Key Pre-distribution in a Non-uniform Network Using Combinatorial Design

Sarbari Mitra and Sourav Mukhopadhyay

Indian Institute of Technology, Kharagpur, India
{sarbari,sourav}@maths.iitkgp.ernet.in

Abstract. In this paper we propose a key pre-distribution scheme using combinatorial design. The network is assumed to be heterogeneous and the rectangular grid structure of the network is non-uniform. During key distribution phase, nodes are placed in the rectangular grid to form a virtual network. The actual network consists of the nodes along with their location in the target region. However, the deployment strategy and the key distribution technique indicate high connectivity of the network. Our scheme demonstrates superior performance compared to the existing similar schemes.

Keywords: key pre-distribution, projective planes, pairwise connectivity, resilience.

1 Introduction

Wireless Sensor network [WSN] is a collection of spatially distributed small, battery-powered, low-cost devices, with limited constraints to transmit data within a specified radio frequency range, known as wireless sensor nodes. Initially the evolution of WSN were motivated by the military applications but now-a-days it plays an active role in industrial application areas, healthcare machines, traffic control etc. Sensor nodes are densely distributed in the intended region for monitoring physical and environmental conditions. They gather information from the environment and actively transmit the collected data to the desired location through the network by communicating among themselves. The location of the sensor nodes in the network is not predetermined as they are deployed from air crafts; hence keys are assigned first to them, before deployment. The method of assigning secret keys to the nodes prior to their deployment in the target region is termed as key pre-distribution. The salient features of a good key pre-distribution scheme (KPS) includes less memory, less computation, greater connectivity and high robustness of the network against node capture.

Random Key Pre-distribution Scheme (KPS) was introduced by Eschenauer and Gligor in 2002 [6]. Combinatorial designs have become one of the most useful mathematical tools for KPS. *Projective planes* are used in [3]. Transversal design based schemes were proposed by Lee and Stinson in [9, 10], which were extended in [4] by merging blocks to construct nodes. Partially Balanced Incomplete Blocks Designs were used in [12] and Codes in [13] for KPS. For details of other combinatorial design based KPS we refer to the surveys [5, 11].

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 155–170, 2013.

A storage-efficient key pre-distribution scheme for a non-uniform rectangular grid structured network is presented in this paper. The nodes are placed at the intersection of the rows and the columns of the grid. Keys are distributed in such a manner that all the nodes on a row and a few columns form projective planes. There exists at least one path of length less than or equal to three, between any two nodes, provided they lie within radio frequency range. However, the key-path between any two nodes is not unique, a sufficient number of paths (of equal or larger length) exists between them. This increases the probability of the two nodes being connected, even after a number of nodes are compromised. With small storage the scheme induces a network of sufficiently large size. We emphasize that apart from storage efficiency, our design also provides better resilience and reasonable connectivity as compared to other existing schemes based on combinatorial designs. Moreover, given the size of the network, the number of rows and columns can be suitably chosen so as to get a desirable trade-off between the evaluation parameters, e.g., storage, connectivity and resilience.

2 Preliminaries

Definition 2.1. A *set-system* is defined as a pair (X, A) such that
(i) X is a set of points or elements,
(ii) A is a subset of the power set of X (i.e. collection of non-empty subsets or blocks of X).
The *degree* (denoted by r) of $x \in X$ is the number of blocks of A containing x; the *rank* (denoted by k) is the size of the largest block in A.
(X, A) is said to be *regular* and *uniform* if all the points in X have the same degree and all the blocks in A have the same size respectively. A regular, uniform set-system with $|X| = v$, $|A| = b$ is known as a (v, b, r, k)*-design* .

Definition 2.2. A (v, b, r, k)-design in which any set of t points is contained in exactly λ blocks, is known as a t - (v, b, r, k, λ)*-design* which is often denoted as t - (v, k, λ)*-design.*

Definition 2.3. A symmetric 2 - $(n^2 + n + 1, n^2 + n + 1, n + 1, n + 1, 1)$-design is known as a *finite symmetric projective plane of order n.* Precisely, it is a pair of a set of $\big(n^2 + n + 1\big)$ points and a set of $\big(n^2 + n + 1\big)$ lines, where each line contains $(n + 1)$ points and each point occurs in $(n + 1)$ lines.

3 Proposed Scheme

3.1 Protocol Requirements

- The nodes are arranged in a virtual rectangular grid during key pre-distribution phase. After key distribution, the nodes are deployed in the target region that the nodes sharing common keys are placed together, so that they lie within radio frequency range.
- It is assumed that all the nodes are not identical. One-third of the total number of nodes are more powerful than the rest. Comparatively “more powerful” nodes have higher radio frequency range and more storage capacity.

3.2 Terminologies and Notations

- Two nodes in the network are said to be *key-connected* or *physically-connected* when they share a common key or lie within radio range of each other respectively. A pair of nodes is said to be connected if it is both key-connected and physically-connected.
- Two nodes are said to be *pairwise connected*, when the common key between them is not assigned to any other node in the network.
- *Combinatorially Complete Graph*: As the name suggests, here we shall make use of a combinatorial design, namely projective planes, to form a complete graph. A projective plane of order p is used in such a way that the graph representing the network containing n nodes is complete with only $p + 1$ keys assigned to each of the nodes, where $n \approx p^2 + p + 1$, for some prime power p, as we discussed in the previous section. The graph thus obtained is referred as a combinatorially complete graph. We say a set of nodes is combinatorially complete, if any two nodes of the set are key-connected.

