SCIS 2007 The 2007 Symposium on
Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics,
Information and Communication Engineers

Key Predistribution Scheme for Wireless Sensor Networks with Higher Connectivity

Zeen Kim * Jangseong Kim * Kwangjo Kim *

Abstract— In wireless sensor network (WSN), preditibution of cryptographic keys is possibly the most practical approach to perfect network communications. In this paper, we propose a new secret key predistribution scheme to achieve a higher connectivity in WSN. For this we combine a random key predistribution scheme and hash chain method based on the prior knowledge of sensor node deployment. The proposed scheme has two advantages. First, the proposed scheme provides a higher connectivity. Second, our scheme reduces the storage requirement for each sensor node. We compare the proposed scheme with previous key predistribution schemes in memory usage, local connectivity, global connectivity, and network resiliency against node capture.

Keywords: Wireless Sensor Network, Random Key Predistribution, Network Connectivity

1 Introduction

In the ubiquitous environment, Wireless Sensor Network (WSN) is the most important infrastructure. WSN usually consists of a large number of tiny sensor nodes with limited computation capacity, memory space and power resource. Typically, WSNs are deployed at high density in regions requiring surveillance and monitoring. Individually, each sensor node senses many interesting phenomena with simple computations and transfers this information to others or base-station using wireless communication channel.

WSNs are, therefore, vulnerable to various kinds of malicious attacks like eavesdropping, masquerading, traffic-analysis, *etc*. Hence, it is important to protect communications among sensor nodes to maintain message confidentiality and integrity. However, for this, the utilization of public key cryptosystems is infeasible since sensor nodes suffer from resource constraints like low power, limited computation capability, communication, *etc*. Therefore, the symmetric key cryptosystems are usually facilitated for WSNs to establish the secure communication channel between sensor nodes. Hence, recent researches mainly focus on the efficient key predistribution scheme for sharing the secret keys between sensor nodes to utilize the symmetric cryptosystems.

Recently, many random key pre-distribution schemes [4, 1, 6, 7, 2, 3] have been proposed. The main advantage of random key pre-distribution schemes is that communication costs per sensor node are constant regardless of the total number of sensor nodes in the WSN. Random key pre-distribution was first proposed by Eschenauer *et al.*. Chan *et al.* extended this scheme to enhance the security and resilience of the network using q-compositeness. Du *et al.* and Liu *et al.* further extended random key pre-distribution approach to pairwise key pre-distribution approach in which the shared key between any two sensors is uniquely computed so that the resilience against node capture is significantly improved. They also proposed the schemes which facilitate the location of each sensor node as pre-deployment knowledge. In 2005, Part *et al.* define the problems of previous random key pre-distribution schemes and propose a memory-conserving scheme that facilitates new pre-deployment knowledge, *state of node* , as a solution.

Our Contribution

In this paper, we propose a new key predistribution method which provides higher network connectivity than previous schemes. Our proposed scheme is designed by combining hash-chain method and key map method. We can reduce memory usages for key ring of each sensor node. Hence, our proposed scheme can be applied to large-scale wireless sensor network.

Organizations

The rest of our paper is organized as follows. In Section 2, we describe the background closely related to ours and introduce some previous key predistribution schemes. We describe detailed our proposed key predistribution scheme in Section 3. In Section 4, we consider the pros and cons of our proposed scheme in the sense of network connectivity, network resiliency against node capture, and memory usages. Then we compare our scheme with previous key predistribution schemes. Finally, we conclude with open problems and future work in Section 5.

* School of Engineering, Information and Communications University, 119, Munjiro, Yuseong Gu, Daejeon, 305-732, Korea. ({zeenkim,withkals,kkj}@icu.ac.kr)

2 Preliminaries and Related Work

2.1 WSN

WSN usually consists of a large number of tiny sensor nodes, which are equipped with limited computing and radio communication capabilities. They operate in various kinds of fields, performing tasks such as environmental monitoring and surveillance. A typical network configuration is composed of sensors working unattended and transmitting their observation values to some processing or control center, the so-called base station, which serves as a user interface. Due to the limited transmission range, sensors that are far away from the base station deliver their data through multi-hop communications, *i.e.*, using intermediate nodes as relays.

Simple application scenario of WSN can be as follows: When nodes senses some interest phenomena such as an invader, *etc.*, they perform some simple computations and then forward data to upstream nodes for aggregation. After data aggregation is completed, data is transmitted to the base station for future and valuable usage of the collected data. For instance, this data may be facilitated for calling the policy directly after sensing the fact that here comes an intruder.

