JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 39, 459-472 (2023)
DOI: 10.6688/JISE.202305_39(3).0001

# A Grid-Based Key Pre-Distribution Scheme Using Dependent Keys in Wireless Sensor Networks*

IUON-CHANG LIN[1,+], YU-WEN WANG[2] AND TING-XUAN TAI[3]
[1]*Department of Management Information Systems*
*National Chung Hsing University*
*Taichung, 402 Taiwan*
[2]*ZYXEL Communication Corp.*
*Hsinchu, 300 Taiwan*
[3]*National Center for High-Performance Computing*
*Tainan, 744 Taiwan*
*E-mail: iclin@nchu.edu.tw; b45246@gmail.com; g7108029205@smail.nchu.edu.tw*

Recently, with the development of the technology, the applications of the wireless sensor networks are getting very common in our life. In order to enhance the security of the wireless sensor network, there are many key distribution protocols have been proposed recently. Among those key distribution protocols in wireless sensor networks, the key pre-distribution protocol is a more effective and more practical method. It enables sensor nodes to communicate with each other by less communication and computation overheads; it will effectively save the energy of the sensor node and extend the lifetime of the networks. In this paper, we propose an improved key pre-distribution scheme based on the basic probabilistic key pre-distribution protocol with grid-based deployment. In grid-based key pre-distribution scheme (GBKD), the keys with a hidden information will pre-distributed to the sensor nodes so they can establish the pair-wise key more effectively. Our performance analysis shows that the proposed schemes can provide better connectivity and lower memory overhead for the wireless sensor networks. The DSN designer also can adjust the variables of the sensor networks to produce an appropriate performance for the requirement of the application.

***Keywords:*** wireless sensor networks, key pre-distribution, grid-based, node capture, key management

## 1. INTRODUCTION

Wireless sensor networks are drawing a lot of industrial and academic attention and become an active research area recently. Due to the development of scientific and technological progress, the wireless sensor network consisting of a large number of low-cost, low-power and multi-functional sensor nodes that communicate and operate with wireless links are become possible. The sensor nodes can cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants [1, 2]. The wireless sensor networks are now mainly use in many military, industrial and civilian application areas such as battlefield surveillance, industrial process monitoring and control, health monitoring, environment monitoring and traffic control [1, 2].

Because of the sensor nodes are usually deployed in an open or hostile environment, the wireless sensor networks are vulnerable to many attacks [2]. Hence, the security of the

Received January 4, 2022; revised February 24, 2022; accepted March 29, 2022.
Communicated by Po-Wen Chi.
* This research was sponsored by Ministry of Science and Technology, Grant Nos. 110-2218-E-005 -008-MBK and 110-2218-E-005-018.

communication between sensor nodes becomes extremely important. However, due to the resource constraints on sensor nodes such as energy, memory, computational speed and bandwidth, it is not feasible for the sensor networks to use traditional cryptography techniques such as public key cryptography or key distribution center to establish keys between communicating sensor nodes [18, 19].

In order to solve the issue, security service such as authentication and key management are critical. Hence, there are many key management schemes have been proposed [3-16]. Most researcher have focus on provide efficient encryption and decryption algorithms that consider the resource constraints.

Eschenauer and Gligor proposed a basic probabilistic key pre-distribution scheme for pair-wise key establishment [4]. The main idea of the scheme is the back-end system randomly assigns a sub-set of keys from a key pool to each sensor nodes before deployment. As a result, any two sensor nodes will have a certain probability to share at least one common key after deployment. The scheme was further developed into two key pre-distribution techniques by Chan *et al.*: *q*-composite key pre-distribution and random pair-wise keys scheme [7]. Both schemes improve the security of the basic probabilistic key pre-distribution.

However, these pair-wise key establishment schemes still have security issue. For the basic probabilistic key pre-distribution, the more sensor nodes were compromised, the more fractions of pair-wise keys were affected. Moreover, the major drawback of the probabilistic key pre-distribution scheme is the connectivity of the networks is relying on the probability, the schemes cannot ensure the key sharing between any two sensor nodes.

In order to solve the problems, Liu *et al.* developed a general framework for pair-wise key establishment based on the polynomial-based key pre-distribution protocol and the probabilistic key pre-distribution scheme [6, 9]. A grid-based key pre-distribution scheme also has been proposed in the paper. The main idea of the grid-based key pre-distribution scheme is assigned each sensor nodes to the unique intersection of a constructed grid; each sensor nodes then distributed two polynomial shares. As a result, the sensor nodes can perform shared key discovery and path discovery based on the polynomial shares. The grid-based key pre-distribution scheme guarantees that any two sensor nodes can establish pair-wise key when there is no compromised sensor nodes, even if there are sensor nodes are compromised, the non-compromised sensor still have a high probability to establish pair-wise key.

