# A Review on Various Key Management Techniques for Security Enhancement in WSN

Deepika#1, Manpreet #2
[1]M.Tech., CSE Department, GRIMT, Radaur, Kurukshetra University, India
[2]Assistant Professor, CSE Department, GRIMT, Radaur, Kurukshetra University, India

***Abstract* —-** A Wireless Sensor Network (WSN) sometimes called actuator networks are the group of sensor nodes which communicate with each other or with the base station. This wireless sensor networks are used to measure the different conditions. Due to the vast use of WSN in various applications like military, air traffic, e-learning it become necessary to enhance the security of sensor networks. There is a lots of security problems which are faced by sensor networks so it become necessary to improve the traditional key management techniques. The objective of this paper is to study the various key management techniques to enhance the security of leach protocol.

**Keywords —** *Wireless Sensor Network; cluster Head; Low Energy Adaptive Clustering Hierarchy; Exclusion Basis System*

**Introduction**

A Wireless Sensor Network (WSN) is a lattice system which consists of spatially distributed devices like wireless sensor meeting points. These sensor nodes measure physical or environmental conditions like sound, temperature and motion. The discrete point is able to sense their environment, processing the data locally and sending data collectively to one or more collection points in a WSN

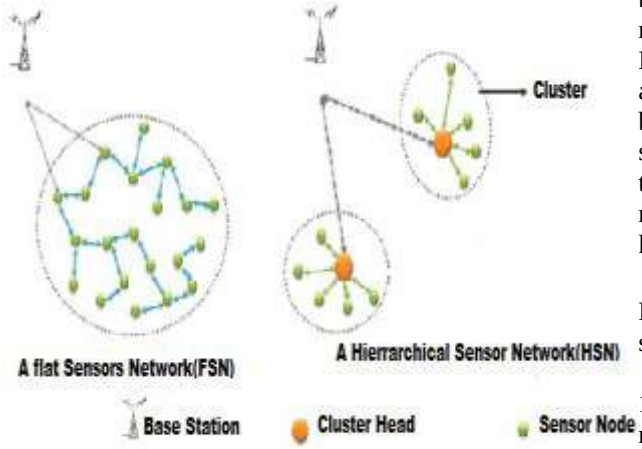


**Fig. 1.Wireless sensors networks architectures**

There are two types of data broadcasting in WSN –

1. Direct broadcasting in which data is send directly to the final node.

2. Multihop broadcasting in which data send via source node and base station through various intermediate nodes. (9)

These networks are commonly used in various fields like military and health. Some of features of the sensor nodes are consuming less power, less bandwidth, less size and less energy. Due to reduced bandwidth, prone to attacks, collisions in channel wireless networks are compel to use. There must be some mechanism to make WSNs secure. Sensor networks are self organized web, which can be used in different situations, but these types of networks become easy target for attack. For this reason we should apply some level of security so that it will be difficult to be attacked, especially when they are used in some important applications. (1)

### A. Security In Wireless Sensor Networks

Security of Wireless networks has become an important issue for organizations.So if we want to use WSN at a large scale, it's necessary to intensify its protection. It is not known before that nodes are going to be in communication range of each other. Some encryption algorithm is applied to the detector nodes, to increase the protection of sensor nodes. Key management will boost network security and build network resistant against attacks on it. Due to restricted computing power and small space, Network security techniques used in the past time are not so useful. All the needs for security cannot be fulfilled by a single key technique as in Wireless sensor networks as a number of messages are transferred between different nodes. WSNs face many security threats so there is a want of special key management techniques for wireless networks.7

For secure communication, the following two security functions are commonly considered:

1. Message confidentiality: Message confidentiality make sure to the sender that the message can be read only by an intended receiver.

2. Message authentication: Message authentication make sure to the receiver that the message was sent by a specified sender and the message was not altered en route.2

### B. LEACH PROTOCOL

In wireless sensor network LEACH was first proposed to lower the total energy utilization. It supposed that each node can send messages to BS using a high enough transmitting power. To balance the energy utilization in sensor networks we apply the clustered hierarchy. There is a cluster heads in every cluster of nodes. Sensors send their messages to cluster heads (CHs). CHs then combined these messages and send them to BS. The nodes which are not involved in CHs consume less energy since they can transmit with less transmission power, but at the same time we consume the energy of CHs. To solve the problem of energy consumption, LEACH proposed a dynamic CH rotation in which at each round the cluster head should be changed. Each round, a new node will become a CH. A distributed algorithm is used by the network to select the CHS and then dynamically clustering the remaining nodes around CHs [1

