A Small-World Key Management for Wireless Sensor Networks

Yung-Tsung Hou*, Chia-Mei Chen, and Bingchiang Jeng

Department of Information Management,

National Sun Yat-Sen University,

Kaohsiung, Taiwan

yungtsung.hou@gmail.com, {cmchen, jeng}@mis.nsysu.edu.tw

Received 9 December 2008; Revised 6 March 2009; Accepted 29 March 2009

Abstract. Most of wireless sensor networks (WSNs) are deployed in hostile environments where communication between sensors may be monitored. For applications that require higher data security, employing some cryptographic scheme is therefore necessary in the networks. However, key management in WSNs is a challenging task due to resource constraints on sensor nodes. In this paper, based on the concept of small worlds, we present a group-based key pre-distribution scheme which enables any pair of sensors to establish a unique shared key. The proposed method for key path establishment uses only local information with logarithmic memory overhead to the number of groups. We also evaluate other performance aspects, including communication and computing overhead. The analysis and simulation results show that the proposed key management method performs better than other known methods.

Keywords: key management, key pre-distribution, small worlds, sensor networks

1 Introduction

Wireless sensor networks (WSNs) are composed of small and inexpensive sensors with limited resources in battery power, memory, computation, and communication. Recent advances in computing and communication technologies have created various applications for WSNs [1] including habitat monitoring, remote climate monitoring, industrial sensing, and other commercial and military applications. In some applications, such as battlefield sensing or critical infrastructure protection, sensor nodes are deployed in a hostile environment under numerous threats including information eavesdropping, sensor compromising, sensor impersonating, and even denial-of-service attacks. Secure transmission therefore becomes an important issue in WSNs.

Key management is a research challenge in WSNs. The approaches used for general computer networks are not applicable for WSNs due to the resource limitations in sensors. Thus, symmetric cryptography, which shares a key between two parties, is considered, and several schemes for pair-wise shared key establishment are developed. Among possible solutions, the key pre-distribution scheme which distributes key information to sensors before the deployment is viewed as an efficient approach to set up shared secret keys. Take the full pair-wise approach as an example. The full pair-wise approach preloads a set of unique keys to each sensor node and each key is shared with another node in the network. Under such a scheme, a node needs to carry $n - 1$ secret keys for a network of n nodes. Hence, its memory overhead is linear to the number of sensor nodes and the scheme becomes impractical when n goes larger. Furthermore, the full pair-wise approach has difficulty in adding new nodes to an existing network since the existing nodes do not have shared keys with the new node.

Random key pre-distribution scheme [2] was first proposed by Eschenauer and Gligor as a remedy for the above situation. The basic idea is to preload each sensor node with a random subset of keys from a large key pool before deployment. Since the keys in different nodes are from the same pool, any two neighboring nodes will have a certain probability to share a common key and they could use it for secure communication. If such a common key does not exist, they will instead establish a key path using intermediary nodes, and then use the secure path to exchange a key to establish a direct link. Chan et al. [3] improved the performance of the previous work by requiring that two sensors must share at least q common pre-distributed keys for pairwise key establishment.

With random key pre-distribution schemes, once the network is bootstrapped, each sensor node needs to communicate with neighbors to find common shared keys. To increase the probability of having common keys with neighbors, a sensor node must carry a large key ring. Hence, those schemes are not efficient in memory utilization. Furthermore, if a sensor can not find a common key with some of its neighbors, it needs a process of key path establishment and consumes extra energy for communication. The memory usage and overall consum-

* Correspondence author

ing energy for communication thus becomes major problems of random key pre-distribution schemes. Several location-aware methods [4, 5, 6] were proposed to improve key pre-distribution schemes. In these improved methods, the locations of sensors are assumed to be known before they are deployed. The deployment knowledge can really help to enhance the performance of key pre-distribution. However, to pre-determine the locations of sensors is not practical in many cases, due to the constraint of sensor deploying schemes. Therefore, how to reduce the consumption of memory and energy without using deployment knowledge is an important challenge in wireless sensor networks.

To solve the above problems, our paper proposes a group-based random key pre-distribution scheme for WSNs which uses a small amount of memory while the communication and computing overhead are also very low. The sensor groups could be distributed randomly or according to pre-determined group locations. Our scheme supports both types of group deployments.

The proposed scheme is based on the concept of small worlds [7, 8], which has the following properties: (1) the local neighborhood is preserved; and (2) the diameter of the network increases logarithmically with the number of nodes in the network, where the diameter is defined as the average shortest path length between any two nodes in terms of node hops. The network created by the proposed scheme will have pre-built secure links that satisfies the criterion of small worlds -- any two nodes in the network can be connected with just a few secure links. In the initial key preloading stage, each node is loaded with a set of keys shared with other nodes in the same group and additional keys shared with the nodes in distant groups based on a probability distribution. With the preloaded shared keys, a node can securely link to its trusted peer nodes that share the keys with it. For any two nodes, this arrangement will be able to find efficiently a secure path connecting them in an average path length logarithmic to the number of sensor groups, according to the localized property of small worlds.

The rest of this paper is organized as follows. In the following section, we review the related literature. In section 2, we present our key pre-distribution scheme. Section 3 analyzes the performance of the proposed scheme. The simulation results are shown in section 4. The last section gives a conclusion of this paper.