The distance function $d(\cdot, \cdot)$ is different from the conventional distance function. the distance between two nodes depends only on the keys stored at them, not on their physical location. The distance function, on the virtual network, is defined as follows:

Define a graph $G{=}(V, E)$, where $V{=}\{\text{Sensor nodes}\}{=}\{N_1, N_2, \cdots, N_N\}$, say, with $\mid V \mid{=}N$. $(N_1, N_2) \in E$ if N_1 and N_2 are key-connected.
Define $d(N_1, N_2) = l$, (in other words, there exists an l-hop path between N_1 and N_2) if $\exists$ a path $N_1 N_{u_1} N_{u_2} \cdots N_{u_{l-1}} N_2$ in G where $(N_1, N_{u_1}) \in E, (N_{u_{l-1}}, N_2) \in E$ and $(N_{u_i}, N_{u_{i+1}}) \in E$, for $i = 1, 2, \cdots, l - 2$.

We use the following notations throughout the paper.

r	Number of rows in the network
c	Number of columns on the network
N	Total number of nodes in the network
k	Average number of keys stored at each node in the network
$N_{i,j}$	The node belonging to the i^{th} row and j^{th} column of the network, where $i \in \{1, 2, \ldots, r\}$ and $j \in \{1, 2, \ldots, c\}$
R_i	i^{th} row of the grid, for $i \in \{1, 2, \ldots r\}$
C_j	j^{th} column of the grid, for $j \in \{1, 2, \ldots c\}$
$d(A, B)$	Distance between the nodes A and B in the virtual network
L_i	The number of i-hop paths in the network
s	The number of nodes compromised
$V(s)$	The fraction of nodes that become disconnected
$fail(s)$	Probability that the link between two uncompromised nodes is broken

3.3 Description of the Scheme

1. The whole network comprised of N nodes is distributed into r rows and c columns such that $rc \geq N$ where $c = 3c_1$, for an integer c_1. We choose prime integers p, q such that $r \leq p^2 + p + 1$, $c \leq q^2 + q + 1$.

2. Two disjoint key-pools of distinct keys are chosen - one for distributing keys along the rows and the other along the columns. Each node is assigned with keys along the corresponding row and the corresponding column.
3. Each row is made combinatorially complete by considering a projective plane of order q, since there are $c \leq q^2 + q + 1$ nodes on each row. So, any two nodes lying on a row are key-connected.
4. Let C_j be a special column. If $j \equiv 2(\mod 3)$ then C_j is made combinatorially complete by considering a projective plane of order p, since there are $r \leq p^2 + p + 1$ nodes on each column.
5. When $j \neq 2(\mod 3)$, the keys given to the node $N_{i,j}$ (along the column) is $\{j, i(\mod r)\}$ and $\{j, i+1(\mod r)\}$. This implies any two adjacent nodes (and the two lying on the boundary) on this column are key-connected.

For convenience, we refer to the combinatorially complete columns as *Special columns* and the rest of the columns as *ordinary column.* We define two types of nodes in the network

(i) Type A nodes - lie at the intersection of a row and a special column.
(ii) Type B nodes - lie at the intersection of a row and an ordinary column.

It follows from the construction that all the Type A nodes form complete graphs along their corresponding row and column. Whereas, any two adjacent Type B nodes on an ordinary column are pairwise connected. Hence, we assume that Type A nodes are provided with higher transmission range and memory as compared to the Type B nodes.

4 Analysis

The following results are developed in the block graph of the network i.e., the number of multi-hop paths are counted on the basis of the keys stored at each node. Two nodes are key connected in k-hop means that there exists at least one key-path of shortest length k, any two adjacent nodes on that path are key-connected. This path is not unique, i.e., there may exist any other k-hop, even $(k+l)$-hop (for, $l > 0$) paths between those two nodes.

We show the multihop paths from a Type A node in Fig. 1 and from a Type B node in Fig. 2 - Fig. 5 as given below. Diamonds, circles and triangles in Fig. 1 - Fig. 5 respectively denote the nodes who are at a distance of single-hop, 2-hop and 3-hop from $N_{i,j}$.

Theorem 4.1. *Any two nodes in the proposed network are key-connected by at least one path of length at most three.*

Proof. Let the nodes N_{i_1,j_1} and N_{i_2,j_2} wish to communicate. We consider the following cases:

Case (i): Let $i_1 = i_2$ i.e., both the nodes lie on the same row R_{i_1}.
From the construction, N_{i_1,j_1} and N_{i_2,j_2} are directly key-connected, i.e., $d(N_{i_1,j_1}, N_{i_2,j_2}) = 1$.

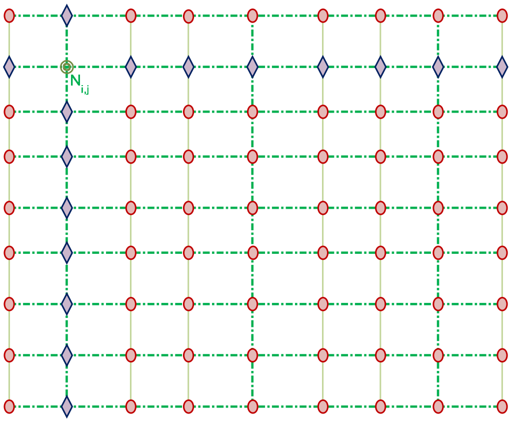

Fig. 1. One-hop and Two-hop paths from a Type A node $N_{i,j}$

Case (ii): Let $i_1 \neq i_2$ and $j_1 = j_2 = 2 \mod 3$ i.e., both the nodes lie on the same special column.