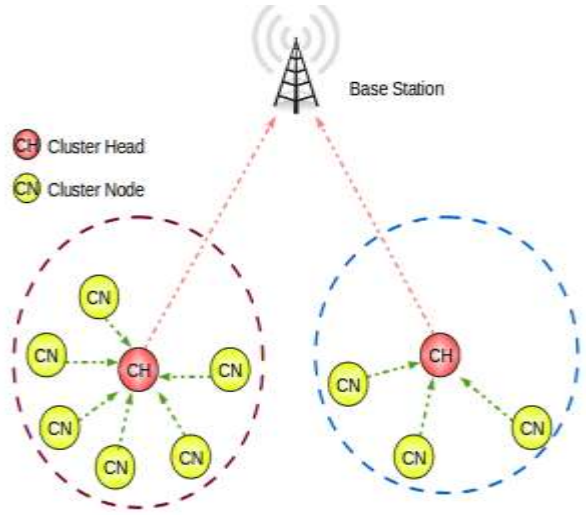


**Fig 2.Illustration of leach protocol**

The operation of LEACH protocol is divide into 2 phases:

I. Set-up phase
II. Steady state phase

**Setup Phase:** At the beginning of setup phase, each node can decide the probability that it can be cluster head for current round independent of other nodes. Then each nodes in the sensor network produce a random number such that 0< random < 1.There is a pre-defined threshold T (n) in sensor network. If the random number generated by the node is less than the T (n), the sensor node becomes cluster-head otherwise that node is the member of the cluster. When node has become CH it will send a message. This message consists of the node ID and a header. Depending on the energy of CH all the nodes other than CH can select the cluster to which it belongs. Once the sensing node has chosen cluster it will notify CH. Each node sends a join-request message to the CHs. The cluster-heads are responsible for transformation of data in their clusters. The cluster-head makes a Time Division Multiple Access (TDMA) schedule which is send to all the nodes in cluster head.

**Steady State Phase:** In the steady-state phase, According to the TDMA schedule received at the setup phase the neighbour are detected by cluster members and the sensed data is forwarded to their CH. The sensor nodes (SN) moves into hibernate mode to lower the energy consumption for other slots. The CH receives all the information sent by its member nodes, collect the data and sends it to BS. After a period of time, a new round is start by the network in which a new CH is selected and Network go back to the setup phase. The process can be break down into frames in which nodes can send their information to cluster-head. Since nodes are not equally distributed so there is difference in the number of nodes in each cluster. The information broadcast by each node to its cluster-head depend on the number of nodes in cluster.7

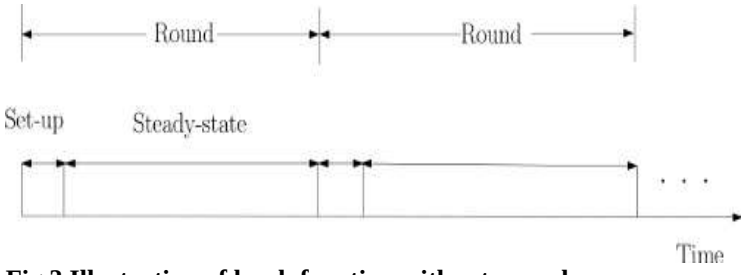


**Fig 3.Illustration of leach function with setup and steady state phase**

### C. KEY MANAGAMENT IN WIRELESS SENSOR NETWORKS:

Key management can be defined as a process that consists of key construction and the preservation of ongoing keying relationship between valid users according to a security policy. The key management in sensor networks consists of construction, sharing and preservation of the secrete keys. So to construct methods for key management for encryption, which can make information sharing more secure and at a same time make less resource utilization, have vital importance in WSNs. Depending on the capability of key preservation schemes to update the cryptographic keys of sensor nodes during their run time, these schemes can be categorized into two different categories:

1. Static
2. Dynamic

1. Static key management:

In this the keys are pre-delivered in the sensor network which means that the keys remain stable for the whole period of the network. In the static key management since the key is same so the chance of attacks increases in the sensor network.

2. Dynamic key management:
In this the keys are not stable instead they are changing throughout the lifetime of the network.
So Dynamic key management is very important type of key management in WSN. Dynamic key management is a mechanism in which keys are shared either repeatedly or on demand as needed by the network. The dynamic key management schemes can enhance network tenacity and network adaptability since the keys of compromised nodes are withdraws in the rekeying process. Mainly the key management schemes can be categorized as:

2.1. Distributed
2.2. Centralized.

2.1 Distributed dynamic key management:
It is a set of mechanism, in which there is no single point of controller, such as a base station or third party, take participate in rekeying process of sensor nodes. Basic idea behind distributed dynamic key management scheme is to avoid a single point of failure by arranging key using a number of key controllers. But these schemes are susceptible to design errors as compromised sensor nodes can participate in node ejection process.

