Location-Aware Key Management Using Multi-layer Grids for Wireless Sensor Networks

JongHyup Lee[1], Taekyoung Kwon[2], and Jooseok Song[1]

[1] Dept. of Computer Science,
Yonsei University, Seoul, 120-749, Korea
{jhlee, jssong}@emerald.yonsei.ac.kr
[2] Dept. of Computer Engineering,
Sejong University, Seoul, 143-747, Korea
tkwon@sejong.ac.kr*

Abstract. Since small low-powered sensor nodes are constrained in their computation, communication, and storage capabilities, it is not easy to achieve secure key establishment in a wireless sensor network where a number of such sensor nodes are spread over. There are many previous studies in the area of secure key establishment without public key cryptography for the wireless sensor networks. Among them, location-aware key management is a considerable approach for easy management and security enhancement. In this paper, we propose a new key establishment scheme by utilizing both the rough sensor location information and the multi-layer grids. As for the multi-layer grids, we devise an extended grid group which covers all nodes deployed in two adjacent basic grids and overlaps each other. With regard to communication and power consumption overhead, our approach shows better performance than the previously proposed schemes without losing its security.

1 Introduction

Sensor nodes are small low-powered devices which are constrained severely in their computation, communication, and storage capabilities. They may sense around themselves and communicate over wireless channels, but within very short ranges. A wireless sensor network is composed of a large number of sensor nodes for covering wider area through multi-hop connections, and has various kinds of applications including environmental monitoring, industrial monitoring, safety and security services, military system, health-care services, etc. The mission critical applications of wireless sensor networks make security and privacy functions required, while secure key establishment is the most fundamental part of them.

* This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

J. Zhou, M. Yung, and F. Bao (Eds.): ACNS 2006, LNCS 3989, pp. 390–404, 2006.

It is widely recognized that the secure key establishment is not easy for wireless sensor networks due to the limited capabilities of sensor nodes that restricts the use of public key cryptography. Another major obstacle to secure key establishment for wireless sensor networks is the high risk of physical attacks to sensor nodes which are deployed in unattended or even hostile environments. Thus, the key management schemes devised for the existing computer networks are not well-suited to the wireless sensor network, and the need for new schemes has arisen indefinitely. Note that symmetric key cryptography is preferred in the wireless sensor network unless there is a significant hardware improvement of the economically-viable sensor nodes in the near future.

Lately, a number of studies have been done in the area of secure key establishment without public key cryptography for the wireless sensor network [3, 4, 5, 6, 7]. Among them, we are interested in the location-aware key management schemes [6, 7]. Though exact positions of the sensor nodes cannot be controlled, it should be a reasonable attempt to partition a sensor deployment area into multiple square areas in a large dense wireless sensor network for easier management and security enhancement. There are three notable schemes in which the sensor location information is utilized for secure key establishment. They are based on the famous Blom scheme [1] and can be found from [3], [7], and [6]. However, two of them [3, 7] are vulnerable to selective node capture attacks allowing the key exposure of non-compromised nodes or introduce additional complexity owing to the uneven distribution of sensors within a given area. The other scheme [6] resists the so-called selective node capture attack and the node fabrication attack, but introduces new problems resulting from the heterogeneity of internal key establishment schemes. The heterogeneity may affect security as well as performance of the entire network. We will discuss this problem in more detail in the following section.

In this paper, we propose a new key establishment scheme utilizing the rough sensor location information but resolving the aforementioned problems. Following the Du-Deng scheme [3], we assume the whole deployment space is divided into multiple small areas, *grids*, where a group of sensor nodes are deployed. Our basic idea is to consider multi-layer grid groups where the grid implies a partitioned square area. As for the multi-layer grids, we devise an extended grid group which covers all nodes deployed in two adjacent basic grids and overlaps each other. In each grid, the key establishment scheme based on the Blom scheme is consistently operated. Our scheme improves the previous schemes in that the the amount of power consumption and communication overheads are reduced, the key connectivity in adjacent grids goes high significantly, and the node replication attack is defeated in the realm of an extended grid.

The rest of this paper is organized as follows. In Section 2, we introduce the heterogeneity problems arising from the grid-group deployment after reviewing the previous key management schemes briefly. In Section 3, we propose a new grid-group deployment scheme in which the aforementioned problems are resolved effectively. Key connectivity, area coverage, and security analysis are manipulated in Section 4, while the performance is evaluated in Section 5 with

regard to communication overhead, power consumption, and storage overhead. This paper is concluded in Section 6.

2 Background: Location-Aware Key Management Scheme

2.1 Key Management in Wireless Sensor Networks

There have been many studies in the area of key establishment without public key cryptography for wireless sensor networks, specifically for pairwise keys. They can be classified into two basic categories, one is a deterministic scheme such as LEAP [8], while the other a probabilistic scheme that includes a number of random-key schemes [5, 2]. Among them, we only focus on probabilistic schemes in this paper.

