key pre-distribution scheme for WSNs:

- *Low Memory Occupation*: To address the limited memory constraint, small number of keys should be promised while supporting same or higher level of security.
- *Higher Connectivity*: With smaller number of keys, the probability that two sensors share at least one common key at given time-interval should be higher.
- *Stronger Resilience Against Node Capture*: Sensors are easily captured by the adversaries. Once captured, they are analyzed and may reveal secret information to the attackers. The proposed scheme should be resilient against node capture.

B. Connectivity

We calculate p_s, the probability that two active-state sensors share at least one common key after deployment at given time-interval. Let A and B be the probabilistic event that two sensors are in active-state at given time-interval and the event that two sensors share at least one common key, respectively. Hence,

$$p_s = Pr[B|A] = \frac{Pr[B \cap A]}{Pr[A]}.$$

First, we will find out the probability that two sensor nodes are in active-state at given time-interval. For this, we need to consider two cases as follows:

- *Case 1*: Two sensors are in same group during key pre-distribution phase.That is, two sensors have high probabilities to be in active-state at the same time-interval.
- *Case 2*: Two sensors are in different group during key pre-distribution phase, and two groups are neighbors each other.

For each case, we can calculate the probability that two sensors are in active-state at given time-interval using (1). Suppose that time-interval T_i is given as $t_i \leq t \leq t_{i+1}$. Then, the active-probability of G_i at T_i can be found as follows:

$$\begin{aligned} h(T_i) &= F(t_{i+1}) - F(t_i) \\ &= \Phi\left(\frac{t_{i+1} - t_m^i}{\rho}\right) - \Phi\left(\frac{t_i - t_m^i}{\rho}\right) \\ &= Q\left(\frac{t_i - t_m^i}{\rho}\right) - Q\left(\frac{t_{i+1} - t_m^i}{\rho}\right) \end{aligned}$$

where i(=1,2,3, $\cdots$) is the index of the time-interval.

Then, we can define the probability that two sensors are in active-state for each case as follow:

$$H(i,j) = \begin{cases} h(T_i)^2, & \text{if } i = j \quad \text{(Case 1)} \\ h(T_i) \times h(T_{i+1}), & \text{if } i - j = 1 \quad \text{(Case 2)} \\ h(T_i) \times h(T_{i-1}), & \text{if } i - j = -1 \quad \text{(Case 2)} \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

Now, we need to calculate the probability that two sensors share at least one common key. This probability can be expressed as 1 - Pr[two sensors do not share any key]. Since the size of GrP is $|S_G|$, the number of keys shared between two GrPs is $\lambda|S_G|$, where λ is 1, a, or 0. According to the value of λ, we should consider three cases for finding the required probability; two sensors come from same group (λ=1), the neighbor two groups (λ=a), and the different groups which are not neighbor each other (λ=0).

We adopt the same overlapping key pool method used in [6], so here we just briefly introduce the procedures and equations for calculating the required probability. The first node selects i keys from the $\lambda|S_G|$ shared keys, it then selects the remaining $R-i$ keys from the non-shared keys. The second node selects R keys from the remaining ($|S_G| - i$) keys from its GrP. Therefore, $p(\lambda)$, the probability that two sensors share at least one key when their GrPs have $\lambda|S_G|$ keys in common, can be calculated as follow:

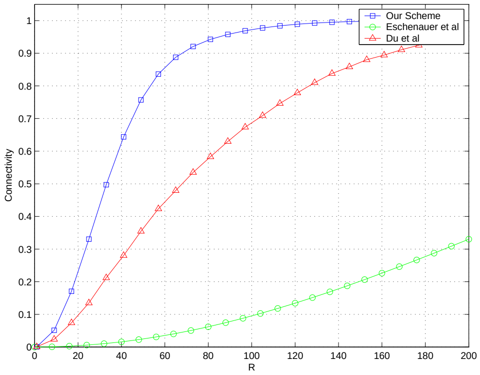

Fig. 5. Connectivity: Probability of sharing at least one key between two sensors

$$\begin{aligned} & p(\lambda) \\ &= 1 - Pr(\text{two sensors do not share any key}) \\ &= 1 - \frac{\sum_{i=0}^{min(R,\lambda|S_G|)} \binom{\lambda|S_G|}{i}\binom{(1-\lambda)|S_G|}{R-i}\binom{|S_G|-i}{R}}{\binom{|S_G|}{R}^2} \end{aligned} \tag{3}$$

Here, if $\lambda = 1$, the above equation can be reduced as $p(\lambda) = 1 - \frac{\binom{|S_G|-R}{R}}{\binom{|S_G|}{R}}$. If $\lambda = 0$, the required probability is simply zero, $p(\lambda) = 0$.

