# A Survey of Key Pre Distribution Schemes in Wireless Sensor Networks

**Leenu Rebecca Mathew[1] Jyothish K John[2]**
[1]Student[M.Tech.] [2]Associate Professor
[1, 2]Department Of Computer Science And Engineering
[1, 2] Federal Institute of Science And Technology(FISAT) Angamaly, India

*Abstract*— Wireless Sensor Network (WSN) is an area of research that has various applications both for mass public and military. A wireless sensor network is composed of many sensors which can be used to monitor physical or environmental conditions, such as temperature, sound, pressure. After collecting these data they should pass this data through the network to a main location. A Sensor Node in Wireless Sensor Network lacks resources such as processing capability, memory capacity, battery power, and communication capability. Because of the limited resources on sensor nodes, the use of conventional key management techniques in wireless sensor networks is limited. Key establishment is the most important cryptographic primitive in all kinds of applications where security is a concern. Authentication and pair wise key establishment are critical in sensor networks. In this paper, we provide a survey of key management schemes in wireless sensor networks.

*Keywords*: Key Pre-distribution, key management, Pair wise key, polynomial pool base, q-composite

## I. INTRODUCTION

Wireless sensor networks (WSNs) comprise a large autonomous devices[13] monitoring environmental conditions. Sensor nodes then pass the collected readings to a central server through a network of sensor nodes. Sensor, wireless communication device, small micro- controller and energy source comprises this small device, called sensor node. The central server collects all the readings and then processes them according to the application. Sensors are not so costly, low-power devices which have limited resources. They are small in size, and have wireless communication capability within short distances.

WSN have many applications in various fields including military [12], environmental, health, industry, data collection in hazardous environments [13] and all these applications require secure communications. Wireless networks are more vulnerable to attacks than wired ones because of the broadcast nature of transmission medium, resource limitation on sensor nodes and uncontrolled environments where they are left unattended .Sybil attacks [1], black hole attacks, DoS attacks, wormhole attacks etc are the major malicious attacks present in WSNs [2]. Therefore, the security in sensor network is extremely important. Many securities had been designed for wired and wireless networks but they can’t be used in wireless sensor networks because of the limited energy, memory and computation capability. Key management protocols are the basis of the secure communications and are the fundamental security mechanism in wireless sensor network.

The remainder of this article is organized as follows: Section describes the key management schemes used .Section III describes the key pre distribution schemes. Section IV gives the comparison of various schemes. Section V gives the new proposal used to minimize the communication overhead. Finally Section VI summarises the technologies used and the aim of future technologies.

## II. KEY MANAGEMENT SCHEMES

In this section, we will discuss various key management schemes. Key management is very much important in WSN security. This can also give confidentiality, authentication, privacy and sometimes integrity. This can also give and less overhead on sensor nodes. There are various applications and network topologies in WSN, So it is highly unlikely that one scheme outperforms all other schemes in all the scenarios.

### A. *Single Network Wide Key*

This is the simplest scheme that can be devised for any class of wireless sensor network[3]. As the name implies this method stores a single key also known as master key in every node. This key is used for performing all the encryption and decryption of messages. The main advantage of this scheme is that communication overhead is minimized. Also as a single key is used, there is very little computation and storage overhead involved and offers infinite scalability .Drawback of this scheme is that if a single node is compromised, the secret key is revealed and the whole network is compromised. Also, it is very weak against cryptanalytic attacks.

### B. *Pair wise Key Establishment*

In this scheme if we are having n nodes, then n-1 keys have to be stored so that each node can communicate with every other node in the network. Each node is having a unique key to communicate with the other node, so they can offer node to node authentication. As this scheme provides node authentication they also minimizes the chance of node replication. This scheme doesn’t have any communication overhead and computation overhead.