Random key pre-distribution. In [5], Eschenauer and Gligor proposed a random key pre-distribution scheme for wireless sensor networks. There are three main phases in this scheme. First, from a large random key pool, a random subset of keys are selected for each node. Second, after the deployment of sensor nodes, if two adjacent nodes have any common key in the respective sub-key pools, they can use it as a shared key and further establish a new pairwise key using the shared key. Third, for the case that those neighbors do not share the same sub-key in their pools, a path key establishment step is proceeded. The procedure has been a standard in the probabilistic key establishment scheme for wireless sensor networks.

Blom scheme with multiple spaces. In [4], Du et al. combines the Blom scheme [1] with the random key pre-distribution. The Blom scheme is actually a key matrix based scheme and guarantees any pair of nodes to compute a secret shared key in the whole key matrix. The multiple space scheme allows the key computation when nodes share at least one key space. As a result, the multiple key space can improve the scalability and the physical capture resistance of the original scheme.

Key graph. Each node could maintain its key graph , $G = (V, E)$, where V is the vertices set and E is the edges set. The set V consists of the neighbor nodes. When two nodes of V share a required number of keys, an edge between those nodes are added.

2.2 Grid-Group Deployment Scheme

In [6], Huang et al. proposed a grid-group deployment scheme that is one of the location-aware key pre-distribution schemes. In this scheme, the sensor deployment area are partitioned into grids. Then two different pre-distribution schemes are used for a single grid and adjacent grids, respectively. In a single grid, they use *I-scheme* in which the multi space Blom scheme is utilized,

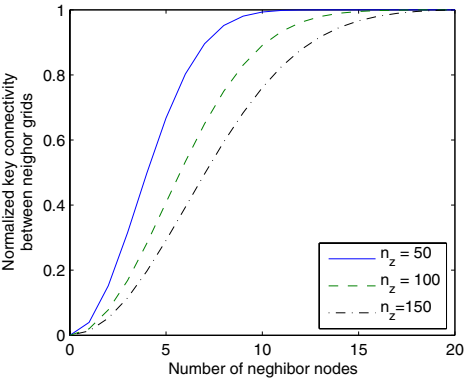

Fig. 1. Degradations of the normalized key connectivity

while *E-scheme* is used for adjacent grids. Note that those two schemes such as I-scheme and E-scheme are different. This disharmony causes the following heterogeneity problems. Readers are referred to [6] for the details of the grid-group deployment scheme.

2.3 Heterogeneity Problems

The grid-group deployment scheme [6] uses two different schemes for key pre-distribution, *I-scheme* based on the multi-space Blom scheme for nodes within the same grids and *E-scheme* based on the random key pre-distribution scheme for nodes between adjacent grids. Therefore, two phases are necessary for both key pre-distribution and key establishment. The key graph connectivity of *I-scheme* should depend on the number of selected key spaces while the total number of nodes in a grid, n_z, affects the key connectivity of *E-scheme*. Figure 1 depicts that, when n_z grows high (from 50 to 150), the key connectivity between adjacent grids (in Y-axis) decreases as the coverage area or communication range becomes smaller due to the number of neighboring nodes (in X-axis). The decrement appears more drastically than that of nodes within a single grid. This unbalanced key connectivity can make the *isolated grid* problem, saying that a node cannot connect with any of adjacent grids even it can communicate within the same grid, in the high n_z environments.

Additionally, since each node should maintain two types of keys for I and E schemes, and the key of each type is used independently to the other in [6], the reusability of keys are limited and two separate stages of key establishment for the same grid and adjacent grids are needed. This may cause needs for additional storage maintenance and extra control messages.

As for security, *I-scheme* and *E-scheme* do not provide the same degree. For example, if a node i located in an angular point of a grid is captured while its *E-scheme* pair j is located in the opposite side of the other diagonal grid, saying they may not detect each other, then the replicated node of i can be added to the diagonal grid of the grid of j by *E-scheme* in spite that *I-scheme* resists it.

This scenario shows the heterogeneity of key establishment affects security of the entire network as well as its performance.

3 Multi-layer Grid-Group Deployment Scheme

3.1 Basic Idea

We assume the deployment area of sensor nodes is divided into two-dimensional squares which called '*grids*'. Each grid has fixed size, $a \times a$ and the whole deployment area is covered by $N_G \times N_G$ squares. Figure 2 shows the grid structure for the sensor deployment. The groups of sensor nodes deployed in the grid located at i^{th} row and j^{th} column of the deployment area is named '*grid groups*' and denoted by $G(i, j)$. We assume sensor nodes are uniformly distributed over the deployment area. We set the total number of sensor node as N and each group has the same number of sensor nodes n_z.