According to our construction, nodes lying on the same special columns form a combinatorially complete graph, hence we must have $d(N_{i_1,j_1}, N_{i_2,j_2}) = 1$.

Case (iii): Let If $i_1 \neq i_2$ and $j_1, j_2 = 2(\mod 3)$ but $j_1 \neq j_2$ i.e., both the nodes lie on the two different special columns.

Now, by case (i) $d(N_{i_1,j_1}, N_{i_1,j_2}) = 1$, and by case (ii) $d(N_{i_1,j_2}, N_{i_2,j_2}) = 1$. Therefore, $d(N_{i_1,j_1}, N_{i_2,j_2}) = d(N_{i_1,j_1}, N_{i_1,j_2}) + d(N_{i_1,j_2}, N_{i_2,j_2}) = 2$.

Case (iv): Let If $i_1 \neq i_2$ and $j_1, j_2 \neq 2(\mod 3)$, $j_1 \neq j_2$.

We consider the following two sub-cases

- Sub-case (a) When $j_2 \equiv 0(\mod 3)$
  We obtain from case (i) $d(N_{i_1,j_1}, N_{i_1,j_2-1}) = 1$, and $d(N_{i_2,j_2-1}, N_{i_2,j_2}) = 1$.
  Since, $j_2 \equiv 0(\mod 3)$, C_{j_2-1} is a special column, and hence by case (ii) we get, $d(N_{i_1,j_2-1}, N_{i_2,j_2-1}) = 1$. Therefore, $d(N_{i_1,j_1}, N_{i_2,j_2}) = d(N_{i_1,j_1}, N_{i_1,j_2-1}) + d(N_{i_1,j_2-1}, N_{i_2,j_2-1}) + d(N_{i_2,j_2-1}, N_{i_2,j_2}) = 3$.
- Sub-case (b) When $j_2 \equiv 1(\mod 3)$
  Hence,C_{j_2+1} is a special column. Proceeding in the similar manner as in the subcase(a), just by replacing $j_2 - 1$ by $j_2 + 1$, we obtain $d(N_{i_1,j_1}, N_{i_2,j_2}) = d(N_{i_1,j_1}, N_{i_1,j_2+1}) + d(N_{i_1,j_2+1}, N_{i_2,j_2+1}) + d(N_{i_2,j_2+1}, N_{i_2,j_2}) = 3$.

In either of the two sub-cases, there exists at leats one 3-hop path between the nodes.

Considering all the case, it is found that there exist at leats one shortest path of length less than or equal to three, between any two randomly chosen nodes, in the block graph of the network. □

Theorem 4.2. *Total number of one-hop paths in the network is* $L_1 = \frac{rc}{6}(r+3c)$.

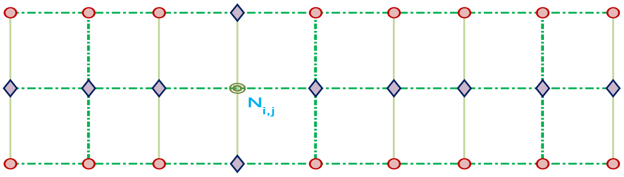

Fig. 2. One-hop and Two-hop paths from a Type B node $N_{i,j}$ when there are exactly three rows in the network

Proof. From Fig. 1 it follows that a Type A node $N_{i,j}$ is key-connected to all the nodes lying on the row R_i (i.e, $N_{i,j'}$ for $j^{'} = 1, 2, \cdots, i-1, i+1, \cdots, r$) and the column C_j (i.e., $N_{i',j}$ for $i^{'} = 1, 2, \cdots, j-1, j+1, c$). Hence, it is key-connected to $r+c-2$ nodes. Again, a Type B node $N_{i,j}$ is key-connected to all the nodes lying on the row R_i (i.e., $N_{i,j'}$ for $j^{'} = 1, 2, \cdots, i-1, i+1, \cdots, r$) and the two adjacent nodes (i.e., $N_{i-1,j}$ and $N_{i+1,j}$) lying on the column C_j. Which implies that a Type B node is key-connected to $r+c-2$ nodes.

The total number of Type A and Type B nodes in the network is $\frac{rc}{3}$ and $\frac{2rc}{3}$ respectively. Therefore, the total number of one-hop paths in the network is $\frac{1}{2}\{(r+c-2)\frac{rc}{2} + (c+1)\frac{2rc}{3}\}$, the factor 1/2 comes, as each of the single-hop path is counted twice corresponding to each extreme of the path. We obtain the desired result on simplification. □

Theorem 4.3. *The total number of two-hop paths in the network is given by*

$$L_2 = \begin{cases} 0, & \textit{if } r < 2; \\ c(c-1), & \textit{if } r = 2; \\ 3c(c-1), & \textit{if } r = 3; \\ \frac{2c}{3}(\frac{23c}{3} - 5), & \textit{if } r = 4; \\ \frac{rc}{6}(\frac{5rc}{3} - r + c + 1), & \textit{if } r \geq 5 \ . \end{cases}$$