### C. *Trusted Key Distribution Center*

This scheme makes use of a trusted third party and this can be a base station or a sensor node. In pair-wise key establishment schemes, pair wise keys are preloaded on sensor nodes and hence the communication between different neighboring nodes takes place .But in this scheme, all pair-wise keys are stored on a trusted server and the key establishment between two sensor nodes is based on the common trust of a third node.

## III. KEY PREDISTRIBUTION SCHEMES

Key Pre Distribution schemes means preloading the sensor nodes with some keys before deployment. Before a WSN can exchange data securely, encryption keys must be established among sensor nodes[16]. After deployment, sensor nodes undergo a discovery process to set up shared keys for secure communications. In order to have a secure communication, they require a pair wise key. In this section the various key pre distribution methods are discussed.

### A. *Random Key Pre distribution*

Random Predistribution scheme was proposed by Eschenauer and Gligor [4]. This scheme is also referred to as Basic Scheme. Here key distribution is divided into three stages: key pre-distribution, shared-key discovery, and path-key establishment.

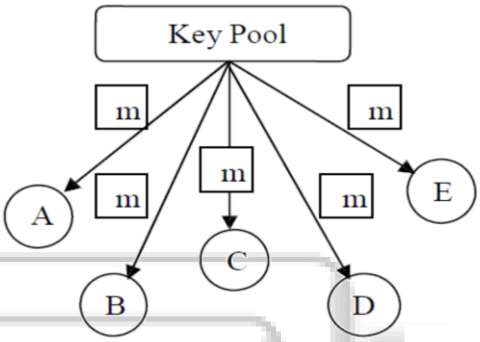


Fig 1.Basic Scheme

In the key pre-distribution stage, a large key pool of keys and their identifiers are generated. Each sensor node receives from the key pool a random subset of keys, which constitutes a key ring including the identifiers of all those keys. Then the nodes broadcast their identifier lists to other nodes to discover its neighbours with which it shares common keys.. Any two nodes able to find at least one common key can use that key as their shared secret to initiate communication. If two sensor nodes can't find any common key in their respective key rings, they make use of a procedure called path key establishment to find a sequence of secure links. Once a sequence of secure links has been achieved between two sensor nodes ,these two sensor nodes can establish their shared key by, for example, sending the shared key from one end to the other end.

### B. *Q-Composite Random Key Pre distribution Scheme*

Chan, Perrig, and Song [5] have introduced variation of the Basic Scheme, Q-Composite Random Key Pre distribution This scheme requires at least q common keys so as to have a communication link between any two nodes. This scheme has the same stages as the basic scheme. In the initialization phase, we pick a set S of random keys out of the total key space. Then we have to select a subset of this keys and assign these keys to every node. In the shared-key discovery phase, each node has to find the common keys which it shares with other nodes.

### C. *Random Pair wise Key Pre distribution*

Chan, Perrig, and Song developed the Random Pair wise scheme in [6] as an extension of the Pair wise Scheme .In the basic version which is called as the *trivial solution*, each node should store exactly ($N - 1$) pair-wise keys; one key with each other sensor in the network. This method provides a high level of resistance against node capture attack. But it suffers from memory consumption for key storage. So in this scheme instead of storing (N-1) keys, there is only Np = Nxp keys by each node, where p is the probability that two nodes in the network are connected. The reason is that not all n -1 keys are required to be stored in a node's key ring.

### D. *Knowledge Based Key Pre distribution*

Knowledge based key pre-distribution scheme [7] is based on the basic scheme in the way that key distribution is done prior to sensors deployment. However, it improves the performance of the basic scheme by reducing the quantity of keys or the key ring size via the use of pieces of information available prior to network deployment. This piece of information is called *node deployment knowledge*. Node deployment knowledge gives an idea about where a node is more likely to reside after deployment. In other words, it gives an idea about the neighbourhood of nodes. Keys that are assigned to a node should be shared only with possible neighbouring nodes.