In our scheme, we define an *extended grid group* for key predistribution and discovery. An extended group has twice size of a square, $a \times 2a$ or $2a \times a$. That is, one extended grid group covers two grid groups. Then, there are 4 overlaid layers of extended grid groups which overlap each other. This forms multilayer grids. Figure 3 and 4 depict the architecture of multilayer grid and the positioning of extended grid groups. Each extended grid group can be identified by a tuple, (*row*, *column*, *layer_number*) as shown in Fig 4. Then $EG(i_E, j_E, l)$ is an identifer for the extended grid group located in i_E^{th} row, j_E^{th} column and l^{th} layer.

The process for Multilayer Grid Group schemes is divided into 4 phases, *Key predistribution, Sensor deployment, Key discovery, Pairwise key establishment.* The detailed processes are described in following sections.

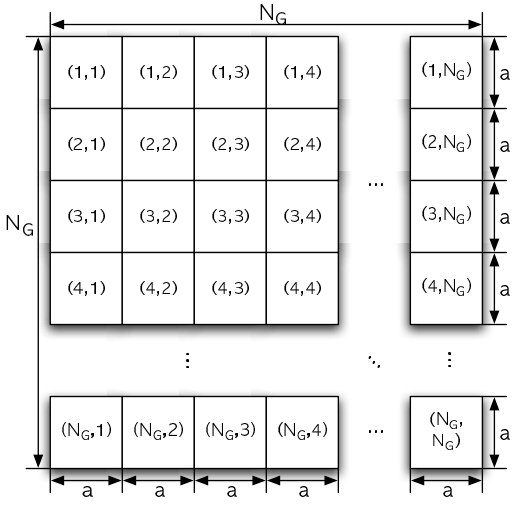

Fig. 2. Grid structure

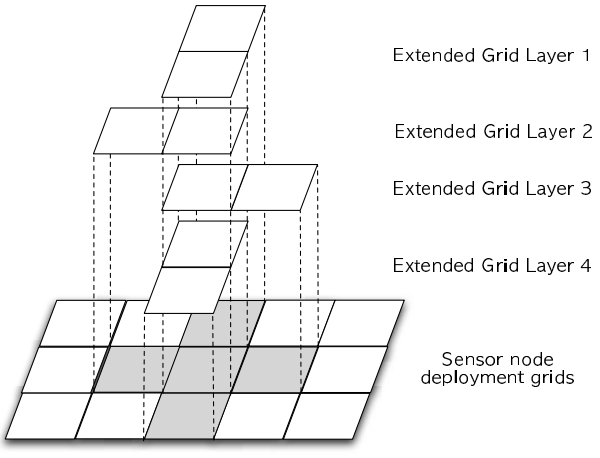

Fig. 3. Multi-layer grid

3.2 Key Predistribution

Before key-predistribution, some constraints are required to guarantee the security of multi-layer grid group scheme. Due to the λ-secure property of Blom scheme and multiple key spaces of [4], we have to limit the upper bound of the number of sensor nodes in a grid. In the λ-secure property, for a given key space, less than λ sensor nodes are allowed. In other words, n_z should be smaller than $\lambda\omega/\tau$. However, an extended grid group covers twice area of grids and twice number of sensor nodes, $2n_z$, when the uniform distribution is assumed for the sensor deployment. Therefore, to satisfy the condition of $2n_z \leq \lambda\omega/\tau_E$ for the extended grid group, we select the τ_E as $\tau_E \leq \frac{\lambda\omega}{2n_z}$ which is a half of τ.

1. Partition N sensor nodes for $N_G \times N_G$ grid groups by the deploy location. Then, according to the configuration of the overlapped extended grid group in Fig 3 and 4, assign sensor nodes to extended grid groups of each layer, $EG(i_E, j_E, l)$. Due to the overlapped nature of extended grid groups, sensor nodes within the same grid share 4 extended grid groups but nodes between adjacent grids share only one extended grid group.
2. The whole key pool P is divided into a number of sub-key pools to assign each sub-key pool to an extended grid group. Additionally, each key pool has ω sub-key spaces, $P(i_E, j_E, l)$ where i_E =1, ..., $N_{Ei,l}$, j_E = 1, ..., $N_{Ej,l}$ and l = 1, ..., 4. From [4], a sub-key space has $N \times (\lambda + 1)$ key matrix A where $A = (D \cdot G)^T$.
3. For each extended grid group, unique IDs within $EG(i_E, j_E, l)$ are given to the nodes. Then, randomly select τ_E sub-key spaces from ω sub-key spaces $P(i_E, j_E, l)$ and allocate keys to each sensor node in $EG(i_E, j_E, l)$.