Since every communication between sensor nodes is transmitted via unreliable wireless communication channel, the data is vulnerable to the eavesdropping attack done by adversaries. If sensitive data is not encrypted, then a loss of confidentiality may occur if someone passively monitors the transmissions emanating from the WSN. Furthermore, without applying authentication mechanism to WSN, data aggregation is also vulnerable to replay attack since authenticating of its downstream peers becomes a critical issue. Besides, DoS, spoofing, resource-exhaustion attack, *etc.*, can be the potential attacks for WSN[9].

To address these security threats, secret key should be pre-loaded to each sensor for guaranteeing the secure operation of WSN. Therefore, secure key management, especially key pre-distribution arises as a prominent research area for WSN. The key pre-distribution means that key information is distributed among all sensor nodes prior to deployment.

2.2 Random Graph

In a WSN without pre-deployment knowledge, sensor nodes can be viewed as random points which are uniformly distributed (*i.e.*, with equal probability). Thus, the sufficiency problem of the secure links resided in a WSN can be reduced to the connectivity problem of the generalized random graph, which, hence, can be mathematically treated using the well known connectivity theory for random graph by Erdös and Rényi [5]. The connectivity of a key graph $G(V, E)$ is then given as: for monotone properties, there exists a value of p such that the property moves from "nonexistent" to "certainly true" in a very large random graph. The function defining p is called the threshold function of a property. If $p = \frac{\ln(n)}{n} + \frac{c}{n}$, with c any real constant then

$$P_c = \lim_{n\to\infty} Pr([G(n,p) \text{ connected}]) = e^{-e^{-c}}$$

where P_c denotes the desired possibility that the key graph is connected. In addition, n denotes network size and d denotes the node degree (*i.e.*, the average number of edges connected to each node) necessary to assure that the key graph is connected with probability P_c. p is the probability that an edge between any two nodes exists in $G(V, E)$:

$$p = \frac{d}{n}$$

Due to the inherent communication constraints in WSNs, a sensor node can only communicate directly with its n' neighboring nodes. Since the expected node degree must be at least d as calculated, the required probability of successfully performing key-setup with some neighboring node is now:

$$p = \frac{d}{n' - 1}$$

This implies that any two nodes in the WSN should share at least one secret key with probability no less than $p_{required}$. Further, the probability of two nodes i and j sharing at least one secret key can be computed as follows:

$$p = Pr(\mathcal{R}_i \cap \mathcal{R}_j \neq \phi) = 1 - Pr(|\mathcal{R}_i \cap \mathcal{R}_j| = 0)$$

where $\mathcal{R}_i$ is size of key ring on node i.

2.3 Key Predistribution Scheme

Let m denote the number of distinct cryptographic keys that can be stored on a sensor node. The basic key predistribution scheme works as follows. Before sensor nodes are deployed, an *initialization phase* is performed. In the initialization phase, the basic scheme picks a random pool (set) of keys S out of the total possible key space. For each node, m keys are randomly selected from the key pool S and stored into the node's memory. This set of m keys is called the node's *key ring.* The number of keys in the key pool, $|S|$, is chosen such that two random subsets of size m in S will share at least one key with some probability p.

After the sensor nodes are deployed, a *key-setup phase* is performed. The nodes first perform key-discovery to find out with which of their neighbors they share a key. Such key discovery can be performed by assigning a short identifier to each key prior to deployment, and having each node broadcast its set of identifiers. Nodes which discover that they contain a shared key in their key rings can then verify that their neighbor actually holds the key through a challenge-response protocol. The shared key then becomes the key for that link.

After key-setup is complete, a connected graph of secure links is formed. Nodes can then set up *path keys* with nodes in their vicinity whom they did not happen to share keys with in their key rings. If the graph is connected, a path can be found from a source node to its neighbor. The source node can then generate a path key and send it securely via the path to the target node.

2.4 Related Work

The Eschenauer-Gligor scheme [4] have been described earlier in this section. We will give a more detailed description of this scheme in Section II. Based on the Eschenauer-Gligor scheme, Chan, Perrig, and Song proposed a q-composite random key pre-distribution scheme [1]. The difference between this scheme and the Eschenauer-Gligor scheme is that q common keys ($q \geq 1$), instead of just a single one, are needed to establish secure communications between a pair of nodes. It is shown that, by increasing the value of q, network resilience against node capture is improved, *i.e.*, an attacker has to compromise many more nodes to achieve a high probability of compromised communication.

Du, Deng, Han, and Varshney proposed a new key predistribution scheme [2], which substantially improves the resilience of the network compared to the existing schemes. This scheme exhibits a nice threshold property: when the number of compromised nodes is less than the threshold, the probability that any nodes other than these compromised nodes are affected is close to zero. This desirable property lowers the initial payoff of smaller scale network breaches to an adversary, and makes it necessary for the adversary to attack a significant proportion of the network. A similar method is also developed by Liu and Ning [6].

The ideas described in this paper can be applied to all of the above pre-distribution schemes to further improve their performance.

