A Space-Efficient Algorithm for Pre-distributing Pairwise Keys in Sensor Networks*

Taekyun Kim[1], Sangjin Kim[2], and Heekuck Oh[1]

[1] Department of Computer Science and Engineering, Hanyang University, Korea
{tkkim, hkoh}@cse.hanyang.ac.kr
[2] School of Internet Media Engineering, Korea University of Technology and Education, Korea
sangjin@kut.ac.kr

Abstract. We propose a space-efficient key pre-distribution scheme based on quasi-orthogonal finite projective plane. This approach, compared to the previous approaches, guarantees full connectivity and the uniqueness of pairwise keys. Moreover, the size of the key ring depends not on the size of the key pool, but on the size of the network. The actual order of the key ring size is only $O(\sqrt{N})$, where N is the size of the network. As a result, our approach provides better scalability than previous approaches.

1 Introduction

We are concerned with establishing pairwise symmetric keys for sensor nodes. These keys are required to provide authenticity of sensor nodes and secrecy of information exchanged between them. Current approach is to initialize each sensor node with some secret information before deployment [1, 2, 3]. After deployment, these sensor nodes perform a protocol with neighboring nodes to establish the required pairwise keys. Some systems [2] need boostrapping to create the new pairwise keys, whereas the other systems [1, 3] pre-distribute randomly selected pairwise keys. Our method is different from the previous probabilistic methods [1, 3] in that we store keys in sensor nodes in a deterministic way.

2 The Proposed Approach

Definition 1. *An **FPP (Finite Projective Plane)** is a geometrical system $\mathscr{G} = (\mathscr{P}, \mathscr{L}, \mathscr{I})$ satisfying the following conditions, where $\mathscr{P}$ is a finite set of points, $\mathscr{L}$ is a finite set of lines, and $\mathscr{I}$ is an incidence relation between $\mathscr{P}$ and $\mathscr{L}$.*

- *For all points $P, Q \in \mathscr{P}$ with $P \neq Q$, there exists a unique line $l \in \mathscr{L}$ that passes through P and Q.*
- *There exist at least 3 points.*
- *For every line $l \in \mathscr{L}$, there exists a point not incident with l.*
- *Every line passes through at least 3 points.*
- *Every pair of distinct lines intersect.*

* This work was supported by the Ministry of Information and Communication, Korea, under the university HNRC-ITRC program supervised by the IITA.

V.S. Sunderam et al. (Eds.): ICCS 2005, LNCS 3516, pp. 958–962, 2005.

$\{1,2,3\}\{1,4,5\}\{1,6,7\}\{2,4,6\}$
$\{2,5,7\}\{3,5,6\}\{3,4,7\}$

(a) order $n = 2$

$\{1,2,3,4\}\{1,5,6,7\}\{1,8,9,10\}\{1,11,12,13\}\{2,5,10,12\}$
$\{2,6,8,13\}\{2,7,9,11\}\{3,5,9,13\}\{3,6,10,11\}\{3,7,8,12\}$
$\{4,5,8,11\}\{4,6,9,12\}\{4,7,10,13\}$

(b) order $n = 3$

Fig. 1. Example of FPPs

$N_1 : \{K_1, K_2, K_3\}$ $N_4 : \{K_1, K_4, K_5\}$
$N_6 : \{K_1, K_6, K_7\}$ $N_2 : \{K_2, K_4, K_6\}$
$N_5 : \{K_2, K_5, K_7\}$ $N_3 : \{K_3, K_5, K_6\}$
$N_7 : \{K_3, K_4, K_7\}$

(a) Using single FPP

$N_1 : \{K_1, K_2, K_3\}, \{K'_3, K'_4, K'_7\}$ $N_4 : \{K_1, K_4, K_5\}, \{K'_1, K'_2, K'_3\}$
$N_6 : \{K_1, K_6, K_7\}, \{K'_1, K'_4, K'_5\}$ $N_2 : \{K_2, K_4, K_6\}, \{K'_1, K'_6, K'_7\}$
$N_5 : \{K_2, K_5, K_7\}, \{K'_2, K'_4, K'_6\}$ $N_3 : \{K_3, K_5, K_6\}, \{K'_2, K'_5, K'_7\}$
$N_7 : \{K_3, K_4, K_7\}, \{K'_3, K'_5, K'_6\}$

