Grid-Based Key Pre-Distribution in Wireless Sensor Networks

Abedelaziz Mohaisen[1], DaeHun Nyang[2], YoungJae Maeng[2], KyungHee Lee[3], and Dowon Hong[1]
[1]Cryptography Research Team, Information Security Division
Electronics and Telecommunication Research Institute, the Korean government,
Daejeon 305-700, Republic of Korea
[e-mail: a.mohaisen@etri.re.kr]
[2]Graduate School of Information and Telecommucation Engineering, Inha University
Information Security Research Laboratory
Incheon 402-751, Republic of Korea
[3]Electrical and Computer Engineering Department, The University of Suwon
Suwon, Republic of Korea.
*Corresponding author : Abedelaziz Mohaisen

*Received January 19, 2009; revised February 28, 2009; accepted March 14, 2009;
published April 25, 2009*

Abstract

In this paper, we introduce a grid-based key pre-distribution scheme in wireless sensor networks, which aims to improve the connectivity and resiliency while maintaining a reasonable overhead. We consider simplification of the key establishment logic and enhancement of the connectivity via plat polynomial assignment on a three-dimensional grid for node allocation and keying material assignment. We demonstrate that our scheme results in improvements via a detailed discussion on the connectivity, resource usage, security features and resiliency. A comparison with other relevant works from the literature along with a demonstrated implementation on typical sensor nodes shows the feasibility of the introduced scheme and its applicability for large networks.

Keywords: Sensor network, security, key pre-distribution, connectivity

A preliminary version of this paper appeared in the proceedings of SSDU 2007 (nominated for the best paper award), LNAI 4819, pp. 527-537. This version includes a concrete analysis and supporting implementation results on MICAz sensor nodes. This research was supported by a research grant from Inha University and the IT R&D program of MKE/IITA, the Korean government [2005-Y-001-04, Development of Next Generation Security Technology].

DOI: 10.3837/tiis.2009.02.005

1. Introduction

The security of wireless sensor networks is a challenging and exciting issue that has attracted a great deal of attention and resulted in many solutions [1]. These solutions considered both symmetric and asymmetric key-based algorithms. For instance, recent works questioned the long-standing assertion that public key cryptography (PKC) is inefficient on resource-constrained sensor nodes; on the contrary they have demonstrated the relevant efficiency [2][3][4][5]. These results establish that the potential remains for typical PKC issues to be studied along with other issues motivated by the characteristics of WSNs, including the design of new public key primitives that are suitable for resource-constrained WSNs, in addition to conventional public key problems such as key authentication, key revocation, and key distribution [6].

In spite of achieving the relevant efficiency, real-world deployment of PKC on typical WSNs based on a long-lived network scenario is still at an early stage [6]. Therefore, symmetric key cryptography, in which secret keys are used at both sides of communication, is still essential. Particularly, symmetric key algorithms are considered computationally light on typical sensor nodes [6]. For symmetric key cryptography, both parties need to agree on a key for secure communication. Traditional key distribution mechanisms that utilize a key distribution center or use a trusted third party that generates and assigns keys for communicating parties are unsuitable for the settings of WSNs. Thus, the notion of key pre-distribution was introduced [7]. In the key pre-distribution process, sets of keys or keying materials are pre-assigned to each sensor node. At the operational time of the network, these materials are used to generate pairwise keys for encrypting/decrypting the communication traffic between different sensor nodes.

In the literature, key distribution schemes are classified according to their structure and characteristics into probabilistic and deterministic key pre-distribution schemes. In probabilistic key pre-distribution schemes, keys are assigned to sensor nodes; the entire network constructs a virtual graph in which nodes are connected according to a given probability. The landmark example of a probabilistic scheme is the EG scheme [7] which is improved in [8], generalized in [9], and modified for a *q-composite* scenario in [10]. In spite of the fact that the probabilistic key pre-distribution schemes are light-weight and have clever designs, these schemes have various limitations; they have low resiliency to node compromise, and relatively low connectivity, which is unacceptable for highly connected networks. On the other hand, the deterministic key pre-distribution schemes always guarantee certain connectivity by providing each node with pre-defined keying materials that are used at the operational time of the network. The keying materials can be symmetric matrices, as in [11] and [12], or symmetric polynomials, as in [13], [14], [15], [16], [17], and [18].

Particularly, Liu et al. introduced several grid-based key pre-distribution schemes that consider the same virtual grid on which nodes are allocated and keying materials are assigned [14][15]. The work of Liu is elegant, in the sense that it provides deterministic connectivity and enables an easy key establishment procedure via direct and indirect links between nodes. However, the shortcoming of Liu's work is that it provides low connectivity and a resiliency to node compromise that is proportional to the square root of the number of the nodes.

In order to exploit the information theoretic security advantage of polynomial-based key pre-distribution and provide good connectivity, an easy-to-use key establishment procedure, and better resiliency than in the work of Liu et al., we develop a grid-based key pre-distribution scheme that utilizes nodes allocation on plats and plat-based key pre-distribution. In practice, our scheme requires slightly more resources than the scheme in Liu et al.'s work, but provides better performance. However, fewer resources are needed than in other grid-based schemes such as HGBS [18].

