*International Journal of Distributed Sensor Networks*, 5: 660–674, 2009

# Revisiting Key Predistribution using Transversal Designs for a Grid-based Deployment Scheme

SUSHMITA RUJ and BIMAL ROY

Applied Statistics Unit, Indian Statistical Institute, Kolkata, India

*We consider a grid-based deployment scheme in which keys are predistributed in sensor nodes following a transversal design. This scheme was first proposed by Ruj, Maitra, and Roy in [19]. In their scheme the RF region was considered to be the a square of appropriate dimension. In this article, we consider the RF region to be the Lee sphere of appropriate radius. This is a better approximation than the square RF region and all calculations of connectivity and resiliency is done with respect to this parameter.*

**Keywords** Combinatorial Design; Connectivity Analysis; Deployment; Key Predistribution; Lee Distance; Secure Communication; Transversal Design; Two Dimensional Grid

## 1. Introduction

Sensor networks consist of resource constrained devices and deployed for both military and civilian purposes. To carry on communication in a secure manner, any two sensor nodes should communicate in an encrypted manner using a common secret key. Towards secure communication, it is important that any two sensor nodes should communicate in an encrypted manner using a common secret key. The designer may predistribute the keys in each sensor node or on-line key agreement strategies may be used. For on-line key agreement strategies, some kind of public key infrastructure is required. Public key techniques involve huge computational costs and are therefore not suitable for the resource constraint sensor nodes. Hence keys are preloaded in the sensors before deployment. Several key predistribution techniques have been discussed in literature. [1–4, 14–17].

To increase resiliency, deployment knowledge may be used. Deployment knowledge has been used in [1, 6, 7, 12, 15, 19, 21, 28]. In [19] Ruj, Maitra, and Roy proposed a grid-based deployment scheme in which keys are predistributed in the sensor nodes using combinatorial designs called transversal designs. As mentioned in [19], grid-based designs have several applications for both military and civilian purposes. They are used in intrusion detection as mentioned in [24] and [18]. Other applications of such a deployment pattern can be used to monitor temperature and pressure in a factory, monitor vehicles in a parking lot, monitor goods in a warehouse, monitor trees in a plantation. To protect commercial confidentiality, sensors may be placed in square grids. In this paper, we consider the grid-based deployment scheme where key predistribution is done according to the Transversal Design *TD* $(k, r)$. We consider the Lee sphere while

Address correspondence to Sushmita Ruj, Applied Statistics Unit, Indian Statistical Institute, 203 BT Road, Kolkata, 700 108, India. E-mail: sush_r@isical.ac.in calculating the connectivity ratio and resiliency. We study the connectivity and resiliency of the network taking the Lee distance into account. The importance of such analysis of Lee distance lies in the fact that we can change the Lee distance according to power requirements.

Given any kind of deployment, the key predistribution techniques may be randomized, deterministic, or hybrid. Key predistribution in sensor networks was first discussed in by Eschenauer and Gligor in [9]. Other key predistribution schemes were discussed in [5, 8, 13–15, 23]. For application of combinatorial designs in key predistribution, one may refer to [2, 4, 16, 17, 20]. In particular, in [16] Lee and Stinson transversal designs for key predistribution has been presented that has been extended later in [4] by Chakrabarti, Maitra, and Roy.

We consider $r^2$ blocks (identify them as sensor nodes) of the *TD* which are placed on a deployment grid of dimension $r \times r$. The connectivity of the network is then analyzed taking into account the Lee distance. The block indexed by $(i, j)$ is placed in the $(i, j)$ th location of the grid. We give a comparison of our scheme with that given by Ruj, Maitra, and Roy in [19]. We show how the connectivity ratio changes with the change of the Lee distance and number of keys in each node. The main idea where our proposal differs from the scheme given by Lee and Stinson [16] in that in their scheme sensor nodes are scattered randomly on an unknown geometry unlike our model where we consider a known grid based deployment.

The rest of this article is organized in the following way. In Section 2, we define basic concepts. In Section 3, we calculate the connectivity ratio (the fraction of nodes that a given node can communicate with within the Lee distance). For interior nodes we calculate the exact number of nodes with which it can communicate, for any given Lee distance. In Section 4, we study the resiliency of the network. We give two parameters for resiliency and find a tight theoretical bound for the first parameter and present experimental results for the second. We conclude in Section 5 with some open problems.

## 2. Preliminaries

**A transversal design** [26, Section 6.3] $TD\ (k, \lambda; r)$, with $k$ groups of size $r$ and index $\lambda$, is a triple $(X, G, A)$ where

1. $X$ is a set of $kr$ elements (varieties),
2. $G = \{G_1, G_2, \ldots, G_k\}$ is a family of $k$ sets (each of size $r$) which form a partition of $X$,
3. $A$ is a family of $k$-sets (or blocks) of varieties such that each $k$-set in $A$ intersects each group $G_i$ in precisely one variety, and any pair of varieties which belong to different groups occur together in precisely $\lambda$ blocks in $A$.

We denote a transversal design with $\lambda = 1$ as $TD(k, r)$. It can be shown that if there exists a $TD(k, r)$, then there exists a $(v, b, r, k)$ design with $v = kr$, $b = r^2$.

Let us now explain $X$, $A$ in a transversal design $TD(k, r)$.

1. $X = \{(x, y): 0 \leq x < k, 0 \leq y < r\}$,
2. For all $i$, $G_i = \{(i, y): 0 \leq y < r\}$,
3. $A = \{\mathrm{A}_{i,j}: 0 \leq i < r \;\&\; 0 \leq j < r\}$.