(b) Using two FPPs

Fig. 2. Construction of key rings for each node using an FPP of order $n = 2$

Definition 2. *For any $n \geq 2$, if each line of an FPP is incident with exactly $n+1$ points, we call this FPP a* ***finite projective plane of order*** *n.*

If $\mathscr{G}$ is an FPP of order n, then there are $n^2 + n + 1$ points and lines in total. An FPP of order n does not exists for all $n \geq 2$. However, it is known that FPPs of order $n = p^k$ exists, where p is a prime number and k is a positive integer. If we map points to numbers and lines to sets, a finite projective plane of order n can be shown as Fig. 1. There are many FPPs for a given order. Each FPP in Fig. 1 is just one of them.

In our method, the lines of an FPP is mapped to sensor nodes and points on a line to the key ring assigned to the corresponding node. For example, Fig 2.(a) shows the key ring assigned to each node when we use a single FPP of order $n = 2$. We denote N_i as a sensor node ID, and K_i as a symmetric key. In this case, the maximum number of nodes we can deploy is $N = n^2 + n + 1$ and the size of key ring in each node is $K = n + 1$. The relationship between N and K is $N = K(K-1) + 1$. Since every pair of distinct lines intersect in an FPP, each pair of node is guaranteed to have a single common key in their respective key rings. However, if we use this common key as the pairwise key, all pairwise keys are not unique. For example, the pairwise key of pairs (N_1, N_4), (N_1, N_6), (N_4, N_6) are all the same.

To make pairwise keys unique, we use an another FPP as shown in Fig 2.(b). Since we used two FPPs, each pair of nodes have a pair of common keys. For example, N_1 and N_4 shares K_1 and K'_3. We use $h(K_1||K'_3)$ as the pairwise key between N_1 and N_4, where h is collision-resistant hash function from $\{0,1\}^*$ to $\{0,1\}^k$, where k is the key length in bits. However, if we randomly assign the second FPP without any constraint, we may still get pairs that uses the same pairwise keys. For example, in Fig 2.(b), N_3, N_4, and N_5 all have K_5 and K'_2 in common. This problem occurs if and only if a triple of nodes that share a common key in the first FPP also share a common key in the second FPP. This problem is independent of the order of FPP used. That is, the problem occurs if this condition holds without regard to the order of FPP used.

To remedy this problem, we interchange the nodes and keys in the FPP. Since FPP satisfies the principle of duality, the resulting plane is also an FPP. We interchange them because we are not concerned with what specific keys are in each node's key ring but with the combinations of nodes that share a common key. Fig 3.(a) shows

an interchanged FPP of Fig 2.(a). To the right of the FPP, we show the combinations of nodes that share the same key. To make each pairwise keys unique, no two combinations appearing on the same row in the first FPP must not also appear on any row in the second FPP. The FPP of Fig 3.(b) satisfies this condition. We say that FPP of Fig 3.(a) and Fig 3.(b) are quasi-orthogonal to each other. More formally, quasi-orthogonality of FPP is defined as below.

$\{N_1,N_4,N_6\}:(1,4),(1,6),(4,6)$	$\{N_1,N_2,N_4\}:(1,2),(1,4),(2,4)$
$\{N_1,N_2,N_5\}:(1,2),(1,5),(2,5)$	$\{N_1,N_3,N_6\}:(1,3),(1,6),(3,6)$
$\{N_1,N_3,N_7\}:(1,3),(1,7),(3,7)$	$\{N_3,N_4,N_7\}:(3,4),(3,7),(4,7)$
$\{N_2,N_4,N_7\}:(2,4),(2,7),(4,7)$	$\{N_2,N_3,N_5\}:(2,3),(2,5),(3,5)$
$\{N_3,N_4,N_5\}:(3,4),(3,5),(4,5)$	$\{N_4,N_5,N_6\}:(4,5),(4,6),(5,6)$
$\{N_2,N_3,N_6\}:(2,3),(2,6),(3,6)$	$\{N_1,N_5,N_7\}:(1,5),(1,7),(5,7)$
$\{N_5,N_6,N_7\}:(5,6),(5,7),(6,7)$	$\{N_2,N_6,N_7\}:(2,7),(2,6),(6,7)$
(a)	(b)