1.1 Contribution and Organization

Our original contribution in this article is the introduction of a grid-based key pre-distribution scheme that utilizes the notion of plats on grids. By this means, we improve the three-dimensional grid-based key pre-distribution scheme in [14] and [15], using an extended plat polynomial assignment. Our contribution also includes node and polynomial assignment in a three-dimensional grid, a performance analysis supporting enhancements of the connectivity and security, and a performance analysis of the different schemes. As an original improvement to previous work in [17], we contribute implementation results and a comparison of grid-based work from the literature.

The rest of this paper is organized as follows. The remainder of this section introduces a summary of various related works in the literature. Section 2 introduces our grid-based key pre-distribution scheme in detail. Section 3 details the analysis of our scheme, focusing on the resulting connectivity and required resources, in terms of the memory, computation and communication overheads. Section 4 introduces an evaluation of the achieved security of our scheme. Section 5 compares our scheme and various grid-based schemes, in terms of the connectivity and resources, along with the implementation results. Finally, Section 6 presents our conclusion.

1.2 Selected Related Works

Symmetric key cryptography, which uses the same key to encrypt/decrypt messages, is very efficient on typical sensor nodes [1]. Due to the weak infrastructure of WSNs, the bottleneck challenge in security is the distribution of keys on different sensor nodes [1]. Traditional key distribution mechanisms using a trusted third party (TTP) or a key distribution center (KDC) are impractical solutions [15]. Therefore, keys need to be distributed in advance on nodes in a pre-deployment phase. This process has evolved into the key pre-distribution (KPD) schemes. In the following, we summarize the most relevant results on KPD in WSNs.

Prior to the development of WSNs, key pre-distribution was studied from the cryptographic perspective. For instance, Blom [11] suggested a square symmetric matrix of size $N \times N$, which stores the different keys for securing a network of size N, where each node in the network has a unique row and column in the matrix; these are exchanged accordingly when the key needs to be constructed. More precisely, if two nodes need to construct a key, they exchange their shared columns and multiply the exchanged columns by the stored rows, for shared keys. The keys are equal, because of the symmetry property of the original matrix construction from which rows and columns are derived. At the same time, Blundo et al. introduced several key pre-distribution schemes for dynamic conferences [13]. In these works, Blundo et al. introduced a key pre-distribution scheme based on symmetric bivariate polynomials. In this scheme, a bivariate polynomial of degree t is used to generate pairwise keys for a network of size N. This construction guarantees the resiliency of the system for the compromise of t+1 number of nodes. Technically, the symmetric bivariate polynomial is a function expressed as:

$$f(x, y) = \sum_{i=0,\, j=0}^{t} a_{ij} x^i y^j , a_{ij} = a_{ji}$$

The corresponding polynomial share of this polynomial, evaluated at the corresponding node's identifier, is stored in the corresponding node. For instance, two nodes s_i, s_j store the corresponding shares $f(i, y) = g(y), f(x, j) = g(x)$, where i, j are the identifiers of the two nodes, respectively. When secure key establishment is needed, the two nodes first exchange their identifiers and then store them in the variable of the stored share at each node's side. The resulting key is equal at both sides, because of the symetry property of the polynomial.

The need for computationally-feasible and secure key pre-distribution schemes is motivated by the evolution of WSN technology. Particularly, there have been many schemes based on the aforementioned schemes, along with others that were introduced especially for WSNs. For instance, Eschenauer and Gligor introduced the EG scheme, the first probabilistic KPD scheme in which keys were drawn randomly from key pools and assigned to different sensor nodes, in order to provide probabilistic connectivity [7]. In order to improve its resiliency, this scheme was generalized for a q-composite scheme in [10] and a two-level pool design in [9].

Furthermore, to reduce the memory overhead in Blom's scheme, Du et al. introduced the notion of the λ security, in which the resulting matrix is generated from a linear construction with a matrix of rank λ [12]. Also, Du et al. utilized the principle of the EG scheme to provide probabilistic connectivity and higher resiliency with fewer resources [12].

Finally, Liu et al. proposed several schemes in [14] and [15] for KPD based on [13]. In [14], Blundo's scheme randomly assigns several polynomials for each node in the same fashion as in [17]. Another scheme constructs a grid of $m \times m$, where $m = \sqrt{N}$ and nodes are deployed on different intersection points of the grid and different polynomials' shares are assigned for its different rows and columns. For any two nodes s_i, s_j, if $R_i = R_j$ or $C_i = C_j$ (i.e. they have the same polynomial share), a direct key establishment is performed. Otherwise, one or more intermediate nodes are used in an indirect key establishment phase. This work has been extended by considering a multi-dimensional grid where polynomials are assigned to the rows and columns of the different plats of each dimension. Similar to this work, except that it guarantees perfect connectivity at the cost of the high resource requirements that may be applicable to WSNs, Mohaisen et al. introduced a hierarchical grid-based KPD scheme in which different polynomials with different degrees are assigned to different hierarchies (i.e., nonexclusive network zones) to secure the traffic residing in different locations [16][18].

