Location Dependent Key Predistribution Scheme for Square Grid and Hexagonal Grid

Monjul Saikia\textsuperscript{1*} and Md. Anwar Hussain\textsuperscript{2}

\textsuperscript{1}Department of Computer Science and Engineering, North Eastern Regional Institute of Science and Technology, NH-415, District Papum Pare, Nirjuli - 791109, Arunachal Pradesh, India; msk@nerist.ac.in
\textsuperscript{2}Department of Electronics and Communication Engineering, North Eastern Regional Institute of Science and Technology, NH-415, District Papum Pare, Nirjuli - 791109, Arunachal Pradesh, India; ah@nerist.ac.in

Abstract

Objective: To design a location aware key pre-distribution scheme for wireless sensor network deployed in square grid and hexagonal grid with minimum possible keys stored in each nodes. Methods/Statistical analysis: In location dependent key predistribution coordinates of the sensor nodes are known prior to deployment. Therefore their connectivity is known prior. Grid structured network is well fitted topology for various types of application in sensor network. Coverage and connectivity issues have been studied in these kinds of network. Security for these special structured is emerging topic of study and key predistribution as well. Findings: To efficient use of preloaded keys of the sensor nodes, the keys need to be distributed smartly. As in case of a square or hexagonal grid locations are known prior therefore it gives advantage in distributing the symmetric keys over the nodes. In this paper, we propose an algorithm using adjacency matrix of the network for square and hexagonal grid network. We analyze resilience against popular attack like node capture attack and node fabrication attack at the end of this paper. Application/Improvements: Staring with single key distribution, pair-wise key distribution, random key distribution and so on, various key predistribution schemes have been proposed in literature. Taking the advantage of structured topology of sensor network the algorithm enhances the overall performance.

Keywords: Deployment Knowledge, Hexagonal Grid Network, Key Predistribution Scheme, Location Dependent, Square Grid Network, Wireless Sensor Network

1. Introduction

Sensor networks are group of tiny battery backed up device used to gather information from sensitive location. During transition of gathered information securely over a vulnerable network some cryptographic system need to be incorporated. Symmetric key cryptographic is simple and efficient and therefore is widely used in sensor network. In a symmetric key cryptosystem a symmetric key must be established among sender and receiver. Key predistribution is a scheme that tries to upload some predetermined key over the sensor node. Key predistribution for the sensor nodes is a challenging task for efficient use of the distributed keys. Recent days, several key predistribution schemes have been proposed for large distributed sensor networks for location independent as well as location dependent. Some of these schemes randomly picks a set of keys from a large set of keys called key pool and loaded the keys in the internal memory of each sensor nodes. Sensor nodes are at the risk of vulnerable to attack due to lack of tamper resistant hardware. Sensor nodes may be captured and attacker can extract data from it or even new nodes can be fabricated and deployed in the network. The gathered information from a captured node can be used to compromise communication in the network by deploying this duplicate version of sensor node. In\textsuperscript{1} first proposed a scheme for key predistribution in location independent sensor network using randomly picked keys from a large key pool. In\textsuperscript{2,3} proposed KPS with the help of prior deployment knowledge to reduce the storage requirements for the sensor node and consequently reducing node capture attack. In\textsuperscript{4,5} discuss the
demands of the application with prior knowledge of sensor locations and with the help of this location knowledge exploits in the design of KPSs that enhances the tradeoff between the said terms. The knowledge of the sensor locations can be represented with the help of a grid formation may be a square grid or a hexagonal grid. Sensing of Soil moisture\(^6\), a nectarine orchard monitoring\(^7\) and measure of water use monitoring in irrigation\(^8\) are a good examples of Grid-based network applications. It is seen that there exist a tradeoff between the storage (i.e. the number of keys that is stored in a sensor node), connectivity (i.e. secure communication links among nodes) and resilience (i.e. the susceptibility of the scheme against attack)\(^9,10\).

Use of the concept of Distinct Difference Configurations (DDCs) for efficient KPSs in a square and hexagonal grid ensuring proper use of the keys is shown in\(^11\). The design of perfect DDC with the help of B\(_2\)-Sequence were discussed in\(^12,13\) that applied to design of KPSs that performs efficiently as compared to other existing schemes. However, search for DDC with desirable properties for a larger size network grid requires sufficient computational time; mathematical theory relating to distinct difference configuration was discussed in\(^14\), where limits on some certain parameters for building DDCs are given.

1.1 Our Contribution

In section 2, we give the concept of knowledge of sensor location and formation of grid in sensor network. In Section 3, give an experimental example with pictorial view of the KPS based on DDC proposed in\(^8\). In section 4, we discuss our proposed scheme with the knowledge of sensor location for efficient minimization of sensor node in its coverage area in square grid as well as hexagonal grids. In Section 5, some experimental results are shown.

### 2. Grid Formation, Distance and Coverage Region

Sensor nodes are considered to be positioned at the centers of the squares in a square grid network and in the center of hexagons in a hexagonal grid network. Each node in the grid fashioned network can be distinguished by the co-ordinate \((i,j)\), indicating the node is located in \(i^{th}\) row and \(j^{th}\) column of the grid. The coordinate assigned for a square grid and hexagonal grid is shown in Figure 1.