Fig. 3. Quasi-orthogonal FPPs of order $n = 2$

Definition 3. *Two FPPs $\mathscr{G}_1 = (\mathscr{P}_1, \mathscr{L}_1, \mathscr{I}_1)$ and $\mathscr{G}_2 = (\mathscr{P}_2, \mathscr{L}_2, \mathscr{I}_2)$ with the same order are* ***quasi-orthogonal*** *if the following conditions hold:*

1. $\mathscr{P}_1 = \mathscr{P}_2$,
2. *For every line $l_1 \in \mathscr{L}_1$ and $l_2 \in \mathscr{L}_2$, there exist at most two points incident with both l_1 and l_2.*

Fig 4 shows two quasi-orthogonal FPPs of order $n = 3$.

$\{N_1,N_5,N_8,N_{11}\},\{N_1,N_2,N_6,N_7\}$	$\{N_1,N_3,N_5,N_{12}\},\{N_1,N_4,N_7,N_8\}$
$\{N_1,N_3,N_9,N_{10}\},\{N_1,N_4,N_{12},N_{13}\}$	$\{N_1,N_6,N_{10},N_{11}\},\{N_1,N_2,N_9,N_{13}\}$
$\{N_2,N_4,N_5,N_9\},\{N_5,N_6,N_{10},N_{12}\}$	$\{N_2,N_3,N_4,N_{10}\},\{N_2,N_5,N_7,N_{11}\}$
$\{N_3,N_5,N_7,N_{13}\},\{N_3,N_4,N_6,N_8\}$	$\{N_2,N_6,N_8,N_{12}\},\{N_3,N_6,N_7,N_9\}$
$\{N_7,N_8,N_9,N_{12}\},\{N_2,N_8,N_{10},N_{13}\}$	$\{N_3,N_8,N_{11},N_{13}\},\{N_4,N_5,N_6,N_{13}\}$
$\{N_4,N_7,N_{10},N_{11}\},\{N_2,N_3,N_{11},N_{12}\}$	$\{N_4,N_9,N_{11},N_{12}\},\{N_5,N_8,N_9,N_{10}\}$
$\{N_6,N_9,N_{11},N_{13}\}$	$\{N_7,N_{10},N_{12},N_{13}\}$

Fig. 4. Quasi-orthogonal FPPs of order $n = 3$

Theorem 1. *Given two quasi-orthogonal FPPs of order n, there is a way to assign key rings to nodes in a network of size n^2+n+1 or smaller, so that all of the pairwise keys are unique. Furthermore, the size of key ring in each node is $2n+2$.*

Proof. If we use two FPPs, uniqueness of pairwise keys are violated if and only if the followings are satisfied.

1. 3 nodes share a common key in the first FPP.
2. These 3 nodes also share a common key in the second FPP.

Since the quasi-orthogonality of FPPs guarantees that no three nodes share a common key in both FPPs, the argument is correct.

The followings are the steps used to construct key rings for sensor nodes of size N.

i) **Step 1:** Construct an FPP of order $n = p^k \geq \sqrt{N}$, where p is prime and k is a positive integer. Given an FPP of order n, the maximum supportable network size is $n^2 + n + 1$. Therefore, if $n \geq \sqrt{N}$, the maximum supportable network size is larger than N. If we consider incremental addition, the number of nodes that will be deployed after initial deployment must be taken into consideration.
ii) **Step 2:** Find a quasi-orthogonal FPP of the FPP constructed in step 1.
iii) **Step 3:** Assign a key to each row of the two quasi-orthogonal FPPs. Since the assigned keys must be different from each other, the total number of keys used is $2N = 2n^2 + 2n + 2$.
iv) **Step 4:** Find the dual FPPs by interchanging keys and nodes of the two quasi-orthogonal FPPs constructed in step 3.
v) **Step 5:** Assign a pair of key rings to each node. Without loss of generality, this procedure can be done at random, i.e., the node ID is meaningless at this point. Furthermore, there is no restriction for making a pair of key rings as long as each ring is from the different dual FPPs. This allows us $N!$ choices of assigning key ring pairs to nodes. From the principle of duality, the key ring size of each node is $2K = 2n + 2$.