Laih *et al.* proposed an adaptive key pre-distribution model with the concept of dependent key in distributed sensor networks [15]. In the scheme, the key pool divided into several group and each group are inserted with additional information during the key pool generation. The keys then randomly distributed to each sensor nodes and the sensor nodes can use the additional information to increase the system performance. This method can greatly increase the connectivity of the networks even if the sensor nodes deployment is non-uniform. Moreover, high connectivity decreases the energy consumption and extends the lifetime of the networks.

In this paper, we briefly review the polynomial-based grid-based key pre-distribution schemes [6] and the adaptive key pre-distribution scheme [15]. We combine the both schemes together and proposed an improved pair-wise key establishment scheme. In our proposed scheme, instead of using polynomial shares in the grid-based key pre-distribution, we use the concept of dependent key in the key pool generation. In our scheme we divide

it into five stages to establish WSN secure connection: Key pool generation, Key pre-distribution, Shared-key discovery and Path-key establishment phases. We generate a pool of keys by Shamir's thresholding scheme and distribute these keys randomly across the sensor network of the grid. The key that this method can hide information will be pre-distributed to the sensor nodes so that they can establish pairwise keys more efficiently.

Our performance analysis shows that the proposed scheme can provide better connectivity compared to the EG scheme [4] and the adaptive key pre-distribution scheme [15]. On the other hand, the memory overhead for each sensor node in the proposed scheme is lower than the polynomial-based grid-based key pre-distribution scheme too [6].

The rest of the paper is organized as follows. We will briefly review the basic probabilistic key pre-distribution scheme, the grid-based key pre-distribution scheme and the adaptive key pre-distribution scheme in Section 2. Section 3 introduces our proposed scheme in detail and followed by a further analysis of the proposed scheme in Section 4. Finally, the conclusions of this paper will provide in Section 5.

## 2. REVIEW OF THE KEY PRE-DISTRIBUTION SCHEMES

In this section, we briefly review some key pre-distribution schemes.

### 2.1 The Basic Probabilistic Key Pre-Distribution Scheme

Eschenauer and Gligor [4] proposed the basic probabilistic key pre-distribution scheme. We call this scheme as EG scheme in the rest of the thesis. The three phases of the EG scheme: key pre-distribution phase, shared key discovery phase, and path key establishment phase.

#### 2.1.1 Key pre-distribution phase

The operation of the key pre-distribution phase is performed offline before the deployment of the sensor node. Firstly, the back-end system generated a key pool and the corresponding key identifiers, then each sensor node randomly selects a sub-set of keys from the key pool to form key ring. Then each sensor node loads the key ring and corresponding key identifier into its memory.

#### 2.1.2 Shared-key discovery phase

After the sensor nodes deployment, the sensor nodes broadcast the list of their key identifiers in plaintext with its neighbors in order to discover the common keys in their key rings. If there is a shared key between two sensor nodes, the two sensor nodes use the shared key to secure their communication.

#### 2.1.3 Path-key establishment phase

After the shared-key discovery phase is completed, the connected graph of the securely communication links in the network are formed. However, some neighboring sensor nodes may not be able to form a secure link because there is no public key in their key ring. Therefore, these sensor nodes must establish path keys. Path keys can be derived from the

source node to the target node through their shared neighbors. Then the sensor node uses the unused key in its key ring as the path key.

This mentioned key pre-distribution scheme can establish a secure connection for WSN, but it is not perfect in establishing a connection path, which will cause waste of connection efficiency.

### 2.2 Polynomial-based Grid-based Key Pre-distribution Scheme

Liu and Ning developed a general framework for pair-wise key establishment based on polynomial-based key pre-distribution protocol and proposed a grid-based key pre-distribution scheme in their paper [6, 9]. We briefly review the polynomial-based key pre-distribution protocol and the grid-based key pre-distribution scheme.

#### 2.2.1 Key pre-distribution phase

The setup server randomly generates a bi-variant $t$-degree polynomial $f(x, y) = \sum_{i,j=0}^{t} a_{ij}x^i y^j$ over a finite field $F_q$, where $q$ is a large prime number. The polynomial has the property of [4, 5] $f(x, y) = f(y, x)$. (In the following, assume all the polynomials have this property.) For each sensor node $i$, the setup server computes a polynomial share $f(i, y)$. For any two sensor nodes $i$ and $j$, sensor node $i$ can compute the common key $f(i, j)$ by evaluating $f(i, y)$ at point $j$. Similarly, sensor node $j$ can compute the same common key $f(j, i) = f(i, j)$ by evaluating $f(j, y)$ at point $i$. To establish a pair-wise key, both sensor nodes need to evaluate the polynomial at the ID of the other sensor node.

#### 2.2.2 Grid-based key pre-distribution scheme

The grid-based key pre-distribution scheme can be divided into three phases: setup phase, polynomial share discovery phase and path discovery phase.