2. Key Pre-distribution with Plat Polynomial Assignment

In this section we introduce our contribution, a plat polynomial assignment mechanism for highly connected secure wireless sensor networks (WSNs), which is a generalized modification of the grid-based KPD scheme. However, before presenting the details of our contribution, we give an overview of some definitions used in our work.

Definition 1 (Grid Structure). Let X, Y, Z be three axes and $N = m^3$ be the network size (nodes). We define $X = \{c_0, c_1, \cdots, c_{m-1}\}$, $Y = \{r_0, r_1, \cdots, r_{m-1}\}$ and $Z = \{h_0, h_1, \cdots, h_{m-1}\}$. The grid is constructed by virtually generating a three-dimensional uniform grid in which nodes are placed on the intersection points of the grid and all nodes with the same c, r, or h belong to the same plat

Definition 2 (Plat). In settings of the grid defined in Definition 1, the plat is the virtual shape confined by all possible values for two variable axes and a constant value in the third axis.

Definition 3. (Node Identifier). For a network of size $N = m^3$, each node has a unique identifier represented as the tuple $< c_i, r_i, h_i >$.

2.1 Keying Material Assignment and Identifiers Structure

On a key management server, the following one-time procedure is performed:

1. Construct the virtual grid as defined in Definition 1 and generate each node's identifier as defined in Definition 3.
2. Each sensor node s_i with an identifier (i) of size $\log_2 N$ bits is mapped to the proper position on the grid described in Definition 1, where the node has the identifier structure $i =< c_x \mid r_y \mid h_z >$.
3. Construct $3 \times m$ different symmetric polynomials, where each polynomial satisfies the condition that $f(x, y) = f(y, x)$ and where these functions' coefficients are randomly generated in a finite field with size q. The parameter q is chosen large enough enough in order to avoid collision in key generation and to achieve a reasonable level of security by generating keys of adequate length. For instance, this parameter does not need to be the same as the length of the key.
4. The different polynomials are grouped in triples that construct all possible outcomes for three groups of size m. Each group also has the notation $< f_{cx}, f_{ry}, f_{hz} >$.
5. Unlike [14], each node with the identifier $i =< c_x \mid r_y \mid h_z >$ selects three polynomials with the indices $\{c_x, r_y, h_z\}$ that are equal to the node's identifier coordinates (i.e. all nodes with the same plat have the same polynomial).
6. For each sensor node s_i with identifier i and polynomials $< f_{cx}, f_{ry}, f_{hz} >$, the server evaluates the shares $g^{c_x} = f^{c_x}(i, y)$, $g^{r_y} = f^{r_y}(i, y)$, $g^{h_z} = f^{h_z}(i, y)$.

Note that this guarantees that all nodes with the same x-axis (i.e. that belong to the same plat defined in Definition 2 of the same dimension) have the same polynomial.

2.2 Key Establishment

2.2.1 Direct Key Establishment:

Assume two nodes s_i, s_j with identifiers $i =< c_{xi} \| r_{yi} \| h_{zi} >$ and $j =< c_{xj} \| r_{yj} \| h_{zj} >$. For these nodes, if $c_{xi} = c_{xj}$ or $c_{yi} = c_{yj}$ or $c_{zi} = c_{zj}$; which means that both nodes belong to at least one common dimension and have a shared single polynomial share; the two nodes use the common polynomial share $g^*(y)$ to generate a common key for securing communication between the two nodes. If more than one share is common between the two nodes, each of the nodes uses the share with the least compromised nodes to establish the keys. Note that the last case, where all coordinates are equal, is concerned with the node itself. Finally, if neither of the node's coordinates is equal, an intermediate node is used to establish a key, using the Indirect Key Establishment phase shown below.

2.2.2 Indirect Key Establishment

If the two nodes do not belong to the same plat of dimension, they must establish a key path that consists of one or more intermediate nodes. For nodes s_i and s_j ,which are communication parties with the identifiers i, j , s_ϕ is selected, where ϕ is the intermediate node's identifier such that any of the following is satisfied:

$$\begin{aligned} &\phi \cdot c_x = i \cdot c_x \text{ and } (\phi \cdot c_y = j \cdot c_y \text{ or } \phi \cdot c_z = j \cdot c_z) \\ &\phi \cdot c_y = i \cdot c_y \text{ and } (\phi \cdot c_x = j \cdot c_x \text{ or } \phi \cdot c_z = j \cdot c_z) \\ &\phi \cdot c_z = i \cdot c_z \text{ and } (\phi \cdot c_x = j \cdot c_x \text{ or } \phi \cdot c_y = j \cdot c_y) \end{aligned} \tag{1}$$

Based on the condition that (1) is satisfied, the corresponding shares in the node ϕ are used (there are at least two) to make the node ϕ an intermediate node. For example, if the first condition is satisfied in (1), a secret key is generated for communicating indirectly via node ϕ: $k_{\phi i} = g_{cx}^{\phi}(i)$, $k_{i\phi} = g_{cx}^{i}(\phi)$, and $k_{j\phi} = g_{cx}^{j}(\phi)$. The same procedure is performed for the remaining six types of key construction of the remaining two intermediate nodes in the corresponding plats, as expressed by Eq. (1).