This completes the proof. □

N_1 : $\{K_1, K_2, K_3, K_4\}, \{K'_1, K'_2, K'_3, K'_4\}$ N_2 : $\{K_1, K_5, K_6, K_7\}, \{K'_1, K'_6, K'_{10}, K'_{12}\}$
N_8 : $\{K_1, K_8, K_9, K_{10}\}, \{K'_2, K'_7, K'_9, K'_{12}\}$ N_{11} : $\{K_1, K_{11}, K_{12}, K_{13}\}, \{K'_3, K'_6, K'_9, K'_{11}\}$
N_2 : $\{K_2, K_5, K_{10}, K_{12}\}, \{K'_4, K'_5, K'_6, K'_7\}$ N_6 : $\{K_2, K_6, K_8, K_{13}\}, \{K'_3, K'_7, K'_8, K'_{10}\}$
N_7 : $\{K_2, K_7, K_9, K_{11}\}, \{K'_2, K'_6, K'_8, K'_{13}\}$ N_9 : $\{K_3, K_5, K_9, K_{13}\}, \{K'_4, K'_8, K'_{11}, K'_{12}\}$
N_{10} : $\{K_3, K_6, K_{10}, K_{11}\}, \{K'_3, K'_5, K'_{12}, K'_{13}\}$ N_3 : $\{K_3, K_7, K_8, K_{12}\}, \{K'_1, K'_5, K'_8, K'_9\}$
N_4 : $\{K_4, K_5, K_8, K_{11}\}, \{K'_2, K'_5, K'_{10}, K'_{11}\}$ N_{12} : $\{K_4, K_6, K_9, K_{12}\}, \{K'_1, K'_7, K'_{11}, K'_{13}\}$
N_{13} : $\{K_4, K_7, K_{10}, K_{13}\}, \{K'_4, K'_9, K'_{10}, K'_{13}\}$

Fig. 5. Key rings allocated to each node when using two FPPs of order $n = 3$

Fig 5 shows key rings assigned to each node when using two quasi-orthogonal FPPs depicted in Fig 4. Here, we assumed that first set of nodes $\{N_1, N_3, N_5, N_{12}\}$ share K'_1, the second set of nodes $\{N_1, N_4, N_7, N_8\}$ share K'_2 and so on. However, the order of assigning keys to second FPP is irrelevant and does affect the uniqueness of pairwise keys. The size of key ring assigned to each node is $2K \approx 2\sqrt{N}$.

3 Conclusion

In this paper, we have shown that it is possible to deterministically construct a key ring for sensor nodes having following characteristics: (i) it guarantees fully direct

connectivity, (ii) it guarantees uniqueness of pairwise keys, (iii) the size of the key ring stored at each node depends on the size of the network, whereas previous approach depends on the size of the key pool, (iv) the order of the key ring stored at each node is $O(\sqrt{N})$, where N is the size of the network.

References

1. Chan, H., Perrig, A., Song, D.: Random Key Predistribution Schemes for Sensor Networks. Proc. of the IEEE Symp. on Security and Privacy, IEEE Press (2003) 197–215
2. Deng, J., Han, R., Mishra, S.: Security Support For In-Network Processing in Wireless Sensor Networks. Proc. of the 1st ACM Workshop on the Security of Ad Hoc and Sensor Networks, ACM Press (2003), 83–93
3. Eschenauer, L., Gligor, V.D.: A Key-Management Scheme for Distributed Sensor Networks. Proc. of the 9th ACM Conference on Computer and Communications Security, ACM Press (2002), 41–47