A Key Pre-Distribution Scheme for Secure Sensor Networks Using Probability Density Function of Node Deployment

Takashi Ito, Hidenori Ohta, Nori Matsuda, and Takeshi Yoneda
Mitsubishi Electric Corporation,
Information Technology R & D Center
5-1-1 Ofuna, Kamakura, Kanagawa 247-8501, Japan
{takashim,hidenori,norim,tyone}@iss.isl.melco.co.jp

ABSTRACT

Pairwise key establishment is a fundamental service provided in secure sensor networks. However, due to resource constraints, establishing pairwise keys is not a trivial task. Recently, a random key pre-distribution scheme and its improvements have been proposed. The scheme proposed by Du et al. uses deployment knowledge to improve the performance and security of sensor networks. However, this scheme assumes group-based deployment in which groups of nodes are deployed from horizontal grid points. This assumption limits applications of the scheme. Therefore, in this paper, we propose an advanced key pre-distribution scheme in which different keys are logically mapped to two-dimensional positions, and the keys that are distributed to a node are determined by positions estimated using a node probability density function. The scheme can be applied to any deployment model provided the node probability density function has already been determined. Furthermore, simulation results show that our scheme achieves higher connectivity than Du et al.'s scheme.

Categories and Subject Descriptors

C.2.0 [**Computer-communication networks**]: General—*Security and protection*

General Terms

Design, Security

Keywords

Key management, probabilistic key sharing, sensor networks

1. INTRODUCTION

Sensor networks consist of a large number of resource-constrained sensor nodes. They are ideal candidates for monitoring buildings and industries; they can also be used in asset tracking, environmental sensing, etc. Generally, sensor nodes communicate with each other through wireless communication; therefore, security services such as encryption and authentication are required to prevent eavesdropping, alteration, and spoofing. These services are achieved by establishing pairwise keys for node-to-node communication. However, due to resource constraints, using public key cryptography for establishing pairwise keys is impractical [1].

One practical solution is key pre-distribution, where key information is distributed to all nodes prior to deployment. If the placement of deployed nodes can be determined in advance, key pre-distribution becomes trivial because a common key can be assigned to two neighboring nodes that are identified by the placement. However, in sensor networks using deployment, it is not feasible to determine the placement of nodes in advance because they are placed almost randomly. Therefore, key information should be pre-distributed to each node so that it can share a key with any neighboring node.

There are several key pre-distribution schemes for secure node-to-node communication. One naive solution involves using a single master key that is distributed to all the nodes, but this is impractical because a compromise of any node causes the compromise of the entire sensor network. Another naive solution is the pairwise keys scheme where each node stores $n-1$ pairwise keys so that it shares one key with other nodes in the sensor network (n is the total number of nodes). However, this scheme is impractical for sensor networks because the storage of $n-1$ keys is too large for resource-constrained sensor nodes. Another drawback of this scheme is the difficulty of adding new nodes.

Recently, a random key pre-distribution scheme was proposed by Eschenauer and Gligor (hereafter referred to as the *Eschenauer-Gligor scheme*) [4]. This scheme generates a large key pool, and keys randomly selected from the key pool are distributed to each node. Therefore, any two nodes can share one common key with a certain probability. In addition, a compromise of one node only causes the compromise of a limited part of the sensor network.

Some improvements of the Eschenauer-Gligor scheme were proposed [2, 3, 5, 6, 7]. One of the improvements developed by Du, Deng, Han, Chan, and Varshney uses deployment knowledge for key pre-distribution (this scheme is hereafter referred to as the *Du et al. scheme*) [3]. In the Du et al. scheme, the target deployment area is divided into rectan-

SASN'05, November 7, 2005, Alexandria, Virginia, USA.

gles; different key pools are assigned to each of these rectangles in a logical manner: the nearer the rectangles, the greater the number of keys shared among key pools associated with the rectangles. Then, for each node to be deployed in a rectangle, keys are randomly selected from the key pool assigned to the rectangle and are pre-distributed to the node. Thus, the Du et al. scheme exhibits better performance (connectivity and memory usage) and it keeps the sensor networks secure. However, it can only be applied to the group-based deployment model.