Setup: The setup server constructs a grid with a set of polynomials. Each row and each column in the grid are associated with a corresponding polynomial. The setup server then assigns each sensor node to a unique intersection in the grid. For the sensor node at the coordinate $(i, j)$, the setup server distributes the polynomial shares of $f_i^c(x, y)$ and $f_j^r(x, y)$ to the sensor node.

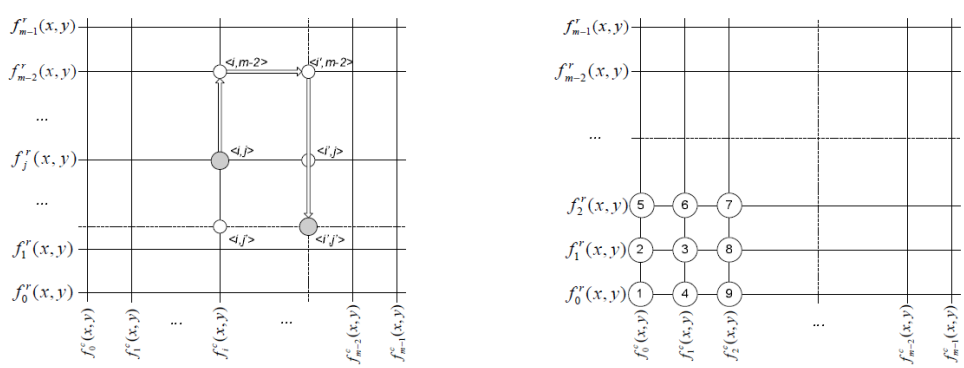



Fig. 1. The polynomial-based grid-based key pre-distribution scheme.

Polynomial share discovery: Assume a sensor node wants to establish a pair-wise key with another sensor node, both sensor nodes check their coordinate *ID*. If they are on the same row or same column in the grid, they will have a common polynomial share and can use the polynomial share to establish a pair-wise key directly like the polynomial-based key pre-distribution scheme.

Path discovery: The sensor nodes need to use path discovery if they are on the different row and different column in the grid. If there is no compromised sensor node, it is guaranteed that there will be at least one sensor node that can be used as an intermediate node between any two sensor nodes.

### 2.3 Multivariate Polynomial-Based Group Key Pre-Distribution Scheme

Harn *et al.* proposed a novel design of secure end-to-end routing protocol in wireless sensor networks [21] based on a group key [22] pre-distribution scheme using a multivariate polynomial [20]. A polynomial-based group key scheme is used to securely route data between sensor nodes. Group keys of different lengths can be established across multiple sensors, where each sensor belongs to a different class. This approach not only reduces the storage and computational overhead of the sensor, but also reduces the attacks captured by the sensor, thereby enhancing the security of the WSN.

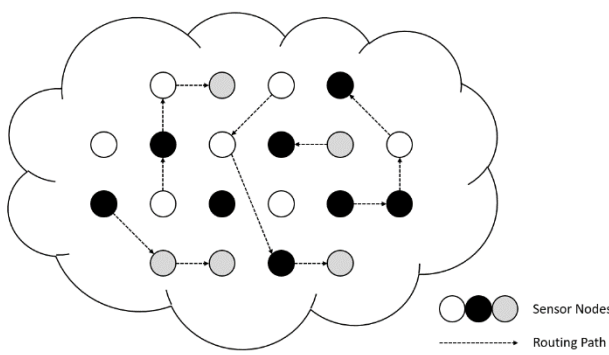



Fig. 2. The key pool generation of the adaptive scheme.

This method reduces the probability of the sensor being attacked in the wireless sensor network, but does not describe the countermeasures when the sensor node is attacked. If the node is attacked, the entire WSN may be paralyzed.

### 2.4 Adaptive Key Pre-Distribution Model

Laih *et al.* proposed an adaptive key pre-distribution model for distributed sensor networks [15] based on the basic probabilistic key pre-distribution scheme [4]. In order to increase the possibility of establishing a paired key, each sensor node can generate additional keys through the key rings. The Adaptive key pre-distribution model has four phases: 'key pool generation', 'key pre-distribution', 'shared key discovery' and 'path key establishment'.

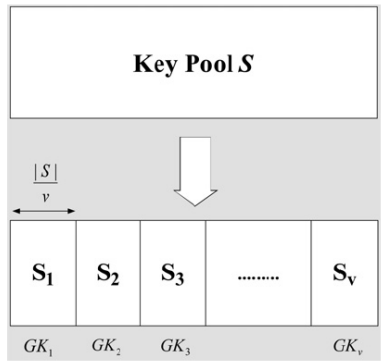



Fig. 3. The key pool generation of the adaptive scheme.