The communication range \((r)\) of a node is the maximum distance from the node to the other nodes that can communicate. Secure communication can happen only when they share a common key and this is referred to as one-hop communication. Nodes without having a common key can establish secure communication with the help of midway nodes. The path is referred to as a multi-hop path. In many schemes it is suggested that multi-hop path must be minimize for efficient use of the network.

Let a point at coordinate \((x,y)\) to be a point in \(i^{th}\) column and \(j^{th}\) row in a grid coordinate system. In programming concept of arrays rows can be indexed from top to bottom and column can be left to right in increasing order. The coordinates of the nearby points of a point at \((i,j)\) for a square grid are:

\[
\{(x_{i-1},y_j), (x_{i+1},y_j), (x_i,y_{j-1}), (x_i,y_{j+1})\}
\]

The distance \(d((x_1,y_1),(x_2,y_2))\) between any two points \((x_1,y_1)\) and \((x_2,y_2)\) in a square grid is the sum of difference in rows and columns, is referred to Manhattan distance defined by

\[
d((x_1,y_1),(x_2,y_2)) = |x_2 - x_1| + |y_2 - y_1|
\]

![Figure 1. The Square and Hexagonal Grids Coordinates.](image-url)
In a hexagonal grid, regular hexagon with side length $\frac{1}{\sqrt{3}}$ is used to form honeycomb structure. As in square grid the nodes are placed in the center of the hexagons. Two points are said to be connected if and only if both hexagon shares an edge. Therefore, neighboring nodes in a hexagonal grid are:

$$\{(x_{i-1}, y_{j-1}), (x_i, y_j), (x_{i+1}, y_{j-1}), (x_i, y_{j+1}), (x_{i+1}, y_j), (x_{i+1}, y_{j+1})\}$$

For any location dependent network the coverage distance can be defined priori with the help of Manhattan distance.

**Figure 2.** Example DD(3,2).

**Figure 3.** Key Identifier using DDC.

### 3. KPS with DDC

With the help of Distinct Difference Configuration proposed schemes for key distribution for a grid-based network. The give algorithm to construct $DD(m, r)$ for a square grid and $DD^*(m, r)$ for a hexagonal grid, where $m$ being the number of nodes that shares a common key that are within a distance $r$. For the construction of a DDC a $B_2$ sequence in $Z_n$ is used for large number of nodes, where the difference between pair of nodes in the set $D = \{d_1, d_2, d_3, ..., d_n\} \subset Z_n$ should be distinct. This distinct set is achieved by applying modulo $n$ operation.

#### Example 1:
Considering $l_1 = 8, l_2 = 6, r = 2$ and to distribute keys using the $DD(3, 2)$ whose points are $\{(0,0), (1,1), (2,0)\}$. This DDC can be depicted as in figure 2. The Figure 3 demonstrates the key identifiers assigned to every node in the square grid.

**Figure 4.** KPS with DD(3,2).

The KPS with $DD(3,2)$ in a square grid assigns three keys for each of the nodes. For programming convenience the square grid shown here is indexed from top to bottom and left to right. In the above table it is seen that there are three integers in each cell indicating three keys. Also each of the integers occurs in three places in the orientation of the 3x3 DDC shown above. The nodes sharing a common key can securely communicate. Node at a distance more than two need to establish a multi-path. An equivalent plot can be show as in the figure 4, whereas in figure 5 it is seen that using this scheme the network is separated to two distinct set of network which is again undesirable.

#### Example 2:
Consider another square grid network of size $l_1 = 8, l_2 = 6, r = 2$ and using $DD(3,2)$ keys can be distributed in points with coordinates $\{(0,0), (2,0), (2,1)\}$. This DDC can be depicted in figure 6. A communication graph is shown in Figure 7.

### 4. The Proposed Scheme

In this paper we propose a scheme for KPS with deployment knowledge in a square and hexagonal grid. We
consider distance \( r \), the communication range of a sensor network as discussed in section 2, i.e. the only neighboring nodes can communicate securely in one-hop sharing a common key and the nodes at distance more than \( r \) need to take help of other nodes.

Algorithm 1: Grid-based KPS- Adjacency Matrix Formation

**Input:** Size of the Grid (n xn)
- Distance= \( r \) [Coverage region]
- \( N \leq nxn \) [Total number of nodes]

**Output:** NxN Adjacency Matrix
- \( Adjm[N,N]=0; \)
- for \( i = 1 \) to \( n \)
  - for \( j = 1 \) to \( n-1 \)
    - if \(|Grid(i,j),Grid(i,j+r)| \leq r\) then
      - \( Adjm[Grid(i,j),Grid(i,j+r)]=1; \)
      - \( Adjm[Grid(j,i),Grid(j+r,i)]=1; \)
      - \( Adjm[Grid(i,j+r),Grid(i,j)]=1; \)
      - \( Adjm[Grid(j+r,i),Grid(j,i)]=1; \)
    - endif
  - end
- end
- return \( Adjm; \)

The algorithm 1 generates an NxN adjacency matrix according to the given coverage range \( r \) and size of the network. Algorithm 2 generates key ring for each of the sensor nodes in the grid network.