2.2 centralized dynamic key management:
It is a set of process that that uses a common key controller, such as a base station or any third party, to arrange the key materials on the network's points. Compared with distributed dynamic key management, the compromised sensor nodes cannot harm the node ejection process in centralized key management scheme. It is further divided into three parts: (9)

2.2.1. Flat centralized Dynamic key management
2.22. Hierarchical centralized Dynamic key management
2.2.3. Heterogeneous Dynamic key management

## II. Related Study

**Mohammed A. Abuhelaleh and Khaled M. Elleithy et.al [1],** proposed a key management module in SOOAWSN for security in wireless sensor networks. In this paper the author focus on how to apply the new and effective key management technique to gain the highest possible level of security that can be used during wireless sensor networks communications. This proposal is a module of a complete solution that the author developed to cover all the aspects of WSN communication which is marked Secure Object Oriented Architecture for Wireless Sensor Networks (SOOAWSN).

**Lein Harn and Changlu Lin et.al [2],** proposed authenticated group key transfer protocol which is based on secret sharing. In this paper, the author propose an authenticated key transfer protocol based on secret sharing scheme that KGC can transmit group key data to all group members at once and only approved group members can recover the group key; but unapproved users cannot recover the group key.

**Jianli Wang,, Li Zhao, and Dan Tian et.al [3],** proposed a LEACH-based key management scheme for WSN based on Exclusion Basis Systems and μ TESLA. It is an effective security routing algorithm for wireless sensor networks. In this paper, the author proposed a LEACH-based key management scheme for WSNS based on Exclusion Basis Systems and μ TESLA. The author use EBS for key development and broadcasting, and use μ TESLA to guarantee the cluster head can update security key after the first round. This algorithm lowers the storage requirements of keys, and the load among network for updating cluster keys.

**Pengcheng Zhao, Yong Xu, Min Nan et.al [4],** proposed a Hybrid key management scheme based on cluster wireless sensor networks. The author proposes a hybrid key management scheme which based on clustered wireless sensor networks. The use of hierarchical clustering, lower the amount of key storage and computing, while supporting network topology, dynamic key management for which aims to stop leakage.

**Ying Zhang, 1 Bingxin Zheng,1 Pengfei Ji,1 and Jinde Cao2,3 et.al [5] ,** proposed a key management method based on dynamic clustering for WSN. In this paper, the author proposed a dynamic key management method to achieve the key changed periodically provided a security scheme for sensor networks to solve the problem of being captured for cluster heads.

**Abdoulaye Diop, Yue Qi, Qin Wang et.al [6] ,**proposed Efficient group key management using symmetric key and threshold cryptography for cluster based WSN.The proposed scheme considers a hierarchical cluster structure of sensor network and uses the pair-wise key management and group key management based on threshold key cryptography to develop and to share the keys efficiently within a cluster and updates regularly keys.

**Yanhong Sun 1, Ming Tang et.al [7],** proposed a enhanced protocol for leach based wireless sensor

networks. In this paper, the author proposed a SA-LEACH network security protocol. The benefit of using this protocol is that it consumes very less energy.

**Sandeep Kumar1, S.M. Kusuma2, B.P. Vijaya Kumar3 et.al [8],** proposed a random key distribution based artificial immune system for security in clustered wireless sensor networks. In this paper, author proposes a scheme, which uses random key distribution based Artificial Immune System (AIS) for detecting spoofing attacks. Result of this paper provide robust security an energy saving.

**Gurpreet Kaur*, Navdeep Kumar et.al [9]**, proposed secure and efficient data collection in wsn. In this paper, the author uses Data Encryption Standard scheme to enhance security in LEACH protocol. The objective of this paper is to add secret encryption scheme to the LEACH protocol. The author used the MATLAB to obtain the desired result.

**Roshani R. Patle, Prof. Rachana Satao et.al [10],** proposed aggregated identity- based signature to transmit data securely and efficiently in clustered WSN.In this paper, the author uses two protocols which are SET-IBS and SET-IBOOS to transmit data securely and efficiently. SET-IBOOS uses Identity-Based Online/Offline Digital Signature scheme whereas SET-IBS security depends on the hardness of Diffy-Hellman problem in the pairing region.

**Gurpreet Kaur*, Navdeep Kumar et.al [11],** proposed various key management schemes for leach in wireless sensor networks. In this paper, the author gives a brief description of wireless sensor networks and also about the leach protocol.