## 3. GRID-BASED KEY PRE-DISTRIBUTION SCHEME USING DEPENDENT KEYS

In this section, we introduce our propose scheme which called "A Grid-Based Key Pre-Distribution Scheme Using Dependent Keys in Wireless Sensor Networks". We call this scheme as GBKD Scheme in the rest of the paper.

The notation used in our propose scheme is shown in Table 1.

**Table 1. Notation of GBKD scheme.**

| Notation | Description |
|---|---|
| $N$ | Network size, the number of nodes |
| $S$ | The global key pool |
| $\|S\|$ | The size of the global key pool |
| $S_i^c$ | The sub-key pool of the column $i$ in the grid |
| $S_j^r$ | The sub-key pool of the row $j$ in the grid |
| $\|d\|$ | The size of the sub-key pool |
| $sk$ | The sub-key |
| $GK$ | The group key, can be obtained by condition-satisfied sub-key set |
| $t$ | Threshold value |

There are five phases in our propose scheme: Sensors assignment, Key pool generation, Key pre-distribution, Shared-key discovery and Path-key establishment phases.

### 3.1 Sensor Nodes Assignment

Suppose the sensor network has $N$ sensor nodes. The setup server constructs an $m \times m$ grid, where $m = \lceil \sqrt{N} \rceil$. The setup server then assigns each sensor node to each unique intersection in the grid. The *ID* of a sensor on the coordinate $(i, j)$ will represent as $\langle i, j \rangle$ or $\langle c, r \rangle$.

### 3.2 Key Pools Generation

The key pool generation in our proposed scheme is based on Shamir's Threshold Sc-

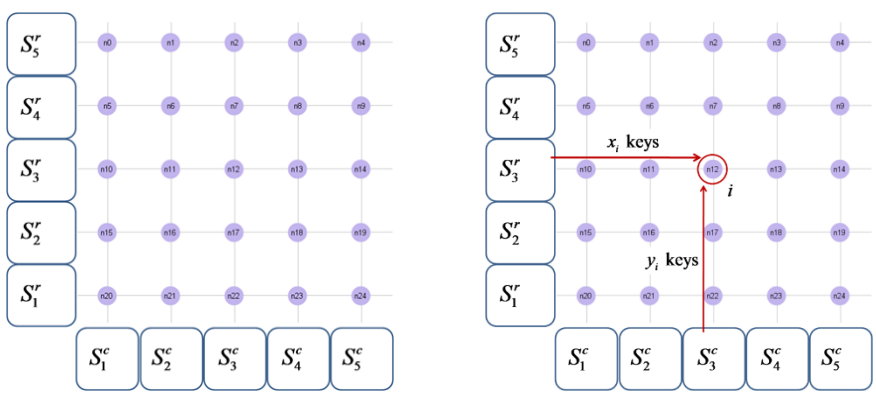
heme. The setup server decides a suitable key pool size $|S|$ and the key pool $S$ generation are divided into $2 \times m$ groups. Each group generates its sub-key pool by using different polynomials. The size of each sub-key pool is $|d| = \frac{|S|}{2 \times m}$. First, each group randomly chooses a polynomial $g_i(x)$ mod $p_i$ with $t - 1$ degree, where $p_i$ is a large prime and $g_i(0)$ is the secret group key $GK_i$ for each group $i$. For simplicity, the threshold value $t$ is the same in each sub-key pool. Then, each group $i$ generates $|d|$ sub-key identifiers $ID_{i1}, ID_{i2}, \ldots, ID_{id}$ and computes the sub-keys $sk_{i1}, sk_{i2}, \ldots, sk_{id}$, where $sk_{ij} = g(ID_{ij})$, $\forall j = 1, 2, \ldots, d$. After that, the sub-key pools distributed to the column and row of the grid. The sub-key pools distributed to the column of the grid are $S^c_{i(i=1,2,\ldots,m)} = \{sk^c_{ik} \mid k = 1, 2, \ldots, d\}$ and the sub-key pools distributed to the row of the grid are $S^r_{j(j=1,2,\ldots,m)} = \{sk^r_{jk} \mid k = 1, 2, \ldots, d\}$. As shown in the Fig. 4 (a), each column $i$ in the grid is associated with a sub-key pool $S^c_i$, and each row $j$ is associated with a sub-key pool $S^r_j$.

Thus, the whole key pool $S = (S^c_1 \cup S^c_2 \cup \ldots \cup S^c_m) \cup (S^r_1 \cup S^r_2 \cup \ldots \cup S^r_m)$.

### 3.3 Key Pre-Distribution Phase

In this phase, all operations are performed off-line and accomplished before the sensor nodes are deployed. As the Fig. 4 (b), sensor node $i$ randomly chooses $x_i$ sub-keys from its corresponding sub-key pool $S^r_i$ and randomly chooses $y_i$ sub-keys from its corresponding sub-key pool $S^c_j$ as its key ring. Thus, the key ring size of a sensor node is $\tau_i = x_i + y_i$. The sensor node records the sub-keys and its corresponding sub-key identifiers ID into their key rings.