Algorithm 2: Grid-based KPS- Key Ring Formation

**Input:** Adjacency Matrix \( Adjm[N,N] \) produced in algorithm 1.

**Key Pool** KP consisting randomly generated keys

**Output:** Key Ring for each of the node
- \( Temp[N,N]=0; \)
- Counter=1
- for \( i = 1 \) to \( N \)
  - for \( j = 1 \) to \( N \)
    - if \( Adjm(i,j)\) then
      - \( Temp(i,j)=KP(counter); \)
      - \( Temp(j,i)=KP(counter); \)
      - counter=counter+1;
    - endif
  - end
- end

//KeyRing formation
- for \( i = 1 \) to \( N \)
  - counter=1;
- for \( j = 1 \) to \( N \)
  - if \( K(i,j)\) then
    - \( KeyRing(i,counter)=Temp(i,j); \)
    - counter=counter+1;
  - endif

Figure 5. Separation in the Network.

Figure 6. DD(3,2) with Coordinates \{\{(0,0), (2,0), (2,1)\}\}.

Figure 7. Communication Graph in Square Grid for Example 2.
return KeyRing;

end
end

Figure 8. Adjacency Matrix for a Network size 3x3.

Figure 9. Secure Communication Graph for 3x3 Square Grid.

5. Experimental Results and Observations

The entries in an adjacency matrix entries is 1 if there two nodes share a common key. An entry 1 in $i^{th}$ row and $j^{th}$ column indicates that node $i$ can communicate securely with node $j$. The algorithm 1 generates an adjacency matrix based size of the network and coverage range $r$ given as input. The algorithm 1 generates an adjacency matrix as show in figure 8 for a small network size (3x3) with $r=1$.

In the algorithm 2 the adjacency matrix generated in algorithm 1 serves as an input to the algorithm along with a large key pool consisting of keys more than total number of nodes in the network. According to the connectivity as in the adjacency matrix the algorithm generates key rings for individual nodes. Table 1 shows the key rings containing the key identifiers for nine nodes in the network.

Table 1. Key Ring

<table>
<thead>
<tr>
<th>Node#</th>
<th>Key Ring</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 2</td>
</tr>
<tr>
<td>2</td>
<td>1 3 4</td>
</tr>
<tr>
<td>3</td>
<td>3 5</td>
</tr>
<tr>
<td>4</td>
<td>2 6 7</td>
</tr>
<tr>
<td>5</td>
<td>4 6 8 9</td>
</tr>
<tr>
<td>6</td>
<td>5 8 10</td>
</tr>
<tr>
<td>7</td>
<td>7 11</td>
</tr>
<tr>
<td>8</td>
<td>9 11 12</td>
</tr>
<tr>
<td>9</td>
<td>10 12</td>
</tr>
</tbody>
</table>

From the table it is seen that key ring of node#1 is $\{1,2\}$, key ring of node#2 is $\{1,3,4\}$, and so on. As node#1 and node#2 shares a common key#1 they can establish a secure communication and so on. The algorithm 1 can be extended to generate adjacency matrix so that the connectivity between nodes form a hexagonal grid. The secure communication graph for 3x3 square grid and a 4x4 hexagonal grid are shown in figure 9 and 10 respectively.

Key pool size and key ring size: Key pool size indicates how many total keys need to be distributed in the network and key ring size indicates how many keys are to be store in each node. Table 2 gives an experimental result for various grid size and required key pool size and key ring size.

6. Conclusion

The scheme projected here is a location dependent key predistribution scheme where keys are allocated to those

end
sensor nodes which are within the range of communication. The technique enhances efficient use of keys assigned to the nodes. We also discuss the use of Distinct Difference Configuration (DDC) for key predistribution with some examples. We have proposed an scheme based on adjacency matrix design and seen that the algorithm efficiently generates adjacency matrix and then the respective key rings for each of the sensor nodes with the help of simple computer programming logic. Experimental results were shown for square grid and hexagonal grid topologies considering coverage range $r=1$. Extension of the coverage range and performance of the scheme is considered as a future work.

**Table 2.** Grid size and key pool size

<table>
<thead>
<tr>
<th>Grid Size</th>
<th>Square Grid</th>
<th>Hexagonal Grid</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Key pool size</td>
<td>Key Ring Size</td>
</tr>
<tr>
<td>2x2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3x3</td>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td>4x4</td>
<td>24</td>
<td>4</td>
</tr>
<tr>
<td>5x5</td>
<td>40</td>
<td>4</td>
</tr>
<tr>
<td>6x6</td>
<td>60</td>
<td>4</td>
</tr>
<tr>
<td>7x7</td>
<td>84</td>
<td>4</td>
</tr>
<tr>
<td>8x8</td>
<td>112</td>
<td>4</td>
</tr>
<tr>
<td>9x9</td>
<td>144</td>
<td>4</td>
</tr>
<tr>
<td>10x10</td>
<td>180</td>
<td>4</td>
</tr>
</tbody>
</table>

7. References