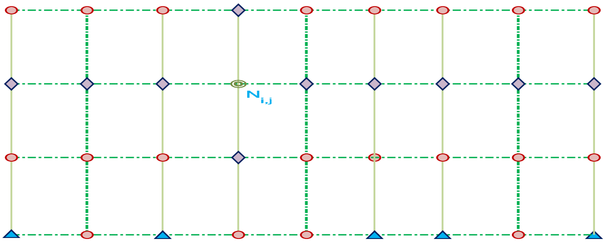

Fig. 3. One-hop, Two-hop and Three-hop paths from a Type B node $N_{i,j}$ when there are exactly four rows in the network

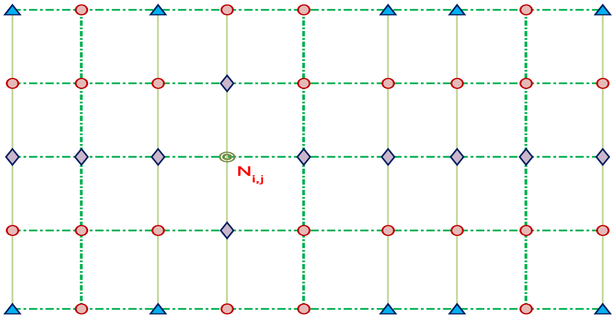

Fig. 4. One-hop, Two-hop and Three-hop paths from a Type B node $N_{i,j}$ when there are exactly five rows in the network

Proof. Let us assume that p_1, p_2 respectively denote the proportion of Type A and Type B nodes, i.e., $p_1 = \frac{rc}{3}$ and $p_2 = \frac{2rc}{3}$. Suppose that the number of nodes to which a Type A and Type B node are connected in 2-hop paths are n_1 and n_2 respectively. Hence we have

$$L_2 = \frac{1}{2}(p_1n_1 + p_2n_2) = \frac{rc}{6}(n_1 + 2n_2).$$

From Fig. 1 it follows that a Type A node $N_{i,j}$ is key-connected to all the nodes, in 2-hop path, who lie neither on R_i, nor on C_j. Thus, we have $n_1 = (r-1)(c-1)$. Hence,

$$L_2 = \frac{rc}{6}\{(r-1)(c-1) + 2n_2\}. \tag{1}$$

We observe that the expression for n_2 depends on the number of rows present in the network. We consider the following cases

Case (i) Let $r < 2$

The only possibility is there is only one row in the network. Since each row forms a completely connected graph, all the nodes are key-connected in a direct path, and hence no two-hop path is there. So, $n_2 = 0$.

Case (ii) Let $r = 3$

From Fig. 2 it follows that a Type B node $N_{i,j}$ is at a distance of two, with the nodes given by $N_{i',j'}$ for $i^{'} = \{i+1, i-1\}$ and $j^{'} \in \{1, 2, \cdots, c\} \setminus j$, i.e., $2(c-1)$ nodes. Thus, $n_2 = 2(c-1)$.

Case (iii) Let $r = 4$

From Fig. 3 it follows that a Type B node $N_{i,j}$ is at a distance of two, with the following nodes

1. $N_{i',j'}$ for $i^{'} = \{i+1, i-1\}$ and $j^{'} \in \{1, 2, \cdots, c\} \setminus j$, i.e., $2(c-1)$ nodes
2. $N_{i',j'}$ where $i^{'} = i+2$ (or $i-2$ since, $R_{i-2} = R_{i+2}$ whenever $r = 4$) and $C_{j'}$ is a special column, i.e., $c/3$ nodes.
3. The node $N_{i+2,j}$

Thus, we have $n_2 = 2(c-1) + \frac{c}{3} + 1 = \frac{7c}{3} - 1$.

Case (iv) Let $r \geq 5$

From Fig. 4 and Fig. 5 it follows that a Type B node $N_{i,j}$ is at a distance of two, with the following nodes

1. $N_{i',j'}$ for $i' = \{i+1, i-1\}$ and $j' \in \{1, 2, \cdots, c\} \setminus j$, i.e., $2(c-1)$ nodes
2. $N_{i',j'}$ where $i' \in \{1, 2, \cdots, r\} \setminus \{i-1, i, i+1\}$ and $C_{j'}$ is a special column, i.e., $\frac{c}{3}(r-3)$ nodes
3. The two nodes $N_{i-2,j}$ and $N_{i+2,j}$

Thus, we have $n_2 = 2(c-1) + \frac{c}{3}(r-3) + 2 = (\frac{rc}{3} + c)$.

Substituting the obtained values in each case for n_2 in equation (1) we get the desired expression as given in the statement of Theorem 4.3. □

Theorem 4.4. *The total number of three-hop paths in the network is given by*

$$L_3 = \begin{cases} 0, & \text{if } r \leq 3; \\ \frac{4c}{3}(\frac{2c}{3} - 1), & \text{if } r = 4; \\ \frac{5c}{3}(\frac{4c}{3} - 2), & \text{if } r = 5; \\ \frac{2rc}{3}(\frac{rc}{3} - c - 1), & \text{if } r > 5 \;. \end{cases}$$

Proof. In this case, we have $p_1 = \frac{rc}{3}$ and $p_2 = \frac{2rc}{3}$, as the previous theorem. We further assume that the number of nodes to which a Type A and Type B node are connected in 3-hop paths is m_1 and m_2 respectively. Hence we have

$$L_3 = \frac{1}{2}(p_1 m_1 + p_2 m_2) = \frac{rc}{6}(m_1 + 2m_2).$$

Now, from Fig. 1, we notice that any Type A node is key-connected to all the nodes of the network, i.e., a Type A node has no 3-hop path as the smallest