$KeyRing_{\langle i,j \rangle} = \{sk^c_{i1}, sk^c_{i2}, \ldots, sk^c_{ix}\} \cup \{sk^r_{j1}, sk^r_{j2}, \ldots, sk^r_{jy}\}$




(a) Key pools assignment. (b) Key pre-distribution.

Fig. 4. The key pools assignment and key pre-distribution of GBKD scheme.

### 3.4 Shared-key Discovery Phase

The share-key discovery phase in our proposed scheme can be divided into two steps as well.

**Step 1:** The two sensor nodes try to establish a secure link from their key rings. They broadcast their key ring's *ID* list in plaintext. If one or more common keys are matched,

the nodes can use the key(s) to encrypt their transmitted messages. Hence, the secure link can be established. The communication key $CK$ will be computed as $CK = h(sk_1||sk_2|| \ldots ||sk_q)$ if more than one key is matched. $h(\cdot)$ is a one-way hash function and $sk_1$, $sk_2$, …, $sk_q$ are the $q$ common sub-keys between the two nodes. The hash function is used to prevent attackers from deriving any sub-keys. This method increases the security of communication as it is difficult for attackers to compromise the entire shared keys between two nodes.

**Step 2:** If there are no common key in Part 1, the two communicating sensor nodes have to use their key rings to derive the respective group key. Assume node $i\langle c_i, r_i\rangle$ and node $j\langle c_j, r_j\rangle$ are the two communicating sensor nodes, node $i$ checks whether $c_i = c_j$ or $r_i = r_j$ with node $j$. If $c_i = c_j$, it means both nodes belong to a same column in the grid. If the number of sub-keys in the two nodes from the same column sub-key pools $S_i^c$ are both exceed the threshold value $t$, the two nodes can use the sub-keys and sub-key identifiers to reconstruct the same Lagrange Interpolating polynomial and obtain the same group key,

$$g(x) = \sum_{s=1}^{t} sk_s \prod_{j=1, j\neq s}^{t} \frac{x - ID_j}{ID_s - ID_j} \bmod p$$

group key $GK = g(0)$. Similarly, if $r_i = r_j$ and the number of sub-keys from the same row sub-key pool $S_j^r$ in the two sensor nodes are both exceed the threshold value $t$, the two nodes can use the sub-keys and sub-key identifiers to reconstruct the same Lagrange Interpolating polynomial and obtain the same group key. After obtain the same group key, the two sensor nodes can use it as their communication key to protect their transmitted messages.

### 3.5 Path-key Establishment Phase

After the shared-key discovery phase completed, the communication of entire sensor network is basically formed. If there is no group key found in Step 2 of the shared-key discovery phase, the nodes have to perform the path-key establishment phase. Assume a source node $s$ wants to communicate with a destination node $d$ and there is an intermediate node $u$ can communicate directly with both of them by communication key. The node $s$ broadcast the path-key establishment request $R = \{ID_s, ID_d\}$ to node $u$. The request message is encrypted by communication key $CK_{s,u}$ between node $s$ and $u$. The node $u$ finds out node $s$ wants to communicate with node $d$ and forward the request message to node $d$. The forward message is encrypted by communication key $CK_{u,d}$ between node $u$ and $d$. Once node $d$ receives the message, it knows that node $s$ wants to communicate with it. The node $d$ then chooses an unassigned sub-key as communication key $CK_{s,d}$ for them and sends it back to node $s$ through the previous path. Finally, the node $s$ and node $d$ can use the communication key $CK_{s,d}$ to protect their transmitted message. Similarly, this path-key establishment method can extend to the path that uses multi nodes as intermediate nodes.

## 4. PERFORMANCE ANALYSIS

In this section, we use the random graph analysis and simulation to show the shared-key connectivity of the sensor networks in our scheme. We also will evaluate the usage of the memory for each sensor in our scheme and analysis the resilience of the sensor net-

works to the node capture attack for our scheme. Given different setup parameters for the sensor networks, we will show the simulated results by using the MATLAB.

### 4.1 Connectivity

According to EG scheme, we know that the most important performance in random key pre-distribution scheme of the sensor network is their connectivity.

For EG Scheme, the "local connectivity" of the scheme is defined as the probability that two sensor nodes share at least one key in their key rings. Assume $p'$ is the probability, the size of the key rings for each sensor node is $k$ and the keys are chosen from a key pool that has $P$ keys.

Thus, $p' = 1 -$ [the probability that two sensor nodes do not share any key],

$$p' = 1 - \frac{C_k^P \times C_k^{(P-k)}}{(C_k^P)^2}.$$

For the Grid-Based key pre-distribution scheme, the scheme guaranteed full connectivity if and only if there are no any compromised sensor nodes in the sensor networks, a sensor can directly determine whether it can establish a pair-wise key with another node by using the shared polynomial.