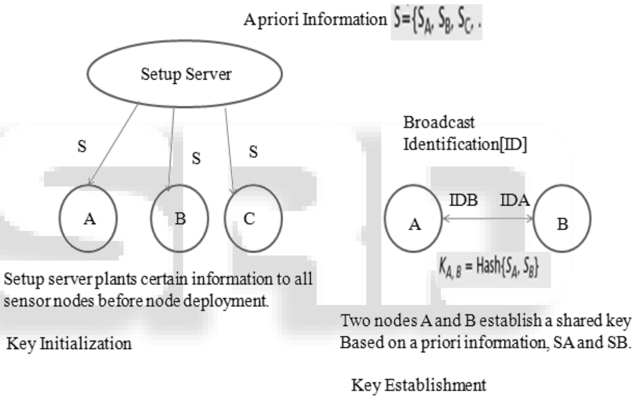

Apriori Information $S=\{S_A, S_B, S_C, .$
Setup Server
S
S
S
A
B
C
Setup server plants certain information to all sensor nodes before node deployment.
Key Initialization
Broadcast Identification[ID]
IDB
IDA
A
B
$K_{A,B} = Hash\{S_A, S_B\}$
Two nodes A and B establish a shared key Based on a priori information, SA and SB.
Key Establishment

Fig. 2: Knowledge Based Key Pre distribution

### E. *Polynomial Based Key Pre distribution*

Polynomial key pre-distribution scheme is the basis of pair-wise keys pre-distribution schemes developed by Liu and Ning (2003) [8]. In polynomial based key distribution, The setup server randomly produces a bivariate symmetric polynomial f(x, y) = f(y, x) of k degree over finite field GF(q), q > n. A key setup server computes a polynomial share of f(x, y), f(i, y) for each sensor i. If two nodes are present ie i and then i can compute the common key f(i, j) by evaluating f(i, y) at point j, while j can compute the same key f(j,i) = f(i, j) by evaluating f(j, y) at point i. To have a pair wise key, both sensor nodes need to evaluate the polynomial at the ID of the other sensor node.

### F. *Polynomial Pool Based Key Pre distribution*

This uses a pool of multiple random bivariate polynomials. Pair wise key establishment is performed in three phases: setup, direct key establishment, and path key establishment [8].

In Setup phase, the setup server randomly produces a set F of bivariate polynomials over the finite field GF(q) of *k*-

degree. For each sensor node i, they will select a subset of polynomials from F and assigns the polynomial shares of these polynomials to node i. In the direct key establishment, if both sensors have polynomial shares on the same bivariate polynomial, then a pair wise key can be directly established using the polynomial-based key pre-distribution. Path Key Establishment takes place, if direct key establishment fails. In this, two sensor nodes establish a pair wise key with the help of other sensors.

### G. *Leap: Localized Encryption and Authentication Protocol.*

This scheme used for heterogeneous network was proposed by Zhu, Setia, and Jajodia[9]. This method can be used for supporting various communication models. The main purpose of this scheme is that they can provide authentication, confidentiality and robustness. Different messages are used for communication between nodes. So they require different types of security requirement. LEAP supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pair wise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network.

### H. *The Babel Scheme*

Scheme was used to give many secret link keys towards the neighbors that have to be connected. The main idea is to find a common bridge node that shares keys with the source node and each of its to-be-connected neighbors. The common bridge node will be the only node other than the source and the receiving nodes knowing the secrets. All other nodes only serve as passive routers without knowing the secrets that they help to forward. This can lower the key disclosure probability.