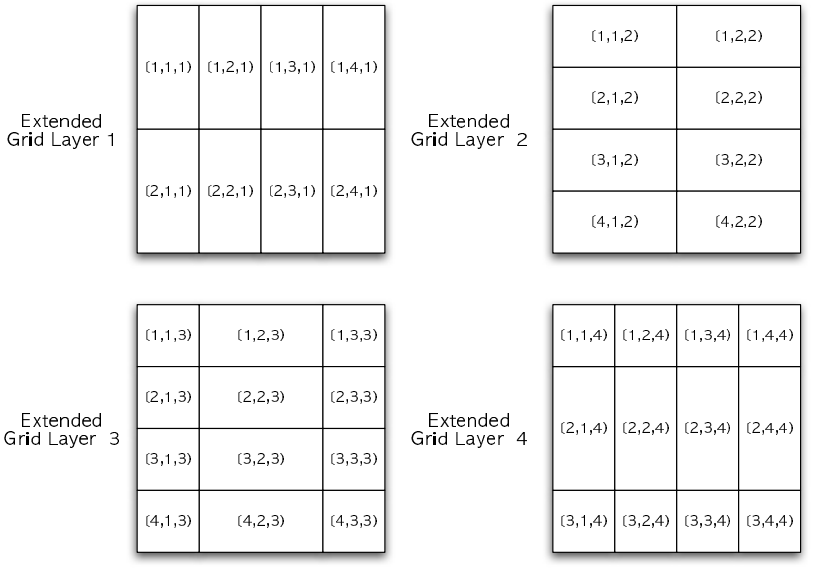

Fig. 4. The configuration of extended grid groups

4. After the key assignment, the sensor node stores pairs of its extended grid group ID and the selected key spaces for the extended group, which will be used in the Key discovery phase.

3.3 Sensor Node Deployment

In the deployment phase, sensor nodes are deployed according to the position of its grid group. Because we assume the uniform distribution of sensor nodes' location, the density of deployed nodes is easily calculated from n_z/a^2. Additionally, a unique identifier, ID_u, is assigned to each sensor node in advance of the deployment.

3.4 Key Discovery and Pairwise Key Establishment

After the deployment of sensor nodes, sensor nodes try to discover neighbor sensor nodes who belong to the same extended grid group and share the same key spaces.

1. (*Key discovery phase*) Each sensor node broadcasts a key list which includes its identifier and series of pairs of an extended grid group ID and key spaces identifiers for the extended grid group. For example, a sensor node u broadcasts $[ID_u, (ID_{EG}^{(1)}, \tau_1^{(1)}, \cdots), (ID_{EG}^{(2)}, \tau_1^{(2)}, \cdots), (ID_{EG}^{(3)}, \tau_1^{(3)}, \cdots), (ID_{EG}^{(4)}, \tau_1^{(4)}, \cdots)]$ where ID_u is the identifier of the node u, $ID_{EG}^{(l)}$ and $\tau^{(l)}$ indicate the identifier of node u's extended grid group of layer l and the selected key space identifiers for the extend grid group, respectively.

2. The node u compares its pair of the extended grid group ID and key spaces with the received key list from neighbor nodes. If there are one or more matching pairs between two nodes, node u creates a key graph which has all neighbor nodes of u as vertices and adds edges to each neighbor-node vertex of the matching pairs.
3. (*Pairwise key establishment phase*) For the key graph connected neighbor nodes, node u sends connection requests. Because the nodes share the same $ID_{EG}^{(l)}$ and $\tau^{(l)}$ pair, they can generate a pairwise key using the key agreement method of [4] in a secure way.
4. If there are unconnected neighbor nodes in the key graph, the node u broadcast the ID list of the unconnected nodes. Then the node u sends a connection request by relaying of the node who shares keys with the unconnected nodes and carries out a pairwise key agreement process. Subsequently, the node u adds edges to the newly key established node in its key graph. This process is repeated until all the neighbor nodes are connected or no connectable node is found anymore.

In the key discovery and pairwise key establishment phases, the process is the same for nodes within the same grid and nodes in the adjacent grid. However, the nodes within the same grid have higher possibilities to connect each other directly since they have all the extended grid group in common while the nodes between adjacent grids share only one extended grid group.

4 Analysis

4.1 Key Graph Connectivity Analysis

Since we use the key predistribution based on [4], we start the probability, p_1, that given two sensor nodes share at least one key space in common. With given ω and τ, the p_1 is

$$p_1 = 1 - \frac{\binom{\omega}{\tau}\binom{\omega-\tau}{\tau}}{\binom{\omega}{\tau}^2}$$

However, in the key discovery phase of the proposed scheme, more than one extended grid groups are overlapped. We use the τ_E for the extended grid group instead of τ. Thus the probability, p_c, that given two sensor nodes are connected without helping of neighbor nodes is

$$p_{c,l} = 1 - \left(\frac{\binom{\omega}{\tau_E}\binom{\omega-\tau_E}{\tau_E}}{\binom{\omega}{\tau_E}^2} \right)^l$$

where l is the number of the sharing extended grid group for given two sensor nodes.