3. Overhead Evaluation

In wireless networks, the communication activities are distributed and modeled using a communication traffic function with a probability distribution function f_R defined on the area R . This is particularly accurate for the realistic assumption that the radio coverage of the sensor node is limited and cannot cover the entire deployment area. In this case, nodes that are deployed close to each other have a high probability of communicating with each other, and nodes that are deloyed far from each other have a lower probability of communicating. In order to exploit this advantage, we introduce $f_R(n)$, which is defined on the area and plats with which nodes are associated. In other words, the input of the distribution function n relates to the number of hops required to establish an indirect key, given that a few sensor nodes are compromised. Considering the aforementioned advantange, we analyze our scheme. Especially, we analyze the connectivity and resource usage (i.e., memory, computation, and communication).

3.1 Connectivity

Let $\delta_x, \delta_y, \delta_z$ be the connectivity provided to any arbitrary pair of nodes. Also, let $m = \sqrt[3]{N}$. We define the direct connectivity as follows:

Definition 4 (Direct Connectivity). *The fraction of nodes out of the overall nodes in the entire network with which an arbitrary node can communicate using its own keying material in a one-hop manner*

That is, the actual connectivity $\mathrm{C}_{\text{actual}}$ in our scheme is the total connectivity for any pair of nodes that belong to an arbitrary plat in *x*, *y*, and *z*, respectively.

$$\mathrm{C}_{\text{actual}} = \sum_{x=1}^{m^2-1}\delta_x + \sum_{y=1}^{m^2-1}\delta_y + \sum_{z=1}^{m^2-1}\delta_z = \sum_{x=1}^{N^{2/3}-1}\delta_x + \sum_{y=1}^{N^{2/3}-1}\delta_y + \sum_{z=1}^{N^{2/3}-1}\delta_z \tag{2}$$

However, the connectivity provided by each node among the nodes in the network is equal to $\frac{1}{N-1}$. Also, the number of nodes that belong to each plat are equal. That is, $\sum x = \sum y = \sum z$. Eq. (2) can be rewritten as

$$\mathrm{C}_{\text{actual}} = \sum_{x=1}^{N^{2/3}-1}\delta_x + \sum_{y=1}^{N^{2/3}-1}\delta_y + \sum_{z=1}^{N^{2/3}-1}\delta_z = 3\left(\sum_{x=1}^{N^{2/3}-1}\delta_x\right) \tag{3}$$

However, by expressing the total as $\delta_x = \delta_y = \delta_z = \frac{1}{N-1}$ we obtain the following

$$\mathrm{C}_{\text{actual}} = 3\left(\sum_{x=1}^{N^{2/3-1}} \frac{1}{N-1}\right) = 3\left(\frac{N^{2/3}-1}{N-1}\right) \approx \frac{3}{N^{1/3}-1} \tag{4}$$

For the basic grid-based key pre-distribution scheme of Liu et al., the single-hop connectivity is

$$\mathrm{C}_{\text{actual}} = 3\left(\frac{m-1}{m^3-1}\right) = \frac{3}{m^2+m+1} \tag{5}$$

This is smaller than the connectivity in our scheme, since

$$\frac{3}{m+1} > \frac{3}{m^2+m+1} \tag{6}$$

For any m such that $m^3 = N$ and $N > 0$. Similarly, we can show that our introduced scheme provides a higher connectivity than the basic grid-based scheme for the multi-hop case. For instance, in the two-hop case, our scheme provides a connectivity of 1, while the basic grid-based scheme provides a connectivity of $\frac{1}{m-1}$. A demonstration of this connectivity compared to various other schemes from the literature is shown in **Fig. 1**.

3.2 Resources Overhead

The resources overhead evaluated in our scheme includes the memory requirements, computation requirements, and communication requirements, detailed as follows.