In this paper, we present an advanced random key pre-distribution scheme by using the probability density function (pdf) of node deployment, which can be applied to various deployment models (e.g., deployment at irregular intervals, mixed deployment by helicopters and cars, etc.). Furthermore, this scheme achieves a higher connectivity than existing schemes.

The rest of this paper is organized as follows. We describe existing random key pre-distribution schemes and their limitations in Section 2. We propose our random key pre-distribution scheme in Section 3. We present the performance of the schemes in Section 4 and summarize our results in Section 5.

2. RELATED WORK

In this section, two representative random key pre-distribution schemes [3, 4] are described.

2.1 Random Key Pre-Distribution Scheme

2.1.1 Overview

The Eschenauer-Gligor scheme proposed in [4] consists of three phases: *key pre-distribution phase*, *shared-key discovery phase*, and *path-key establishment phase*.

The key pre-distribution phase, which is at the core of this scheme, is performed before deployment. In this phase, a large key pool of n keys is generated. Then, m keys are randomly selected from the n keys (the key pool) and are distributed to each node. Therefore, any two nodes have one common key with a certain probability. For example, if $n = 10000$ and $m = 83$, the probability that two nodes have at least one common key is 50 %.

After this phase, the nodes with pre-distributed keys are deployed. Then, the next phase—the shared-key discovery phase—is executed, in which two neighboring nodes try to determine whether they share a key. If they have no shared key, the path-key establishment phase is executed, in which two nodes attempt to find an indirect secure path via one or more nodes.

2.1.2 Problems

It is recommended that a large key pool be generated for increasing network resilience against node capture (see Section 4.1). However, with an increase in the size of the key pool (n), the number of keys stored by each node (m) should be increased to maintain a certain connectivity. For example, if $n = 100000$ and the required connectivity is 50 % (i.e., the probability that two nodes have at least one common key is 50 %), m must be greater than 260. This value is too large for resource-constrained sensor nodes.

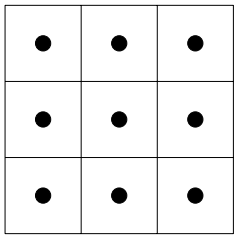

Figure 1: Rectangles and their deployment points

2.2 Random Key Pre-Distribution Scheme Using Deployment Knowledge

2.2.1 Overview

The Du et al. scheme proposed in [3] is one of the improvements of the Eschenauer-Gligor scheme. It assumes the *group-based deployment model*, which is explained below.

- All nodes are divided into l groups.
- The target deployment area is divided into l rectangles, and each node group formed as described above is associated with each rectangle in a one-to-one manner.
- Nodes in a group associated with a rectangle are deployed from air, that is, just above the center of the rectangle.

Fig. 1 shows an example in which the target deployment area is divided into 3×3 rectangles. A deployment vehicle (e.g., a helicopter) moves to just above the center point (indicated by the black point) and deploys the nodes associated with the rectangle. In this paper, we refer to the point from which a node is deployed as the *deployment point* and the point at which the node is finally located as the *resident point*.

In this scheme, the nearer the rectangles, the greater the number of keys shared among key pools associated with the rectangles. As a result, two nodes deployed to neighboring rectangles can share keys with a high probability. Therefore, keys can be efficiently distributed to nodes while achieving high connectivity and maintaining security against key compromise upon node capture.

Similar to the Eschenauer-Gligor scheme, the Du et al. scheme consists of three phases: key pre-distribution phase, shared-key discovery phase, and path-key establishment phase. The last two phases are the same as in the Eschenauer-Gligor scheme. Therefore, we focus on the first phase: the key pre-distribution phase.

2.2.2 Key Pre-Distribution Phase

The key pre-distribution phase of the Du et al. scheme is executed as follows.

Preliminary

1. Set security parameters n, m, and l. The parameter n is the size of the key pool, m is the number of keys stored by each node, and l is the number of groups.
2. Divide the target deployment area into l rectangles of the same size.

3. Generate n keys.

4. Determine l subsets of the key pool (referred to as *subset key pool*s) and associate them with l rectangles in a one-to-one manner. The determination and association are done so that two subset key pools associated with neighboring rectangles have more common keys.

