# A Proficient And Protected Node Validation In Wireless Sensor Network

**Vipin Kumar[1], Kuldeep Singh[2,] Sunil Bisht[3]**

***Abstract*** **-** Wireless sensor networks are about the field of networks that consists of small, large number of sensing nodes which is having the sensing, computational and transmission power but sensing nodes also suffer from many limitation such as low power (usually operated by battery), low processing ability, communication and storage limitations. Key management is the fundamental security mechanism in wireless sensor network. To achieve security in WSN it is important to be able to encrypt the messages sent among the sensor nodes. In our paper, we present an enhanced heterogeneous tree based symmetric key cryptography scheme for security of wireless sensor networks. Here, we design the networks into the node matrix arrangement (nodes addressing) due to its tree based scheme for link establishment then we generate the key for each session which provides an authenticity using deterministic symmetric key cryptography. This proposed crypto system is session based and the session key is changed after expire of each session. This combination of scheme provides the good performances and efficiency in terms of network connectivity, key storage overhead as well as in terms of attack of node capture. In the end we compared our scheme with EG schemes and our scheme gives better security and performances.

***Keywords*** **-** Deterministic Key, Broadcast Authentication, key generation, wireless sensor network.

## 1. INTRODUCTION

**1.1 Wireless Sensor Network:** A wireless sensor network [1], consisting of a large number of small low cost devices called sensor nodes or motes [2]. A sensor node is contained information about the battery, transceiver, micro-controller and sensors. These sensor nodes are tiny resource constrained devices with the limitations of low battery power and communication range and small computation and storage capabilities. They are usually deployed in open environments where they collaboratively monitor the physical and environmental data such as temperature, pressure, vibration etc., and report/relay the sensed data to other sensor nodes over a wireless network. The final destination of this data is a base station [3] also called a sink node which is a powerful device, e.g., a laptop. The base station acts as a gateway and links the WSN to the outer network e.g., the Internet as shown in Figure 1.1.

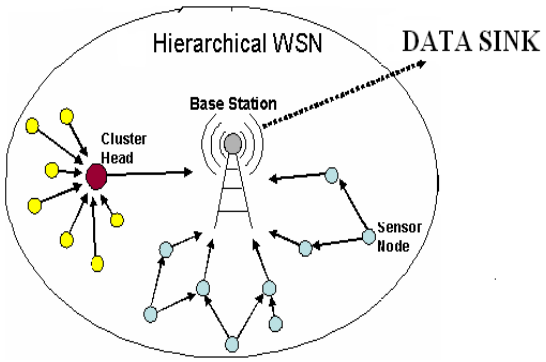


Figure 1.1: Base station (sink node)

### 1.2 Applications of Wireless Sensor Networks:

Sensor networks are tools to bridge the gap between the physical and the virtual world. They allow automatically collecting information about physical phenomena, immediately processing this information and transferring the results into background information systems. This processing delivers high-level information according to the application's requirements. Sensor nodes organize themselves autonomously, work in a collaborative manner, and are designed for energy efficiency. This allows it to monitor large geographical areas or inaccessible spaces over long periods of time without the need of human intervention. A comprehensive survey of sensor network architectures and applications can be found in.

#### 1.2.1 Surveillance:

An important application class for sensor networks is their use for the protection of assets or people. By definition, sensor networks are highly suitable for data collection. This capability can be exploited for surveillance purposes, most importantly for the detection of intruders or physical security breaches, or more generally for "perimeter protection" [8], where an area around a threatened entity (which is possibly moving) is under surveillance. Today, there already exists an industry for surveillance tools such as video cameras, motion detectors, burglar alarms, etc. Sensor networks

add two new qualities to such systems, first the large number of tiny devices that can be deployed in an ad hoc manner, and second the self-organization of these devices for communication and configuration.

**1.2.2 Context Awareness:**

Pervasive and ubiquitous computing concepts assume a tight relationship between computing devices and human users. Since the behavior of humans is closely related to the context in which current activities take place, the notion of this concept has gained much attention in this research area. It is assumed that by understanding context, applications can adapt their behavior to the specific needs of the human user and his environment. A prominent example is the mobile phone that autonomously recognizes situations where an audible ringtone is inappropriate, for example a work team meeting or sitting in a cinema. Sensor networks can be used as a tool for deriving contextual information.

**1.2.3 Other Applications:**

Several sensor networks have been prototypically deployed for scientific, military and other purposes. A survey of projects can be found. Examples include

1. Environmental monitoring, e.g. in wine yards, forests, and glaciers.

2. Self-repairing minefields.

3. Improved care for the elderly through activity monitoring.

4. Equipment monitoring in industrial installations.

5. Sniper detection.

**1.2.4 Security Concerns:**

Although prototypical deployments of sensor networks have not been equipped with security measures until now, it is foreseeable that adequate security is prerequisite for the success of sensor networks in practice. The main reason is that sensor networks will play a critical role in monitoring and protecting valuable assets and people. Their open architecture makes sensor networks highly vulnerable. If they could be easily deactivated or manipulated by competitors or criminals, the consequence could be serious financial damage or even threats to human lives. The following scenarios are intended to illustrate these dangers.