We define a block $A_{i,j}$ by

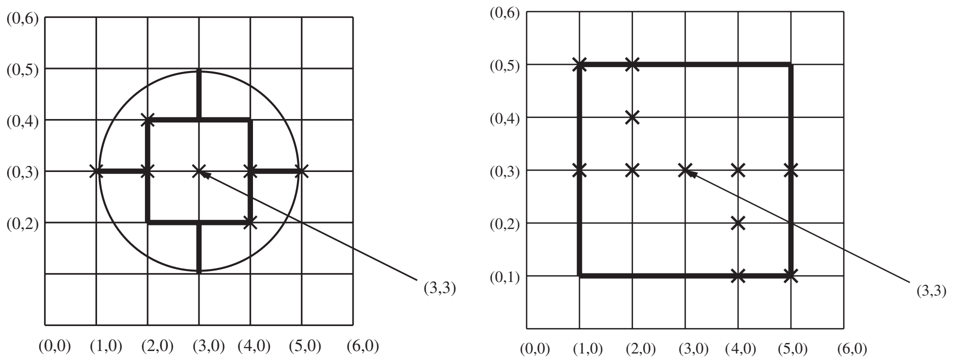
$$A_{i,j} = \{(x, xi + j \bmod r) : 0 \leq x < k\} \tag{1}$$

We consider an $r \times r$ grid such that there are $r^2$ points of intersection. For our purpose, we take a prime power $r$. We map the $r^2$ blocks to the $r^2$ sensor nodes and place block $A_{i,\ j}$ at the location $(i, j)$ of the grid as shown in Fig. 1a. We represent the node at $(i, j)$ by $n_{i,\ j}$. The varieties are mapped on to the secret keys in the sensor nodes. Thus we establish a correspondence between $TD(k,\ r)$ and the placement of sensor nodes on a $r \times r$ square grid. Note that any two blocks have either no key or one key in common and the algorithm to check whether the two nodes actually share a common secret key is efficient (see [16] for more details).

The sensor nodes can carry on effective communication only inside a particular range called the Radio Frequency (RF) range. The RF range with respect to a particular point is actually a circular region with center as that point and some radius around that. The *Manhattan distance* between two points is the sum of the horizontal and vertical distance between the points.

Consider a square grid (as shown in Fig. 1a). A *Lee Sphere* [1] of radius $\rho$ centered at a given point $P$ consists of the set of points that lie at a Manhattan distance of at most $\rho$ from $P$. $\rho$ is called the Lee distance. The triangle inequality implies that the Manhattan distance between two nodes is greater than the Euclidean distance. This implies that all the nodes within the Lee sphere of radius $\rho$ centered at a point $P$ are also contained in the RF region of radius $\rho$ centered at $P$. We see that a Lee sphere is a better approximation than a square RF region. (As given in Fig. 1a and b). We assume that two nodes can communicate with each other provided they are within Lee distance and have a common key.

*Definition 1.* Physical neighbor: *For a given node a located at (i, j) and a given Lee Distance $\rho$, a node $\beta$ ($\neq \alpha$) located at $(i', j')$ is said to be a physical neighbor of $\alpha$, if $\beta$ is within the Lee sphere of radius $\rho$ centered at $\alpha$. Mathematically, $|i - i'| \leq \rho$* and *$|j - j'| + |i - i'| \leq \rho$.*



(a) RF region is a Lee Sphere

(b) RF region is a Lee Sphere

**Figure 1.** A $7 \times 7$ grid with $k = 3$, $\rho = 2$. The physical neighbors of the node at (3, 3) occur along the dark lines and the key sharing neighbors are marked by crosses.

Note that the maximum number of physical neighbors is $2\rho(\rho + 1)$. For nodes at (or close to) the boundary, the number of physical neighbors is less.

*Definition 2.* Key sharing neighbor: *For a given node $\alpha$ located at $(i, j)$ and its physical neighbor $\gamma$ $(\neq \alpha)$ located at $(i', j')$, $\gamma$ is said to be a key sharing neighbor of $\alpha$, if $\gamma$ has a key common with $\alpha$.*

### *2.1. Key Exchange*

We now present the key exchange protocol between two sensor nodes. We consider a $r \times r$ grid, where $r$ is a prime power, such that each node contains $k$ keys. The Lee Distance $\rho$ is small for practical purposes and can be assumed to be much less than $\frac{r+1}{2}$. We see that node $n_{i,j}$ shares the common key $(0, j)$ with nodes $n_{0,j}, n_{1,j}, \ldots, n_{i-1,j}, n_{i+1,j}, \ldots, n_{r-1,j}$ and node $n_{i,\,j}$ do not share a common key with any of the nodes $n_{i,0}, n_{i,1}, \ldots, n_{i,j-1}, n_{i,j+1}, \ldots, n_{i,r-1}$. That is, all the nodes along a given row share a common key, and all nodes along a given column never share a common key. One may refer Fig. 1a as an example. Two nodes $n_{i,j}$ and $n_{i',\,j'}$ share a common key [4, 16] if for some $x$, $0 \leq x < k$, $xi + \mathrm{j} \equiv xi' + j' \bmod r$ (by Eq. (1)). It follows that, for $0 \leq x < k$, $x(i - i') \equiv j' - j \bmod r$ holds. So if $x \equiv (j' - j)\,(i - i')^{-1} \bmod r$, where $0 \leq x < k$, and $|i - i'| + |j - j'| \leq \rho$, then the nodes $n_{i,j}$ and $n_{i',j'}$ will share a common key. If $i = i'$, then $n_{i,j}$ and $n_{i',j'}$ do not share a common key. If $i \neq i'$, $x = (j' - j)\,(i - i')^{-1} \bmod r$, where $0 \leq x \leq k$ is a common key. Note that since $p$ is prime and $i \neq i'$, $(i - i')^{-1}$ exists. The common key can thus be efficiently calculated, since the inverse can be calculated efficiently by Extended Euclidean Algorithm in $O(\log_2^2 r)$ time as shown in [25, Chapter 5]. If two $i$ and $j$ nodes do not share a common key, then there exists an intermediary $t$ node such that $i$ and $t$ share some common key $k_{it}$ and $j$ and $t$ share a common key $k_{it}$. Node $i$ chooses some random key $K$ encrypts it with $k_{it}$ and sends it to $t$. $t$ decrypts it using $k_{it}$ and encrypts it using $k_{jt}$ and sends it to $j$. $j$ decrypts $K$ using $k_{jt}$. All communications between $i$ and $j$ takes place using the key $K$.

## 3. Connectivity Analysis

In this section we calculate the number of nodes within Lee distance which share a common key with a given node.

Fix a node $\alpha$ located at $(i, j)$ and Lee distance $\rho$. Consider the set $A_\rho^{(i,j)}$ of key sharing neighbors of $\alpha$ within the Lee Distance $\rho$ and the set $B_\rho^{(i,j)}$ of physical neighbors of $\alpha$ within a Lee Distance $\rho$. We will calculate $\left|A_\rho^{(i,j)}\right|$ in Theorem 1 later.