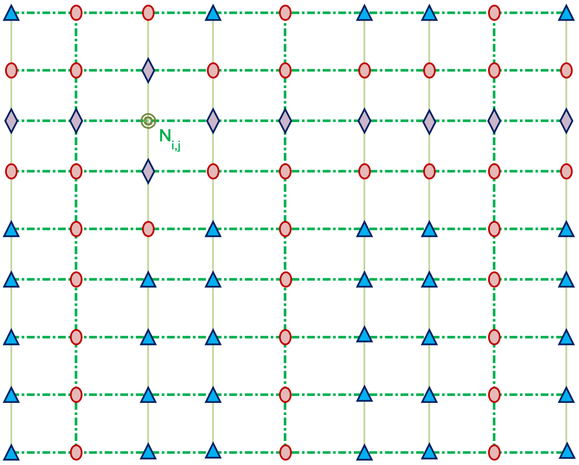

Fig. 5. One-hop, Two-hop and Three-hop paths from a Type B node $N_{i,j}$ when there are more than five rows in the network

path. So, we have $m_1 = 0$. Hence, we obtain

$$L_3 = \frac{rc}{3} m_2. \tag{2}$$

We observe that the expression for m_2 depends on the number of rows present in the network. We consider the following cases

Case (i) Let $r \leq 3$
From Fig. 2, we observe that if there are less than three rows in the network, then there will be no 3-hop path as the smallest path between any two nodes. Thus, in this case $m_2 = 0$.

Case (ii) Let $r = 4$
From Fig. 3 it follows that a Type B node $N_{i,j}$ is at a distance of two, with the nodes given by $N_{i',j'}$ for $i^{'} = i + 2$ (or $i - 2$ since, $R_{i-2} = R_{i+2}$, when $r = 4$) and $C_{j'}$ is an ordinary column but $j^{'} \neq j$. So, $m_2 = \frac{2c}{3} - 1$.

Case (iii) Let $r = 5$
From Fig. 4 we have a Type B node $N_{i,j}$ is at a distance of two, with the nodes given by $N_{i',j'}$ for $i^{'} = i + 2, i - 2$ and $C_{j'}$ is an ordinary column but $j^{'} \neq j$. So, $m_2 = \frac{2c}{3} - 1$. So, $m_2 = 2\left(\frac{2c}{3} - 1\right)$.

Case (iv) Let $r > 5$
From Fig. 5 it follows that a Type B node $N_{i,j}$ is at a distance of two, with the following nodes

1. $N_{i',j'}$ for $i^{'} = \{1, 2, \cdots, r\} \setminus \{i-1, i, i+1\}$ and $C_{j'}$ is an ordinary column but $j^{'} \neq j$, i.e., $(r - 3)(\frac{2c}{3} - 1)$ nodes
2. $N_{i',j}$ where $i^{'} = \{1, 2, \cdots, r\} \setminus \{i - 2, i - 1, i, i + 1, i + 2\}$, i.e., $(r - 5)$ nodes

Thus, we have $m_2 = (r - 3)(\frac{2c}{3} - 1) + (r - 5) = 2(\frac{rc}{3} - c - 1)$.

Substituting the obtained values in each case for m_2 in equation (2) we get the desired expression as given in the statement of Theorem 4.4. □

4.1 KeyPath Establishment

We discuss the key path establishment phase between two randomly chosen nodes, $P : N_{i_1,j_1}$ and $Q : N_{i_2,j_2}$, from the network. The nodes first broadcast their node identifiers : node P broadcasts i_1, j_1 and node Q broadcasts i_2, j_2. Algorithm 4.5 discusses how to find the intermediate node or intermediate key-path between P and Q, if exists.

The expressions (corresponding values for fixed r), obtained in Theorems 4.2, 4.3 and 4.4 adds up to give $\frac{1}{2}rc(rc - 1)$, which is the total number of possible links in the network. This alternatively verifies the validity of Theorem 4.1. It follows from Theorem 4.1 that all the nodes in the network are connected by at least a path of distance at most three. Note that, the one-hop, 2-hop and 3-hop paths between any two nodes are not unique. Moreover, paths of length more than three, also exist on the network. Therefore, when few nodes becomes inactive, and the shortest path between any two communicating nodes do not exist, they look for the alternative paths of same or larger length.

```
Algorithm 4.5
Input: The node identifiers $P : N_{i_1,j_1}$ and $Q : N_{i_2,j_2}$
procedure FindKeyPath
    if ($j_1 \equiv 2 \mod 3$) then
        if (($i_1 = i_2$) || ($j_1 = j_2$))
            print "$P$ and $Q$ are directly connected";
        else if ($j_2 \equiv 2 \mod 3$) then
            $N_{i_1,j_2}$ or $N_{i_2,j_1}$ is an intermediate node;
            else if $N_{i_2,j_1}$ is an intermediate node;
            end if
        end if
    else if ($j_1 \equiv 0 \mod 3$) then
            if ($j_2 \equiv 2 \mod 3$) then
                $N_{i_1,j_2}$ is an intermediate node;
            else
                The key-path is $N_{i_1,j_1} \rightarrow N_{i_1,j_2-1} \rightarrow N_{i_2,j_2-1} \rightarrow N_{i_2,j_2}$;
            end if
    else if ($j_1 \equiv 1 \mod 3$) then
            if ($j_2 \equiv 2 \mod 3$) then
                $N_{i_2,j_1}$ is an intermediate node;
            else
                The key-path is $N_{i_1,j_1} \rightarrow N_{i_1,j_2+1} \rightarrow N_{i_2,j_2+1} \rightarrow N_{i_2,j_2}$;
            end if
    end if
end FindKeyPath
```

5 Overall Performance

In this section we evaluate the efficiency of our scheme on the basis of connectivity, resilience and memory. For convenient comparison, we consider a network consisting of nearly 2000 nodes. We further consider fifteen sets of combinations of the number of rows and columns which lead to network of size almost 2000. We carry out all the computations and comparisons with these fifteen sets of values.