1.1 Related Work

Eschenauer and Gligor [2] first proposed a random key pre-distribution scheme for key management in WSNs. The basic idea of their scheme is as described in the previous section. Several studies [3, 9, 10, 11] were proposed later to improve the performance of the work in [2]. Chan et al. [3] presented new mechanisms for key management in which a pair of sensor nodes was required to share at least q common pre-distributed keys. A random-pairwise keys scheme was also presented, which preserves the secrecy of a network when any sensor is compromised. In summary, random key pre-distribution methods utilize the high connectivity property of a random graph when the average degree of its nodes exceeds a threshold. Although communication overhead is constant in these methods, the memory overhead increases linearly with the number of sensor nodes. Furthermore, the performance of these schemes depends on the network's topology, which might degrade rapidly if the nodes are sparsely or non-uniformly distributed in the network.

Key pre-distribution schemes can utilize the deployment knowledge to improve their performance. Du et al. [11] proposed a key management using deployment knowledge. In their method, sensors are divided into groups and the deployment points of sensor groups are known. Other papers [5, 6, 12] also presented similar group-based schemes, in which sensor fields are cut into grids, and a group of sensors is then assigned to an unique grid. With such location knowledge, each sensor node can carry fewer keys comparing to previous methods.

PIKE [13] is a deterministic scheme for key pre-distribution. In the method, any two sensors in the network have an intermediary node that has shared keys with both of them. This intermediary node is used as a trusted peer, through which the two nodes can securely establish a key path. If the scheme is used in two-dimensional field, it is referred as PIKE-2D and if the scheme is used in three-dimensional field, it is referred as PIKE-3D. PIKE shows significantly improvement over random key pre-distribution schemes. However, the intermediary node may be located anywhere in the sensor field, and thus PIKE might require network-wide communication to establish the key path. Its communication overhead is in order, which makes PIKE unsuitable for large sensor networks.

The small world concept was first studied by Milgram [7, 14, 15] in the 1960's. His experiments in mail delivery using acquaintances resulted in an average of six degrees of separation. After that, several network models have been proposed to study the small world phenomenon. Watts and Strogatz [8] proposed a refined network model and showed that the small world phenomenon is pervasive in a wide range of networks both in nature and in technology. Based on statistical properties, small-world networks could be classified into three different classes [16]: (a) scale-free networks: the connectivity distribution follows the power law; (b) broad-scale networks: the connectivity distribution has a power law regime followed by a sharp cutoff; and (c) single-scale networks: the connectivity distribution has a fast decaying tail. Since scale-free networks are not suitable for sensor networks, our method will try to build a single-scale network with preloaded secure links.

In small-world networks, how to find a path connecting a pair of nodes is a critical searching problem. Kleinberg [17] solved it by defining an infinite family of network models that generalizes the one proposed by Watts and Strogatz in [8]. In his method, only one unique model in the family has an efficient decentralized algorithm capable of finding short paths with a high probability. Based on the characteristics of WSNs, our method will use and refine Kleinberg's model as a framework for key management in WSNs. The construction details will be presented in the following sections.

2 The Proposed Key Management Solution

We assume that n homogenous sensors are deployed in a two-dimensional square field. Before the deployment of the network, sensors are assigned into $m \times m$ groups. Each sensor group has equal number of sensors and is arranged to a unique cell in a virtual key distribution space, which is partitioned into $m \times m$ square cells. Figure 1 depicts the square virtual space for sensor groups. Let $G_{i,j}$, where $i = 1, \ldots, m$ and $j = 1, \ldots, m$, denote the sensor group which is assigned to the cell of row i and column j in the virtual space. A unique group ID is then assigned to each sensor group and pre-loaded to the sensors in the group. The distribution of sensor locations in a group depends on the sensor deploying method. Without lost of generality, we assume that the sensors belonged to the same group are deployed closed to each other and the deployment distribution of the sensors inside a group follows a two-dimensional Gaussian distribution.

Our scheme does not restrict to any specific group deployment scheme. In this paper, we discuss two common group deployment methods: (1) sensor groups are randomly distributed; (2) sensor groups are distributed according to pre-determined group locations. In the later section, we will discuss the performance of both group deployment methods.

If sensor groups are deployed to pre-determined locations, one possible deployment method is to dispatch a number of mobile robots to sweep the sensor field along preplanned routes. The robots are equipped with global positioning systems (GPS) and could place the sensors of the same group into the pre-assigned group location. With the pre-determined group deployment, we assume that the sensor field is also partitioned into $m \times m$ square cells, and group $G_{i,j}$ is deployed at the cell in row i and column j of the sensor field. We also assume that the probability of a sensor being deployed outside its cell is very small. Thus, the group ID of a sensor can be used to approximate the sensor's location and a geographical routing method could be used as the underlying routing method.

The distance between two groups is defined as the minimal number of other groups between the two groups in the virtual key space, and is calculated as below:

$$Distance\ (G_{i1,\,j1}, G_{i2,\,j2}) = max\ (\ |i_1 - i_2|, |j_1 - j_2|\ )\ .$$

Figure 1 illustrates an example of the group distance from the view of $G_{1,\,1}$, where the value in a cell presents the group distance from this group to group $G_{1,1}$. With such approximated distance, the proposed solution can pre-assign a key shared by $G_{1,1}$ and a number of distance groups so that, based on small world theory, a sensor in $G_{1,1}$ can build a secure path to any sensor with a minimum number of secure links.