We call a node $n_{i,j}$ an *interior* node (not around the boundary), if $i \geq \rho$, $(r - 1 - i) \geq \rho$, $j \geq \rho$, $(r - 1 - j) \geq \rho$. For all the interior nodes $n_{i,\,j}$,

$$\left|B_\rho^{(i,j)}\right| = 2\rho(\rho + 1) \tag{2}$$

*Definition 3.* Connectivity Ratio: *The connectivity ratio $R_\rho^{(i,j)}$* of a node $n_{i,j}$ *is defined as the ratio of the number of key sharing neighbors of $n_{i,\,j}$ and the number of physical neighbors of $n_{i,j}$. Mathematically, $R_\rho^{(i,j)} = \frac{|A_\rho^{(i,j)}|}{|B_\rho^{(i,j)}|}$.*

We calculate the value of connectivity ratio for an interior node.

### 3.1. Calculation of Connectivity Ratio $R_\rho^{(i,j)}$ of Interior Node

We give the value of $A_\rho^{(i,j)}$ for an interior node $n_{i,}$, when $\rho \le \frac{r-1}{2}$. Consider an interior node $n_{i,\,j}$ that contains the keys indexed by $(0, j)$, $(1, (i+j) \bmod r)$, . . ., $(k-1, (i(k-1)+j) \bmod r)$. According to our transversal design, any two nodes can share a maximum of one key. Therefore, to find the key sharing neighbors of the node $n_{i,j}$, it is sufficient to find the number of nodes in which each of the $(x, (xi+j) \bmod r)$ keys occur, where $0 \le x < k$. Suppose the node $n_{i,\,j}$ contains the key $(x, y)$. We find the number of nodes within the Lee distance $\rho$ which also contain the key $(x, y)$. Given a key $(x, y)$, we find the nodes $n_{i,\,j}$ such that $y = xi + j \bmod r$. Hence the nodes $n_{i,\,j}$ must satisfy the equation

$$j = (y - xi) \bmod r \tag{3}$$

Note that the key $(x, y)$ occurs in nodes $n_{0,\,y}, n_{1,\,y-x}, \ldots, n_{n-1,\,y-x(n-1) \bmod r}$.

The node $n_{i,\,j}$ contains the keys $(x, y = xi + j \bmod r)$ where $0 \le x < k$. By Eq. (3), if $n_{i+t,\,j'}$ is a key sharing node of $n_{i,j}$, then $j' = (y - x(i+t)) \bmod r$. So $j' = (j - xt) \bmod r$. The key sharing neighbors of $n_{i,\,j}$ which share the key $(x, y)$ are the following: $n_{i+1,j-x}$, $n_{i+2,j-2x}, \ldots, n_{i+t,\,j-xt}$ and $n_{i-1,\,j+x}, n_{i-2,\,j+2x}, \ldots, n_{i-t,\,j+xt}$.

To find ($n_{i',j'}$ the key sharing neighbors of $n_{i,\,j}$, we refer to the Fig. 2. We find the key sharing neighbors in the four quadrants. The following cases arise.

*Case a.* When $i' < i$, we consider the nodes $(i-1, j+x)$, $(i-2, j+2x)$, . . ., $(i-t, j+tx)$, where $0 \le x \le k-1$.

If $j \le j'$ (when the neighboring nodes are in quadrant I), then the following conditions must be satisfied.

$$0 < t \le \min\{i, \rho\}, 0 \le x < k \textit{ and } tx \bmod r \le \min\{\rho - t, r - 1 - j\} \tag{4a}$$

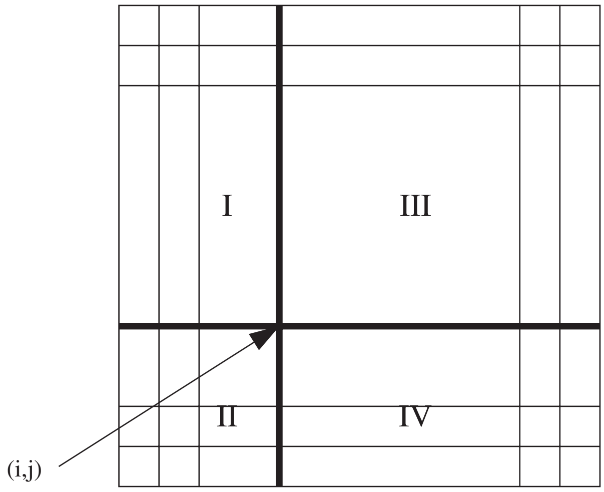


**Figure 2.** A $n \times n$ grid showing the four types of neighboring nodes.

If $j > j'$ (when the neighboring nodes are in quadrant II), then the following conditions must be satisfied.

$$0 < t \leq \min\{i, \rho\}, 0 \leq x < k \, and \, r - (tx \bmod r) \leq \min\{\rho - t, j\} \tag{4b}$$

*Case b.* When $i' > i$, we consider the nodes $(i + 1, j - x)$, $(i + 2, j - 2x)$, . . ., $(i + t, j - tx)$, where $0 \leq x \leq k - 1$.

If $j \geq j'$ (when the neighboring nodes are in quadrant IV), then the following conditions must be satisfied.

$$0 < t \leq \min\{r - 1 - i, \rho\}, 0 \leq x \leq k - 1 \, and \, tx \bmod r \leq \min\{\rho - t, j\} \tag{5a}$$

If $j < j'$ (when the neighboring nodes are in quadrant III), then the following conditions must be satisfied.

$$0 < t \leq \min\{r - 1 - i, \rho\}, 0 \leq x \leq k - 1 \, and \, r - (tx \bmod r) \leq \min\{\rho - t, r - 1 - j\} \tag{5b}$$

Now we consider an interior node $n_{i,\ j}$. We find the key-sharing neighbors of $n_{i,j}$. We consider the neighbors in the four quadrants. Since $r - i - 1 \geq \rho$, $r - i - 1 \geq \rho - t$, and $min\{r - i - 1, \rho - t\} = \rho - t$. Hence Eq. (4a) reduces to (6a). Similarly we obtain the other equations, Eqs. (6b), (7a), and (7a) from (4a), (4b), (5a), and (5b).

*Case a.* When $i' < i$, we consider the nodes $(i - 1, j + x)$, $(i - 2, j + 2x)$, . . ., $(i - t, j + tx)$, where $0 \leq x < k$.

If $j \leq j'$ (when the neighboring nodes are the quadrant I), then the following conditions must be satisfied.

$$0 < t \leq \rho, 0 \leq x < k \, and \, tx \bmod r \leq \rho - t \tag{6a}$$

If $j > j'$ (when the neighboring nodes are in quadrant II), then the following conditions must be satisfied.

$$0 < t \leq \rho, 0 \leq x < k \, and \, r - (tx \bmod r) \leq \rho - t \tag{6b}$$

*Case b.* When $i' > i$, we consider the nodes $(i + 1, j - x)$, $(i + 2, j - 2x)$, . . ., $(i + t, j - tx)$, where $0 \leq x < k$.