Key distribution to each node

5. For a node S, select m keys randomly from the subset key pool associated with the deployment rectangle of S.

6. Store m keys selected in step 5 to node S.

7. Repeat steps 5–6 for all nodes.

In this scheme, two nodes deployed to the same rectangle can share keys with a high probability because their subset key pools are the same. Two nodes deployed to neighboring rectangles share keys with a lower probability because their subset key pools have fewer common keys. If two nodes are deployed to non-neighboring rectangles, the probability of key sharing is zero. Therefore, the damage due to the compromise of one node is limited to neighboring rectangles, and hence, the network is resilient against node capture.

2.2.3 Problems

This scheme assumes the group-based deployment model, and the deployment points should be horizontal grid points. For other deployment models, the manner in which the target deployment area should be divided and the subset key pools should be generated are not clearly described, and performing these tasks appears to be difficult. Moreover, if the pdf of node deployment is not a two-dimensional normal distribution or if it changes in real time (e.g., the wind direction changes during deployment), this scheme does not appear to work.

3. RANDOM KEY PRE-DISTRIBUTION SCHEME USING PROBABILITY DENSITY FUNCTION

In this section, we propose an advanced key pre-distribution scheme. The Du et al. scheme [3] uses deployment rectangles whose sizes strongly depend on the pdf of node deployment. In contrast, our scheme does not use such rectangles; instead, it uses a *key-position map* and the pdf of node deployment.

The key-position map shows which key is assigned to which position; this is specified by coordinates in a two-dimensional coordinate system. Although we can easily extend the concept of the key-position map to three dimensions (including height), we do not describe that in this paper. The pdf of node deployment can be determined by physical laws or previous results.

Similar to the Eschenauer-Gligor scheme, our scheme consists of three phases. The last two phases are the same as in the Eschenauer-Gligor scheme. Therefore, we focus on the first phase: the key pre-distribution phase.

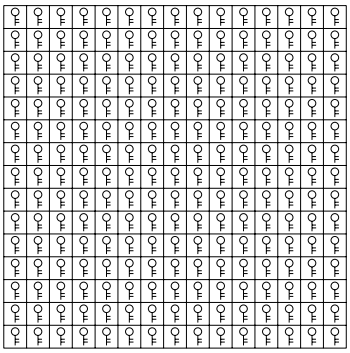

Figure 2: Key-position map

3.1 Prerequisite

If nodes are deployed from air as described above, their resident points on the ground vary widely because of air resistance. This unevenness of the deployment can be modeled using pdfs. In our scheme, we assume that the pdfs of the nodes are known or can be estimated. For example, the pdf $\Pr(x, y)$ is a two-dimensional normal distribution.

In addition, our scheme employs the communication range of the nodes, denoted as r. For simplicity, we assume that r is a constant.

3.2 Key Pre-Distribution Phase

The key pre-distribution phase of our scheme is performed as follows.

Preliminary

1. Set security parameters n, m. The parameter n is the size of the key pool and m is the number of keys stored by each node. These parameters are determined according to the resources of the nodes and requirements of network connectivity/resilience (see Section 4.1).

2. Divide the target deployment area into n areas of the same size. We refer to each area as a *subarea*. The shape of subareas can be rectangular, square, hexagonal, etc. For simplicity, we use rectangles as subareas in this paper. Note that unlike the Du et al. scheme, the size of the subarea does not depend on the deployment model.

3. Generate n keys.

4. A key-position map is created by assigning n keys to n subareas in a one-to-one manner. Fig. 2 shows an example of the resulting key-position map.

Key distribution to each node

5. For a node S, select one expected resident point P according to the pdf of S, $\Pr(x, y)$.

6. Randomly select one point Q within a circle of radius r and center P.

7. Let A be the subarea that includes Q. Store the key assigned to A (in step 4) to node S. If the same key already exists in S, start again from step 5.

8. Repeat steps 5–7 until node S has m keys.

9. Repeat steps 5–8 for all nodes.

Figs. 3–6 show a simplified example of the key distribution process described in steps 5–8. For simplicity, let the pdf be constant in a certain circle and zero otherwise, and let $m = 5$. In step 5, an expected resident point P of node S is randomly selected within the circle that represents the area of the possible resident points (Fig. 3). In step 6, a point Q is randomly selected within the communication range of P (Fig. 4). In step 7, a key corresponding to Q (gray color in Fig. 5) is selected and distributed to the node. Step 8 is performed by repeating steps 5–7, and finally, five keys are selected and distributed to S (Fig. 6).