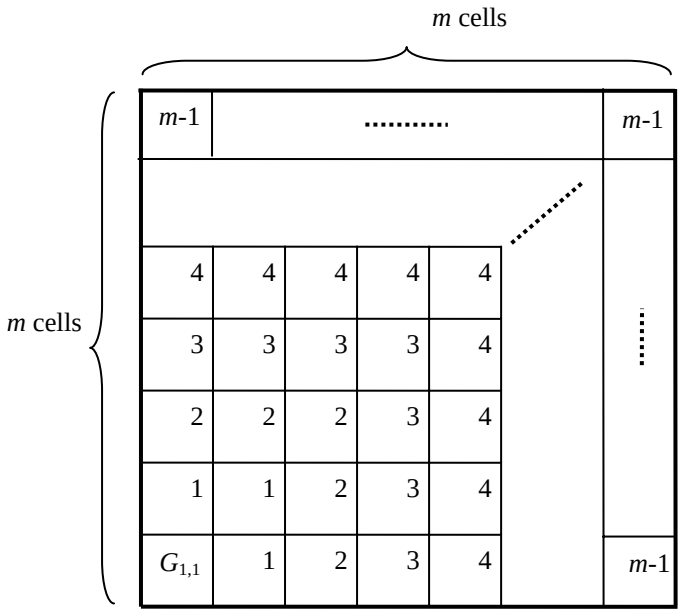


Fig. 1. An illustration of group distance from $G_{1,1}$ to other groups in the virtual key distribution space
The number in a cell presents the value of distance

Each sensor node is identified by a unique sensor ID from 1 to n. Without loss of generality, we assume that the sensors in group $G_{i,j}$ have the sensor ID from $(i-1) \times (n/m) + (j-1) \times n/(m \times m) + 1$ to $(i-1) \times (n/m) + (j-1) \times n/(m \times m) + n/(m \times m)$. Therefore, a sensor node can infer the group ID from the sensor ID.

2.1 The Proposed Key Pre-Distribution Scheme

Each sensor is pre-loaded with a certain number of shared keys. For intra-group sensors (sensors in the same group), each pair of sensors is preloaded with a unique shared key and two sensors in a pair consider each other as a trusted peer node. Such intra-group pre-distribution has memory overhead linear to the group size, and is acceptable if the group is kept small. For example, if a group is of size 50 and the key length is 64 bits, each sensor requires only 8*49 = 392 bytes to store the intra-group keys.

In addition, each sensor possesses few long-range shared keys to sensors in distant groups. These inter-group shared keys should be distributed nearly uniformly over all the group distance scales. The scheme to implement such near-uniform key-predistribution on distant groups is described below and illustrated in Figure 2. Given a sensor node s of group $G_{i,j}$, for each neighboring group ($G_{i-1,j}$, $G_{i+1,j}$, $G_{i,j-1}$ or $G_{i,j+1}$), a shared key is established with a sensor node randomly chosen from that group. The rest of groups are partitioned into sets A_0, A_1, .., $A_{\log m}$, where A_k consists of the groups whose distance to $G_{i,j}$ is between 2^k to 2^{k+1}. According to the above definition, all groups in A_k are at approximately the same distance to group $G_{i,j}$. Within set A_k, a group is selected arbitrarily and a shared key is generated for s and a node randomly chosen from the group. In total, each sensor node needs to store at most $4 + 2 \log m$ inter-group shared keys and the memory overhead for storing the keys is in a logarithmic order to the number of groups.

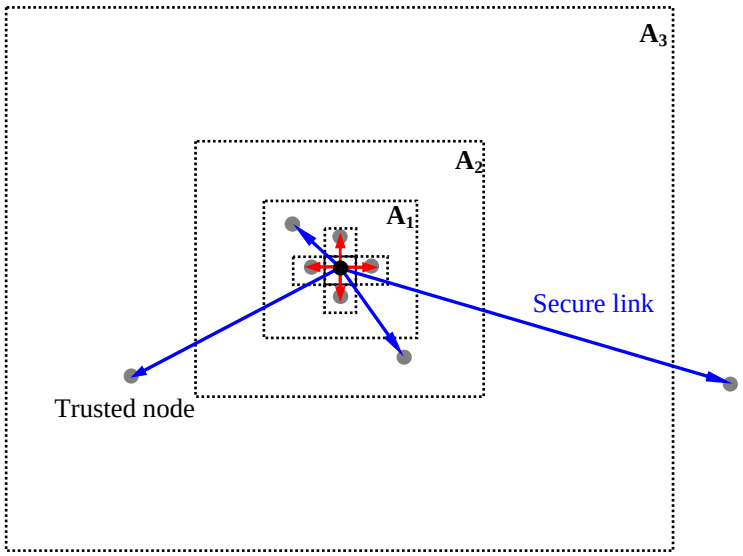


Fig. 2. A sensor node and its secure links to distant trusted peer nodes in the virtual key distribution space

2.2 Key Path Establishment

After the deployment of a sensor network, a key path establishment process is needed in order to build a secure path between any pair of sensor nodes. For any two intra-group sensors, because a shared key is pre-loaded into them, they can communicate securely with each other by using this key directly. However, for inter-group sensors, they need a key path establishment due to the lack of direct shared keys.

In this section, we present two methods for key path establishment: the pure greedy and the 1-hop greedy key path establishment. Since each sensor is only aware of local neighboring information, both two methods use only local information for key path establishment: the pure greedy method uses only a sensor node's own information to search for a path to the destination node, while 1-hop greedy method uses not only the local information but also the information from its neighbors for path establishment.

