# Tree based Key Generation and Distribution Scheme in WSN

Aher Nisha N.
ME (computer),
PVPIT, Bavdhan,
Pune-21

N. D. Kale
Asst. Professor,
PVPIT, Bavdhan,
Pune-21

## ABSTRACT
Wireless sensor network is become more popular because of its various applications in day to day life. Communication security is one of the most important challenges in wireless sensor network. Key generation and distribution are also important in wireless sensor network, so we have effective security mechanism for that. Tree based key generation techniques uses shortest path matrix and MRD code matrix for key generation and distribution. It raises the security as well as scalability of the network than the other techniques. Communication established between the two nodes and If a node get added after that, then the node information is updated without changing the information of those two nodes.

## General Terms
Matrix, Tree,

## Keywords
Rank Codes, Key-Distribution, Wireless Sensor Network,

## 1. INTRODUCTION
Wireless sensor network is most widely used in the various fields like medical applications, military applications, wildlife tracking, weather checking applications, traffic control applications. Sensor nodes are used to detect enemy intrusion in battle field as well as they can be used to measure various environmental variables so in order to keep the information secret it is important to establish a secure communication between the sensor nodes. For secure communication between two sensor nodes a secret key is present. The sensor nodes have low processing power, less memory capacity and less battery life. Along with these constraints in WSN the wireless nature of network, unknown topology of network, and lack of fixed infrastructure use the cryptographic technique in wireless sensor network is some kind difficult task. We have to check the resource availability at each node. If we use symmetric key cryptography means if there are N nodes then there should be (N-1) keys in the network. These criteria should be maintained in whole network. In case if the value of N is large then the memory space is wasted to store the large key value. So it should not the memory efficient. If we use the public key cryptography system, it needs huge computation power but the sensor have less processing power so the public key cryptography system is not efficient in the WSN. Key pre-distribution technique is the most promising technique in wireless sensor network. In this key pre-distribution technique, each sensor node is assign set of keys from the large pool of keys before deployment, so that after deployment the two nodes which establish a communication to each other have at least one common key between them. Using the key of higher probability, the secure communication will establish in the two nodes of WSN.

### 1.1 Motivation for Using Rank Codes
Blom [16] uses the generator matrix of MDS codes (maximum separable distance) and symmetric matrix. But in matrix based method [2] they use MRD (maximum rank distance) codes instead of MDS code and one symmetric matrix because to compromise the whole network, an adversary has to capture nodes equal to the number of linearly independent columns of generator matrix G. Therefore the use of MRD codes instead of MDS codes raises the security parameter from k to N, where $k \leq N$.

### 1.2 Tree-Based Key Pre Distribution in Network
Sensors (or nodes) inside a network are deployed in clusters [10] is a common model for WSN. We do follow this model, we also make and assumption that sensors in the same partition are more likely to be neighbors or they are close to each other. Construction of binary tree for each node is the preferred technique for solving key management problem [4]. This way efficient key management can be achieved.

## 2. LITERATURE SURVEY
There are many key pre-distribution techniques are invented. Before going in detail to these techniques let's take some introduction about the key pre-distribution.

The method of distribution of keys onto nodes before the deployment this method is known as key pre-distribution. After deployment i.e. when nodes reach to their target by using the secret key, the node creates the network, There are basic 3 phases for key pre distribution:

1. Key distribution
2. Shared key discovery
3. Path-key establishment

During these three phases, after creating secret keys, they are placed in sensor nodes and each node searches another node for communication in its communication range. A secure link is established when two nodes discover one or more common keys (this differs in each scheme), and communication is done on that link between those two nodes. Afterwards, paths are established connecting these links, to create a connected graph. The result is a wireless communication network functioning in its own way, according to the key pre-distribution scheme used in creation.