If $j \geq j'$ (when the neighboring nodes are in quadrant IV), then the following conditions must be satisfied.

$$0 < t \leq \rho, 0 \leq x \leq k - 1 \, and \, tx \bmod r \leq \rho - t, \tag{7a}$$

If $j < j'$ (when the neighboring nodes are in quadrant III), then the following conditions must be satisfied.

$$0 < t \leq \rho, 0 \leq x < k - 1 \, and \, r - 1 \, (tx \bmod r) \leq \rho - t, \tag{7b}$$

So, the number of solutions ($t$, $x$) satisfying the above Eqs. (6a), (6b), (7a), and (7b) give the number of the interior node $n_{i,\,j}$ within the Lee distance $\rho$ which share key ($x$, $y$).

The following lemma is crucial in finding the exact value of $\left|A_\rho^{(i,j)}\right|$. This lemma was given in [19] but for the sake of completeness we give it again here.

*Lemma 1. Let w be a prime such that $w \geq 2T - 1$. Then the number of solutions* ($t$, $x$) *satisfying the equation*

$$0 < S' \leq tx \bmod w \leq S \leq w - 1 \tag{8}$$

*where, $0 < t \leq T < w$ and $0 \leq x \leq X < w$, is given by $\sum_{t=1}^{T}\sum_{l=0}^{t-1} S_1$ where $u_1 = (wl + S')/t$, $u_2 = (wl + S)/t$ and*

$$S_1 = \begin{cases} 0, & \textit{if}\, X + 1 \leq \lceil u_1 \rceil \leq \lfloor u_2 \rfloor, \\ X + 1 - \lceil u_1 \rceil & \textit{if}\, \lceil u_1 \rceil < X + 1 \leq \lfloor u_2 \rfloor, \\ \lfloor u_2 \rfloor - \lceil u_1 \rceil + 1 & \textit{if}\, \lfloor u_2 \rfloor < X + 1. \end{cases}$$

*Proof.* When $t = 1$, three conditions can arise.

Case (i): If $X + 1 \leq S'$, then there are no values of $x$ which satisfy (8).
Case (ii): If $S' < X + 1 \leq S$, $x = S', S' + 1, S' + 2, \ldots, X$ satisfy (8). So there are $X + 1 - S'$ solutions.
Case (iii): If $S \leq X$, $x = S', S' + 1, S' + 2, \ldots, S$ satisfy (8). So there are $S - S' + 1$ solutions.

When $t = 2$, three conditions can arise.

Case (i): If $X + 1 \leq \lceil \frac{S'}{2} \rceil$, then there are no values of $x$ which satisfy (8).
Case (ii): If $\lceil \frac{S'}{2} \rceil < X + 1 \leq \lfloor \frac{S}{2} \rfloor$, then $x = \lceil \frac{S'}{2} \rceil, \lceil \frac{S'}{2} \rceil + 1, \ldots, X$ satisfy (8). So, there are $X + 1 - \lceil \frac{S'}{2} \rceil$ solutions.
Case (iii): If $\lfloor \frac{S}{2} \rfloor \leq X$, then $x = \lceil \frac{S'}{2} \rceil, \lceil \frac{S'}{2} \rceil + 1, \ldots, \lfloor \frac{S}{2} \rfloor$ satisfy (8). So there are $\lfloor \frac{S}{2} \rfloor - \lceil \frac{S'}{2} \rceil + 1$ solutions.

When Case (iii) arises, then again consider the three sub cases.

Case (iii a): If $X + 1 \leq \lceil \frac{w+S'}{2} \rceil$, then there are no values of $x$ which satisfy (8).
Case (iii b): If $\lceil \frac{w+S'}{2} \rceil < X + 1 \leq \lfloor \frac{w+S}{2} \rfloor$, then $x = \lceil \frac{w+S'}{2} \rceil, \lfloor \frac{w+S'}{2} \rfloor + 1, \cdots, X$ satisfy (8). So there are $X - \lceil \frac{w+S'}{2} \rceil + 1$ such solutions.
Case (iii c): If $\lfloor \frac{w+S}{2} \rfloor \leq X$, then $x = \lceil \frac{w+S'}{2} \rceil, \lceil \frac{w+S'}{2} \rceil + 1, \cdots, \lfloor \frac{w+S}{2} \rfloor$ satisfy (8).

So there are $\lfloor \frac{w+S}{2} \rfloor - \lceil \frac{w+S'}{2} \rceil + 1$ such solutions.

Note that for $\lfloor \frac{S}{2} \rfloor < x < \lceil \frac{w+S'}{2} \rceil$, there is no solution when $t = 2$. The above cases give all the solutions when $t = 2$, since $\lceil \frac{lw+S'}{2} \rceil > w$, $l > 1$. So, the number of solutions when $t = 2$, is $\sum_{l=0}^{1} S_1$, where $S_1$ is as given.

Proceeding as above, $t = m$, three conditions can arise.

Case (i): If $X + 1 \leq \left\lceil \frac{S'}{m} \right\rceil$, then there are no values of $x$ which satisfy (8).
Case (ii): If $\left\lceil \frac{S'}{m} \right\rceil < X + 1 \leq \left\lfloor \frac{S}{m} \right\rfloor$, then, $x = \left\lceil \frac{S'}{m} \right\rceil, \left\lfloor \frac{S'}{m} \right\rfloor + 1, \cdots, X$ satisfy (8). So, there are $X + 1 - \left\lceil \frac{S'}{m} \right\rceil$ solutions.

When Case (iii) arises, then again consider the three sub cases.

Case (iii a): If $X + 1 \leq \left\lceil \frac{w+S'}{m} \right\rceil$, then there are no values of $x$ which satisfy (8).
Case (iii b): If $\left\lceil \frac{w+S'}{m} \right\rceil < X + \leq \left\lfloor \frac{w+S'}{m} \right\rfloor$, then $x = \left\lceil \frac{w+S'}{m} \right\rceil, \left\lfloor \frac{w+S'}{m} \right\rfloor + 1, \cdots, X$ satisfy (8). So there are $X - \left\lceil \frac{w+S'}{m} \right\rceil + 1$ such solutions.
Case (iii c): If $\left\lfloor \frac{w+S}{2} \right\rfloor \leq X$, then $x = \left\lceil \frac{w+S'}{m} \right\rceil, \left\lceil \frac{w+S'}{m} \right\rceil + 1, \cdots, \left\lfloor \frac{w+S}{m} \right\rfloor$ satisfy (8). So there are $\left\lfloor \frac{w+S}{m} \right\rfloor - \left\lceil \frac{w+S'}{m} \right\rceil + 1$ such solutions.

