SECURE AND EFFICIENT KEY PRE DISTRIBUTION SCHEMES FOR WSN USING COMBINATORIAL DESIGN

IshwaryaMathi Manickavasagam[1], MadanMohan Anbalagan[2], Sivasankar Sundaram[3]

[1]*Department of ECE, Chennai, India*
[2]*Department of ECE, Chennai, India*
[3]*Department of ECE, Chennai, India*

Abstract

Efficient Key Distribution is essential among sensor nodes. Pairwise and Triple Key Distribution in wireless sensor networks is established using Combinatorial Design. Sensor networks which are used in many applications require secure communication between the nodes. The need for secure communication is to protect the information from unauthorized access and to provide authentication between nodes. In this paper, the combinatorial Design which is used, is followed by Randomized key predistribution are applied to sensor nodes. The algorithm used in this scheme is to improve and increase the connectivity and resilience factor between the nodes. This scheme aims at increasing computation efficiency, communication and security.

Keywords—*pair wise, triple key distribution, randomized key pre distribution, resilience*

----------***----------

1. INTRODUCTION

A WSN is spatially distributed sensors which are used to observe physical or environmental conditions such as sound, pressure and temperature, etc and to pass their information all the way through the network to a main location.

The improvement of WSN was aggravated by military applications such as battlefield observation. Today such networks are used in many consumer and industrial applications, such as machine health monitoring, industrial process monitoring and control, etc.

The WSN is built of 'notes' from a few to several hundreds or even thousands, where each node is connected to one or several sensors. Each such sensor network node has typically several parts: a micro controller, a radio transceiver with an internal antenna or connection to an external antenna, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A Sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning 'motes' of authentic microscopic dimensions have yet to be created. The cost of the sensor node is variable which depends upon the complication of the individual sensor nodes. Depending upon the size and cost on sensor nodes results in corresponding constraints on resources such as memory, energy, communication bandwidth and computational speed. The topology of the WSN can vary from a simple star network to a advanced multi-hop wireless mesh network. The transmission technique between the hops of the network can be routing or flooding. Sensor nodes can be expected as small computers, extremely basic in terms of their interfaces and their components. They usually consist of processing unit with limited computational power and limited memory, sensors or MEMS, a communication device and a power source usually in the form of battery.

The connectivity of the network involves two aspects:
Local connectivity requires that neighboring nodes either share or there exists a path between them consisting of secure links.

Global connectivity requires that there exist a path between any two nodes in the network, consisting of hops with link keys.

Sensor nodes can be imagined as small battery powered devices which are deployed in large number to sense abd collect information for various applications ranging from health care to military applications.

2. RELATED WORK

Ruj S., Nayak, A. and Stojmenovic, I., proposed the scheme based on selected key distribution and the cost of using this scheme in combinatorial design is very high when compared to other schemes [1]. Camtepe, S.A. and Yener, B., futher extended the idea and developed randomized key distribution scheme. The main disadvantage of using this scheme is that it is not scalable [2]. Khalid S.,Ahmad F., Beg M.A., in this scheme, the nodes are assumed to be deployed based on Trivial Pairwise key distribution and this scheme is scalable and is limited in memory size [3]. Lee, J. and Stinson, D., proposed Single secret key which results in compromise of single nodes

lead to compromise of all nodes and it is not suitable for large networks [4]. Chakrabarti D., Maitra S and Roy B., nodes are assumed to be deployed based on Randomized block merging which results in terms of loss in connectivity. By using Orthogonal latin square, it is increased in terms of connectivity and resilience factor. This scheme shows a improved link establishment and connectivity graph when compared to other schemes.

3. KEY PRE DISTRIBUTION

A good key pre distribution scheme should be resilient to node compromise. There are two ways of distributing the keys to the nodes. One way of pre distribution is to load all the nodes with a single common master key, resulting in an finest storage and full connectivity of the network. However if one node is compromised then the entire network becomes insecure. At the other extreme, each pair of nodes can share a unique key.
Initially after deployment of sensor nodes, the key pre distribution is done, where key pre distribution is carried out in three phases. After the deployment of sensor nodes, the keys are distributed to the nodes which are considered, where keys are generated depending upon the algorithm of orthogonal latin squares. Then shared key discovery phase takes place in which the nodes look for common keys in the sensor nodes and the next phase is path key establishment phase in which if there are common keys between two nodes then a path will be established between the nodes.

There are three phases for key pre distributions:

3.1 Key Pre Distribution Phase:

Prior to the deployment of the sensor network, all nodes obtain a distinct subset of keys, based on the scheme. Every sensor node is equipped with a fixed number of keys randomly chosen from the number of nodes assigned.

3.2 Shared Key Discovery Phase:

When two nodes in wireless communication range look for their common keys and if the nodes have common keys then link will be established between the sensor nodes.

3.3 Path Key Establishment Phase:

Assigns a path key to selected pairs of sensor nodes in wireless communication range at the end of shared key Discovery phase

4. COMBINATORIAL DESIGN

Combinatorial Design provides a fitting balance of key at ease in various sensor nodes. Using this policy maximum number of node pair can communicate directly using pairwise common key. Combinatorial Design consist s of many types and Orthogonal latin square is one of the type, which deals depending upon the matrix.