Pure Greedy Key Path Establishment

Suppose a sensor node receives a key establishment requirement from another node which contains the destination sensor ID. The sensor node reads the content of the message and it now needs to decide which sensor node is the next target to forward to, and processes it with a localized mechanism described as follows.

```
1. Determine the group which the destination sensor belongs to from the
   destination sensor ID.
2. S_next ← NULL
3. if (the destination sensor is in the same group)
4. {    S_next ← the destination sensor       }
5. else
6. {
7.      S_next ← the trusted node that is nearest to the destination in the
   sense of group distance.
8. }
9. Encrypt and delivery the key path establishment message to the selected
   node, S_next, using the corresponding shared key.
```

1-Hop Greedy Key Path Establishment

1-Hop Greedy method is motivated by real world experiences. When we look for some target, we search our memory first. If it is not found, we then ask our friends nearby for help. This is what 1-Hop Greedy method does, in which a sensor uses its own information and the neighbors' information for key path establishment. We define that a sensor is in phase j if the group distance between the sensor's group and the destination's group is greater than 2^j and less than or equal to 2^{j+1}. When such a sensor receives a request for key path establishment, it will check its own information first. If the sensor finds a trusted peer node that belongs to a phase less than j (the group distance to destination is at most 2^j), it forwards the message to that peer node. Otherwise, it broadcasts a message to its intra-group neighboring nodes to acquire their nearest trusted peers, and chooses the best one from the responses to forward to.

```
1. Determine the group which the destination sensor belongs to from the
   destination sensor ID.
2. j ← the phase number
3. S_next ← NULL
4. if (the destination sensor is in the same group)
5. {    S_next ← the destination sensor       }
6. else
7. {    S_next ← the trusted node that is nearest to the destination.
8.      if (S_next can not enter the phase less than j)
9.      {     Send messages to intra-group neighbors querying about their
                nearest trusted nodes to the destination.
10.           S_t ← the neighbor who has minimal result.
11.           S_r ← the nearest trusted peer node of S_t
12.           if (S_r can enter the phase less than j)
13.                S_next ← S_t
14.     }
15.}
16.Encrypt and deliver the message to S_next using the corresponding shared
   key.
```

Although both of the above key path establishment methods use greedy heuristic, the procedure terminates definitely and does not fall into an infinite loop. Because each sensor node has trusted peer nodes in its neighboring groups, the group distance from the message holder to the destination decreases strictly (at least 1) after each relay. This ensures the termination of the key path establishment procedure in both greedy methods.

3. Performance Metrics and Analysis

In this section, we will formally evaluate the performance of the proposed key management scheme. As described in the previous section, the memory overhead for key storage is logarithmic to the number of groups in the network. Another concerning performance is the number of intermediate trusted peer nodes in the key path between the two communicating ends. Fewer intermediate peers mean fewer number of decrypt/encrypt operations in total and thus save more energy and delay time. We also examine the communication overhead which presents extra energy for key path establishment.

In the proposed scheme, both the key preloading and key path establishing processes do not involve the real geography of the sensor field. Therefore, the performance of memory overhead and computing overhead is irrelevant to the method of group deployment. Only communication overhead concerns in the group deployment method.

3. 1 Memory Overhead

We estimate the number of keys that each node needs to preload for the key establishment scheme. This measure does not count the temporary storage that is needed during the execution of the scheme. In section 2.1, we have analyzed the number of preloaded keys needed for each node in our method; the memory overhead increases linearly with the group size and logarithmically with the number of groups.

Suppose that a group has l sensors and there are m^2 groups in the network. Each sensor has shared keys with all other sensors in the same group. Hence a sensor needs to store (l–1) intra-group keys. For inter-group keys, a sensor needs to share keys with non-diagonal neighboring groups. Since there are at most 4 non-diagonal neighboring groups around it, at most 4 such inter-group keys are required. For distant groups, it has a distant shared key with a group in set A_k, where k is at most $\log m$. Hence it needs to keep at most $2\log m$ such keys. In total, the number of keys preloaded in a sensor is at most $(l-1)+4+2\log m = l+2\log m+3$.

3.2 Computing Overhead

During the key path establishment, the request messages are relayed to the destination sensor node through a set of intermediated trusted peer nodes, where messages are decrypted to read the content and encrypted again to relay to the next trusted node. Hence, the total number of the decrypt/encrypt operations for a key path establishment is considered as the computing overhead which is proportional to the number of the intermediated trusted peer nodes along the established path.

3.2.1 Performance Analysis of Pure Greedy Key Path Establishment

We first analyze the upper bound of the expected total number of intermediate peer nodes in pure greedy method. Suppose sensor s is the sensor that holds the message and is in phase j, i.e. the group distance to the destination is greater than 2^j and at most 2^{j+1}. The value of j is at most log m. If sensor s can find a trusted peer node s' which can enter a phase less than j, s' must be in a group whose group distance is at most 2^j to the destination. Let B_j be the set of groups whose distance is within 2^j to the target group and A_j be the set of groups whose distance to the group of the message holder, s, is greater than 2^j and at most 2^{j+1} as described in section 2.1. The number of groups in the set A_j is at most

$$\begin{aligned}|A_j| &\le (2\times 2^{j+1}+1)^2-(2\times 2^j+1)^2\\ &= 12\times 2^{2j}+4\times 2^j.\end{aligned}$$