5.1 Memory

It has already been mentioned that storage in each node is limited. Although authors claim that storing even 150 keys per node is permitted [7], it is always better to keep storage (i.e., the average number of keys to be stored per node) as small as possible.

In this section we discuss the memory requirement of the proposed network. Note that the number of keys to be stored by a node depends on the Type of the node. Let us assume that k_A and k_B denote the number of keys to be stored

Table 1. Memory

r	c	N	p	q	k_A	k_B	k
7	285	1995	2	17	21	20	≤ 21
13	156	2028	3	13	18	16	≤ 18
21	96	2016	4	11	17	14	16
29	63	1827	5	8	15	11	≤ 14
31	66	2046	5	8	15	11	≤ 14
37	54	1998	7	7	16	10	14
57	36	2052	7	7	16	10	14
73	27	1971	8	5	15	8	≤ 13
91	21	1911	9	4	15	7	≤ 14
133	15	1995	11	4	17	7	≤ 14
167	12	2004	13	3	18	6	14
222	9	1998	16	3	21	6	16
333	6	1998	19	2	23	5	17
666	3	1998	27	2	31	5	≤ 23

by a Type A and Type B nodes respectively. Let us suppose that k represents the average memory of any randomly chosen node from the network.

In Table 1 we show the memory requirements of a network composed of more or less 2000 nodes, with different choice of the number of rows and columns. From the table it is evident that the memory requirement is very small in our network.

5.2 Connectivity

We assume that the nodes on each row and special columns are deployed together so that the nodes sharing common key also lie within radio frequency range. However, in this section we investigate the connectivity based on the key distribution of the network. For fixed size of the network (i.e., $N \approx 2000$), we provide the percentage of one-hop, two-hop and three-hop paths and the average path-length between any two nodes in the network. The target of our scheme is to minimize the average path-length between any two nodes. Theorems 4.2, 4.3 and 4.4 give the number of single-hop, 2-hop and 3-hop paths in the network. Therefore, the average path-length between two nodes in the network is $d = (L_1 + 2L_2 + 3L_3)/(L_1 + L_2 + L_3)$.

The percentage of one-hop two-hop and 3-hop paths denoted by l_1, l_2 and l_3 respectively, and the average path length d between any two randomly chosen nodes, corresponding to each of the fifteen sets are listed in Table 2.

From Table 2 we note that the average path length has its value in the range (2.10 to 2.40). the network is best connected when the number of rows are very small compared to the number of columns. Note that, the average path-length corresponds to the key-connectivity only.

Table 2. Connectivity

r	c	N	l_1	l_2	l_3	d
7	285	1995	14.41	60.25	25.34	2.109328
13	156	2028	7.91	57.95	34.14	2.262292
21	96	2016	5.11	56.84	38.04	2.329363
29	63	1827	3.98	56.22	39.80	2.358160
31	66	2046	3.73	56.17	40.10	2.363651
37	54	1998	3.32	55.88	40.79	2.374729
57	36	2052	2.68	55.26	42.06	2.393792
73	27	1971	2.61	54.82	42.57	2.399662
91	21	1911	2.69	54.38	42.93	2.402443
133	15	1995	2.98	53.63	43.40	2.404213
167	12	2004	3.38	53.02	43.60	2.402230
222	9	1998	4.16	52.04	43.80	2.396428
333	6	1998	5.86	50.14	44	2.381405
666	3	1998	11.27	44.53	44.20	2.329327

5.3 Resilience

Resilience is one of the most important evaluation parameters, to quantify the efficiency of a network. Resilience measures the robustness of a network under adversarial attack.

We consider the *random node capture* as the attack model. We assume that the adversary can listen and eavesdrop any communication over the channel between two nodes, but cannot tamper it. Under random node capture attack, the adversary also captures a large number of nodes and extracts all the keys stored at them. Now, the remaining nodes cannot further use those keys for communication. We address the measure of resilience in two ways: on the nodes and on the links (direct key-path between two nodes), in the following subsections node disconnection and link failure.

Node Disconnection. A node is said to be disconnected from the network if all the keys stored at the node are known to the adversary. In this section, we find the effect of adversary on the rest of the nodes. We quantify node disconnection by $V(s)$, the fraction of total number of nodes, that becomes disconnected when s nodes are compromised from the network. We obtain an expression for $V(s)$ with the help of the following results.

Theorem 5.1. *Minimum number of nodes to be compromised to disconnect a node $N_{i,j}$ completely from the network is given by*

$$\begin{cases} p+q+2, & \text{if } N_{i,j} \text{ is a Type A node;} \\ p+3, & \text{if } N_{i,j} \text{ is a Type B node.} \end{cases}$$

Proof. A node $N_{i,j}$ gets disconnected from the network if all the connections from $N_{i,j}$ are destroyed, i.e., all the nodes having a common key with $N_{i,j}$ get captured. We consider the following two cases:

Case (i): Let $N_{i,j}$ be a Type A node.