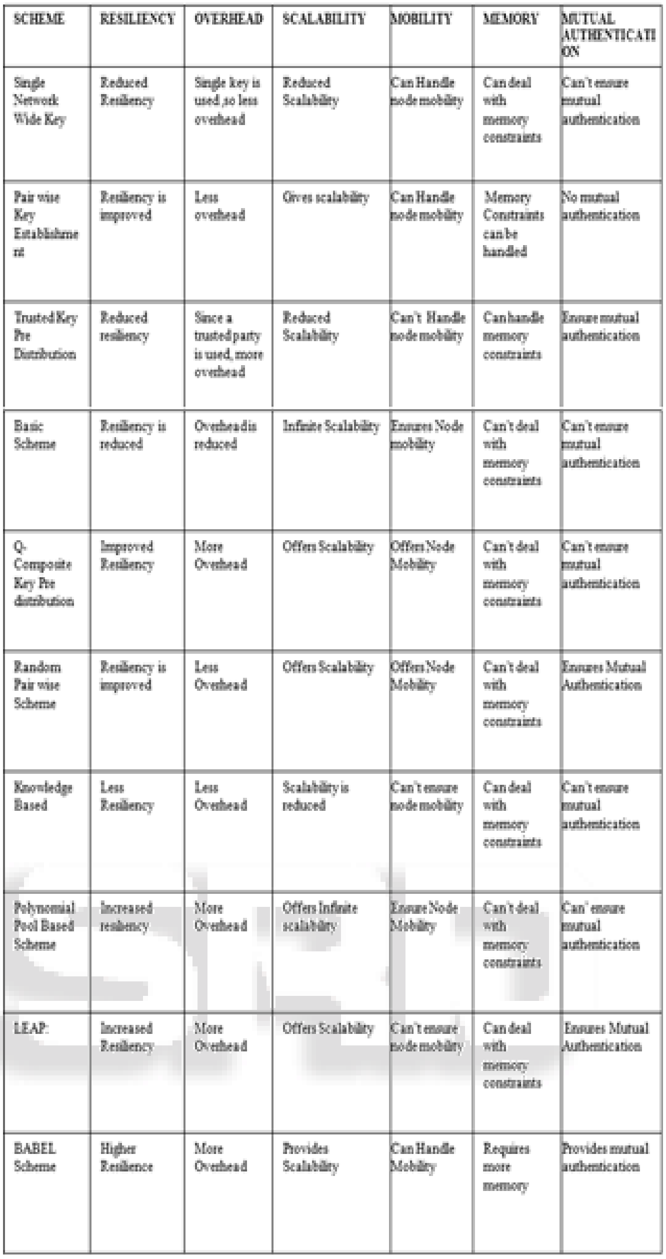
## IV. COMPARISON OF DIFFERENT KEY DISTRIBUTION SCHEMES

Key management protocols in traditional networks are assessed based on some evaluation metrics.

1) Resiliency: Key management schemes must be resilient against node capture because nodes may possess keys shared with many others .If any of these keys is lost, and then the entire network is compromised.
2) Mutual Authentication: Nodes should authenticate each other so that they can prevent unauthorized entities from gaining access to the network.
3) Memory-Fitness: Memory space required to store keys or intermediate parameters should be as reduced as possible.

## V. PROPOSED SYSTEM

The existing schemes suffer from many drawbacks. In order to avoid all these shortcomings a new method was proposed by Liu *et al.* [6] i.e. the grid-based key pre distribution scheme based on the polynomial scheme. All the earlier schemes have communication overhead and this method actually reduces the communication overhead and establishes a connection between nodes easily.