In general, two nodes that are supposed to communicate with each other should share keys, whereas those that need not communicate do not have to share keys. In sensor networks using deployment, two nodes that should communicate are placed near each other, i.e., each node is included within the other node's communication range. Therefore, in order to achieve efficient key sharing, the key sharing scheme should be implemented in a manner such that the nearer the nodes, the higher the probability that they can share keys.

Using Figs. 7 and 8, we can explain how our scheme achieves efficient key sharing in the manner described above. Let us suppose two nodes are deployed. In Figs. 7 and 8, the transparent circle and five selected keys for the first node have the same meaning as in Fig. 6, while the dark circle represents the area of the possible resident points of the second node[1]. Figs. 7 and 8 correspond to the cases in which the deployment of the second node is close to and far from the first node, respectively. It is evident that the intersection of the two circles in Fig. 7 is larger than that in Fig. 8. Since our scheme maps keys to positions (subareas), a larger intersection has more keys to be shared.

Therefore, the larger the intersection, the higher the probability that two nodes can share keys. In this manner, at a fine granularity (subarea level), our scheme has the characteristic that the nearer the nodes, the higher the probability that they can share keys. In contrast, the Du et al. scheme exhibits this characteristic at a lower granularity (rectangle level). The finer granularity is one reason behind the higher connectivity achieved by our scheme.

3.3 Comparison with the Du et al. Scheme

Our scheme and the Du et al. scheme are similar in that some subset of the key pool is assigned to one deployment point. However, there are some differences between the two schemes. The Du et al. scheme can only be applied to the group-based deployment model, and its deployment points depend on the division of rectangles. In contrast, our scheme has no restriction on the deployment points, and hence, it can be applied to various deployment models (deployment at irregular intervals, mixed deployment by helicopters and cars, etc.). Moreover, all the deployment points need not be decided before deployment; therefore, we can deploy nodes on an ad hoc basis. In other words, we can move to any point, measure the current location, distribute keys to the node (according to the location and the pdf), and deploy

[1]Actually, the area of selectable keys is slightly larger than the area of the possible resident points due to the influence of r, but for explanation purpose we ignore the difference.