In 2005, Part *et al.* proposed a novel random key predistribution scheme [8] that exploits new deployment knowledge, ***state of sensors***, to avoid unnecessary key assignments and reduce the number of required keys that each sensor node should carry while supporting higher connectivity and better resilience against node captures.

In 2005, Ito *et al.* proposed an advanced key predistribution scheme in which different keys are logically mapped to twodimensional positions, and the keys that are distributed to a node are determined by positions estimated using a node probability density function. [10]

3 Our Proposed Scheme

In this section, we propose an advanced key predistribution scheme. Our proposed scheme consists of three phase; key pool generation, key ring assignment, and shared key discovery. Key pool generation phase and key ring assignment phase is proceeded in offline. Only shared-key discovery phase works in online.

Key Pool Generation

The key pool generation phase of our scheme is performed as follows.

1. Set security parameters k, l. The parameter k is the size of the key block and l is the number of keys stored by each block. These parameters are determined according to the resources of the nodes and requirements of network connectivity/resilience.

2. Divide the target deployment area into $k \times l$ areas of the same size. We refer to each area as a subarea. 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 *seed* and k block seed g_i $(1 \leq i \leq k)$.

4. Compute the key chain of block i from *seed* and g_i. m-th key chain value is computed by

$$H^m(seed, g_i = H(H^{m-1}(seed, g_i), g_i)$$

Fig. 1 shows an example of the resulting key-position map example (k=4, l=9).

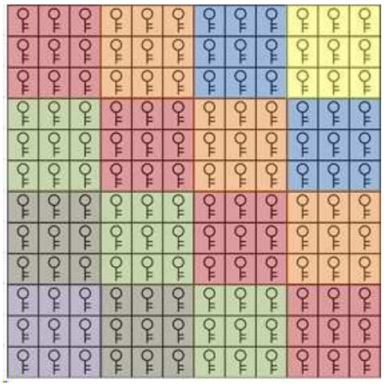

Figure 1: Key Position Map

Key Ring Assignment

The key ring assignment phase of our scheme is performed as follows.

1. For a node S, select one highly expected resident point P according to the pdf of $S, Pr(x, y)$. Send the seed and block seed where the P is positioned to S.

2. Randomly select one point Q within a circle of radius r and intersection area of another key block and communication range.

3. Store the key assigned to Q to node S. If the key from same block already exists in S, start again from step 2.

4. Repeat steps 1 ∼ 3 until node S has r keys.

5. Repeat steps 1 ∼ 4 for all nodes.

Following Figure 2 shows an example of key ring assignment.

Shared-Key Discovery

When network deployment is completed, each sensor node send their own block and key information. The index information is defined as $BlockNumber||K_1, K_2, \cdots, K_r$ where $K_i = BlockNumber||ChainNumber$. After each node knows what block and keys are contained in its neighbor, shared-key discovery process between node N_i and N_j is as follows.

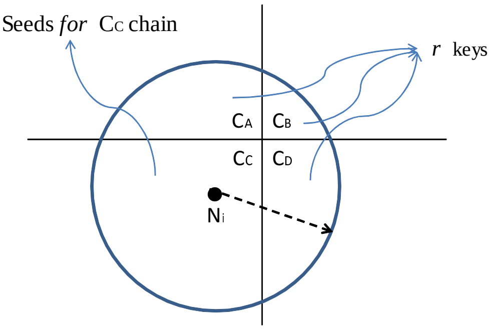

Figure 2: Key ring assignment

1. Check the $BlockNumber$ is same or not. If two nodes have same block number, then their shared key is $H(seed, g)$.
2. If two nodes have different block index, initiator node find a key index K_x which belongs to initiator's key block from the random key index of responder node.
3. Initiator compute the key value k_x of matched key index by hash computation with block seed value. When the computation is completed, two nodes can communicate using the shared key k_x

4 Analysis and Comparison

4.1 Evaluation Metrics

The performance of random key pre-distribution schemes can be evaluated on the basis of several criteria. In particular, we choose connectivity and resilience against node capture as the criteria for performance evaluation.

4.2 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. Global connectivity is the ratio of the size of the largest connected component to the size of the entire network. We also present the results of simulations for comparing the connectivity and network resiliency of the previous key predistribution schemes with that of our scheme. In the simulations, we use the common conditions listed below.

Each node can compute whole keys in their own block. So, we can easily prove the following theorem.

Theorem 1 *If r random keys cover the whole blocks which have intersection with communication range, then two nodes which lie in communication range share a shared key with probability 1.*

The following figure is local connectivity connectivity when communication range and cell size are same size of area.

- The size of the key pool is 100000.