In a proposed scheme by Eschenauer and Gligor [2], the key pool which has large pool of keys was generated offline before any node deployment happens. After generation of key pool, key ring from this pool is generated by randomly assigning set of keys from the key pool. A secure link could

be established in two sensor nodes which have one or more common keys in their key ring with the help of any shared key. In cases where nodes do not share common key, need to use a path key discovery procedure. Path key discovery transfers secret key to destination node via non compromised nodes. Link between two non compromised nodes may get compromised in attempt to capture one node along the path. To prevent this and strengthen the link keys in [2], a modified scheme called 'q-composite' is proposed in [11]. In this scheme, if two nodes share at least q common keys in their key rings they can establish a link between them. Key ring size is increased to ensure the connectivity. In [19] proposed multi-map matrix is based on random key pre-distribution scheme. In this scheme, On the basis of nodes position, nodes are assigned the keys. Modified version of [16] is proposed in [20]. In this case, the idea is to assign t key spaces to each node. These t key spaces are from the v key spaces which are generated using multiple D matrices. These nodes can establish direct link between them which share common key spaces. In [18], a key pre-distribution scheme was proposed by Lee and Stinson. This key pre-distribution scheme is based on transversal design which is combinational structures. Block of these transversal designs is associated with nodes and points to keys. In each associated block node has keys corresponding to the points. In this scheme, memory usage, connectivity and resilience of the network can be changed by choosing parameters. The investigators also proposed a scheme which is combination of transversal designs and Blom's scheme. This variant of the scheme is named as 'multiple space scheme'. In [14] a key pre-distribution scheme is proposed based on Blom's idea. In this scheme, direct relationship between matrix D and matrix A is broken using a certain random noise. This noise was added using constrained random perturbation. High computation overhead is required for this scheme. In some cases key pre-distribution schemes combine key pre-distribution and node deployment knowledge. In these schemes the location of the groups is considered to be known before deployment. Groups are the node groups deployed together. In [3, 4] polynomial-based key pre-distribution schemes are proposed considering a square grid. On the other side in [5], scheme based on triangular grids based scheme is proposed.

# 3. PROPOSED METHODOLOGY

A tree-based key pre-distribution scheme proposes to have sensor nodes arranged in a tree structure, in which each sensor node communicates with its parent node. This was key establishment is done between neighboring nodes along aggregation tree. Before a new node joins in a network, it receives two tickets which can be verifies by two existing but randomly selected nodes by network administrator. A pairwise key is generated for parent the new node is deployed into the network. To transmit the key securely to the parent from the child node, the new node splits the key into two parts. These two parts are sent with its tickets to the nodes selected by administrator. On receiving the tickets these selected nodes added to the network. The merit of the tree-based key pre-distribution system is that, it significantly reduces the memory code.

## 3.1 Rank of a Vector

Let $F_q$ be a finite field of q elements and let $F_q^N$ be an extension field of degree N. Assume $x=(x_1,x_2,x_3.....x_N)$ be a vector having co-ordinates in extension field $F_q^N$ then the rank of x is denoted by $R_k(x|F_q)$ and it is defined as maximum number of x ,which are linearly independent over the base field $F_q$. The rank distance between two vectors x and y is defined as the rank of the difference between the two vectors which is (x-y) and denoted as $d(x-y) = R_k(x-y|F_q)$. The rank over the base field is greater than or equal to rank over the extension field that is denoted as $R_k(M \mid F_q) \geq R_k(M \mid F_q^N)$

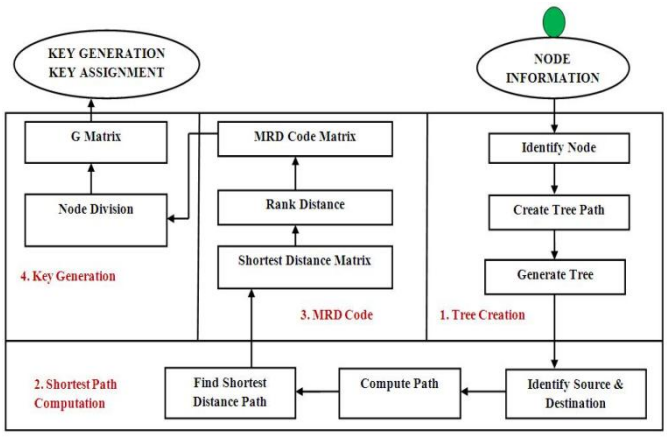


**Fig 1 – system overview diagram**

# 4. KEY GENERATION BASED ON MRD CODES

In this approach, key generation is divided into three phases. In those first two phases are offline whereas third phase is done after node deployment