Let I_j denote the intersection of B_j and A_j. Sensor s is in phase j and the group distance to the destination is at most 2^{j+1}. Therefore, I_j has at least $(2^j+1)^2-1$ groups as shown in Figure 3. Since sensor s has a preloaded secure link to a randomly chosen group in A_j, the probability that this chosen group falls into I_j is

$$\begin{aligned}\frac{|B_j\cap A_j|}{|A_j|}=\frac{|I_j|}{|A_j|} &\ge \frac{(2^j+1)^2-1}{12\times 2^{2j}+4\times 2^j}\\ &= \frac{2^{2j}+2\times 2^j}{12\times 2^{2j}+4\times 2^j}\\ &\ge \frac{2^{2j}+2^j}{12\times 2^{2j}+12\times 2^j}=\frac{1}{12}.\end{aligned}$$

Hence, the probability that sensor s has an intermediate peer s' which can enter into a phase less than j is at least 1/12, as shown in Figure 3. In the case of Figure 3(a), A_j has maximal number of groups. The destination group

is as far as possible and the intersection of A_j and B_j , i.e. I_j is minimal. The probability that sensor s' locates in I_j is minimal but it is at least 1/12. In the case of Figure 3(b), the group of s is near the corner of the virtual space. A_j has fewer groups but I_j still has at least $(2^j + 1)^2 - 1$ groups. The probability that sensor s' locates in I_j is larger then 1/12.

Let X_j denote the total number of intermediate peer nodes that are in phase j. (X_0 is at most 1.) For $1 \le j \le \log m$, the expected number of X_j, is at most

$$EX_j \le \sum_{1}^{\infty} \left(\frac{1}{12}\right)\left(\frac{11}{12}\right)^{i-1} \times i = 12.$$

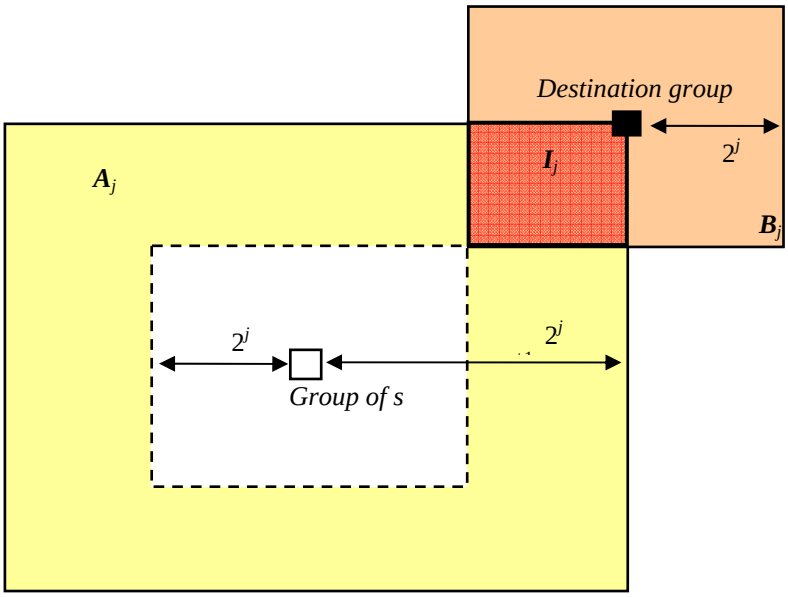
Let X be the total number of intermediate peer nodes, i.e.,

$$X = \sum_{j=0}^{\log m} X_j.$$

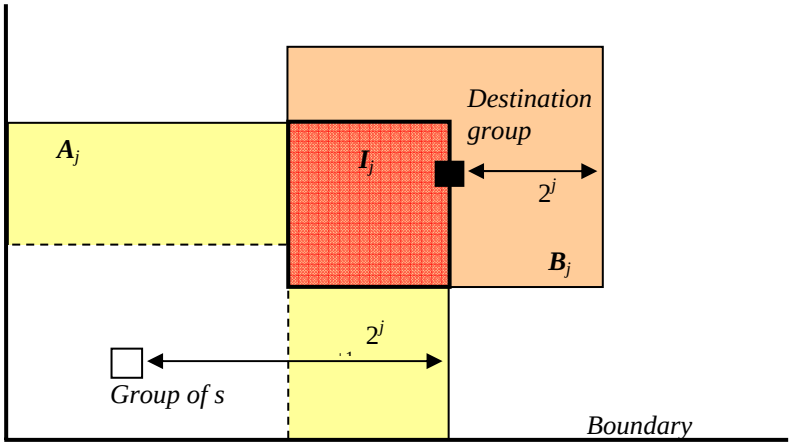
The average number of X is

$$EX \le 1 + 12 \log m.$$

Therefore, the upper bound of the expected total number of intermediate peer nodes by pure greedy method is logarithmic to the number of groups in the sensor network. This property makes the network a small world.



(a). A_j has maximal number of groups.



(b). The group of s is near the corner of the virtual space.

Fig. 3. A illustration of the probability that sensor s' locates in I_j

3.2.2 Performance Analysis of 1-Hop Greedy Key Path Establishment

Assume the node which is holding the message is in phase j and it has k intra-group neighbors. Let p be the probability that the neighbors have at least one trusted peer which can enter into a phase less than j. Then the value of p is

$$p \geq 1-(\frac{11}{12})^k.$$

X_j denotes the total number of intermediate peer nodes that are in phase j. Therefore, the upper bound of the expected number of X_j is

$$\begin{aligned} EX_j \leq\ & 1\times\frac{1}{12} + 2\times\frac{1}{12}\times p \\ & + 2\times\frac{1}{12}\times\frac{11}{12}(1-p) + 3\times p\times\left(\frac{11}{12}\right)^2\times(1-p) \\ & + 3\times\frac{1}{12}\times\left(\frac{11}{12}\right)^2(1-p)^2 + 4\times p\times\left(\frac{11}{12}\right)^3\times(1-p)^2 + \ldots \\ =\ & \sum_{i=1}^{\infty}\{i\left(\frac{1}{12}\right)\left(\frac{11}{12}\right)^{i-1}(1-p)^{i-1} + (i+1)p\left(\frac{11}{12}\right)^i(1-p)^{i-1}\}. \end{aligned}$$