$$l = \begin{cases} 4 & \text{within the same grid} \\ 1 & \text{between adjacent grids} \\ 0 & \text{otherwise} \end{cases}$$

Key Graph Connectivity within the Same Grid. In order to connect a neighbor node within the same grid, a sensor node can connect directly (1 hop) or with relaying of neighbor nodes (more than 1 hop). Let $N_u(i, j, R)$ be the number of neighbor nodes within the same grid of a node u with its communication range R and $N_u(i\pm, j\pm, R)$ be the number of neighbor nodes between horizontally and vertically adjacent grids. When a node u connects to a node v, the probability of the former case is $P_{u,v}[1 \text{ hop}] = p_{c,4}$ and that of the later case is

$$P_{u,v}[2 \text{ hop}] = 1 - (1 - p_{c,4})^{p_{c,4} \cdot N_u(i,j,R)} \cdot (1 - p_{c,1})^{p_{c,1} \cdot N_u(i\pm,j\pm,R)}$$

where $(1 - p_{c,4})^{p_{c,4} \cdot N_u(i,j,R)}$ is the probability of that all the neighbor nodes within the same grid are not connected to the node v and $p_{c,4} \cdot N_u(i, j, R)$ is the average number of connected neighbor nodes. Likewise, $(1 - p_{c,1})^{p_{c,4} \cdot N_u(i\pm,j\pm,R)}$ means the unconnecting probability of all the neighbor nodes in the horizontally and vertically adjacent grids to the node v. Therefore, when we consider the connectivity within 2 hops, the probability of key graph connectivity between nodes within the same grid is

$$\begin{aligned} P_{u,v} &= P_{u,v}[1 \text{ hop}] + (1 - P_{u,v}[1 \text{ hop}])P_{u,v}[2 \text{ hop}] \\ &= p_{c,4} + (1 - p_{c,4})\{1 - (1 - p_{c,4})^{p_{c,4} \cdot N_u(i,j,R)} \cdot (1 - p_{c,1})^{p_{c,1} \cdot N_u(i\pm,j\pm,R)}\} \end{aligned} \tag{1}$$

Key Graph Connectivity between Horizontally and Vertically Adjacent Grids. In a similar way to the connectivity within grids, $P_{u,v\pm}$ is the probability that given two nodes between adjacent grids connect each other with the help of all neighbor nodes.

$$\begin{aligned} P_{u,v\pm} &= P_{u,v\pm}[1 \text{ hop}] + (1 - P_{u,v\pm}[1 \text{ hop}])P_{u,v\pm}[2 \text{ hop}] \\ &= p_{c,1} + (1 - p_{c,1})\{1 - (1 - p_{c,1})^{p_{c,4} \cdot N_u(i,j,R)} \cdot (1 - p_{c,4})^{p_{c,1} \cdot N_u(i\pm,j\pm,R)}\} \end{aligned} \tag{2}$$

where $(1 - p_{c,1})^{p_{c,4} \cdot N_u(i,j,R)}$ and $(1 - p_{c,4})^{p_{c,1} \cdot N_u(i\pm,j\pm,R)}$ are probabilities for the help of nodes in the same grid and in the adjacent grid respectively. From Eq. 2, we can derive the probability that a sensor node u can connect to the horizontally and vertically adjacent grid with the help of all its neighbor nodes.

$$P_{u\pm} = 1 - \{(1 - p_{c,1})^{N_u(i\pm,j\pm,R)}\}^{p_{c,4} \cdot N_u(i,j,R)} \tag{3}$$

Key Graph Connectivity between Diagonally Adjacent Grids. Since extended grids do overlay each other only in horizontal and vertical directions, we consider neighbor nodes in diagonally neighboring grid separately. Let N_u $(i\pm, j\mp, R)$ be the number of neighbor nodes in diagonally adjacent grid of a node u. In order to connect to the diagonally adjacent grid, the help of neighbor

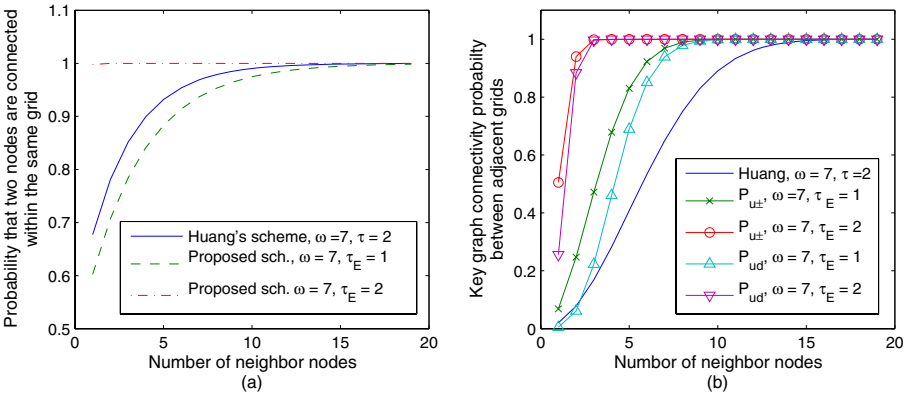

Fig. 5. The key graph connectivity within the same grid and between the adjacent grids

nodes in horizontally and vertically adjacent grids is required. In other words, the connection request must be relayed to the diagonally adjacent grid by the neighbor nodes. Therefore, the P_{ud} is probability that a sensor node u can connect to the diagonally adjacent grid.