Structural integrity of building, Traffic assistance, Healthcare, Military surveillance, Logistics

## 2. SYSTEM MODEL

### 1.1 Wireless Sensor Network Architecture

There are basically two components in the infrastructure of a wireless sensor network [1]: sink nodes and sensor nodes. But it is described by four parameter that as shown in Figure 1.1.

**1.1.1 Sensor motes (Field devices)** : capable of routing packets on behalf of other devices.

**1.1.2 Gateway or Access points** – A Gateway enables communication between Host application and field devices.

**1.1.3 Network manager** – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.

**1.1.4 Security manager** – The Security Manager is responsible for the generation, storage, and Management of keys.

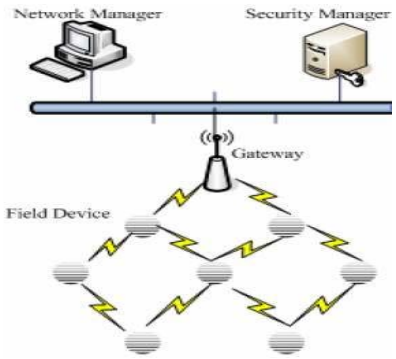


Figure 1.1 **WSN Architecture**

## 3. PROPOSED METHODOLOGY

**3.1 Proposed Matrix Distribution Scheme For Key Generation:** Base station generates the all symmetric keys matrixes at the time when we establish a secure node to node communication over network. Here some steps for the key generation. We proposed a new key pre-distribution scheme [21][30] called a deterministic Key Pre-Distribution Scheme [23] with matrix composition and its composition fulfill the concept of symmetric matrix (that describes in definition 1) for WSNs. The following procedure is executed by base station in order to construct symmetric key [34] matrix and also node arrangement matrices scheme.

**Step 1: Generation of large pool of keys:** Base station generates a large pool of keys ($2^{-18}$~$2^{21}$ Keys) as shown in Figure3.1. Those generated keys are then used to construct

a symmetric matrix composition in further steps.

**Step 2: Forming a symmetric matrix using the pool of elements:** Construct a (2×2) matrix using the randomly selected elements from the key pool. We are used the (2 × 2) dimension matrix in our proposed algorithm (3.2.2). Here some condition for assigning rows and column value

1. The first condition for selecting elements from the large pool is that all elements present in a column should be multiple of the diagonal element of the same column, some elements should be zero, some elements should be same as diagonal element and all the selected elements should be large.

2. One more condition for this matrix is that summation of all the diagonal elements should not be divisible by the number of columns of the lower triangular matrix.

### 3.2 Proposed Sensor Nodes Matrix Arrangement for Broadcast Authentication:

We propose a new scheme for node to node mutual authentication [35] by using node matrix arrangement scheme, in this scheme we provide a cryptographic [31] method for secure communication, which is described in the following steps:

**Step 1: Tree construction:** We define the number of levels in tree = *L*, and number of nodes in this level is *N* so, that the most $2^N$ nodes at level (*L*+1).

With the help of this step we can draw a matrix arrangement for nodes of tree. There is an condition for this scheme, *l*<= 99 and also it's used to store information about only first, maximum number of nodes in each level is *n*<= 99.

**Step 2: Node matrix management scheme:** With the help of step1, we can draw a matrix arrangement for level=0 and node=1 means that it's a root node in the tree. Matrix in (2×2) form, upper row defines the level of tree *l* = 0, 1,2,3,4,5,6,7.....99 and lower row define about the maximum number of node (*n*<= 99) at this present level then the matrix at

(1) Level, $l_0$=[0 0] and Node, n= [0 1].

(2) Level, $l_1$=[0 1] and Node n=[0 1 or 0 2].

And same as for the next node to n<=99, matrix management scheme can apply.

(99) Level $l_{99}$= [9 9] and Node n=[0 1], [0 2], [0 3]…[9 9]

**Step 3: Secure link establishment and computation:** The path key establishment stage makes provision for link between two nodes even when they do not share a common key. In this step we used to compute both matrix that node matrix arrangement and the symmetric key [36]. Here we can represent the node matrix management by ($M_m$) and symmetric matrix key by ($S_k$). There are Different three situation of broadcasting a setup message.

**Step 4: Node to node link establishment**: When a node *A*($N_A$) creates to broadcasting a message to another node means that the $M_m$, matrix arrangements of node gives a matrices with an $S_k$, symmetric key matrices, that both matrices using simple hill cipher algorithm an creates an encrypted message to the node B($N_B$).