Let $r = \frac{11}{12}(1-p)$. We have

$$EX_j \leq \frac{1}{12(1-r)^2} + \frac{11}{12}p(\frac{1}{r(1-r)^2} - \frac{1}{r}).$$

As the number of neighbors, k, is no smaller than 10, the expected number is smaller than 2.5, and the limit is 1.917 as k approaches infinity. The graph of the upper bound of EX_j as a function of k is shown in Figure 4. When k is no smaller than 10, the average number of the total number of intermediate nodes is smaller than or equal to 1 + 2.5 log m. The resulting order of 1-hop greedy method is the same as the one in pure greedy method but has smaller coefficient.

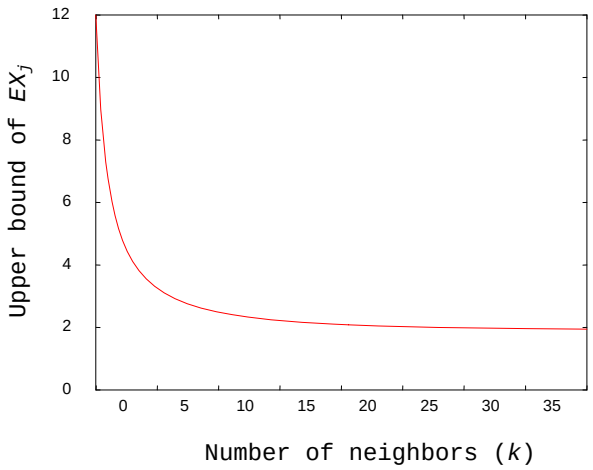


Fig. 4. The upper bound of the expected number of intermediate peer nodes in phase j

3.3 Communication Overhead

Similar to computing overhead, the communication overhead is proportional to the number of intermediate hops (i.e., the sensor nodes along a path) that a message routes though. If a key path is longer, the number of intermediate hops is larger too. Therefore, we define the communication overhead to be the total length of the secure links in the established key path. The communication overhead is related to the method of group deployment. In this section, we discuss the communication overhead for pre-determined group deployment and random group deployment.

3.3.1 Communication Overhead of Pre-Determined Group Deployment

Given two sensor nodes, if they have a shared key, they can build a direct secure link and the length of the link is the distance between them, hence the theoretical minimal communication overhead is the Euclidean distance between two sensors. If sensor nodes are uniformly distributed into a square of area *A*, the average distance between two sensor nodes [18] is $0.52\sqrt{A}$. Therefore, the expected communication overhead is better if the value is closer to $0.52\sqrt{A}$.

In pre-determined group deployment scheme, we assume that group $G_{i,j}$ is deployed into the cell of row *i* and column *j* in the sensor field. Thus, the group distance is proportional to the Euclidean distance. As the key path establishment algorithm tries to find a closest next sensor node in the sense of group distance, it also tries its best to find a shorter route to the destination in the same time. Consequently, the length of the key path is closed to the distance between the two end nodes.

For PIKE-2D [13], the intermediate trusted node for the two communication nodes may locates anywhere in the filed. Hence its expected communication overhead is twice of the theoretical minimal, i.e. $1.04\sqrt{A}$.

3.3.2 Communication Overhead of Random Group Deployment

Our scheme works well when groups are randomly deployed to the field. In our scheme, both the key preloading and key path establishing processes do not involve the real geography of the sensor field. The secure-link graph depicted in Figure 2 is an arrangement in the virtual key space and is not necessarily a real geographic map for group deployment. The performance of random group deployment including memory overhead and computing overhead is the same as that of pre-determined group deployment.

However, the performance of communication overhead and the underlying routing protocol are different. If the sensor groups are randomly distributed to the sensor field, the next target of sensor node may locate anywhere in the field. The expected length of a single secure link is thus $0.52\sqrt{A}$, where *A* is the area of the sensor field. Hence the expected communication overhead is $0.52\sqrt{A}$ multiplied by the number of intermediate secure links. With random group deployment, the group ID has no relationship with the geographical location. Therefore, geographical routing methods could not be applied directly. Other routing schemes such as directed diffusion [19] and GPSR [20] are possible solutions for the underlying routing protocol. GPSR is a globally addressable communication infrastructure, in which the locations of arbitrary nodes could be discovered efficiently via a geographic hash table, and a geographic routing could be used as the routing protocol.

4. Simulations

We also use simulations to verify the performance of the proposed key distribution scheme. The simulation results including memory overhead, computing overhead, and communication overhead are compared to the PIKE-2D scheme [13]. The proposed schemes are implemented in C language and run under an Intel Intel® Core™ Duo machine.

In the experiments, sensor groups are deployed in a pre-determined scheme. The sensor field is partitioned into *m*×*m* square cells, where *m* is the number of groups. Group $G_{i,j}$ is then placed into the cell of row *i* and column *j* in the sensor field. The number of the sensor nodes varied from 10,000 to 250,000 and the number of sensors per group was set to 25. Sensors for a group were deployed according to a two-dimensional Gaussian distribution in the corresponding group cell. The average density of sensors is 0.01 node per square meter. The default wireless communication range is 30 meter. Hence the number of neighbors in communication range is about $30^2\pi * 0.01 \fallingdotseq 28$.