For the Adaptive key pre-distribution scheme, the defined of the "local connectivity" is the probability of two neighboring sensor nodes sharing at least one key to establish a secure link in the shared-key discovery phase. Since the shared-key discovery phase of the scheme can be divided into two steps, the local connectivity can be derived by $P = P_{step1} + (1 - P_{step1}) \times P_{step1}$ where $P_{step1}$ is similar with the connectivity of EG scheme and $P_{step1}$ is the probability in Step 2.

The local connectivity in GBKD scheme can be divided into two steps just like the Adaptive scheme. $P = P_{step1} + (1 - P_{step1}) \times P_{step2}$.

Since the sensor networks of GBKD scheme is based on an $m \times m$ grid, any two sensor nodes have a certain probability to locate in a same column or same row of the grid.

The probability is

$$p = \frac{2 \times m \times C_2^m}{C_2^N}.$$

Only the sensor nodes that belong in a same column or same row of the grid can establish a pair-wise key directly by perform the shared-key discovery phase. Thus, our analysis in this scheme will only consider this situation.

Assume that the two sensor nodes are belong to a same row of the grid, the connectivity of Step 1 is defined as the probability of the two sensor nodes sharing at least one key to establish a secure link.

In this situation, the key ring of the sensor $A$ and sensor $B$ are randomly selected from a same sub-key pool $S_j^r$ and a different sub-key pools $S_k^r$. Assume the sub-key pool size is $|d|$, the key ring size is $\tau$, the sensor $A$ select $x_a$ keys from the sub-key pool $S_j^r$ and the sensor $B$ select $x_b$ keys from the same sub-key pool $S_j^r$.

The probability of the sensor $A$ select $x_a$ keys from $S_j^r$ is $\frac{(C_{x_a}^d \times C_{\tau - x_a}^d)}{C_\tau^{2 \times d}}$. The probability

of the sensor $B$ select $x_b$ keys from $S_j^r$ is $\frac{(C_{x_b}^d \times C_{\tau-x_b}^d)}{C_\tau^{2\times d}}$. Then, the probability of them sharing at least one key is $\left(1-\frac{C_{x_a}^d \times C_{x_b}^{d-x_a}}{C_{x_a}^d \times C_{x_b}^d}\right)$.

Thus,

$$P_{step1} = \sum_{x_a=1}^{\tau}\sum_{x_b=1}^{\tau}\left(1-\frac{C_{x_a}^d \times C_{x_b}^{d-x_a}}{C_{x_a}^d \times C_{x_b}^d}\right)\times\left(\frac{(C_{x_a}^d \times C_{\tau-x_a}^d)\times(C_{x_b}^d \times C_{\tau-x_b}^d)}{(C_\tau^{2\times d})^2}\right).$$

When there are no common key found in Step 1 of the shared-key discovery phase, and the number of sub-keys possessed by the sensor $A$ and sensor $B$ are exceeds the threshold value $t$, then the sensor nodes can derive the group key.

The connectivity of Step 2 is defined as the probability that both sensor nodes can derive the group key

$$P_{step2} = \left(1-\sum_{x_a=1}^{t-1}\frac{(C_{x_a}^d \times C_{\tau-x_a}^d)}{C_\tau^{2\times d}}\right)\times\left(1-\sum_{x_b=1}^{t-1}\frac{(C_{x_b}^d \times C_{\tau-x_b}^d)}{C_\tau^{2\times d}}\right).$$

In the simulation, we assume there is a 10,000-nodes sensor network, and the grid is a 100×100 grid. We fixed the sub-key pool size $|d|$ = 250 and change the threshold value $t$ from 5 to 25. The relationship between the connectivity and the key ring size is shown in Fig. 5. We can observe that, when the sub-key pool is fixed, the connectivity increases as the number of keys stored in the sensor nodes increases. The threshold value $t$ also affects the connectivity because when the threshold value is smaller, it is much easier for the sensor to derive the group key in the shared-key discovery phase.

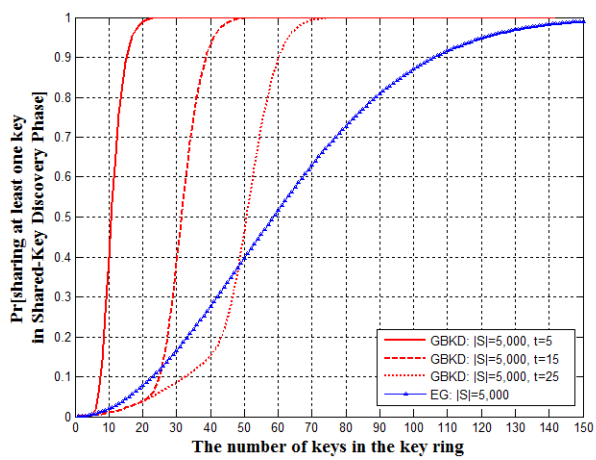



Fig. 5. The connectivity of GBKD scheme.