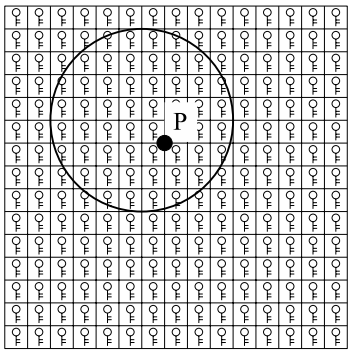

Figure 3: Expected resident point of S

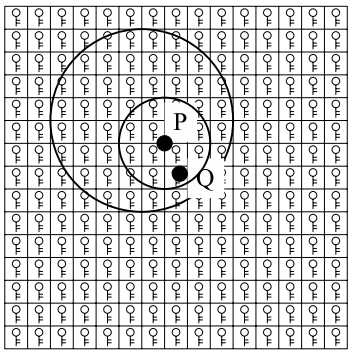

Figure 4: A point near P

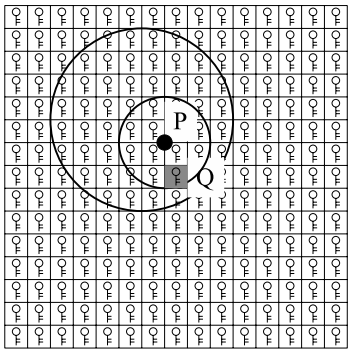

Figure 5: A key corresponds to Q

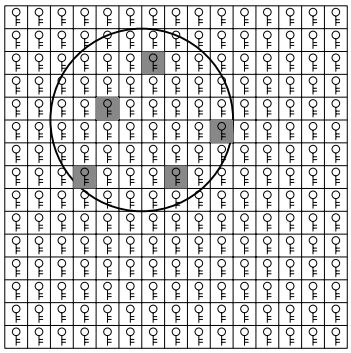

Figure 6: Keys to be distributed to S

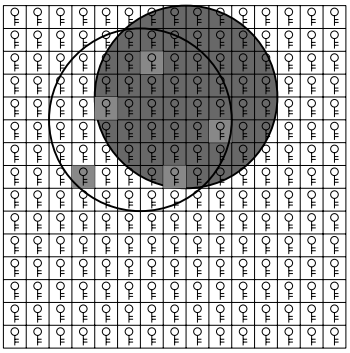

Figure 7: Second node near the first

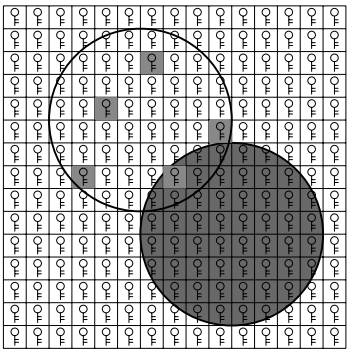

Figure 8: Second node far from the first

the node from that point. With regard to deployment from air, it is much easier to measure the exact location than to move to a particular location. Hence, using our scheme, deployment can be executed in a shorter duration and at a lower cost.

4. EVALUATION

In Section 3, we showed that our scheme has qualitative advantages. In this section, we describe the performance evaluation of our scheme.

4.1 Evaluation Criteria

The performance of random key pre-distribution schemes can be evaluated on the basis of several criteria [2, 3, 4, 5, 6, 7]. In particular, we choose *connectivity* and *resilience against node capture* as the criteria for performance evaluation.

- Connectivity
  There are two types of connectivity: *local connectivity* and *global connectivity*. Local connectivity is the probability that any two neighboring nodes within their communication range have at least one common key. The higher the local connectivity, the less frequent the occurrence of the path-key establishment phase; hence, it leads to low communication overhead. Global connectivity is the ratio of the size of the largest connected component to the size of the entire network[2].

[2]Nodes which are not within the communication ranges are excluded.

- Resilience against node capture
  If one node is captured and m keys are compromised, the fraction m/n of communication can be eavesdropped. Therefore, we define *compromise rate* as m/n. The smaller the compromise rate, the more secure against node capture.

Note that there is a trade-off between the connectivity and the resilience. Let us suppose n is fixed. Then, if the number of distributed keys (m) is high, the connectivity is greater and there is less resilience against node capture.

4.2 Comparison with the Du et al. Scheme

In this subsection, we present the results of simulations for comparing the connectivity of the Du et al. scheme with that of our scheme. In the following four simulations, we use the common conditions listed below.

- The size of the key pool is 100000.
- The target deployment area is 1000 meters square.
- The pdf of node deployment is a two-dimensional normal distribution, whose mean is the deployment point and standard deviation is 50 meters.
- The communication range of the nodes is 40 meters.
- In the Du et al. scheme, the overlapping factors[3] are $a = 0.167$ and $b = 0.083$.

4.2.1 Group-Based Deployment Model

This is the same model as described in [3]. The specific conditions in this simulation are as follows.

- The number of sensor nodes is 10000.
- The target deployment area is divided into 10×10 rectangles.
- The center of each rectangle is the deployment point.
- The number of simulations is 10.

Under these conditions, there are about fifty nodes within the communication range of each node. Figs. 9 and 10 show the local and global connectivity, respectively. As shown in Fig. 9, the local connectivity of our scheme is slightly lower if $m < 70$ and slightly higher if $m \geq 70$. As shown in Fig. 10, the global connectivity of our scheme is almost the same as that of the Du et al. scheme.

4.2.2 Group-Based Deployment Model (Sparse Deployment Case)

In general, deploying fewer nodes is desirable because it leads to lower cost; thus, we evaluate the connectivity for the sparse deployment case. The specific conditions in this simulation are as follows.

- The number of sensor nodes is 1000.
- The target deployment area is divided into 10×10 rectangles.

[3]The parameter a (resp. b) is the ratio of common keys, which are shared by two horizontally/vertically (resp. diagonally) neighboring subset key pools, to the size of each subset key pool. Note that $a + b = 0.25$.