## 4.1 Key Generation

Key spaces are generated in this phase. The finite field $F_q$ is used to generate the different matrices. The key generation phase is composed of following four steps

*Step 1* – generate a matrix from tree structure D:

Generate a matrix D from the tree based structure over the finite field $F_q$

*Step 2* - Node Division:

Suppose there are total n nodes in the network. Divide n nodes into t groups having (k-λ) nodes in each group where λ is any number ≥ 1. Reason for choosing group size (k-λ) is directly related to security of nodes

*Step 3* - Generating G matrices:

Generate t generator matrices. The construction of generator matrices is that only elements of generating vector (first row) are linearly independent, rest of the rows are generated by taking the frobenius power of the corresponding element in previous row.

*Step 4* – Generating key spaces:

In this step, A matrices for each of the group will be calculated as

$$A_i = (DG_i)^T$$

where i= 1,2,…….,t.

## 4.2 Key Assignment

In this phase, one row from the matrix $A_i$ will be randomly assigned to each node in the $i_{th}$ group where i = 1, 2, . . . , t. As there are (k-λ) nodes in each group and also N ≥ k, there will be always (N-k+λ) unassigned rows in each of the $A_i$ matrices. These unassigned rows will give us freedom of assigning different rows in different groups. Some of the information about matrix G will also be stored at each sensor node. Any column of generator matrix G can be calculated if first element of that column is known. The column position of the stored element of $G_i$ must be the same as the row number of the $A_i$, for example, if a node $S_i$ in the $i_{th}$ group is assigned $p_{th}$ row from the $A_i$ matrix, then it will also have the first element of the $p_{th}$ column of the $G_i$. To calculate the link key, each node from the $i_{th}$ group will have one row from the matrix $A_i$ and first element of the column of the matrix $G_i$, that means each node is needed to have $(k + 1) \times \tau$ bits, t is the number of bits required to store one element of the GF(q).

## 4.3 Key Establishment

Once the nodes are deployed in the field, they need to establish link keys with each of their neighbors or with other distant nodes whenever it is required. Two nodes can find a link key using these steps:

*Step 1* – Information exchange: Each node will broadcast its node ID and its seed for the column from matrix G. It is completely safe to exchange this information before the establishment of the link key because of two reasons. Firstly, it is incomplete information for adversary to construct a generator matrix; even if an adversary is present before the network deployment and he/she has captured all the t(k-λ) packets for whole network, he/she still cannot construct any of the t generator matrices because each generator matrix consists of N columns not (k-λ) columns and we have not stored remaining (N-k+λ) columns of each generator matrix on any node in the network. Secondly, even if an adversary successfully constructs a generator matrix that generator matrix does not reveal any part of the secret matrix D. Thus, it is completely safe to exchange seeds as plaintext before key establishment.

*Step 2* – Generating column from seed: Once a node has received the broadcast packet, it will calculate the column of matrix G from the seed it received, by raising it to $k_{th}$ element. For q= 2, each element is just the square of the previous element.

*Step 3* – Calculating link key: After calculating the column, the node will multiply this column with its own row from matrix A. The result will be the link key between sender and receiver. Similarly, the other node will do the same to calculate the common link key.

# 5. MATHEMATICAL MODEL

## 5.1 Set Theory

1. Let $S = \{s_1, s_2, s_3 \ldots\ldots s_n\}$ be as a System for key generation and distribution system

2. Identify input as $N = \{n_1, n_2, n_3 \ldots . n_i\}$ [i]

Where $n_i$ = number of nodes in WSN

$S = \{N\}$ [ii]

3. Identify K as Output i.e. Keys

$S = \{N, K\}$ [iii]

4. Identify process P

$S = \{N, K, P\}$ [iv]

$P = \{ M_d, N_e, M_{rd}, T_r\}$ [v]

Where,

Md = as minimum distance

$N_e$=Neutralizing errors

$M_{rd}$=Maximum rank distance

$T_r$ = Tree based distribution

5. $S = \{N, K, M_d, M_{rd}, T_r, D_j\}$ [vi]

## 5.2 Mathematical Model for Proposed System

1. Initialize requesters filed

$N = \{\}$

2. Initialize Minimum Distance

$M_d = \{\}$

3. Calculate the minimum distance by using Djakstra algorithm -

$D_i = \min [D_i, D_a + l (c,i)]$ [vii]

Where,

$M_d$ = minimum distance between the two nodes.

d(x, y) = rank distance between the two vectors x,y.