3.2.1 Memory Overhead

The required memory is mainly dependent on the desired security level. Let α be a security parameter such that $0 \le \alpha \le 1$, which determines the level of security for the nodes that hold the shares of a given polynomial, and the required memory for storing the coefficients $a_0, a_1, \cdots, a_t$ of the polynomial terms $x^0, x^1, \cdots, x^t$ is $(t+1)\log_2 q$. This can be written as

$(\alpha N+1)\log_2 q$. Let N_c be the number of compromised nodes, and the required memory per sensor node is M. The memory required can be represented as follows

$$M = 3(N_c+1)(\lceil \log_2 N^{1/3} \rceil) + 3(t+1)\log_2 q \qquad (7)$$

However, by expressing the security parameter in terms of the number of nodes and another parameter between zero and one, i.e., $t = \alpha N$, we obtain the following

$$M = (N_c+1)(\lceil \log_2 N \rceil) + 3(\alpha N+1)\log_2 q$$

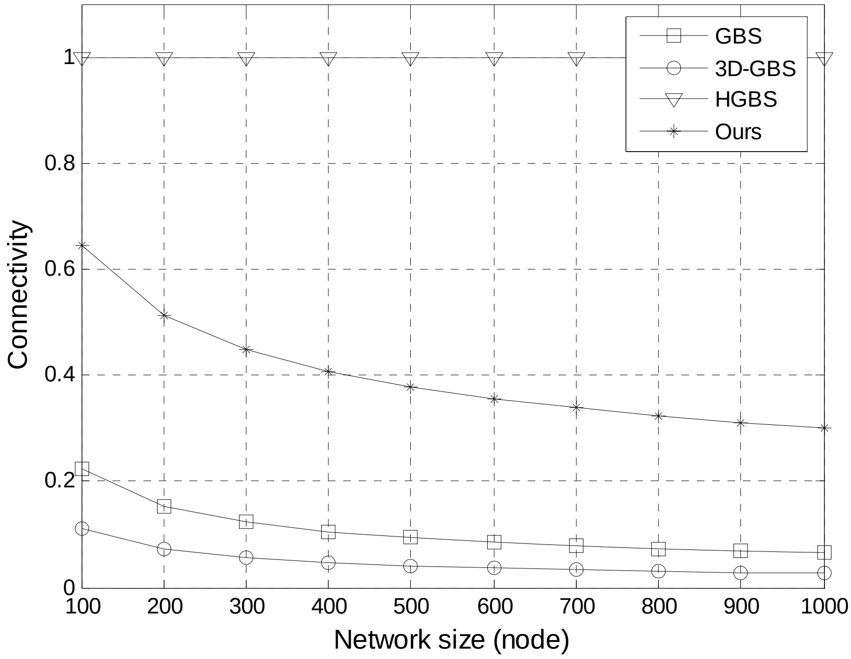


Fig. 1. Comparison of our scheme with selected schemes from the literature, in terms of the connectivity for a single-hop commnication

For the initial case where $N_c = 0$ (which means that no nodes are compromised), the memory requirement is $M = 3\lceil \log_2 N^{1/3} \rceil + 3(t+1)\log_2 q$. A comparison between our scheme and other related schemes from the literature, in terms of the memory, is shown in **Fig. 2**.

3.2.2 Communication Overhead

A security-related communication overhead is required to exchange two nodes identifiers. For key establishment when a small fraction of nodes is compromised, there are two different cases: Direct key establishment, which requires a single ID exchange, and key establishment via an intermediate node, which requires the exchange of two identifiers. Based on the identifier structure presented earlier, $3\times\log_2 N^{1/3}$ bits are required to represent it. On average, the required communication overhead (bits) is the average required to exchange the IDs in the two cases, which is $\mathrm{C}_{\text{communication}} = \frac{1+2}{2}\times 3\lceil \log_2(\sqrt[3]{N}) \rceil = 4.5\lceil \log_2(\sqrt[3]{N}) \rceil$.

However, for the general model that considers the usage of the communication traffic function [18], the communication overhead is defined as follows (the comparison with other schemes is shown in **Fig. 3**):

$$C_{\text{communication}} = 3\left\lceil \log_2(\sqrt[3]{N}) \right\rceil \times \sum_{i=1}^{n} if_R(i) = \left\lceil \log_2(N) \right\rceil \times \sum_{i=1}^{n} if_R(i) \tag{9}$$

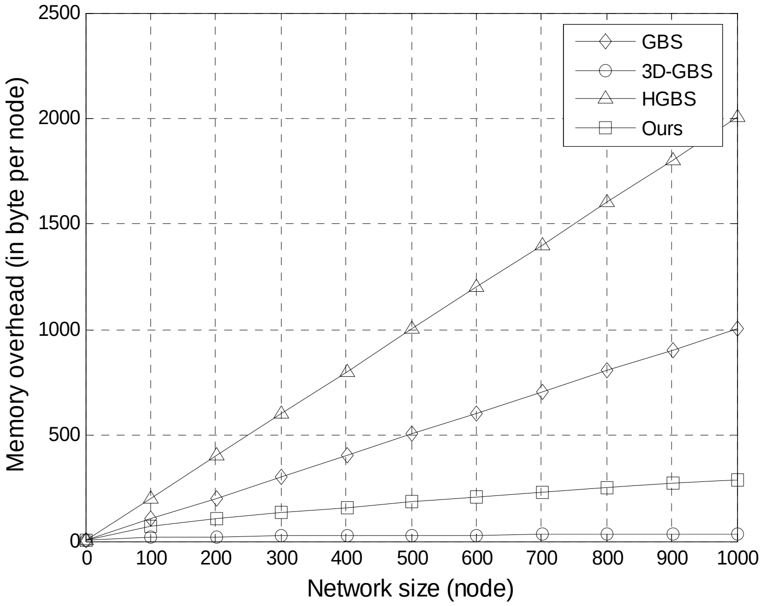


Fig. 2. Comparison of our scheme with various other schemes, in terms of memory requirements