Figure 5 shows the memory overhead of our scheme and PIKE-2D. Our method requires very low memory for key storage. For a sensor network of m^2 groups, with group size *l*, our method preloads $l + 3 + 2\ log\ m$ keys to each sensor as described in the previous section. In contrast, the memory overhead of PIKE-2D is $\left\lceil \sqrt{n} \right\rceil + 1$, where *n* is the total number of sensors. Thus, our scheme has better performance on memory overhead than the latter, especially when the network size is large.

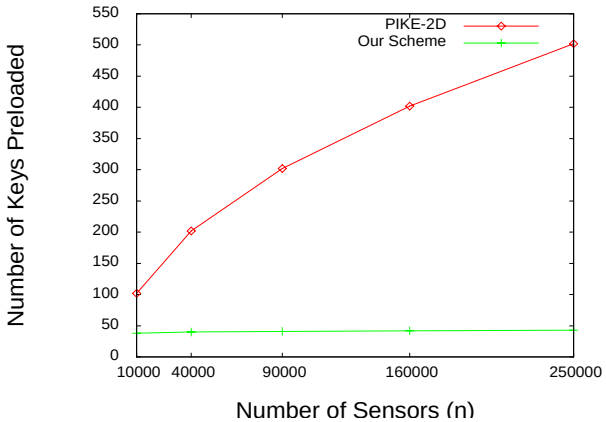


Fig. 5. Memory requirement in our scheme and PIKE-2D

Figure 6 shows the computing overhead of our scheme and PIKE-2D. The computing overhead of our method is logarithmic to the number of sensor groups according to the analysis in section 3. Hence the average number of intermediate peer nodes increases very slowly with respect to the network size. The simulation result for pure greedy method shows that even when the network size is 250,000, the value is still smaller than 8. The result for 1-hop greedy method is even better than pure greedy method.

For the scheme of PIKE-2D, there is always an intermediate trusted node between any two nodes. Therefore, the average number of intermediate nodes for it is always 1. Although our results are worse than PIKE-2D's, they are nearly in the same order, i.e., they are all smaller than 8. This is a trade-off between memory overhead and computing overhead. Our method spends much less memory space for key storing with only a little increase in computing overhead.

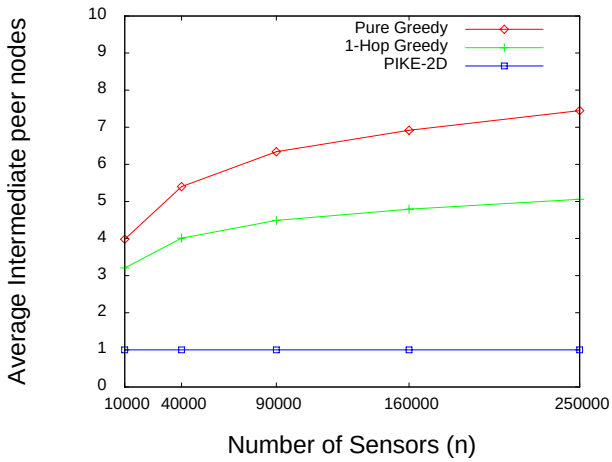
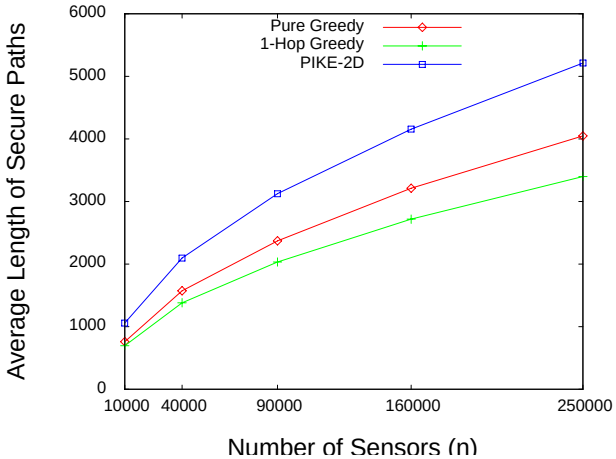
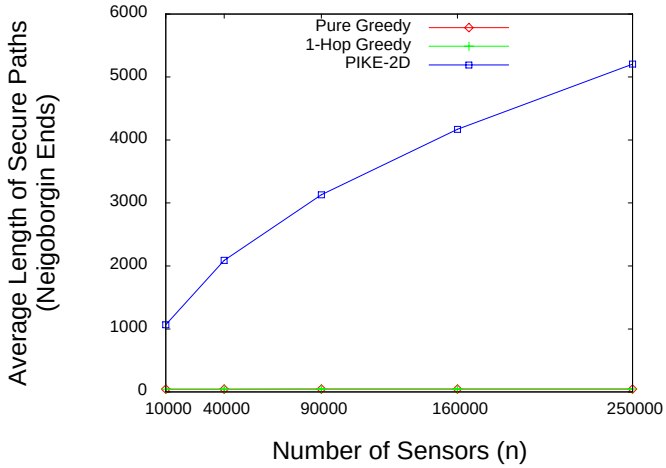


Fig. 6. Computing overhead in our scheme and PIKE-2D

On the other hand, although PIKE-2D has constant computing overhead, it consumes more energy for communication and routing. The intermediate trusted node for communication could be located anywhere in the sensor field; hence a sensor needs to route to the distant trusted node and makes the communication overhead very high. Figure 7 shows simulation results of communication overhead. In Figure 7(a), randomly selected pairs are used as the source node and the destination node. Both of our methods outperform PIKE-2D. The 1-Hop Greedy method has lower average length of secure paths than that of the Pure Greedy method, because the 1-Hop Greedy method uses more information than the Pure Greedy method. In Figure 7(b), neighboring pairs of nodes are used as the source node and the destination node. In this case, the average length of secure paths of both our methods is 2, because in our methods, there is a direct secure link between the neighboring pair of nodes.