Finally, we can calculate p_s using (2) and (3). We define Ψ as the set of all groups in our scheme. Suppose that two sensors, s_i and s_j, are selected from G_i and G_j of Ψ. Since the event that two sensors share at least one common key is independent of the event that two sensors are in active-state at given time-interval, we can calculate the probability that s_i and s_j are in active-state at given time-interval, and two sensors share at least one common key using (2) and (3) as:

$$p(\lambda(i,j)) \cdot H(i,j) \tag{4}$$

where $\lambda(i,j)$ is defined as follow:

$$\lambda(i,j) = \begin{cases} 1, & \text{if } i = j \\ a, & \text{if } |i - j| = 1 \\ 0, & \text{otherwise} \end{cases}$$

Then, p_s is the average of the value in (4) for all groups, and can be calculated as follow:

$$p_s = \frac{\sum_{i\in\Psi}\sum_{j\in\Psi} H(i,j) \cdot p(\lambda(i,j))}{\sum_{i\in\Psi}\sum_{j\in\Psi} H(i,j)}$$

Fig. 5 illustrates the connectivity versus the number of keys each sensor carries under $|S|$ = 100,000, L = 100, and a = 0.25. We compare our proposed scheme with Eschenauer *et al.*'s scheme and Du *et al.*'s scheme. The proposed scheme offers the better performance improvement compared

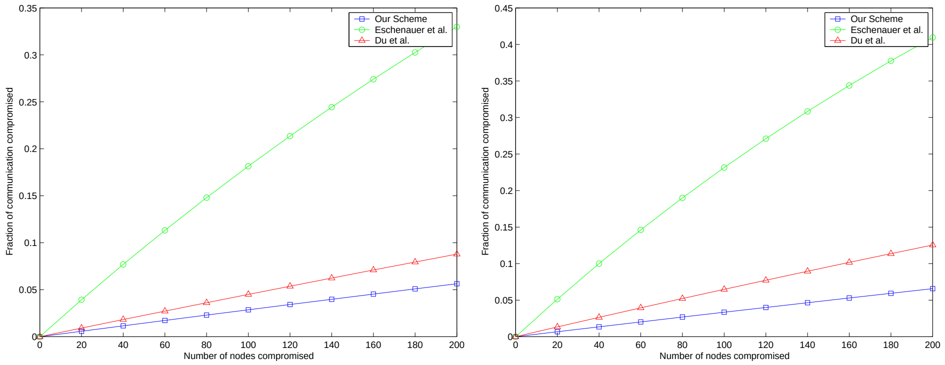

Fig. 6. Resilience Against Node Capture: left: p_s=0.33; right: p_s=0.50

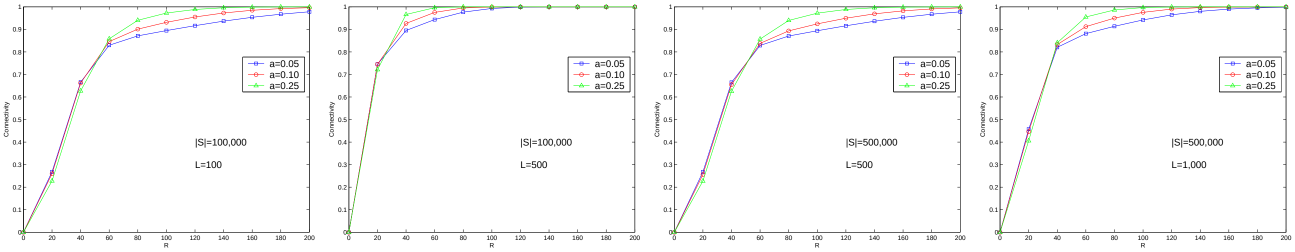

Fig. 7. p_s vs. a under different values of $|S|$ and L

to two schemes. To achieve the same probability, our proposed scheme requires much smaller number of keys.

C. Resilience against node capture

A scheme's resilience toward node capture is calculated by estimating the fraction of total network communications that are compromised by a capture of x-nodes not including the communications in which the compromised nodes are directly involved. To evaluate our key pre-distribution scheme against node capture, we apply the same method used in [6]. Note that the number of required keys that each sensor should carry is an important factor for evaluation of the scheme. In our scheme, we can reduce the number of keys that each sensor should store in its memory drastically compared to the previous schemes. In [6], the estimation of the expected fraction of total keys being compromised is calculated by

$$1 - (1 - \frac{R}{|S|})^x$$

where x is the number of compromised nodes.