***TABLE I***

***COMPARISON OF VARIOUS KEY MANAGEMENT TECHNIQUES***

| S.No | Key Management Technique | Proposed By | Based On | Findings |
|---|---|---|---|---|
| 1 | SOOAWSN | Mohammed A. Abuhelaleh and Khaled M. Elleithy | key distribution | Increase security in key exchanging. |
| 2 | Authenticated Group Key | Lein Harn and Changlu Lin | Secret sharing of keys | Provide group key authentication and security from possible attacks. |
| 3 | LEACH-based key management | Jianli Wang, Laibo Zheng, Li Zhao, and Dan Tian | EBS for key generation and distribution, and μ TESLA | EBS decrease the storage space for keys and communication load. μ TESLA update the security of CHs. |
| 4 | Hybrid key management | Pengcheng Zhao, Yong Xu, Min Nan | Clustered wireless sensor networks | Anti-attack ability become strong and energy consumption is small. provide reliability to nodes. |
| 5 | DKMM | Ying Zhang,1 Bingxin Zheng,1 Pengfei Ji,1 and Jinde Cao2,3 | Dynamic clustering for sensor networks | Security of CHs increase. |
| 6 | Symmetric key and Threshold cryptography | Abdoulaye Diop, Yue Qi, Qin Wang | Clustered based for WSN | Provide better connectivity and scalability and provide security from malicious attacks. |
| 7 | Secure and Efficient data collection | Gurpreet Kaur*, Navdeep Kumar | Performance in Leach | Provide security to LEACH |

| | | | | |
|---|---|---|---|---|
| 8 | Aggregated identity Based signature | Roshani R. Patle | Identity based signature | Increase security in data transmission |
| 9 | SA-LEACH | Yanhong Sun 1, Ming Tang 2 | Leach protocol | Provided security in CHs |
| 10 | Random key distribution | E. Sandeep Kumar1, S.M. Kusuma2, B.P. Vijaya Kumar3 | Artificial Immune system | Security against spoofing attacks and increases the detection up to 90%. |

## III. CONCLUSIONS

In this paper, we studied about the LEACH protocol and various key management techniques to secure the working of LEACH protocol. From our study, we conclude that SOOAWSN technique based on distribution of keys among various nodes and this technique provide security in key distribution.DKKM scheme based on dynamic clustering for sensor networks and this technique provide security to CHs.Random key distribution scheme based on artificial immune system increase the detection ability of sensor networks up to 90% that whether there is a malicious node or not.SA-LEACH is secure leach which provide security to CHs.So this paper gives a comparison of various key management techniques used in WSN along with their findings.

### *REFERENCES*


1. Applications (IJNSA), Vol.2, No.4, October 2010. Mohammed A. Abuhelaleh and Khaled M. Elleithy, "Security In Wireless Sensor Networks: Key Management Module In SOOAWSN", International Journal of Network Security & Its
2. Lein Harn and Changlu Lin," Authenticated Group Key Transfer Protocol Based on Secret Sharing" IEEE TRANSACTIONS ON COMPUTERS, VOL. 59, NO. 6, JUNE 2010.
3. Jianli Wang, Laibo Zheng, Li Zhao, and Dan Tian, "LEACH-Based Security Routing Protocol for WSNs", Advances in CSIE, Vol. 2, AISC 169, pp. 253–258, © Springer-Verlag Berlin Heidelberg 2012
4. Pengcheng Zhao, Yong Xu, Min Nan," A Hybrid Key Management Scheme Based on Clustered Wireless sensor Networks" Copyright © 2012 SciRes.
5. Ying Zhang, Bingxin Zheng, Pengfei Ji and Jinde Cao, "A Key Management Method Based on Dynamic Clustering for Sensor Networks", November.
6. Abdoulaye Diop, Yue Qi, Qin Wang, and Shariq Hussain, "An Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Networks", International Journal of Computer and Communication Engineering, Vol. 1, No. 4, November 2012
7. Gurpreet Kaur*, Navdeep Kumar," Secure and Efficient Data Collection in WSN" Volume 5, Issue 5, May 2015,IJARCSSE.
8. Roshani R. Patle, Prof. Rachana Satao," aggregated identity- based signature to transmit data securely and efficiently in clustered WSNs". © 2015 IEEE.
9. Gurpreet Kaur*, Navdeep Kumar, "survey on various key management schemes for leach in wireless sensor networks". Volume 5, Issue 3, March 2015,IJARCSSE
10. Yanhong Sun 1, Ming Tang,"A Enhanced protocol for leach based wireless sensor networks", © 2014 IEEE
11. E. Sandeep Kumar1, S.M. Kusuma2, B.P. Vijaya Kumar3 ," A random key distribution based artificial immune system for security in clustered wireless sensor networks" ©2014 IEEE.