(a) Average communication overhead for random selected pairs.



(b) Average communication overhead for neighboring pairs.

Fig. 7. Communication overhead in our scheme and PIKE-2D

5. Conclusions

We have proposed a group-based key pre-distribution scheme based on the concept of small worlds. With the proposed scheme, any two sensor nodes in the network can efficiently establish a secure transmission path. Our scheme does not require a specific group deployment method. The memory overhead for key storage is logarithmic to the number of sensor groups; hence, each sensor node needs only to carry few keys even if the size of the sensor network is very large.

Our paper presents two different greedy methods for the key path establishment. Both methods use only local information from nearby sensors, and hence they are practical under the resource constraints on wireless sensor networks. We evaluated the performance of our method both by analysis and by simulations. The results indicate that the presented scheme is superior to current methods.

In this paper, we only consider the secure communications among homogenous sensors. However, hierarchical network structures usually enable more efficient use of scarce resources. How to integrate our key management scheme with sensor clustering techniques is a challenging problem, and will be our study in future. In addition, how to improve the performance when the sensor groups are randomly deployed remains another interesting problem.

6. Acknowledgement

This work was partially supported by the TWISC@NCKU project sponsored by the National Science Council, Taiwan, under the Grant Nos. NSC 98-2219-E-006 -001 and NSC 95-2221-E-110 -083.

References

[1] F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks," *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-114, 2002.

[2] L. Eschenauer and V. Gligor, "A Key-management Scheme for Distributed Sensor Networks," *Proceedings of the 9th ACM Conference on Computer and Communication Security*, Washington, DC, USA, pp. 41-47, 2002.

[3] H. Chan, A. Perrig, D. Song, "Random Key Pre-distribution Schemes for Sensor Networks," *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, California, USA, pp. 197-213, 2003.

[4] W. Du, J. Deng, Y. S. Han, S. Chen, P. Varshney, "A Key Management Scheme for Wireless Sensor Networks using Deployment Knowledge," *Proceedings of IEEE INFOCOM* 2004, pp. 590-597, 2004.

[5] D. Huang, M. Mehta, D. Medhi, L. Harn, "Location-aware Key Management Scheme for Wireless Sensor Networks," *Proceedings of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks*, pp. 29-42, 2004.

[6] Z. Yu and Y. Guan, "A Key Pre-distribution Scheme using Deployment Knowledge for Wireless Sensor Networks," *Proceedings of ACM/IEEE International Conference on Information Processing in Sensor Networks*, pp. 261-268, 2005.

[7] S. Milgram, "The Small World Problem," *Psychology Today*, Vol. 61, No. 1, pp. 60-67, 1967.

[8] D. Watts and S. Strogatz, "Collective Dynamics of Small-world Networks," *Nature*, Vol. 393, pp. 440-442, 1998.

[9] S. A. Camtepe and B. Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks," *IEEE/ACM Transactions on Networking*, Vol. 15, No. 2, pp. 346-358, 2007.

[10] W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, A. Khalili, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks," *ACM Transactions on Information and System Security*, Vol. 8, No. 2, pp. 228-258, 2005.

[11] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," *ACM Transactions on Information and System Security*, Vol. 8, No. 1, pp. 41-77, 2005.

[12] D. Liu, P. Ning, W. Du, "Group-based Key Predistribution for Wireless Sensor Networks," *ACM Transactions on Sensor Networks*, Vol. 4, No. 2, 2008.

[13] H. Chan and A. Perrig, "PIKE: Peer Intermediaries for Key Establishment in Sensor Networks," *Proceedings of IEEE INFOCOM 2005*, Miami, USA, pp. 524-535, 2005.

[14] C. Korte and S. Milgram, "Acquaintance Networks between Racial Groups: Application of the Small World Method," *Journal of Personality and Social Psychology*, Vol. 15, No. 2, pp. 101-108, 1978.

[15] J. Travers and S. Milgram, "An Experimental Study of the Small World Problem," *Sociometry*, Vol. 32, No. 4, pp. 425-443, 1969.

[16] L. A. N. Amaral, A. Scala, M. Barthelemy, H. E. Stanley, "Classes of Small World Networks," *PNAS*, Vol. 97, No. 21, pp. 11149-11152, 2000.

[17] J. Kleinberg, "The Small-world Phenomenon: An Algorithm Perspective," *Proceedings of 32nd ACM Symposium on Theory of Computing*, Portland, Oregon, USA, pp. 163-170, 2000.

[18] B. Ghosh, "Random Distances within a Rectangle and between Two Rectangles," *Bulletin of the Calcutta Mathematical Society*, Vol. 43, pp. 17-24, 1951.

[19] C. Intanagonwiwat, R. Govindan, D. Estrin, “Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks,” *Proceedings of the 6th Annual International Conference on Mobile Computing and Networkin*g, pp.56-67, 2000.

[20] B. Karp and H. T. Kung, “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks,” *Proceedings of the Sixth International Conference on Mobile Computing and Networking*, Boston, Massachusetts, USA, pp. 243-254, 2000.