In this paper, we perform the algorithm of Orthogonal Latin Squares based on Combinatorial Design.

4.1 Orthogonal Latin Square

In Orthogonal Latin Squares n x n matrix or n matrix can be considered to generate the keys for the assigned sensor nodes. Depending upon the order of the matrix which is considered. The keys are assigned accordingly.

Example: 1

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

In this case, we consider 3x3 matrix and keys are generated as (r,c,s)

Where r represents the row and c represents the column and s represents the symbol from the matrix.

The keys from the assigned matrix are generated as (1,1,1), (1,1,1), (1,2,2), (1,3,3), (2,1,2), (2,2,3), (2,3,1), (3,1,3), (3,2,1), (3,3,2).

Example: 2
When 2 matrixes say L1 & L2 are considered. The keys can be generated as

$$L1=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \quad \& \quad L2=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

(1,1),(2,2), (3,3), (2,3), (3,1), (1,2), (3,2), (1,3), (2,1) and thus keys are generated.

4.2 Link Establishment

The Key Distribution between sensor nodes takes place by assigning key values to the nodes in the sensor network and distributing the keys to the nodes in the network. The sensor node which has a common key will establish a link.

In Orthogonal Latin Square based key pre distribution scheme, depending upon the algorithm, the key values are generated and is distributes randomly to all the sensor nodes which is present. The sensor nodes which share a common key will establish a link between the nodes. In this scheme a new approach has been proposed to establish a secure communication between the sensor nodes with desired scalability and resiliency.

When two nodes share more than one shared key, the amount of data transferred will be high when compared to one shared key and the bandwidth consumption will also be less when compared to the others.

Flow Chart for Link Establishment using Orthogonal Latin Square

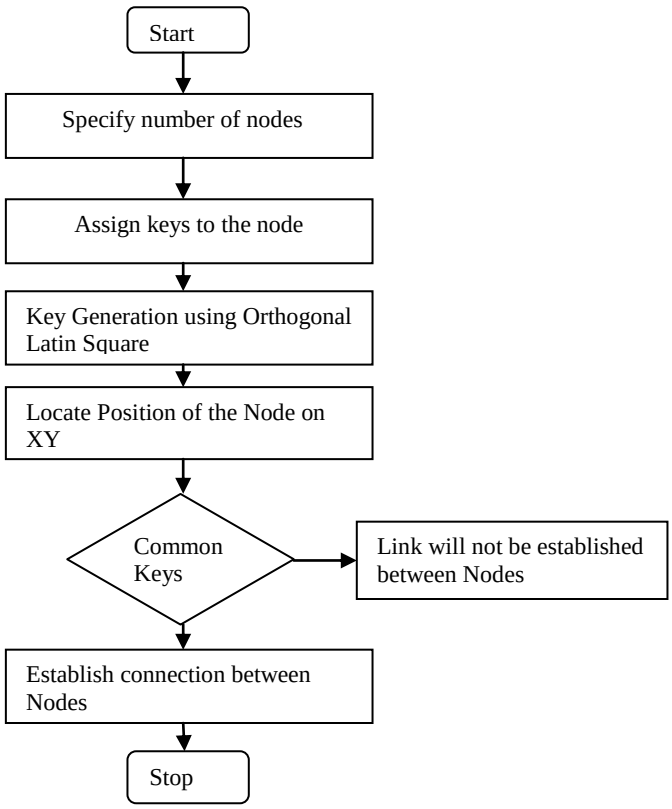

Fig: 1 Flow Chart for Link Establishment

Fig.1 shows the flow chart for link establishment how keys are established depending upon the algorithm of orthogonal latin squares, if there is common key then link will be established between those nodes and if there is no common keys then it will look again with other nodes for common keys.

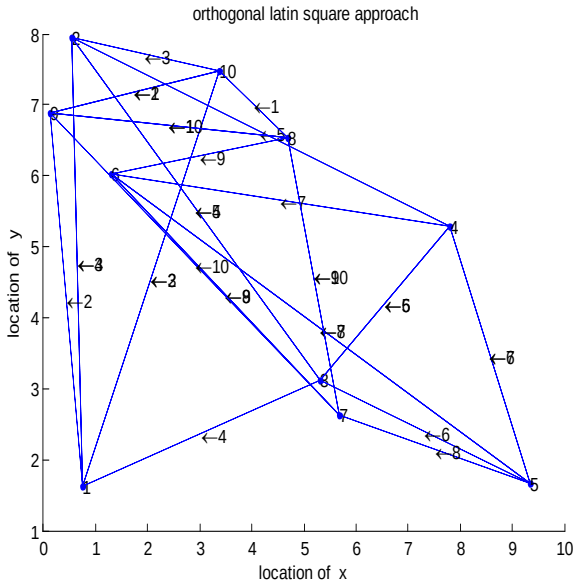

Fig.2 Link Establishment between sensor nodes

Fig.2 shows the graph between the sensor nodes. In this Figure, the number of nodes considered 10 and order of the matrix is 10. Depending upon the algorithm of Orthogonal Latin square, the keys are generated and distributed among the sensor nodes. If there is common key between the nodes, then link will be established. The overlapping of common keys shows that there are more than one common key. If there is more than one common key, the data transferred will be more and bandwidth consumption will be less when compared to the others.