Now, it can be noted that, all the keys, stored at the node $N_{i,j}$, distributed to the nodes in the same column and same row of $N_{i,j}$ should be captured in order to disconnect $N_{i,j}$. There are $(c-1)$ more nodes in the row. From the property of the projective plane of order p, which has $p^2+p+1 \geq c$ nodes, it follows that in order to disconnect one node, at least $p+1$ nodes should be destroyed. According to the assumption C_j is a special column. There are $(r-1)$ more nodes in the column C_j, arranged according to a projective plane of order q, i.e., $q^2+q+1 \geq r$. Similarly at least $q+1$ nodes need to be captured. Therefore, one Type A node $N_{i,j}$ will be disconnected provided $q+1$ nodes along this column C_j and $p+1$ nodes along the row R_i get captured.

Case (ii): Let $N_{i,j}$ be a Type B node.

It can be observed observe that to disconnect $N_{i,j}$, all the nodes along the same row of $N_{i,j}$ and the two adjacent nodes of $N_{i,j}$ along the same column as $N_{i,j}$ should be destroyed. Therefore, total number of nodes to be captured to disconnect $N_{i,j}$ completely is $(p+1)+2=p+3$ nodes.

This completes the proof of the theorem. □

Corollary 5.2. Average number of nodes disconnected when s nodes are captured is given by $v_1(s) = \frac{3s}{(3p+q+8)}$.

We skip the proof due to page restrictions.

The measure of node disconnection, defined as the fraction of nodes that become disconnected when s nodes are compromised is given by

$$V(s) = \frac{v_1(s)}{N-s} = \frac{3s}{(3p+q+8)(N-s)}.$$

In Table 3, we provide the values $V(s)$ for increasing values of s, the number of compromised nodes. The total number of nodes in the network are assumed to be almost 2000. From the table it follows that we obtain better node disconnections when there are large number of rows and very small number of columns.

Table 3. Node disconnection of the proposed network

r	c	N	$V(100)$	$V(150)$	$V(200)$	$V(250)$	$V(300)$
7	285	1995	0.005107	0.007868	0.010783	0.013864	0.017128
13	156	2028	0.005187	0.007987	0.010941	0.14061	0.017361
21	96	2016	0.005051	0.007779	0.010658	0.013700	0.016919
31	66	2046	0.004973	0.007656	0.010485	0.013471	0.016628
29	63	1827	0.005604	0.008656	0.011896	0.015342	0.019013
37	54	1998	0.004391	0.006764	0.009270	0.011918	0.014723
57	36	2052	0.004269	0.006572	0.008999	0.011561	0.014269
73	27	1971	0.004334	0.006679	0.009157	0.011778	0.014557
91	21	1911	0.004248	0.006552	0.008992	0.011578	0.014325
133	15	1995	0.003518	0.005420	0.007428	0.009551	0.011799
167	12	2004	0.003151	0.004854	0.006652	0.008552	0.010563
222	9	1998	0.002679	0.004127	0.005656	0.007272	0.008984
333	6	1998	0.002359	0.003634	0.004981	0.006404	0.007911
666	3	1998	0.001737	0.002676	0.003667	0.004715	0.005825

Link Failure. A link is said to exist between two nodes if they share a common key. From the construction it follows that there is at most one common key between any two nodes, i.e., in this case, each link corresponds to a key. If the common key between any two key-connected nodes is captured by the adversary, one link is said to be destroyed.

The anti-resilience of a scheme is given by [9]:,

$$fail(s) = 1 - \left(1 - \frac{r^{'} - 2}{N - 2}\right)^{s} \tag{3}$$

where $fail(s)$ denotes the probability that a link between two uncaptured nodes is broken when s nodes are compromised in a network of size N and each key is assigned to $r^{'}$ number of nodes. Our grid-based scheme is neither regular nor uniform, i.e., the number of nodes to which each key is assigned varies in our case. Hence we modify eqn. (3) as follows:

$$fail(s) = 1 - \left(1 - \frac{m - 2}{N - 2}\right)^{s} \tag{4}$$

where m is the average number of nodes to which each key is assigned. We now find an expression for m.

Theorem 5.3. The average number of nodes to which each key is assigned, is

$$m = \frac{p + 3q + 8}{6}.$$

We skip the proof due to page restrictions.

Table 4. Link failure of our scheme

r	c	N	$fail(10)$	$fail(20)$	$fail(30)$	$fail(50)$	$fail(100)$	$fail(200)$	$fail(500)$	$fail(1000)$
7	285	1995	0.015776	0.031303	0.046584	0.076429	0.147016	0.272418	0.548451	0.796104
13	156	2028	0.014709	0.029202	0.043482	0.071414	0.137729	0.256489	0.523329	0.772784
21	96	2016	0.015612	0.030981	0.046110	0.075662	0.145599	0.269999	0.544689	0.792692
29	63	1827	0.017217	0.034137	0.050766	0.083170	0.159422	0.293429	0.580348	0.823892
31	66	2046	0.015385	0.030533	0.045448	0.074594	0.143623	0.266618	0.539399	0.787847
37	54	1998	0.019861	0.039327	0.058406	0.095436	0.181763	0.330489	0.633230	0.865479
57	36	2052	0.019342	0.038309	0.056910	0.093039	0.177422	0.323366	0.623396	0.858170
73	27	1971	0.020961	0.041483	0.061574	0.100503	0.190905	0.345365	0.653264	0.879774
91	21	1911	0.023324	0.046104	0.068353	0.111305	0.210221	0.376250	0.692725	0.905582
133	15	1995	0.027256	0.053769	0.079560	0.129052	0.241449	0.424600	0.748855	0.936926
167	12	2004	0.031189	0.061404	0.090678	0.146514	0.271562	0.469378	0.794902	0.957935
222	9	1998	0.038559	0.075631	0.111274	0.178489	0.325120	0.544538	0.859999	0.980400
333	6	1998	0.044988	0.087952	0.128983	0.205590	0.368913	0.601729	0.899897	0.989979
666	3	1998	0.064041	0.123981	0.180082	0.281736	0.484097	0.733844	0.963454	0.998664

In Table 4, we provide the values $fail(s)$ for increasing values of s, the number of compromised nodes. Table 4 indicates that we obtain better resilience, i.e., smaller values of $fail(s)$ when there are small number of rows and large number of columns.