| SCHEME | RESILIENCY | OVERHEAD | SCALABILITY | MOBILITY | MEMORY | MUTUAL AUTHENTICATION |
|---|---|---|---|---|---|---|
| Single Network Wide Key | Reduced Resiliency | Single key is used ,so less overhead | Reduced Scalability | Can Handle node mobility | Can deal with memory constraints | Can't ensure mutual authentication |
| Pair wise Key Establishment | Resiliency is improved | Less overhead | Gives scalability | Can Handle node mobility | Memory Constraints can be handled | No mutual authentication |
| Trusted Key Pre Distribution | Reduced resiliency | Since a trusted party is used, more overhead | Reduced Scalability | Can't Handle node mobility | Can handle memory constraints | Ensure mutual authentication |
| Basic Scheme | Resiliency is reduced | Overhead is reduced | Infinite Scalability | Ensures Node mobility | Can't deal with memory constraints | Can't ensure mutual authentication |
| Q-Composite Key Pre distribution | Improved Resiliency | More Overhead | Offers Scalability | Offers Node Mobility | Can't deal with memory constraints | Can't ensure mutual authentication |
| Random Pair wise Scheme | Resiliency is improved | Less Overhead | Offers Scalability | Offers Node Mobility | Can't deal with memory constraints | Ensures Mutual Authentication |
| Knowledge Based | Less Resiliency | Less Overhead | Scalability is reduced | Can't ensure node mobility | Can deal with memory constraints | Can't ensure mutual authentication |
| Polynomial Pool Based Scheme | Increased resiliency | More Overhead | Offers Infinite scalability | Ensure Node Mobility | Can't deal with memory constraints | Can' ensure mutual authentication |
| LEAP: | Increased Resiliency | More Overhead | Offers Scalability | Can't ensure node mobility | Can deal with memory constraints | Ensures Mutual Authentication |
| BABEL Scheme | Higher Resilience | More Overhead | Provides Scalability | Can Handle Mobility | Requires more memory | Provides mutual authentication |

Table (1): Comparison of Various Key Pre Distribution Schemes

## VI. PROPOSED SYSTEM

The existing schemes suffer from many drawbacks. In order to avoid all these shortcomings a new method was proposed by Liu *et al.* [6]ie the grid-based key pre distribution scheme based on the polynomial scheme . All the earlier schemes has communication overhead and this method actually reduces the communication overhead and establish a connection between nodes easily.

### A. *Architecture Of Proposed System*

If a network consists of N sensor nodes, an (m x m) grid with a set of 2m polynomials is constructed, where m=√N. Each row i in the grid is associated with a polynomial fi r(x, y) and each column of the grid is associated with a polynomial share
fi c(x, y).

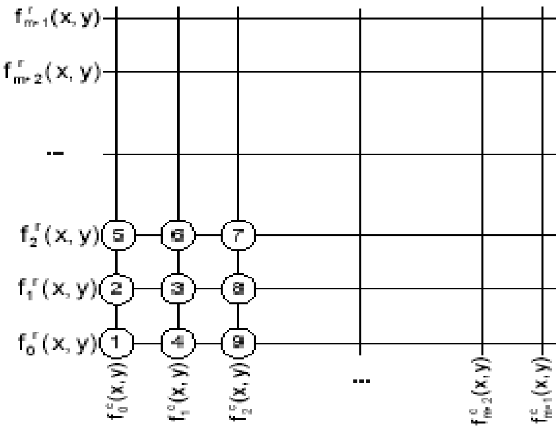


Fig. 3:Grid System

In the first stage, the setup server gives an intersection in the grid to each node, and then gives the polynomial shares of that particular column and row to the node so as to use this information for key discovery and path key establishment. We represent an ID constructed from the coordinate (i, j) as<i, j>. In the second stage, if a node i want to establish a pair wise key with node j, it checks for common rows or columns with j i.e., ci = cj or ri = rj. If ci=cj then both nodes may have the fci c (x, y) and they can use the polynomial-based key Predistribution scheme to establish a pair wise key directly. If ri=rj then both nodes may have the fri r(x,y) they both have polynomial shares of fri r (x, y), and can establish a pair wise key accordingly. If neither of these conditions is true, nodes i and j go through path discovery to establish a pair wise key. To do so, node i can find an intermediate node through which it can establish a pair wise key with node j. The main advantage of this scheme is that they can reduce the communication overhead and can give the exact number of polynomials.