We compared the connectivity of GBKD scheme to EG scheme in Fig. 4. We can observe that the connectivity of our proposed scheme is better than EG scheme. On the other hand, the threshold value $t$ is an important variable for the DSN designer. If the DSN

designer prefers a higher connectivity and a lower memory overhead over the security of the network, he/she should choose a smaller threshold value *t*. Otherwise, the DSN designer should choose a greater threshold values *t* to make the sensor networks more secure. Therefore, this is a trade-off situation for the DSN designer.

### 4.2 Memory Overhead

We evaluate the memory overhead for the proposed scheme in this section and compare it to the polynomial-based grid-based scheme. Memory overhead of a scheme is defined as the required memory to store the keys in each sensor node to reach certain connectivity.

We assume the keys are being used in our proposed scheme, the EG scheme and the Adaptive scheme are the 64 bits keys. According to the Fig. 5, we can observe that each sensor node in the EG scheme needs to store at least 150 keys to guarantee 100% connectivity and our proposed scheme needs to store at least 50 keys. On the other hand, the polynomial-based grid-based key pre-distribution scheme uses the polynomial to establish the pair-wise key. We assume the large prime number $q$ is a 64 digits prime number that is large enough to accommodate the polynomial key. The memory overhead of the scheme is depending on the size of sensor network. The bigger sensor network size requires the bigger polynomial to guarantee the connectivity.

Table 2 shows that the memory overhead for different schemes. We can find that the memory overhead in our propose scheme is significantly improved when compared to other schemes.

**Table 2. The memory overhead in each sensor node of different schemes.**

| | Storage requirements | Total Storage Overhead |
|---|---|---|
| EG Scheme | 150 keys + 150 keys ID | 11,443 bits |
| Adaptive Scheme | 80 keys + 80 keys ID | 6,103 bits |
| Polynomial-based grid-based scheme | 2 t-degree polynomials + $t$ +1 nodes ID | 14,100 bits |
| GBKD Scheme | 50 keys + 50 keys ID | 3,815 bits |

### 4.3 Security – Resilience Against Node Capture

The term “Resilience” is defined as the resiliency of the key management scheme against the sensor node capture attack. Node capture attack is a general threat in wireless sensor networks, it is possible for an attacker to attack on a sensor node and compromise the key material of the sensor node. Thus, it is necessary to estimate the capability of a key management scheme to remain secure against this attack.

In GKPS [20], they establish a secure connection by reducing the probability of sensors being attacked in wireless sensors network, however, they do not describe the countermeasures for sensor nodes when they are attacked.

In GBKD scheme, the attacker may randomly capture the sensor nodes and compromises the keys of the sensor nodes. Supposed the attacker capture a sensor node = $\langle u, u \rangle$, he/she may compromise the keys that stored in the sensor node, which are come from the sub-key pools $S_u^r$ and $S_u^c$. Those keys will only share by the sensor nodes that are locate in

the *u*th column or the *u*th row of the grid. Thus, the capture of each sensor node will only affect at most $2\times m$ sensor nodes which are using the direct shared key to communicate.

For example, in a 10,000-nodes sensor network, the best-case scenario for the security of GBKD scheme is when the attacker only captures the sensor nodes all in a same column or a same row of the grid. It will only affect the communication among at most 200 sensor nodes.

Even if the attacker captures the sensor nodes in a different column and different row, the DSN designers can set a greater threshold value *t* to harder the group key derivation. Because when the sensor nodes are communicating by using the path key, the node capture attack will take the least effect to the communication among the sensor nodes, the security of the network will be greater.

## 5. CONCLUSIONS AND FUTURE WORK

In this paper, we propose a new key pre-distribution scheme based on the basic probabilistic key pre-distribution protocol with grid-based deployment. In our propose scheme, the keys with a hidden information will pre-distributed to the sensor nodes, hence the sensor nodes can establish the pair-wise key more effectively.

The performance analysis shows that the GBKD scheme can provide better connectivity and a lower memory overhead for the wireless sensor networks. The DSN designer also can adjust the variables of the sensor networks to produce an appropriate performance for the requirement of the application.

However, there are still some problems to be solved in our solution. During the path key establishment stage, if several sensors in the WSN are attacked, it may happen that the two sensors do not have a common node that can be used as the node for the path key establishment. As a result, a secure connection cannot be established.

There are some issues in our proposed scheme can be discussed in the future. The resilience of our proposed scheme should be discussed in more detail and the explicit equation of the resilience should be derived, so that the security analysis of the schemes can be analyzed more exactly.