Note that for $\left\lfloor \frac{S}{m} \right\rfloor < x < \left\lceil \frac{w+S'}{m} \right\rceil$, there is no solution when $t = m$.

Again for Case (iii c), three cases can arise. Continuing similarly, we notice that if $\left\lfloor \frac{(m-2)\,w+S}{m} \right\rfloor \leq X$, then three conditions will arise.

Case (a): If $X + 1 \leq \left\lceil \frac{(m-1)\,w+S'}{m} \right\rceil$, then there are no values of $x$ which satisfy (8).
Case (b): If $\left\lceil \frac{(m-1)\,w+S'}{m} \right\rceil < X + 1 \leq \left\lfloor \frac{(m-1)w+S}{m} \right\rfloor$, then $x = \left\lceil \frac{(m-1)w+S'}{m} \right\rceil, \left\lceil \frac{(m-1)w+S'}{m} \right\rceil + 1, \cdots, X$ satisfy (8). So there are $X - \left\lceil \frac{(m-1)\,w+S'}{m} \right\rceil + 1$ such solutions.
Case (c): If $\left\lfloor \frac{(m-1)\,w+S}{m} \right\rfloor \leq X$, then $x = \left\lceil \frac{(m-1)\,w+S'}{m} \right\rceil, \left\lceil \frac{(m-1)\,w+S'}{m} \right\rceil + 1, \cdots, \left\lfloor \frac{(m-1)\,w+S}{m} \right\rfloor$ satisfy (8). So there are $\left\lfloor \frac{(m-1)\,w+S}{m} \right\rfloor - \left\lceil \frac{(m-1)\,w+S'}{m} \right\rceil + 1$ such solutions.

Note that for $\left\lfloor \frac{(m-2)\,w+S}{m} \right\rfloor < x < \left\lfloor \frac{(m-1)\,w+S'}{m} \right\rfloor$, there is no solution when $t = m$. These are the only solutions when $t = m$, since $\left\lceil \frac{m''w+S'}{m} \right\rceil > w$, for $m'' > m$. So, the number of solutions when $t = m$, is $\sum_{l=0}^{m-1} S_1$, where $S_1$ is as given.

Hence for all values of $t$, $1 \leq t \leq T$, there are $\sum_{t=1}^{T} \sum_{t=0}^{t-1} S_1$ solutions satisfying (8).

We give the example given in [19] to demonstrate the above theorem. We consider the equation

$$0 < tx \bmod 7 \leq 5 \, and \, 0 < t \leq 3 \, and \, 0 \leq x \leq 4. \tag{9}$$

Note that $w$ is a prime and $w \geq 2T - 1$. For $t = 1$, the tuples (1, 1), (1, 2), (1, 3), (1, 4) satisfy (9). So, there are four solutions when $t = 1$. Here $\lceil u_1 \rceil = 1$, $\lfloor u_2 \rfloor = 5$. Since $1 < X + 1 \leq 5$, from the formula in Lemma 1 there are $X + 1 - \lceil u_1 \rceil = 4 + 1 - 1 = 4$ solutions.

For $t = 2$, the tuples (2, 1), (2, 2), (2, 4) satisfy (9). So, there are three solutions when $t = 2$. When $l = 0$, $\lceil u_1 \rceil = 1$, $\lfloor u_2 \rfloor = 2$. Since $X > 2$, there are $\lfloor u_2 \rfloor + 1 - \lceil u_1 \rceil = 2 + 1 - 1 = 2$ solutions. When $l = 1$, $\lceil u_1 \rceil = 4$, $\lfloor u_2 \rfloor = 6$. Since $\lceil u_1 \rceil < X + 1 \leq \lfloor u_2 \rfloor$, there are $X + 1 - \lceil u_1 \rceil = 4 + 1 - 4 = 1$ solutions.

For $t = 3$, the tuples (3, 1), (3, 3), (3, 4) satisfy (9). So, there are three solutions when $t = 2$. When $l = 0$, $\lceil u_1 \rceil = 1$, $\lfloor u_2 \rfloor = 1$. Since $X > 1$, there is $\lfloor u_2 \rfloor + 1 - \lceil u_1 \rceil = 1 + 1 - 1 = 1$ solutions. When $l = 1$, $\lceil u_1 \rceil = 3$, $\lfloor u_2 \rfloor = 4$. Since $X \geq \lfloor u_2 \rfloor$, there are $\lfloor u_2 \rfloor - \lceil u_1 \rceil = 4 - 3 + 1 = 2$ solutions. When $l = 2$, $\lceil u_1 \rceil = 5$, $\lfloor u_2 \rfloor = 6$. Since $X + 1 \leq 5$, there is no solution. All these three cases provide the overall count.

Using Lemma 1 and conditions (6a), (6b), (7a), and (7b) we arrive at the following theorem.

*Theorem 1.* $\left|A_\rho^{(i,j)}\right| = 2\rho + 2\sum_{t=1}^{\rho-1}\left(\sum_{t=0}^{t-1} A + \sum_{l=1}^{t} B\right)$ *where*, $a_1 = (rl + 1)/t$, $a_2 = (rl + \rho - t)/t$, $b_1 = (rl - \rho + t)/t$, $b_2 = (rl - 1)/t$, *and*

$$A = \begin{cases} 0, & \text{if } k \leq \lceil a_1 \rceil \leq \lfloor a_2 \rfloor, \\ k - \lceil a_1 \rceil & \text{if } \lceil a_1 \rceil < k \leq \lfloor a_2 \rfloor, \\ \lfloor a_2 \rfloor - \lceil a_1 \rceil + 1 & \text{if } \lfloor a_2 \rfloor < k, \end{cases}$$

*and*

$$B = \begin{cases} 0, & \text{if } k \leq \lceil b_1 \rceil \leq \lfloor b_2 \rfloor, \\ k - \lceil b_1 \rceil & \text{if } \lceil b_1 \rceil < k \leq \lfloor b_2 \rfloor, \\ \lfloor b_2 \rfloor - \lceil b_1 \rceil + 1 & \text{if } \lfloor b_2 \rfloor < k, \end{cases}$$

*Proof.* When $x = 0$, $(i - 1, 0), (i - 2, 0), \ldots, (i - \rho, 0)$ satisfy (6a).