$$P_{ud} = P_{u\pm} \cdot [1 - \{(1 - p_{c,1})^{N_u(i\pm,j\mp,R)}\}^{p_{c,4} \cdot N_u(i\pm,j\pm,R)}] \tag{4}$$

Using the system configuration of Huang scheme[6], Figure 5 depicts the probability of key graph connectivity for the change of the number of neighbors($n_z = 100$). Figure 5 (a) is for the probability within the same grid. In case of $\tau_E = 1$, the connectivity of two nodes is 7% lower than Huang scheme of $\tau = 2$ as the maximum, but the difference decreases under 2% when the number of neighbor nodes is more than 10. Figure 5 (b) shows the probability that a sensor node can connect to adjacent grids. The proposed scheme has 3.4 times higher key graph connectivity between adjacent grids as the maximum. In case of $\tau_E = 2$, the proposed scheme outperforms in both cases drastically.

4.2 Area Coverage vs. Key Graph Connectivity Analysis

The number of neighbor nodes is determined by the communication range, R, and the density of the deployed sensor nodes, ρ. For accurate calculation of the key connectivity, the coverage area should be considered separately by 3 cases: within the same grid, in horizontally and vertically adjacent grids and in diagonally adjacent grids. The value of ρ can be calculated by $\frac{n_z}{a^2}$ since the assumption of the uniform distribution.

We use the coverage analysis of [6]. For a given R, the number of neighbor nodes are like as followings:

$$\begin{aligned} N(i,j,R) &= \lfloor \rho \cdot C_b(i,j,R)|_{(x,y)}) \rfloor \\ N(i\pm,j\pm,R) &= \lfloor \rho \cdot (C_b(i,j^-)|_{(x,y)} + C_b(i^+,j)|_{(x,y)}) \rfloor \\ N(i\pm,j\mp,R) &= \lfloor \rho \cdot C_b(i^+,j^-)|_{(x,y)} \rfloor \end{aligned}$$

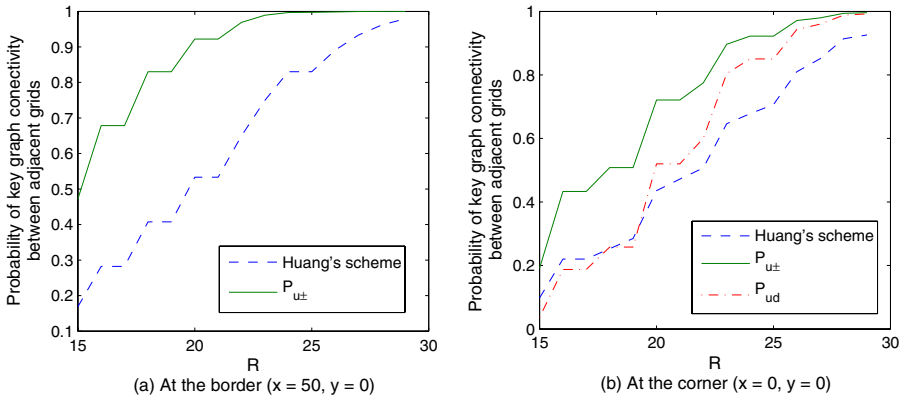

Fig. 6. Area Coverage vs. Key graph connectivity($\omega = 7, \tau = 2, \tau_E = 1$)

where $C_b(i, j, R)|_{(x,y)}$ is the coverage within the same grids. $C_b(i, j^-)|_{(x,y)}$ and $C_b(i^+, j)|_{(x,y)}$ are the coverages for horizontally and vertically adjacent grids, respectively, and that of diagonal adjacent grids is $C_b(i^+, j^-)|_{(x,y)}$. Please refer the appendix of [6] about $C_b(\cdot)$.

Figure 6 shows the probability of key graph connectivity as the increase of R. In Figure 6 (a), the node locates at the border between grids. The connectivity to the neighboring grid increases as the coverage area becomes wider and our proposed scheme shows the higher connectivity at the same coverage area. In case of Figure 6 (b) that the node is at the corner of the grid, the diagonally adjacent grids are also concerned. The connectivity to the diagonally adjacent grid are a bit lower than Huang scheme under $R = 19$ but the connectivity to the horizontally and vertically adjacent grids are higher than Huang scheme at any case.