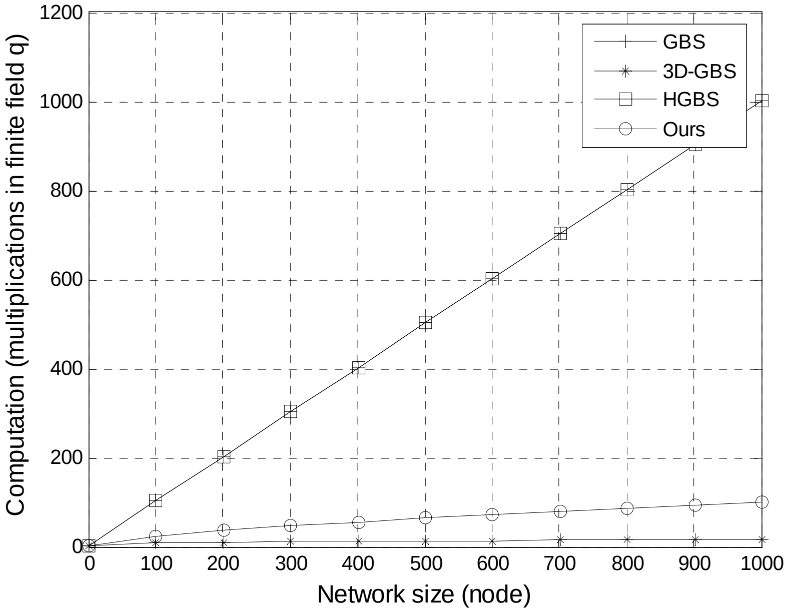


Fig 3. Comparison of our scheme with selected schemes from the literature, in terms of computation. Note that the required computation in both HGBS and GBS is equal on average.

3.2.3 Computation Overhead

As with the communication case, computation has two different cases: (i) One polynomial evaluation of degree t is required if the two nodes are in the same plat and (ii) Two or more polynomial evaluations are required when the two nodes belong to two different plats. For the general case, we use the communication traffic function $f_R(n)$ to determine the required average computation within the network operational life-time. Based on this, the required computation for the first case is $\mathrm{C}_{\mathrm{m}} = 2t - 3$ [18] integer multiplications in a large field (i.e., 64 or 128 bits), to evaluate a polynomial of degree $t = \alpha m^2$, where $m = N^{1/2}$. For the second case, where $f_R(n)$ is used, the following computation overhead is required:

$$\mathrm{C}_{\text{computation}} = C_m \times \sum_{i=1}^{n} i f_R(i) \tag{10}$$

Based on [14], two integer multiplications on a finite field of 16 or 64 bits require 16 or 27 8-bit multiplications, respectively. An 8-bit based formulation can be derived from Eq. (10) accordingly. A comparison of this computation requirement with other schemes from the literature is shown in **Fig. 4**.

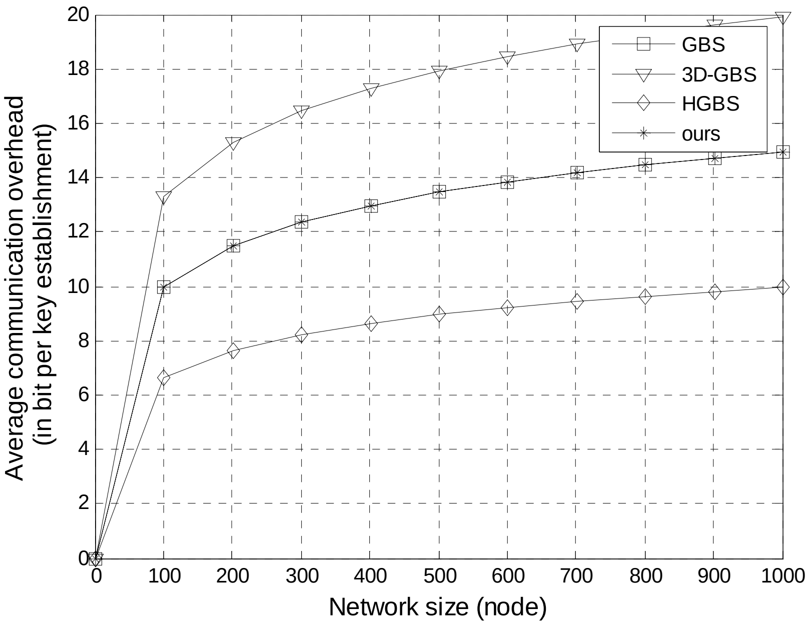


Fig. 4. Comparison of our scheme with various schemes from the literature, in terms of the communication overhead. Note that the required communication overhead of our scheme is equal to that of 3D-GBS.