For $x \neq 0$, we can map (6a) to Lemma 1. Here, $w = r$, $S' = 1$, $S = \rho - t$, $T = \rho - 1$, $X = k - 1$. So the number of solutions satisfying (6a) is given by $\rho + \sum_{t=1}^{\rho-1}\sum_{l=0}^{t-1} A$. The number of solutions satisfying (6b) is given by $\sum_{t=1}^{\rho-1}\sum_{l=1}^{t} B$.

Since we are considering the interior node, the number of key sharing neighbors in quadrant IV is the same as quadrant I and the number of key sharing neighbors in quadrant III is the same as quadrant II. Hence the total number of key sharing neighbors of $n_{i,j}$ will be $2\rho + 2\sum_{t=1}^{\rho-1}\left(\sum_{l=0}^{t-1} A + \sum_{l=1}^{t} B\right)$. Hence the theorem. □

Note that the value of $\left|A_\rho^{(i,j)}\right|$ from the above theorem and the value of $\left|B_\rho^{(i,j)}\right|$ from Eq. (2) directly provides the connectivity ratio $R_\rho^{(i,j)} = \frac{\left|A_\rho^{(i,j)}\right|}{\left|B_\rho^{(i,j)}\right|}$ for all interior node $(i, j)$.

Table 1 compares the connectivity ratio with respect to the Lee sphere are square RF regions for an interior node. Though the connectivity ratio for square RF region is better we can see from the figures that Lee sphere is a better approximation of RF region. Figure 3

**Table 1**
Connectivity Ratio $R_\rho$ for Interior Nodes with a Change in the Lee Distance or RF Radius as Defined in [19], for a 47 × 47 Grid with 30 keys per Node

| $\rho$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $R_\rho$ (Lee Distance) | 0.5 | 0.5 | 0.5833 | 0.55 | 0.57 | 0.5952 | 0.5892 | 0.5833 |
| $R_\rho$ (Square RF region) | 0.5 | 0.5833 | 0.5833 | 0.57500 | 0.60000 | 0.60714 | 0.61607 | 0.61111 |

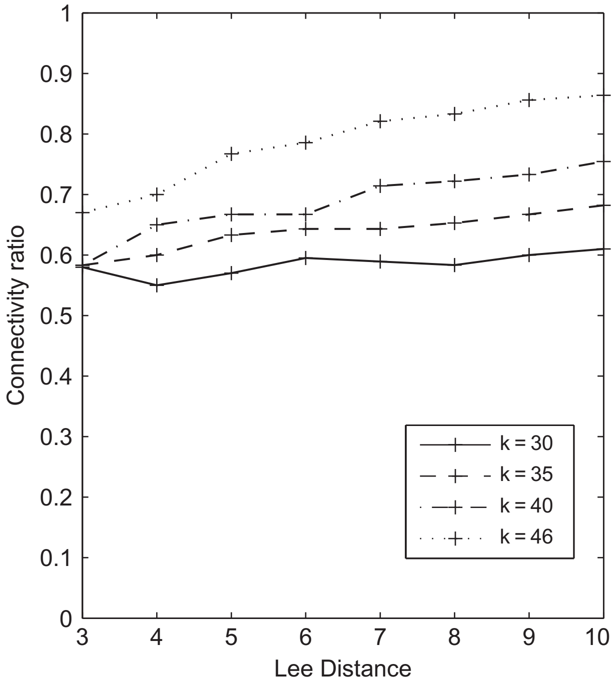


**Figure 3.** Comparison of connectivity ratio $R_\rho$ with changing lee distance $\rho$ and number of keys $k$ on 47 × 47 grid.

presents the connectivity ratio with varying $k$ (the number of keys in each sensor). We see that as the number of keys increases, the connectivity ration increases.

## 4. Resiliency

Sensor nodes are prone to failure and node capture or compromise. In case of node compromise, all the keys present in the compromised nodes are rendered ineffective. According to our design any two nodes share at most one common key. So all links which communicate via an exposed key are compromised (exposed). We give two parameters of resiliency of a Wireless Sensor Network (WSN), one based on the proportion of links that are broken and the other based on the proportion of nodes being disconnected.

1. $E(s)$, which is defined as

$$E(s) = \frac{\text{Number of links exposed after } s \text{ nodes are compromised}}{\text{Number of links present before compromise}}$$

2. $V(s)$ which is the probability of a node (which is not among the compromised nodes) being disconnected when $s$ nodes are compromised. A node (which is not among the compromised nodes) is considered disconnected if all the keys in the disconnected node are present in one or more compromised nodes.

We find an upper bound for $E(s)$ and give some experimental results for $V(s)$.

### 4.1. *Estimation of* E*(s)*

Let us denote the total number of links by $T$. Hence $T = \frac{1}{2}\sum_{i=0}^{r-1}\sum_{j=0}^{r-1}|A_{\rho}^{(i,j)}|$.

There are a total of $rk$ keys. If the nodes are compromised such that all $rk$ keys are compromised, then all the links are broken. However, for simplicity we assume that only a small fraction of the nodes are compromised. Suppose $s$ nodes are compromised. Maximum number of links are broken when the nodes compromised have disjoint sets of keys and occur in the interior.

Let the number of links broken when $s$ nodes are compromised be denoted by $C_s$.

Consider a node $n_{i,j}$ which has been compromised. Let it contain key $(x, y)$. We find the nodes $n_{i',j'}$ within Lee distance of $n_{i,j}$ which share the key $(x, y)$. By the analysis of $A_{\rho}^{(i,j)}$, we see that the nodes $n_{i-1,j+x}, n_{i-2,j+2x}, \ldots, n_{i-t,j+tx}$ and $n_{i+1,j-x}, n_{i+2,j-2x}, \ldots, n_{i+t,\, j-tx}$ are the key sharing neighbors of the node $n_{i,j}$. So $|t| \leq \rho$ and either $tx \bmod r \leq \rho - t$ or $r - |\, tx \bmod r| \leq \rho - t$. Since $x$ is known, the number of nodes sharing key $(x, y)$ within the Lee distance is the same as finding the number of values of $t$ which satisfy the equations

$$|t| \leq \rho \text{ and } |tx \bmod r| \leq \rho - t \tag{10a}$$

and

$$|t| \leq \rho \text{ and } r - |tx \bmod r| \leq \rho - t \tag{10b}$$

We consider a key $(x, y)$. Let us denote the number of links compromised when $(x, y)$ is compromised is less than $c_x$. Let the following keys be exposed when $s$ nodes are compromised. $(x_1, y_{11}), (x_1, y_{12}), \cdots, (x_1, y_{1s_1}), (x_2, y_{21}),\ (x_2, y_{22}), \cdots, (x_2, y_{2s_2}), \cdots, (x_{k-1}, y_{k-11}), (x_1, y_{k-12}), \cdots, (x_1, y_{k-1s_{k-1}})$. Each key occurs $r$ times. So the number of links compromised is less than $r(\sum_{i=0}^{k-1} c_{x_i}, s_i)$. In reality the position of the compromised node and the position of the nodes which contain the exposed keys will determine the number of links compromised. Since the position of the nodes and the keys exposed cannot be determined, it is difficult to calculate an upper bound for the number of links