## REFERENCES

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks*, Vol. 38, 2002, pp. 393-422.
2. Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Computer and Communications*, Vol. 30, 2007, pp. 2314-2341.
3. A. Perring, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "SPINS: Security protocols for sensor networks," in *Proceedings of the 7th Annual ACM/ IEEE International Conference Mobile Computing and Networking*, 2001, pp. 189-199.
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*, 2002, pp. 41-47.
5. W. Du, J. Deng, Y. Han, and P. Varshney, "A pairwise key predistribution scheme for

wireless sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, 2003, pp. 42-51.
6. D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proceeding of the 10th ACM Conference on Computer and Communications Security*, 2003, pp. 52-61.
7. H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proceedings of IEEE Symposium on Research in Security and Privacy*, 2003, pp. 197-213.
8. W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Transactions on Information and System Security*, Vol. 8, 2005, pp. 41-77.
9. D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions on Information and System Security*, Vol. 8, 2005, pp. 228-258.
10. H. Chan, V. D. Gligor, A. Perrig, and G. Muralidharan, "On the distribution and revocation of cryptographic keys in sensor networks," *IEEE Transactions on Dependable and Secure Computing*, Vol. 2, 2005, pp. 233-247.
11. M. G. Sadi, D. S. Kim, and J. S. Park, "GBR: Grid based random key predistribution for wireless sensor network," in *Proceedings of the 11th International Conference on Parallel and Distributed Systems*, Vol. 2, 2005, p. 310.
12. W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge," *IEEE Transactions on Dependable and Secure Computing*, Vol. 3, 2006, pp. 62-77.
13. A. Mohaisen, Y. J. Maeng, and D. H. Nyang, "On grid-based key pre-distribution: Toward a better connectivity in wireless sensor network," in *Proceedings of Pacific-Asia Conference on Knowledge Discovery and Data Mining*, LNCS, Vol. 4819, 2007, pp. 527-537.
14. A. Mohaisen, D. H. Nyang, and T. Abuhmed, "Two-level key pool design-based random key-distribution in wireless sensor networks," *KSII Transactions on Internet and Information Systems*, Vol. 2, 2008, pp. 222-238.
15. C. S. Laih, M. K. Sun, C. C. Chang, and Y. S. Han, "Adaptive key pre-distribution model for distributed sensor networks," *IET Communications*, Vol. 3, 2009, pp. 723-732.
16. A. Mohaisen, D. H. Nyang, Y. J. Maeng, K. H. Lee, and D. Hong, "Grid-based key pre-distribution in wireless sensor networks," *KSII Transactions on Internet and Information Systems*, Vol. 3, 2009, pp. 195-208.
17. C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Proceedings of Annual International Cryptology Conference*, LNCS, Vol. 740, 1993, pp. 471-486.
18. M. A. Simplício. Jr., P. S. L. M. Barreto, C. B. Margi, and T. C. M. B. Carvalho, "A survey on key management mechanisms for distributed wireless sensor networks," *Computer Networks*, Vol. 54, 2010, pp. 2591-2612.
19. J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," *Journal of Network and Computer Applications*, Vol. 33, 2010, pp. 63-75.
20. A. Albakri and L. Harn, "Non-interactive group key pre-distribution scheme (GKPS) for end-to-end routing in wireless sensor networks," *IEEE Access*, Vol. 7, 2019, pp. 31615-31623.

21. L. Harn, C.-F. Hsu, O. Ruan, and M.-Y. Zhang, "Novel design of secure end-to-end routing protocol in wireless sensor networks," *IEEE Sensors Journal*, Vol. 16, 2016, pp. 1779-1785.
22. L. Harn and C. F. Hsu, "Predistribution scheme for establishing group keys in wireless sensor networks," *IEEE Sensors Journal*, Vol. 15, 2015, pp. 5103-5108.

**Iuon-Chang Lin** received the Ph.D. in Computer Science and Information Engineering in 2004 from National Chung Cheng University, Chiayi, Taiwan. He is currently a Professor and Chair of the Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan. His current research interests include electronic commerce, information security, blockchain security, and cloud computing.

**Yu-Wen Wang** received a master's degree in the Department of Management Information Systems in 2011 from National Chung Hsing University, Taichung, Taiwan. She is currently a Senior Engineer of the Product Software Quality Assurance Department, ZYXEL Communication Corp., Hsinchu, Taiwan. Her current interests include enhance technology learning and Software verification capacity.

**Ting-Xsuan Tai** received a master's degree in the Department of Management Information Systems in 2021 from National Chung Hsing University, Taichung, Taiwan. He is currently an Engineer of the Network and Cyber Security Division, National Center for High-Performance Computing, Tainan, Taiwan. His current research interests include blockchain platform services and penetration test.