Fig.6 illustrates the theoretical results. We compare our scheme with the existing random key pre-distribution schemes such as Eschenauer *et al.*'s scheme and Du *et al.*'s scheme. The figure shows that our proposed scheme lowers the fraction of compromised communication after x-nodes are compromised. The most important reason for this improvement is that, to achieve the same connectivity while using the same key pool size $|S|$, our proposed scheme only requires much smaller R keys. For instance, to achieve p_s = 0.33 under $|S|$ = 100,000, the Eschenauer *et al.*'scheme and Du *et al.*'s scheme require R = 200 and 46, respectively. However, our scheme only needs R = 25. In the case p_s = 0.50, the same improvement can be found. By adopting new deployment knowledge, we enable to reduce the number of unnecessary keys carried by each sensor node.

D. Memory Usage

As described in the previous section, our proposed scheme requires much smaller number of keys compared to the previous scheme. If we assume 64-bit keys and less than 4KB data memory of each sensor [1], for p_s=0.33, the memory occupation of our proposed scheme can be calculated as 5%. This percentage is much smaller than 9.2% (Du *et al.*'s scheme) and 40% (Eschenauer *et al.*'s scheme). In the similar way, for p_s=0.50, we also can verify that much less memory space is required in our proposed scheme.

E. Performance Analysis

To examine the performance of our proposed scheme depending on the various application scenarios, we vary the values of the parameters related to the connectivity. For instance, in the case of large scale WSNs, large size of GlP and many groups are required. In some scenarios, each group doesn't have to share keys with others. For all scenarios, higher connectivity should be guaranteed. Depending on the size of GlP $|S|$, the number of groups L, and the overlapping factor a, the connectivity is diverse. Fig. 7 shows the performance of our proposed scheme under the different parameters. By referring each figure, our proposed scheme requires only small number of keys for high connectivity on the various application scenarios.

V. Conclusion

In this paper, we propose a novel random key predistribution scheme that exploits new deployment knowledge, *state of sensors*. By facilitating this knowledge, we can make keys be shared with sensors which have high probabilities to be in active-state at the same time. Therefore, we can remove the unnecessary key assignments while achieving the higher connectivity with smaller number of keys compared to the previous schemes. Through this accomplishment, we can expect the save of large memory space for each sensor node and also improvement of resilience against node captures. We show the outstanding performance and security strength of our proposed scheme through the simulation.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments.

References

[1] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, “SPINS: Security Protocols for Sensor Networks”, *In Proceedings of the 7th Annual ACM International Conference on Mobile Computing and Networks (Mobicom 2001)*, Rome Italy, July 2001.

[2] Laurent Eschenauer and Virgil D. Gligor, “A key-management scheme for distributed sensor networks”, *Conference on Computer and Communications Security, Proceedings of the 9th ACM conference on Computer and Communications Security 2002*, Washington D.C., USA.

[3] H. Chan, A. Perrig, and D. Song, “Random Key Predistribution Schemes for Sensor Networks”, *IEEE Symposium on Research in Security and Privacy*, 2003.

[4] D. Liu and P. Ning, “Location-Based Pairwise Key Establishments for Relatively Static Sensor Networks”, *2003 ACM Workshop Security of Ad Hoc and Sensor Networks (SASN03)*, October 31, 2003 George W. Johnson Center at George Mason University, Fairfax, VA, USA.

[5] Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod Varshney, “A Pairwise Key Predistribution Scheme for Wireless Sensor Network”, *In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS)*, Washington D.C., October 27-31, 2003.

[6] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen, and Pramod Varshney, “A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge”, *IEEE INFOCOM 04*, March 7-11, 2004, Hong Kong.

[7] D. Liu and P. Ning, “Establishing Pairwise Keys in Distributed Sensor Networks”, *To appear in the 10th ACM Conference on Computer and Communications Security (CCS03)*, Washington D.C., October, 2003.

[8] D. W. Carman, P. S. Kruns, and B. J. Matt, “Constrains and approaches for distributed sensor network security”, *Technical report, NAI Labs*, 2000.

[9] Amit Sinha and Anantha P. Chandrakasan, “Operating System and Algorithmic Techniques for Energy Scalable Wireless Sensor Networks”, *Proceedings of 2nd International Conference Mobile Data Manage*, Hong-Kong, Jan 2001.

[10] A. Perrig, R. Canetti, D. Song, and D. Tygar, “Efficient authentication and signing of multicast streams over lossy channels”, *In Proceedings of IEEE Security and Privacy Symposium*, May 2000.

[11] A. Perrig, R. Canetti, D. Song, and D. Tygar, “The tesla broadcast authentication protocol”, *In RSA Cryptobytes*, 2002.

[12] Feng Zhao and Leonidas J. Guibas, “Wireless Sensor Networks: An Information Processing Approach”, *Elsevier Science & Technology Books*.

[13] C. S. Raghavendra, Krishina M. Sivalingam, and Taieb Znati, “Wireless Sensor Networks”, *Kluwer Academic Publishers*.

[14] M. Ilyas and I. Mahgoudb, “Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems”, *CRC Press*.