**Table 2**
Experimental Value of $E(s)$ for 100 Runs and Bound for $E(s)$, when Number of Nodes in the Grid is $r^2$, Keys per Node is $k$ and the Lee Distance (RF radius) is $\rho$

| $r$ | $k$ | $\rho$ | $s$ | $E(s)$ (Lee Distance) | $E(s)$ (RF radius of [19]) |
|---|---|---|---|---|---|
| 23 | 15 | 7 | 5 | 0.1990 | 0.2006 |
| 23 | 15 | 5 | 5 | 0.1981 | 0.2008 |
| 31 | 20 | 7 | 5 | 0.1526 | 0.1516 |
| 31 | 25 | 7 | 5 | 0.1528 | 0.1513 |
| 37 | 30 | 7 | 5 | 0.1289 | 0.1283 |
| 53 | 49 | 7 | 5 | 0.0913 | 0.0915 |
| 53 | 49 | 7 | 10 | 0.1756 | 0.1736 |

exposed. $C_s \leq r(\sum_{i=0}^{k-1} c_{xi}\, s_i)$. $E(s) = \frac{C_s}{T}$, where $T \leq \frac{1}{2}\sum_{i=0}^{r-1}\sum_{j=0}^{r-1}\left|A_{\rho}^{(i,j)}\right|$.

We give the experimental values of $E(s)$ in Table 2.

### 4.2. *Experimental Results for* V*(s)*

$V(s)$ can be defined as the probability that a node is disconnected, given that $s$ nodes are compromised. Mathematically,

$$V(s) = \frac{\text{Number of nodes disconnected}}{r^2 - s}.$$

As discussed in [19] if $s < k$, no node is disconnected. For any node to be disconnected each of its $k$ keys must be present in some compromised node. However, no two or more keys that are present in the disconnected node can be present in any compromised node, since any pair of nodes share at most one key. Hence there is no node which will have all the $k$ keys in the compromised $s$ sensor nodes.

Since the number of nodes disconnected when $s$ nodes are compromised does not depend on the RF radius, we get the same results for $V(s)$ as obtained in [19].

The experimental results for the calculation of $V(s)$ is given in Table 3.

## 5. Related Works

Key predistribution using deployment knowledge has been studied in [1, 6, 7, 12, 15, 21, 28]. In this article, we use the Lee sphere approximation of RF region as discussed by Blackburn, Etzion, Martin, and Paterson in [1]. In [1] Blackburn, Etzion, Martin, and Paterson proposed a key predistribution scheme for a grid-based deployment scheme. They used combinatorial structures like Costas arrays and Distinct - difference configuration for key predistribution. However, their design is applicable, provided suitable Costas arrays and Distinct-difference configurations exist. The construction of Distinct-difference configuration which matches the desired requirements has not been presented

**Table 3**
Experimental Value of $V(s)$ for 100 Runs when Number of Nodes in the Grid is $r^2$, Keys per Node is $k$ and $s$ Nodes are Compromised

| $r$ | $k$ | $s$ | $V(s)$ |
|---|---|---|---|
| 11 | 5 | 9 | 0.0180 |
| 13 | 9 | 9 | 0.0250 |
| 37 | 5 | 30 | 0.0350 |
| 47 | 5 | 30 | 0.0150 |
| 47 | 6 | 30 | 0.0096 |
| 47 | 7 | 30 | 0.0027 |
| 47 | 9 | 30 | 0.0004 |
| 53 | 13 | 30 | 0.0000 |

in the paper. In our scheme all nodes are connected by a maximum of two-hop paths. However, using Costas arrays this is not guaranteed. (As the example of 3 × 3 Costas array in [1] shows.) Our design is simple and results in high resiliency in terms of $V(s)$ and $E(s)$ as already mentioned in the previous section. Though the number of groups is chosen to be $r^2$, where $r$ is a prime power, the design discussed above works in all those cases where the dimension $n$ of the grid is not a prime power. This can be done by simply choosing a prime power $r > n$ and neglect the regions which fall out of the $n \times n$ grid.

## 6. Conclusion and Future Research

In this article, we revisit the grid-based deployment scheme as proposed by Ruj, Maitra, and Roy in [19]. Transversal designs are used for key predistribution. RF region is assumed to be a square of appropriate dimension in [19]. In [1] Blackburn et al. introduced Lee sphere as an approximation of the RF region. We use Lee distance while calculating the connectivity ratio and resiliency of the grid based network as proposed in [19]. The main reason for doing so is that Lee sphere provides a better approximation than the square RF region. This scheme is much better than the scheme proposed by Blackburn et al. mainly because it is very simple to construct transversal designs.

However, in the discussed key predistribution scheme a particular node may share keys with nodes which are not within its Lee distance. This is clearly a underutilization of resources. In future we would like to construct key predistribution schemes such that only nodes which are within Lee distance share keys with one another.

## About the Authors

**Sushmita Ruj** received her B.E. degree in Computer Science from Bengal Engineering College, Shibpur, India in 2004, and M. Tech. degree in Computer Science from Indian Statistical Institute, Kolkata, India in 2006. She was a Ph. D. Student in Indian Statistical Institute, Kolkata from 2006 to 2009. Currently, she is a post-doctoral fellow at Lund University, Sweden. Her interests are combinatorics, cryptography and network security.

**Bimal Roy** obtained his B. Stat and M. Stat degrees from the Indian Statistical Institute, Calcutta, India in 1978 and 1979, respectively, and Ph.D. from University of Waterloo, Canada in 1982. He is currently a professor at the Indian Statistical Institute, Kolkata. His research area includes cryptography, security, combinatorics, etc. His special topics of interest are sensor networks, visual cryptography, hash functions and stream ciphers.