5.4 Comparison with Existing Schemes

In Figure 6, we provide the comparison of link failure of our scheme with some existing schemes. To keep up N in our scheme comparable with other schemes, we consider a network with 13 rows and 156 columns i.e., $p = 3$ and $q = 13$, where the total number of nodes in the network being 2028.

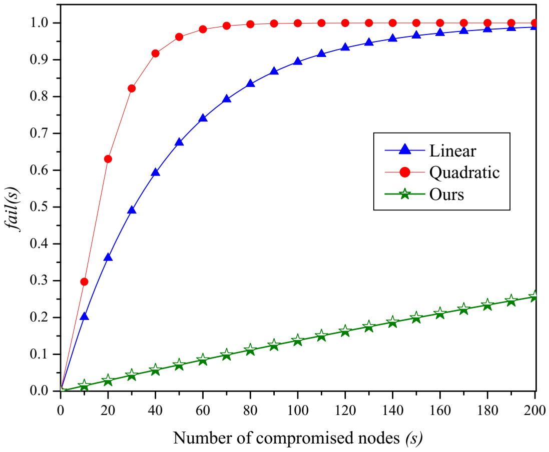

Fig. 6. Comparison of link failure

6 Conclusion

We present a KPS for a non-uniform rectangular grid adapting a deterministic approach. The nodes are assumed to be of two types depending on the resources provided to them. It is seen that the network is well connected, any two nodes can communicate (either directly or via a key-path) whenever they are within radio frequency range. The existence of multiple key-paths (of different lengths) between any two nodes increase the smooth relay of the data throughout the network even under adversarial attack. The results indicate that a large network is supported with a small memory requirement. The obtained results show that the scheme is well-resilient when compared to existing schemes.

References

1. Bag, S., Ruj, S.: Key Distributions in Wireless Sensor Networks Using Finite Affine Plane. In: Workshop of International Conference on Advanced Information Networking and Applications, pp. 436–441. IEEE Computer Scociety (2011)
2. Blackburn, S.R., Etzion, T., Martin, K.M., Paterson, M.B.: Efficient Key Predistribution for Grid-Based Wireless Sensor Networks. In: Safavi-Naini, R. (ed.) ICITS 2008. LNCS, vol. 5155, pp. 54–69. Springer, Heidelberg (2008)
3. Camptepe, S.A., Yener, B.: Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. ACM Trans. Netw. 15(2), 346–358 (2007)
4. Chakrabarti, D., Maitra, S., Roy, B.: A Key Pre-distribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design. In: Zhou, J., López, J., Deng, R.H., Bao, F. (eds.) ISC 2005. LNCS, vol. 3650, pp. 89–103. Springer, Heidelberg (2005)
5. Chen, C.Y., Chao, H.C.: A survey of Key Predistribution in Wireless Sensor Networks. Security Comm. Networks (2011)
6. Eschenauer, L., Gligor, V.D.: A Key-management Scheme for Distributed Sensor Networks. In: ACM CCS, pp. 41–47. ACM (2002)
7. Lee, J., Stinson, D.R.: Deterministic Key Predistribution Schemes for Distributed Sensor Networks. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 294–307. Springer, Heidelberg (2004)
8. Lee, J., Stinson, D.R.: Common Intersection Designs. Journal of Combinatorial Designs 14, 251–269 (2005)
9. Lee, J., Stinson, D.R.: A Combinatorial Approach to Key Predistribution for Distributed Sensor Networks. In: IEEE WCNC, pp. 1200–1205 (2005)
10. Lee, J., Stinson, D.R.: On The Construction of Practical Key Predistribution Schemes for Distributed Sensor Networks Using Combinatorial Designs. ACM Trans. Inf. Syst. Secur. 11(2) (2008)
11. Paterson, M.B., Stinson, D.R.: A Unified Approach to Combinatorial Key Predistribution Schemes for Sensor Networks. IACR Cryptology ePrint Archive (2011)
12. Ruj, S., Roy, B.: Key Predistribution Using Partially Balanced Designs in Wireless Sensor Networks. In: Stojmenovic, I., Thulasiram, R.K., Yang, L.T., Jia, W., Guo, M., de Mello, R.F. (eds.) ISPA 2007. LNCS, vol. 4742, pp. 431–445. Springer, Heidelberg (2007)
13. Ruj, S., Roy, B.: Key Predistribution Schemes Using Codes in Wireless Sensor Networks. In: Yung, M., Liu, P., Lin, D. (eds.) Inscrypt 2008. LNCS, vol. 5487, pp. 275–288. Springer, Heidelberg (2009)
14. Stinson, D.R.: Combinatorial Designs: Constructions and Analysis. Springer, New York (2003)