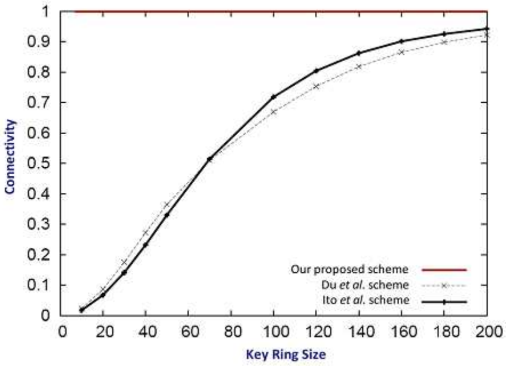

Figure 3: Local connectivity

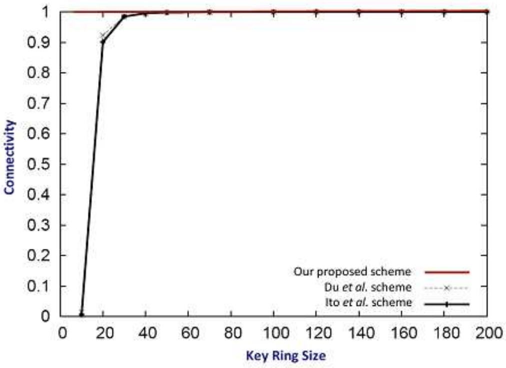

Figure 4: Global connectivity

- 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 factors3 are $a = 0.167$ and $b = 0.083$.

The higher the local connectivity, the less frequent the occurrence of the path-key establishment phase; hence, it leads to low communication overhead. So our proposed scheme is very useful for communication overhead for key agreement between any two sensor nodes.

Following figure is global connectivity under the same condition, communication range is same size of area with cell area.

4.3 Network Resiliency

Our proposed scheme is designed for providing almost perfect connectivity with reducing the effect from node capture. This scheme can be obtained enough security level by changing the block size. Now we prove that it is impossible to compute key chain without block seed value. The key chain for each block is computed by $H^k(seed, g_i) = H(H^{k-1}(seed, g_i), g_i)$ (where g_i is key seed for block i. If an adversary get $H^k(seed, g_i)$, it is infeasible to compute previous hash value by the one-way property of hash functions. It is also hard to find next hash value without knowing seed value for key block since hash computation use the seed value as its input. From this we can derive the following theorem.

Theorem 2 *If any key on the key position block is compromised, the adversary cannot get any information without knowing block seed value.*

4.4 Memory Usage

Each sensor node stores only one common seed value, one block seed value, and r random keys. Hence we can reduce the memory usage for predistributed keys through control of block size and key chain length. The requirements of value r is just larger than the number of blocks where neighbor sensor nodes exists. In the case of cell area is same as communication range, $r = 3$ is enough to get same network connectivity.

5 Concluding Remarks

In this paper, we have proposed a new key predistribution scheme for wireless sensor network which provide higher network connectivity. Our proposed scheme is designed as flexible for balance control between connectivity and network resiliency. When the key block area is larger than communication range of sensor node, network resiliency against node capture attack is decreased. The novelty of this approach is that, instead of requiring the sensor nodes store all the assigned keys, the majority of the keys are represented and stored in term of key generation sets with a very small size by carefully designing the key pool, which significantly reduces storage space. The proposed scheme is hence, highly scalable to the larger network sizes.

As the future work, we would like to find optimal trade-off between network connectivity and resiliency against node capture attack. Another work is design a new key predistribution scheme from different deployment knowledge. To the best of our knowledge, there are two deployment knowledge; *location* and *state* of sensor nodes. We need to research on light-weight cryptography for wireless sensor network. Further, we will take different types of active attacks into consideration besides random node capture attack and optimize the scheme accordingly.

References

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

[2] W. Du, J. Deng, Y. S. Han, and P. Varshney, "A Pairwise Key Predistribution Scheme for Wireless Sensor Network", *In Proc. of 10th ACM Conference on Computer and Communications Security (CCS)*, Washington D.C., October 27-31, 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", *IEEE INFOCOM 04*, March 7-11, 2004, Hong Kong.

[4] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", *In Proc. of 9th ACM conference on Computer and Communications Security 2002*, Washington D.C., USA.

[5] Erdös and Rényi. On random graphs I. Publ. Math. Debrecen, 6:290–297, 1959.

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

[7] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks", *In Proc. of 10th ACM Conference on Computer and Communications Security (CCS03)*, Washington D.C., October, 2003.

[8] J. Park, Z. Kim, and K. Kim "State-based key management scheme for wireless sensor networks," Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on 7-10 Nov. 2005

[9] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, *Wireless Sensor Networks*, *Kluwer Academic Publishers.*

[10] Takashi Ito, Hidenori Ohta, Nori Matsuda, and Takeshi Yoneda, "A Key Pre-Distribution Scheme for Secure Sensor Networks Using Probability Density Function of Node Deployment", SASN05, November 7, 2005, Alexandria, Virginia, USA.