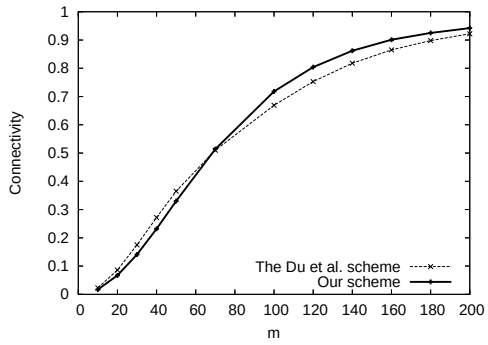

Figure 9: Local connectivity

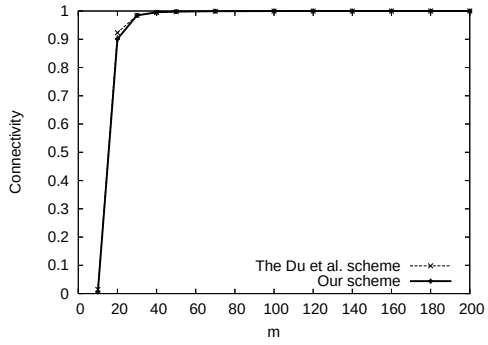

Figure 10: Global connectivity

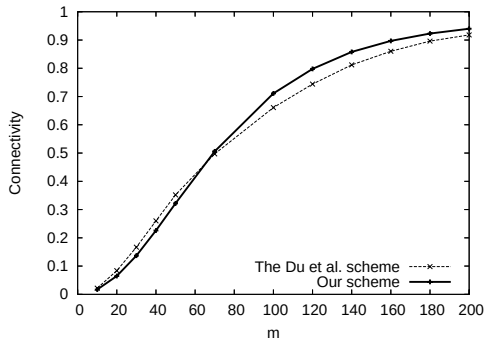

Figure 11: Local connectivity (sparse)

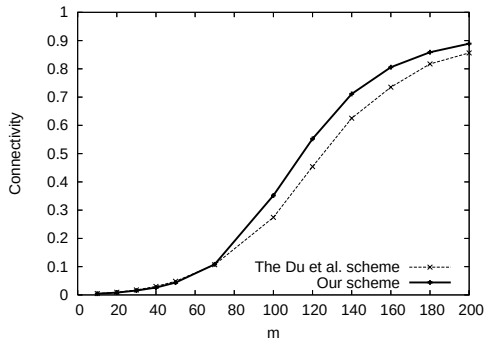

Figure 12: Global connectivity (sparse)

- The center of each rectangle is the deployment point.
- The number of simulations is 1000.

Under these conditions, there are only about five nodes within the communication range of each node. Figs. 11 and 12 show the local and global connectivity, respectively. Although the global connectivity achieved by both schemes is lower than that shown in Fig. 10, our scheme achieves a higher global connectivity than the Du et al. scheme.

4.2.3 Group-Based Deployment Model with Prediction Error

Since both the Du et al. scheme and our scheme use information on deployment, it is important to predict the pdf correctly. On the other hand, robustness against a prediction error is a desirable feature of the scheme. Therefore, we evaluate the connectivity for the case in which a prediction error occurs. The specific conditions in this simulation are as follows.

- The number of sensor nodes is 10000.
- The target deployment area is divided into 10×10 rectangles.
- The center of each rectangle is the deployment point.
- During the key pre-distribution, the predicted standard deviation of the pdf is 50 meters, but its actual standard deviation is 100 meters.
- The number of simulations is 10.

Figs. 13 and 14 show the local and global connectivity, respectively. Although the local connectivity achieved by both schemes is lower than that shown in Fig. 9, our scheme has more robustness (less degradation) than the Du et al. scheme.

4.2.4 Random Deployment Model

One of the advantages of our scheme is that we can deploy nodes from any point rather than only horizontal grid points; this is because pre-distributed keys of a node are determined only by its deployment point, and the deployment points of other nodes do not matter. Thus, it is possible to select deployment points randomly within the target deployment area. In contrast, the Du et al. scheme cannot be directly applied to this deployment model. Hence, we customize the Du et al. scheme for comparing it with our scheme. In the customized Du et al. scheme, the key pre-distribution phase is the same as in the Du et al. scheme, and the deployment points are not horizontal grid points but uniformly random points. The specific conditions in this simulation are as follows.

- The number of sensor nodes is 10000.
- The deployment points are randomly selected within the target deployment area.
- In the customized Du et al. scheme, the target deployment area is divided into 10×10 rectangles, and the nodes whose deployment points are in the same rectangle are regarded as a group. Then, the same key pre-distribution phase described in Section 2.2 is executed.