4.3 Connectivity Analysis

We have analyzed that presence of our scheme based on connectivity between sensor nodes in the network. For security, we present the probability of the node being compromised.

A network node should be able to securely communicate to its local neighbors means a network node physically located within transmission range.

Using connectivity theory, we can obtain the necessary expected node degree d (i.e average number of edges connected to each node) for a network of size N, when N is large, in order to achieve a given global connectivity, pc.

$$d = \frac{(N-1)}{N}[\ln(N) - \ln(-\ln(pc))] \qquad (1)$$

Where N is the number of node, pc gives the probability of connectivity.

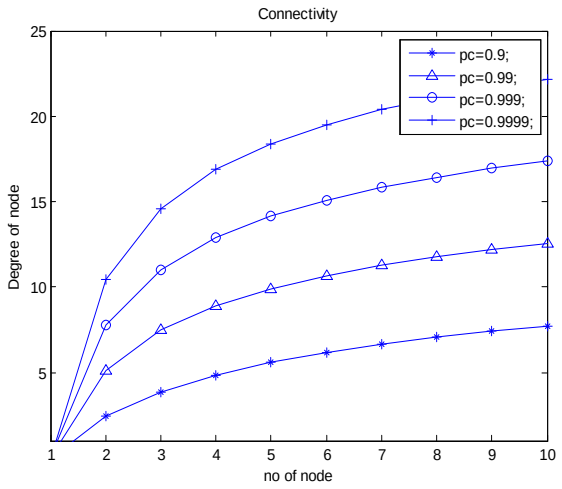

Fig 3 Connectivity Analysis between sensor nodes

Fig.3 shows number of node versus degree of node. From the graph we infer that connectivity increases as the number of node increase and hence this scheme is not scalable. When 3 be the number of node considered, for pc value 0.999, we get approximately 18 as degree of node. When 6 be the number of node considered, for pc value 0.9999, we get approximately 18 as degree of node.

We have analyzed that presence of our scheme based on connectivity between sensor nodes in the network. For security, we present the probability of the node being compromised. Using connectivity theory, we can obtain the necessary expected node degree d (i.e average number of edges connected to each node) for a network of size N, when N is large, in order to achieve a given global connectivity, pc.

5. SIMULATED RESULTS

We implement our proposed scheme using MATLAB tool. For Link Establishment between sensor nodes in wireless sensor network we assigned the number of sensor nodes to be 10. Link Establishment between sensor node is based on the algorithm of Orthogonal Latin Square. For connectivity analysis, we simulated the results by assigning the total number of sensor nodes in the network n to be 10, and degree of the node to be 15 and graph is plotted by varying different pc values.

6. CONCLUSIONS

From the above simulated results, we conclude that our Orthogonal Latin Square scheme which is carried by randomized key pre distribution has increased probability of connectivity. Our scheme provides security framework provides better resilient.

REFERENCES

[1] Ruj S., Nayak A. and Stojmenovic I.,(Nov. 2013) 'Pairwise and Triple Key Distribution in Wireless Sensor Networks with Applications', IEEE Trans. On Computers., Vol.62, No.11, pp.2224-2237.

[2] Camtepe, S.A. and Yener, B.,(April 2007) 'Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks', IEEE/ACM Trans. on Networking., Vol.15, No.2, pp.346-358.

[3] Khalid S.,Ahmad F., Beg M.A.,(2012), 'Secure Key Pre-distribution in Wireless Sensor Networks Using Combinatorial Design and Traversal Design Based Key Distribution', Vol.No.1, Issue-4, pp.2248-9738.

[4] Lee, J. and Stinson, D.,(2004) 'Deterministic key predistribution schemes for distributed sensor networks', SAC, LNCS Vol.No.3357, pp. 294-307.

[5] Chakrabarti D., Maitra S .and Roy B.,(March 2006), ' A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design', Vol.No.5, pp.105-114.

[6] Behrouz A.Forouzan , Debdeep Mukhopadhyay, *Cryptography and Network Security*,2nd Edition,,Tata Mc Graw Hill Education private edition

[7] William Stallings,*cryptography and network security principles and practice*, Fourth Edition,Pearson Publications ,2006.

[8] Ruj, S., Nayak, A. and Stojmenovic, I.,(April 2011) 'Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs', INFOCOM, 2011 Proceedings IEEE , Vol., No. 10, pp.326-330.

[9] C. J. Colbourn and J. H. Dinitz, The CRC Handbook of Combinatorial Designs. CRC Press, 1995.

[10] H. Chan, A. Perrig, and D. X. Song, "Random key predistribution schemes for sensor networks," in IEEE Symposium on Security and Privacy. IEEE Computer Society, 2003, pp. 197–213.

[11] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Trans. Inf. Syst. Secur., vol. 8, no. 2, pp. 228–258, 2005.