4. Create Matrix S using Shortest Distance

$$Sij = \sum_{i=1}^{c} \sum_{j=1}^{r} fx(d(c_i \rightarrow r_j)) \quad \text{[viii]}$$

5. Calculate MRD code

Any linear (n, k, d) code C ∈ $F_N^q$

Satisfies the singleton bound for the rank distance

$K \leq n - d+1$ if $n \leq N$

$N_k \leq (N - D+1)\, n$ if $n \geq N$ [ix]

The code C that reaches this bound is called MRD code.

# 6. RESULTS

## 6.1 Comparison of With Different Key Distribution Techniques

We implement our proposed approach on Windows 7 machine with processor of 2.4 GHZ with RAM memory of 2GB.We tested our setup for key distribution time delay which tested with the other methods also which gives the output shown on following output table.

**Table 1:- Comparison of different key distribution techniques**

| Node Numbers | Pairwise key | Path Key | Group Key | Tree Based key |
|---|---|---|---|---|
| 2 | 0.21 | 0.21 | 0.21 | 0.18 |
| 3 | 0.48 | 0.79 | 0.71 | 0.34 |
| 4 | 0.78 | 0.79 | 1.25 | 0.44 |
| 5 | 0.93 | 0.81 | 1.58 | 0.71 |
| 6 | 1.301 | 0.81 | 2.31 | 0.94 |
| 7 | 1.402 | 0.82 | 2.58 | 0.99 |
| 8 | 1.98 | 0.825 | 3.77 | 1.13 |
| 9 | 2.92 | 0.83 | 5.71 | 1.34 |
| 10 | 3.01 | 0.91 | 6.02 | 1.89 |
| 11 | 3.11 | 0.92 | 6.35 | 1.93 |

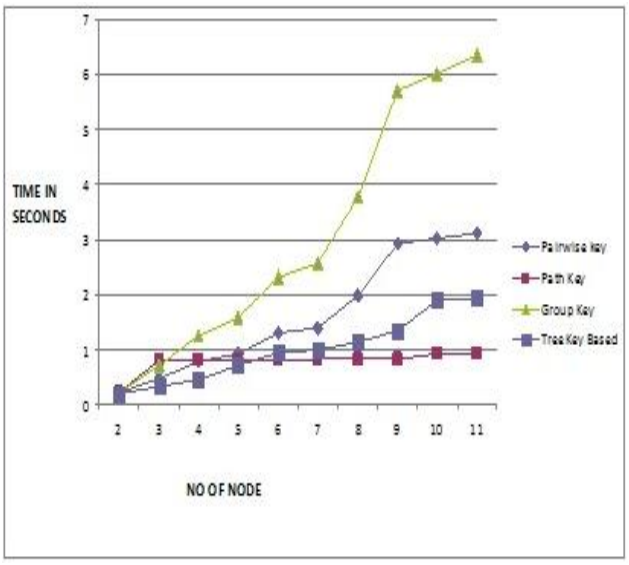


**Fig 2 - Comparison of tree based key distribution techniques with other techniques**

Fig shows the total time for our key establishment schemes. First, we see that as the network becomes denser, the time for pair wise key establishment grows longer. For example, for a two node network, the time for pair wise key setup is about 0.21 seconds, and for a ten node network, the time is about 2.77 seconds. Another finding is that the number of messages for the key setup scheme will significantly affect the completion time for that protocol. In the graph it is clearly indicating that our system takes much comparatively less time to establish and distribute keys.

## 7. CONCLUSION & FUTURE SCOPE

In our tree based approach, we are using tree structure with higher hierarchy level to maintain the distribution more. For the experimental results our system uses a self designed data set for the WSN which consist of some fields like node ID, node IP, node distance, pool ID and transmission speed. For efficient pre-distribution scheme our system efficiency uses MRD codes for the traversing pattern of the tree. This actually interfaces the key distribution with greater accuracy with less complexity.