4.3 Security Analysis

Security of the proposed scheme is mainly dependent upon that of Blom's scheme [1] and that of Huang's grid scheme [6]. The λ-secure property of the key matrix is preserved in overlaid grids by allowing more efficient key computation than [3, 4], saying that pairwise keys are secure if no more than λ nodes are compromised in each extended grid while the restricted number of nodes within an extended grid reduces the number of modular multiplication operations for deriving a pairwise key, due to $n_z = \lambda\omega/\tau$. As for the Huang's grid scheme, however, we already mentioned that the heterogeneity of key establishment in *I-scheme* and *E-scheme* may affect security of the entire network in Section 2.3. Say, a node replication attack is possible by adding the replicated node to the network through *E-scheme*. Our scheme solves this problem and resists the node replication attack as well. We discuss the resistance against three attacks below.

Node capture attack. Since we restrict n_z under $\lambda\omega/\tau$ and the number of nodes in an extended grid group under $\lambda\omega/\tau_E$ at the key predistribution phase,

the secret key matrix is not revealed without regard to the number of captured sensor nodes by the λ-secure property. The security of our scheme against the random node capture attack and selective node capture attack can be observed from the same perspectives of Huang's scheme. The resistance against the node capture attack is discussed well in [6].

Node fabrication attack. The attacker who captured a sensor node can modify and use the information from the captured node, such as the secret keys pre-installed in that node, for fabricating a new node with new identity. When random key pre-distribution scheme is used improperly without identification method, this kind of attack can cause severe problems with regard to security of the entire network. For example, if an adversary captures two nodes containing m keys respectively, (s)he can fabricate $\binom{2m}{m}$ new nodes over the network. However, since our scheme follows the multiple space Blom scheme by using the node's id as identification of the row of matrix A, the node fabrication attack could easily be defeated.

Node replication attack. As we mentioned already, the heterogeneity of key establishment in Huang's scheme may allow a node replication attack in which *E-scheme* is only exploited. If a node i located in an angular point of a grid is captured while its *E-scheme* pair j is located in the opposite side of the other diagonal grid, then the replicated node of i can be added to the diagonal grid of the grid of j by *E-scheme*. Note that *I-scheme* which follows the multiple space Blom scheme resists the replication attack by restricting it in a single grid only where a replicated node could be excluded more easily. In our scheme, the multiple space Blom scheme is only used in an extended grid along with path key establishment, and the node replication attack is defeated in that sense.

5 Performance Evaluations

5.1 Communication Overhead

When the two nodes are not directly connected, extra communications between neighbor nodes are required. This makes more communication overhead in a sensor node. Figure 7 depicts the probability of connectivity directly (1 hop) and with the help of neighbor nodes (2 hop), separately. The result shows the portion of direct connection grows larger as the number of neighbor nodes. In other words, the communication overhead to connect adjacent grids goes lower as the number of neighbor nodes increases.

Further, due to the unified key establishment scheme for both case of same grid and adjacent grids, there is no need to have separate stages of key establishment. Therefore, the total control messages for the key establishment of nodes at the border of grid can decrease by a half.

5.2 Power Consumption

Based on free-space propagation model, the power density p_t is given by $p_t = \frac{P_T}{4\pi d^2}$ where P_T and d are transmitted signal power and distance, respectively.

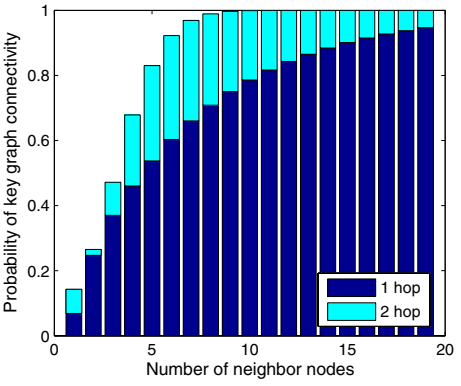

Fig. 7. Communication overhead for the probability of the key graph connectivity between adjacent grids

In other words, to widen the communication range twice, 2^2 times of transmission power is required. Using on the result of Section 4.2, Figure 8 depicts required transmission power to achieve the given probability of key graph connectivity between adjacent grids. Because the proposed scheme has higher key graph connectivity between adjacent grids than that of Huang scheme, the required transmission power of the proposed scheme is only 36% of Huang scheme for achieving the same connectivity. Therefore, our proposed scheme can reduce power consumption of a sensor node with guaranteeing the equal connectivity. With considering the lower communication overhead of the proposed scheme, the effect of power saving can be amplified.

5.3 Storage Overhead

The number of nodes in a grid should not exceed $\lambda\omega/\tau$ to preserve λ-secure property of [4]. Additionally the area of a extended grid group is twice of that of a grid and each node belongs to 4 extended grid group. Therefore, in our scheme, each node has to store $m = 4(\lambda+1)\tau$ keys and it is restricted by $n_z = \lambda\omega/\tau$. In other words, $\lambda = 2n_z\tau_E/\omega$ where $\tau_E = \tau/2$.