4. Security Analysis

The security of any polynomial-based scheme is based on the fact that the polynomial is secure as long as the number of compromised nodes is less than $t+1$. In the following, we examine the various cases of our scheme.

4.1 Compromise of single node

A single node holds one share for a concerned polynomial, even if it holds two other shares for two different polynomials. Thus, compromise of a single node will not reveal more than the share of the sensor node and other internal information.

4.2 Compromise of single plat

We define a single plat by the nodes that hold the same polynomial's shares, which are required to recover a polynomial when $\alpha = 1$. The probability p_c of this event occuring, for a given number of compromised nodes N_c is as follows

$$p_c = 1 - \sum_{i=0}^{t} \left(\frac{N^{2/3}!}{i!(N^{2/3} - i)!} \right) F_c^i (1 - F_c)^{N^{2/3} - i} \tag{11}$$

where F_c is the fraction of compromised nodes, i is the number of compromised shares of a given polynomial, and N is the network size. As an example that illustrates the difference between our scheme and the scheme in [14], if $N = 1000$ and $F_c = 0.5$, then $p_c \approx 0.2$ in our scheme, while $p_c \approx 0.4$ for the same network size in [15].

4.3 Attack against the network

An attack against the entire network to break the security of pair-wise communication between the sensor nodes is possible, by compromising every single polynomial using the aforementioned approach. Even though there is a large overlap between the nodes that hold shares for different polynomials, the network can resist the attack until a high fraction of nodes have been compromised, and the revealed shares will be useless up to a given threshold fraction determined by α.

4.4 Possible intermediate nodes for key path establishment - Resiliency

Unlike the basic grid scheme in [15], which provides $3 \times \sqrt[3]{N}$ possible intermediate nodes for any two-hop key path establishment, our scheme provides $3 \times (\sqrt[3]{N})^2$ nodes for the same process, for the assumption that limited nodes are compromised.

5. Comparison with Other Schemes and Implementation

The security of our scheme is based on the security of the polynomial share [13]. The comparison of our scheme with other schemes is defined in terms of the resource usage, as shown earlier. **Table 1** summarizes the comparison of our scheme with other related works, in terms of resources for key distribution in WSNs. This includes grid and three-dimensional grid-based schemes [14][15], our work, and the hierarchical grid scheme [18].

The comparison shows that the resource usage of the schemes is comparable, while the connectivity is much better than the previous work. A demonstration of this comparison is shown in **Fig. 1** (connectivity), **Fig. 2** (memory), **Fig. 3** (communication) and **Fig. 4** (computation).

Table 1. Comparison of our proposed scheme with selected other schemes from the literature. Our comparison is limited to these schemes that are grid-based in terms of communication (bits), memory (bits), and computation (multiplications over a finite field)

	Comm.	**Memory**	**Computation**	**Conn.**
GBS	$\frac{3}{2}\log_2 N$	$\frac{3}{2}\log_2 N + (\alpha N + 1)\log_2 q$	$2\alpha N + 1$	$\frac{2}{\sqrt{N} - 1}$
3D-GBS	$2\log_2 N$	$2\log_2 N + (\alpha\sqrt[3]{N} + 1)\log_2 q$	$2\alpha\sqrt[3]{N} + 1$	$\frac{3}{2}\log_2 N$
Proposed scheme	$\frac{3}{2}\log_2 N$	$\frac{3}{2}\log_2 N + 3(\alpha\sqrt[3]{N^2} + 1)\log_2 q$	$2\alpha\sqrt[3]{N^2} + 1$	$\frac{3}{\sqrt[3]{N}}$
HGBS	$\log_2 N$	$\log_2 N + (\alpha N + 1)\log_2 q$	$2\alpha N + 1$	1

We also implemented our scheme on the MICAz sensor platform [19]. The goal was to measure the required time, energy, memory and communication for key generation (KG). Table 2 shows a summary of the results. Particularly, these requirements demonstrate the applicability of our scheme on the current generation of sensor networks in terms of the desired performance advantage.

Table 2. Implementation settings and results for key generation on a typical platform**.**

Network size	1,000 nodes	α	1
Key length	128 bit	Platform	MICAz
Length of $q^{'}$	16 bit	Coefficient length	16 bit
RAM	2+16 Bytes	ROM	200 Byte
K Generation time	115.2 ms	Key generation energy	0.92 mJ

6. Conclusion

To improve the connectivity of grid-based key pre-distribution, we introduced a plat-based polynomial assignment method that guarantees a higher connectivity and maintains better security. We analyzed the performance of our modification in terms of the required computation, communication, and memory. Our modification provides a scheme for promising applications that require high connectivity for large networks, at the cost of more resource usage than in currently deployed schemes.

References

[1] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," ACM Communications, vol.47, no.6, pp.53-57, 2004.

[2] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography," in *First IEEE Int. Conf. on Sensor and Ad Hoc Comm. and Networks*, pp.71-80, 2004.