This system can be enriched by considering multiple trees with distributed pool nodes can be managed with different traversing techniques based on the requirement of pool.

## 8. REFERENCES

[1] Abedelaziz Mohaisen, YoungJae Maeng, and DaeHun Nyang. On grid based key pre-distribution: Toward a better connectivity in wireless sensor network. In PAKDD Workshops, pages 527–537, 2007.

[2] Carlo Blundo, Alfredo De Santis, Amir Herzberg, Shay Kutten, Ugo Vaccaro and Moti Yung. Perfectly secure key distribution for dynamic conferences. In CRYPTO, pages 471- 486, 1992

[3] Dijiang Huang, Manish Mehta 0003, Deep Medhi, and Lein Harn. Location-aware key management scheme for wireless sensor networks. In SASN, pages 29–42, 2004.

[4] Donggang Liu and Peng Ning. Establishing pairwise keys in distributed sensor networks. In ACM Conference on Computer and Communications Security, pages 52–61, 2003.

[5] Donggang Liu and Peng Ning. Location-Based pairwise key establishments for static sensor networks. In SASN, pages 72–82, 2003.

[6] Donggang Liu, Peng Ning, and Rongfang Li. Establishing pairwise keys in distributed sensor networks. ACM Trans. Inf. Syst. Secur., 8(1):41–77, 2005.

[7] Donggang Liu, Peng Ning, and Wenliang Du. Group-based key pre-distribution in wireless sensor networks. In Workshop on Wireless Security, pages 11–20, 2005.

[8] Donggang Liu, Peng Ning, and Wenliang Du. Group-based key pre-distribution for wireless sensor networks. TOSN, 4(2), 2008.

[9] E Khan, E Gabidulin, B. Honary, A. Ahmed. Matrix based symmetric key generation and pre-distribution scheme for wireless sensor network. IET Wirel. Sens. Syst.,2(2):108-114,2012

[10] Eric Ke Wang, Lucas C.K.Hui and S.M.Yiu. A NEW KEY ESTABLISHMENT SCHEME FOR WIRELESS SENSOR NETWORKS, International Journal of Network Security &Its Applications (IJNSA), Vol 1, No 2, July 2009.

[11] Haowen Chan, Adrian Perrig and Dawn Song. Random key pre-distribution scheme for sensor networks. In SP'03: Proceeding of the 2003 IEEE Symposium on security and Privacy, Page 197, Washington, DC, USA, 2003

[12] Katerina Simonova, Alan C. H. Ling, and Xiaoyang Sean Wang. Location-aware key pre-distribution scheme for wide area wireless sensor networks. In SASN, pages 157–168, 2006.

[13] Keith M. Martin, Maura B. Paterson, and Douglas R. Stinson. Key pre-distribution for homogeneous wireless sensor networks with group deployment of nodes, 2008.

[14] Laurent Eschenauer and Virgil D. Gligor. A key-management scheme for distributed sensor networks. In CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, pages 41–47, New York, NY, USA, 2002.

[15] R. Kannan S.S. Iyengar R. Kalidindi and A. Durresi. Sub-grid based key vector assignment: A key pre-distribution scheme for distributed sensor networks. Journal of Pervasive Computing and Communications, 2(1):35–43, 2006.

[16] Rolf Blom. An optimal class of symmetric key generation systems, In EUROCRYPT, pages 335-338, 1984.

[17] Shruthi P., M.B.Nirmala. Secured modified bloom's based q-composite key distribution for wireless sensor networks. International Journal on Advanced Computer Theory and Engineering (IJACTE), 2(3): 2319 – 2526, 2013

[18] Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod K. Varshney. A key pre-distribution scheme for sensor networks using deployment knowledge. IEEE Trans. Dependable Sec. Comput., 3(1):62–77, 2006.

[19] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen, and Pramod K Varshney. A Key management scheme for wireless sensor network using deployment knowledge. In INFOCOM, 2004.

[20] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen, and Pramod K Varshney. A pairwise key distribution in wireless sensor networks. In ACM conference on computer and communications security, pages 42-51, 2003