## VII. CONCLUSION

Key management for wireless sensor networks is an important issue that has been researched by various researchers and many schemes were found. Because of the nature of limited resources on wireless sensor nodes, many researchers have conducted different techniques to propose different types of key distribution mechanisms. All the schemes have some advantages as well as some disadvantages. We have to choose a management scheme that provides a balance between the requirements and resources of a WSN. Still key distribution in wireless sensor networks is an active research area.

Many other schemes should be developed so as to make use of the limited resources of sensor nodes. Techniques for compromised node discovery and efficient methods to revoke compromised nodes should be the main aim of Future research.

## REFERENCES

[1] B.J. Culpepper and H.C. Tseng, “Sinkhole Intrusion Indicators in DSR MANETs,” Proc. First Int’l Conf. Broadband Networks (Broad- Nets ’04), pp. 681-688, Oct. 2004.

[2] [Lai B, Kim S, Verbauwhede I. Scalable session key construction protocol for wireless sensor networks. In: Proceedings of the IEEE workshop on Large Scale Real-time and Embedded Systems LARTES, December 2002.

[3] Chan H, Perrig A. PIKE: peer intermediaries for key establishment in sensor networks. In: Proceedings of the 24th annual joint conference of the IEEE computer and communications societies (INFOCOM ‟05), Miami, FL, USA, March 2005. p. 524–35.

[4] L. Eschenauer and V.D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proc. ACM Conf. Computer Comm. Security (CCS ’02), pp. 41-47, 2002.

[5] H. Chan, A. Perrig, and D. Song, “Random Key Pre-Distribution Schemes for Sensor Networks,” Proc. IEEE Symp. Research in Security and Privacy, 2003.

[6] D. Liu, P. Ning, and R.Li. “Establishing, Pairwise Keys in Distributed Sensor Networks,” Proc. 10th ACM Conf. Computers and Comm. Security (CCS ’03), pp. 52-61, Oct. 2003.

[7] Deng, Y. S. Han, S. Chen, and P. K. Varshney. A Key Management Scheme for Wireless Networks Using Deployment Knowledge. In The 23rd Conference of the IEEE Communications Society (Infocom),Hong Kong, March 2004.

[8] H. Chan, A. Perrig, and D. Song, “Key Distribution Techniques for Sensor Networks,” Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.

[9] S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” Proc. 10th ACM Conf. Computers and Comm. Security (CCS ’03), pp. 62-72,Oct. 2003.

[10] D. Liu and P. Ning, “Location-Based Pairwise Key Establishments for Static Sensor Networks,” Proc. First ACM Workshop Security Ad Hoc and Sensor Networks, 2003.

[11] [Sanjay Kumar, Deepti Dohare and Mahesh Kumar “An Efficient Key Distribution Scheme for Wireless Sensor Networks using polynomial based schemes” 2012 International Conference on Information and Network Technology (ICINT 2012).

[12] Zhiguo Wan, Kui Ren, Bo Zhu, Bart Preneel, and Ming Gu, “Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh Networks,”ieee transactions on vehicular technology, vol. 59, no. 2, February 2010.

[13] H. Deng, W. Li, and D.P. Agrawal, “Routing Security in Wireless Ad Hoc Networks,” Proc. IEEE Comm. Magazine, pp. 70-75, 2002.
W. Zhang, G. Cao, and T. La Porta, “Data Dissemination with Ring-Based Index for Wireless Sensor Networks,”Proc. IEEE Int’l Conf. Network Protocols (ICNP), pp. 305-324, Nov. 2003.

[14] K. Ren, K. Zeng, and W. Lou. A new approach for random key pre-distribution in large-scale wireless sensor networks. Wireless communication and mobile computing, 6(3):307–318, 2006.

[15] F. Zhao and L. Guibas. Wireless sensor networks. Elsevier Inc, pages 23–24, 2004.

[16] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, ―Wireless sensor network security: A survey,‖ in Security in Distributed, Grid, and Pervasive Computing, Y. Xiao, Ed. Boca Raton, FL: CRC, 2007.