[3] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and rsa on 8-bit cpus," in *CHES*, pp.119-132, 2004

[4] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *PerCom*, pp.324-328, 2005.

[5] R. J. Watro, D. Kong, S. F. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: securing sensor

networks with public key technology," in *SASN*, pp.59-64, 2004.

[6] W. Du, R. Wang, P. Ning, "An efficient scheme for authenticating public keys in sensor networks," in *MobiHoc*, pp.58-67, 2005.

[7] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *ACM CCS*, pp.41-47, 2002.

[8] J. Hwang and Y. Kim, "Revisiting random key pre-distribution schemes for wireless sensor networks," in *SASN*, pp.43-52, 2004.

[9] A. Mohaisen, D. Nyang, T. AbuHmed, "Two-level Key Pool Design-based Random Key Pre-distribution in Wireless Sensor Networks," *KSII TIIS*, vol.2, no.5, pp.222-238, 2008.

[10] H. Chan, A. Perrig, and D. X. Song, "Random key pre-distribution schemes for sensor networks," in *IEEE Symposium on Security and Privacy*, 2003.

[11] R Blom, "An optimal class of symmetric key generation systems," in *Proceeding of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques*, pp.335- 338, New York, NY, USA, 1985.

[12] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key pre-distribution scheme for wireless sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol.8, no.2, pp.228-258, 2005.

[13] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *CRYPTO*, pp.471- 486, 1992.

[14] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *ACM CCS*, pp.52-61, 2003.

[15] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol.8, no.1, pp.41-77, 2005.

[16] A. Mohaisen and D. Nyang, "Hierarchical grid-based pairwise key pre-distribution scheme for wireless sensor nets," in *EWSN*, pp.83-98, 2006.

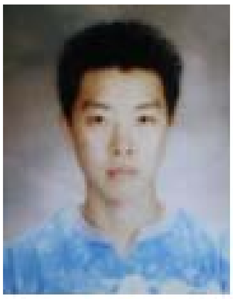
[17] A. Mohaisen, Y. Maeng, and D. Nyang, "On Grid-Based Key Pre-distribution: Toward a Better Connectivity in Wireless Sensor Network," in *PAKDD*, pp.527-5372007.

[18] A. Mohaisen, D. Nyang, and K. Lee, "Hierarchical Grid-Based Pairwise Key Pre-distribution in Wireless Sensor Networks, *IJNS*, vol.8, no.3, pp.282-292, 2009.

[19] Crossbow Technology. Wireless sensor networks, http://www.xbow.com/

Abedelaziz Mohaisen is a member of the engineering staff at the Electronics and Telecommunication Research Institute (ETRI), Korea. He received a Bachelor of Engineering degree in computer engineering from the University of Gaza in 2005, and a Master of Engineering degree in information and telecommunication engineering from Inha University, Korea, in 2007. His research interests include network security, data privacy, and applied cryptography.

DaeHun Nyang received a B.Eng. degree in electronic engineering from Korea Advanced Institute of Science and Technology, and M.S. and Ph.D. degrees in computer science from Yonsei University, Korea in 1994, 1996, and 2000, respectively. He has been a senior member of the engineering staff at the Electronics and Telecommunications Research Institute, Korea from 2000 to 2003. Since 2003, he has been an assistant professor at the graduate school of Information Technology and Telecommunication, Inha University, Korea, where he is also the founding director of the Information Security Research Laboratory. He is also a consultant for the Korean Information Security Agency, and a member of the board of directors and editorial board of the Korean Institute of Information Security and Cryptology. Dr. Nyang's research interests include cryptography and information security, privacy, biometrics and their applications to authentication, and public key cryptography. Also, he is interested in the security of WLANs, RFIDs, WSNs, and MANETs.



YoungJae Maeng was born in 1983, Seoul, Korea. He received a B.Sc. degree in computer science and engineering in 2006, and an M.E. in information and telecommunication engineering in 2008 from Inha University, Incheon, Korea, where he is currently a Ph.D. student. His research interests include the security of wireless sensor networks, home networks, and Internet and computers.

KyungHee Lee received B.S., M.S. and Ph.D. degrees in computer science from Yonsei University, Korea. She was a researcher at the LG Soft Company, Korea, from 1993 to 1996. She was a senior member of the engineering staff at the Electronics and Telecommunications Research Institute, Korea, from 2000 to 2005. Since 2005, she has been an assistant professor of Electrical Engineering at University of Suwon, Korea. Her research interests include information security, privacy, biometrics, image processing, artificial intelligence and pattern recognition.

Dowon Hong received his B.S., M.S. and Ph.D. degrees in mathematics from Korea University, Seoul, Korea in 1994, 1996, and 2000, respectively. He is currently a senior member of the engineering staff, and the team leader of the Cryptography Research team at the Electronics and Telecommunication Research Institute, Korea, where his research interests are broadly in the areas of applied cryptography, network security, and digital forensics.