## References

1. S. R. Blackburn, T. Etzion, K. M. Martin and M. B. Paterson. ‘‘Efficient key predistribution for Grid-based Wireless sensor networks,’’ in the Proceedings of *Information Theoretic Security, Third International Conference, ICITS 2008*, Calgary, Canada, LNCS 5155, pp. 54–69, August 2008.
2. S. A. Camtepe and B. Yener, ‘‘Combinatorial design of key distribution mechanisms for wireless sensor networks,’’ in *Proceedings of Computer Security- ESORICS 2004*, Springer-Verlag, LNCS 3193, pp. 293–308, 2004.

3. S. A. Camtepe, B. Yener and Moti Yung. ''Expander Graph based Key Distribution Mechanisms in Wireless Sensor Networks,'' in *The Proceedings of IEEE International Conference on Communications (ICC) 2006*, pp. 2262–2267, June 2006.
4. D. Chakrabarti, S. Maitra and B. K. Roy, ''A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design,'' in *International Journal of Information Security*, vol. 5, Issue 2, pp. 105–114, April 2006.
5. H. Chan, A. Perrig and D. Song. ''Random Key Predistribution Schemes for Sensor Networks,'' in *The Proceeding of IEEE Symposium on Security and Privacy*, California USA, pp. 197–213, 2003.
6. H. Chan and A. Perrig. ''PIKE: Peer Intermediaries for Key Establishment in Sensor Networks,'' In the Proceeding of INFOCOM 2005, pp. 524–535, March 2005.
7. W. Du, J. Deng, Y. S. Han and P. K. Varshney, ''A key predistribution scheme for sensor networks using deployment knowledge,'' in *IEEE Transaction on Dependable and Secure Computing*, vol. 3, No. 1, pp. 62–77, January–March 2006.
8. W. Du, J. Deng, Y. S. Han and P. K. Varshney, ''A pairwise key predistribution scheme for wireless sensor networks,'' in *Proceedings of 10th ACM Conference on Computer and Communication Security (CCS)*, pp. 52–61, 2003.
9. L. Eschenauer and V. D. Gligor, ''A Key-Management scheme for Distributed Sensor Network,'' in *IEEE Symposium on Security and Privacy*, pp. 41–47, 2002.
10. A. Gallais, J. Carle, D. Simplot-Ryl and I. Stojmenovic, ''Localized sensor area coverage with low communication overhead,'' in *Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom)*, Italy, March 14–17, pp. 328–337, 2006.
11. D. Hwang and Y. Kim. ''Revisiting Random Key Pre-distribution Schemes for Wireless Sensor Networks,'' in the Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, SASN, Washington, USA, pp. 43–52, 2004.
12. D. Huang, M. Mehta, D. Medhi, L. Harn. ''Location-aware Key Management Scheme for Wireless Sensor Networks,'' in the Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington DC, USA, pp. 29–42, 2004.
13. R. Kalindi, R. Kannan, S.S. Iyenger and A. Durresi, ''Sub-Grid based Key Vector Assignment: A key Pre-distribution for sensor networks,'' in *Journal of Pervasive Computing and Communications*, vol. 2, no 1. pp. 35–43, 2006.
14. D. Liu and P. Ning, ''Establishing pairwise keys in distributed sensor networks,'' in *Proceedings of ACMCCS 2003*, New York, USA, pp. 52–61, 2003.
15. D. Liu and P. Ning, ''Location-based pairwise key establishments for static sensor networks,'' in *Proceedings of the 1st ACM Workshop on Security in Ad Hoc and Sensor Networks*, October, pp. 72–82, 2003.
16. J. Lee and D. Stinson, ''A combinatorial approach to key predistribution for distributed sensor networks,'' in *IEEE Wireless Communications and Networking Conference (WCNC 2005)*, New Orleans, LA, USA, pp. 1200–1205, 2005.
17. J. Lee and D. Stinson, ''Deterministic key predistribution schemes for distributed sensor networks,'' in *Proceedings of SAC 2004*, LNCS 3357, pp. 294–307, 2004.
18. H. Pishro-Nik, ''Analysis of finite unreliable sensor grids,'' in *Proceedings of WiOpt 2006*, Boston, Massachusetts, pp. 1–10, 2006.
19. S. Ruj, S. Maitra and B. Roy. ''Key Predistribution using Transversal Design on a Grid of Wireless Sensor Network,'' in *Ad Hoc & Sensor Wireless Networks*, Volume 5, Number 3–4, pp. 247–264, 2008.
20. S. Ruj and B. Roy, ''Key predistribution using partially balanced designs in wireless sensor networks,'' in *Proceedings of ISPA 2007*, LNCS 4742, pp. 431–445, 2007.
21. K. Simonova, A. C. H. Ling and X. S. Wang. ''Location-aware key predistribution scheme for wide area wireless sensor networks,'' in the Proceedings of the 4nd ACM Workshop on Security of Ad Hoc and Sensor Networks, Virginia, USA, pp. 157–168, 2006.
22. I. Stojmenovic. *Handbook of sensor networks: algorithms and architecture*, Wiley Interscience, 2005.

23. M. G. Sadi, Dong S. Kim and J. S. Park, ‘‘GBR: Grid Based random key predistribution for Wireless Sensor Network,’’ in *Proceedings of ICPADS*, Fukuoka, Japan, pp. 310–314, 2005.
24. S. Shakkotai, R. Srikant and N. Shroff, ‘‘Unreliable sensor grids: coverage, connectivity and diameter,’’ in *The proceedings of IEEE INFOCOM’03*, San Francisco, CA, pp. 1073–1083, 2003.
25. D. Stinson, *Cryptology: theory and practice*. 2nd edn. Chapman & Hall, CRC Press, Boca Raton, Florida, 2002.
26. A. P. Street and D. J. Street, *Combinatorics of Experimental Design*. Clarendon Press, Oxford, 1987.
27. M. F. Younis, K. Ghumman and M. Eltoweissy. ‘‘Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks,’’ in *IEEE Transactions on Parallel and Distributed Systems*, Volume 17. No. 8, pp. 865–882, August 2006.
28. L. Zhou and J. Ni and C. V. Ravishankar. ‘‘Supporting Secure Communication and Data Collection in Mobile Sensor Networks,’’ in the *Proceedings of INFOCOM 2006*, pp. 1–12, April 2006.