**Step 5: Node authentication and security:** Node authentication [35] means that it gives information about the other node whose generate the setup message and broadcast the message. Also given an security over there.

**Step 6: Node authentication and verification**: If the value of $M_m$= *M*, then we can say that the broadcasting of message is form safe, secure and authentic [36], [35] node. If not then is not an authentic node

$$M_m = M$$

## 4. SIMULATION/EXPERIMENTAL RESULTS

### 4.1 Analysis of Network Connectivity

The connectivity in a tree based key management scheme depends on the number of nodes (*n*), the number of keys in the tree (*k*), and the number of keys stored in a node (*s*).

Also, we will evaluate the network connectivity and compare it with Eschenauer and Gligor scheme [13]. In our proposed complete binary tree based key management scheme network connectivity is taken as the concept of probability (*P*). In our scheme, only one key is used for sharing of data between any two nodes.

### 4.2 Analysis of Resilience against Node Capture

In wireless sensor networks, Information of compromised nodes provides misguiding information to the entire network, and creates disturbance the whole network security. In this we evaluated that the proposed scheme improves WSNs resilience by calculating the fraction of compromised nodes (*c*) among non-compromised nodes (*c*'). We compare our scheme with Eschenauer and Gligor schemes [18] based on performance.

### 4.3 Memory Usage Analysis

In the proposed scheme, any two sensor nodes establish the shared key by using hill cipher algorithm using with symmetric based key pre-distribution scheme. Memory is used to store the matrices information. We proposed an efficient method to identification and verify a node address and also its identity/location value using matrices arrangement. This technique is especially suitable for large wireless senor networks.

## 5. CONCLUSION

We propose an enhanced non uniform Complete Binary Tree which is based on key management scheme for wireless sensor networks that ensures security and efficiency. In our scheme at first we assign a sensor network as complete binary tree structure that provides sensor nodes structure and this complete binary tree structure also stores the information about nodes location or node arrangement. All the nodes in complete binary tree structure reside in strictly secure matrices arrangement. Then we use the deterministic symmetric key distribution to initiate the security of WSN, which mainly support node-to-node security and a mutual trust authentication mechanism. In this scheme security is fortified by using cryptographic scheme and transpose operations to provides confirmation about secure link-establish to node, whenever a node broadcasting a message to another node or in node-to-node link establishment. In contrast to other similar security solutions, the salient advantage of this work is that we addressed challenging security issues of runtime phase by real time rekey, which can efficiently protect the network against attacks of eavesdropping or captured nodes compromise and so on.

## 6. FUTURE SCOPES

We have got some better resiliency than some of the existing schemes. Also our scheme gives better performance in terms of connectivity, computation and storage or memory usage when we compared with the EG-schemes. We propose to seamlessly integrate WSN security with a promising protocol that provides more security and more efficiency. There is still lot of scope for future works on generation of keys and on the advancement of cryptographic scheme for highly encryption of information on node in the WSN.

## REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensonetworks: A survey,” *Computer Networks*, vol. 38, no. 4, pp. 393-422, 2002.

[2] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, “Wirelessensor networks for habitat monitoring,” in *Proceedings of the 1st ACM InternationaWorkshop on Wireless Sensor Networks and Applications*, pp. 88-97, 2002.

[3] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, “Systemarchitecture directions for networked sensors,” *SIGOPS Operating System Review*vol. 34, no. 5, pp. 93–104, 2000.

[4] D. Puccinelli and M. Haenggi, “Wireless sensor networks: Applications andchallenges of ubiquitous sensing,” *IEEE Circuits and Systems Magazine*, vol. 5, no. 3pp. 19-29, third quarter 2005.

[5] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attackand countermeasures,” *Ad Hoc Networks*, vol. 1, no.2-3, pp. 293-315, Septembe2003.

[6] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensonetworks: A survey,” *Computer Networks*, vol. 38, no. 4, pp. 393-422, 2002.

[7] G. Hoblos, M. Staroswiecki, and A. Aitouche, “Optimal design of fault toleransensor networks,” in *Proceedings of IEEE International Conference on ControApplications*, Anchorage, AK, September 2000, pp. 467–472.

## AUTHOR'S PROFILE

**Vipin Kumar** has received his M.Tech Degree in Computer Science and Engineering from Faculty of Technology, University Campus Dehradun in the year 2013.

**Kuldeep Singh** has received his M.Tech Degree in Computer Science and Engineering from J.B Institute of Technology, Dehradun in the year 2014.

**Sunil Bisht** has received his M.Tech Degree in Computer Science and Engineering from G.B Pant Engg College Pauri Garhwal in the year 2013.