The total number of keys that to be preinstalled in a sensor node is:

$$m = 4(\lceil \frac{2n_z\tau_E}{w} \rceil + 1)\tau_E \tag{5}$$

From the required number of keys in a sensor node from Huang scheme, $m_h = (\lceil \frac{n_z\tau}{\omega} \rceil + 1)\tau + \gamma\alpha$, the value of m is slightly lower than the twice of m_h by the amount of $2\gamma\alpha$.

$$\begin{aligned} m &= 4(\lceil \tfrac{2n_z\tau_E}{\omega} \rceil + 1)\tau_E \\ &= 2(\lceil \tfrac{2n_z\tau}{2\omega} \rceil + 1)\tau \\ &= 2(\lceil \tfrac{n_z\tau}{\omega} \rceil + 1)\tau \end{aligned}$$

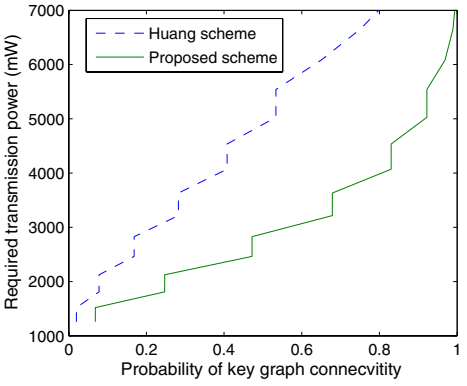

Fig. 8. Required transmission power for the probability of key graph connectivity between adjacent grids ($n_z = 100$, $a = 100$m, $\omega = 7$, τ_E=1, $\tau = 2$ and $p_t = 0.001$)

Table 1. Required key storage

n_z	ω	τ_E	Key size(bits)	Storage(bytes)
50	7	1	64	512
100	7	1	64	960
200	7	1	64	1888
50	7	1	128	1024
100	7	1	128	1920
200	7	1	128	3776
50	7	2	64	1920
100	7	2	64	3776
200	7	2	64	7424

Table 1 shows the key storage overhead on various configurations. Based on configurations of [4] and [6], in which they use $\omega = 7$, $\tau = 2$ ($\tau_E = 1$) and 64-bit (8 byte) key, the required key storage for the proposed scheme is under 1 kbytes. Even in the cases of 128-bit key and $\tau_E = 2$, the key storage does not exceed several kbytes. Hence, keys are small enough to be pre-installed to the memory of sensor nodes because MICAz sensor nodes usually have a 128-kbyte program memory and a 512-kbyte secondary memory.

6 Conclusion

We propose a new location-aware key management scheme using multi-layer grids. Our approach is simple and efficient on the basis of configuration of the overlaid grids. We extend the multi-space Blom scheme to both within the same grid and between adjacent grids. We pointed out the heterogeneity problems such as an isolated grid problem from the previous location-aware key management scheme [6]. Our scheme resolves those problems intrinsically because the

same key establishment scheme is used within or between the grid groups. The improved key graph connectivity between adjacent grids resolves the isolated grid problem and guarantees the better connectivity of grids. With regard to communication and power consumption overhead, our approach shows better performance than the previously proposed schemes without losing its security.

References

1. R. Blom, "An optimal class of symmetric key generation system," in *Eurocrypt'84*, Lecture Notes in Computer Science, vol. 209, Springer-Verlag, pp. 335-338, 1985.
2. H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. of IEEE Syposium on Security and Privacy*, pp. 197-215, 2003.
3. W. Du, J. Deng, Y. S. Han, S. Chen and P. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," in *Proc. of IEEE INFOCOM*, March 2004.
4. W. Du, J. Deng, Y. Han, P. Varshney, J. Katz and A. Khalili, "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks," *ACM Trans. on Information and System Security*, vol. 8, no. 2, pp. 228-258, 2005.
5. L. Eschenauer and V. D. Gligor, "A Key-management Scheme for Distributed Sensor Networks," in *Proc. of the 9th ACM Conference on Computer and Communication Security (CCS'02)*, pp. 41-47, Nov. 2002.
6. D. Huang, M. Mehta, D. Medhi and L. Harn, "Location-aware Key Management Scheme for Wireless Sensor Networks," in *Proc. of the 1st ACM workshop on Security of ad-hoc and sensor networks (SASN'04)*, pp. 29-42, Oct. 2004.
7. D. Liu and P. Ning, "Location-based pairwise key establishments for static sensor networks," in *Proc. of the 1st ACM workshop on Security of ad-hoc and sensor networks (SASN'03)*, pp. 72-82, Nov. 2003.
8. S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in *Proc. of the 10th ACM Conference on Computer and Communication Security (CCS'03)*, Nov. 2003.