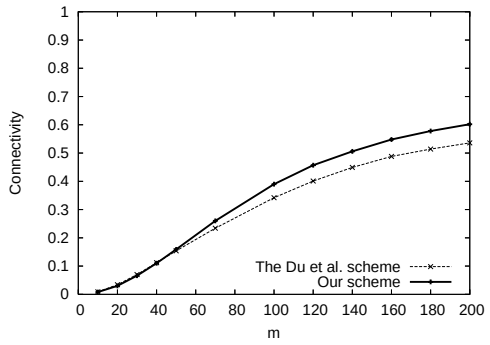

Figure 13: Local connectivity (error)

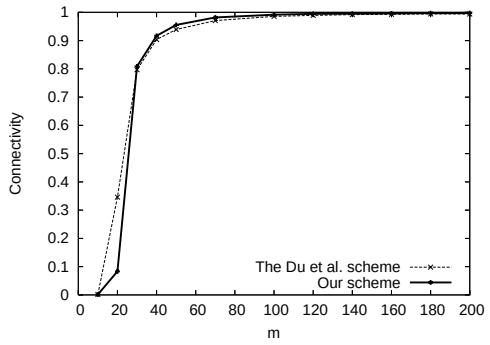

Figure 14: Global connectivity (error)

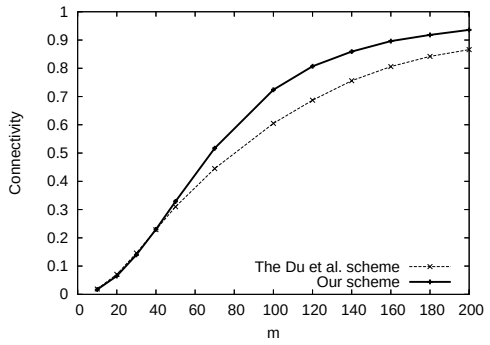

Figure 15: Local connectivity (random)

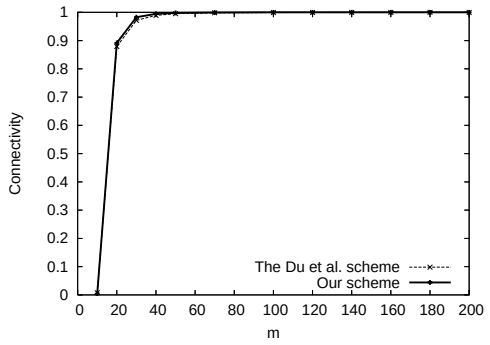

Figure 16: Global connectivity (random)

- The number of simulations is 10.

Figs. 15 and 16 show the local and global connectivity, respectively. The connectivity results of our scheme are almost the same as the previous results (Figs. 9 and 10); however, the local connectivity of the customized Du et al. scheme is degraded.

5. CONCLUSIONS AND FUTURE WORK

We proposed an advanced key pre-distribution scheme using the pdf of node deployment. When our scheme is employed, multiple choices exist for deployment from the viewpoint of sequences and positions of deployment. Furthermore, sensor nodes can be deployed in a short duration because the deployment vehicle (e.g., a helicopter) is not required to move to each particular horizontal grid point. Finally, we showed that our scheme achieved better performances than the Du et al. scheme.

However, much work remains to be done, for instance, the performance of our scheme should be analyzed theoretically. Further, practical deployment models should be specified and the performance under such conditions should be evaluated.

6. REFERENCES

[1] D. W. Carman, P. S. Kruus, and B. J. Matt. Constraints and approaches for distributed sensor network security. Technical report, NAI Labs, September 2000.

[2] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 197–213, May 2003.

[3] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. In *Proceedings of the IEEE INFOCOM 2004*, pages 586–597, March 2004.

[4] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 41–47, November 2002.

[5] D. Huang, M. Mehta, D. Medhi, and L. Harn. Location-aware key management scheme for wireless sensor networks. In *Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04)*, pages 29–42, October 2004.

[6] D. Liu and P. Ning. Location-based pairwise key establishments for static sensor networks. In *Proceedings of the 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03)*, pages 72–82, October 2003.

[7] Z. Yu and Y. Guan. A key pre-distribution scheme using deployment knowledge for wireless sensor networks. In *Proceedings of the 4th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN 2005)*, pages 261–268, April 2005.