International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-6)

Research Article

June 2015

Security Enhancement in Leach Protocol

Nidhi Sharma
Assistant Prof. (ME Dept.), SDDIet,
Barwala, India

Monika
M.Tech Scholar (ME Dept.), SDDIET,
Barwala, India

Abstract--

A wireless sensor network comprises of small nodes with computation, sensing, and wireless communications capabilities. A number of protocols have been specifically designed for WSNs where an essential design issue is energy awareness. Routing protocols in WSNs may vary depending on the application and network architecture. In this paper, we present a survey of LEACH(Low Energy Adaptive Clustering Heirarchy) protocol along with the key management issues. We first outline the homoeomorphic encryption in LEACH routing protocol in WSNs followed by a comprehensive survey of key management techniques. Overall, a secure keypool architecture is proposed that deals with the security issues of LEACH protocol. We analyze and compare the trade-offs between energy consumed, data transmitted and number of alive nodes. We also highlight the advantages of SKPA and security issues of WSNs.

Keywords---WSN, SKPA, LEACH, cluster, routing.

I. INTRODUCTION

"A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as sound, vibration, pressure, motion, temperature, or pollutants, at adverse locations." [14].

Although wireless sensor networks are originally motivated by military applications such as battlefield surveillance and counterterrorism, nowadays they are also employed for civilian applications such as healthcare applications, home automation, and traffic control [12]. Another popular application field of wireless sensor networks is the monitoring a geographical area for environmental data.

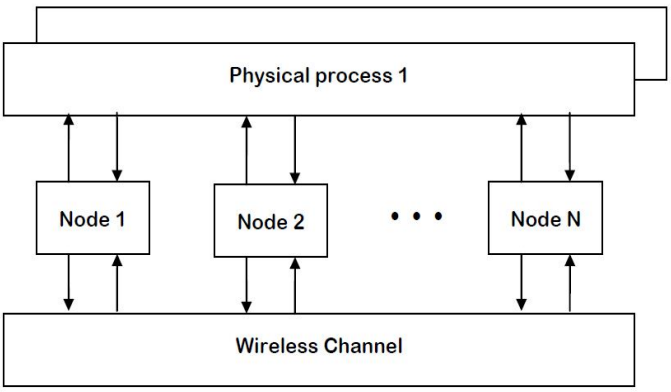

Figure 1: Structure of WSN

With respect to traffic classes wireless sensor networks may be divided into two groups, namely-
-synchronous and
-asynchronous wireless sensor networks [13].

• **Synchronous wireless sensor networks:** Synchronous wireless sensor networks are employed for real-time monitoring applications such as traffic monitoring where the monitored data is fluctual and transmitted to the authorized reader device in real-time.

• **Asynchronous wireless sensor networks:** In contrast to synchronous wireless sensor networks, the data monitored in asynchronous wireless sensor networks is not fluctual and transmitted to the authorized reader device only when requested.Therefore, wireless sensor applications with asynchronous character need to store the monitored data itself

II. PROTOCOL OVERVIEW

Routing Protocols in WSNS

WSN routing protocol is the main research, because the sensor nodes acquire power through battery that in turn,limits its capacity and makes it difficult to replace the battery. Therefore, the energy saving of routing protocol for wireless sensor networks is the current research spot.Cluster routing protocol is a low energy routing protocol, and it separates the whole WSN network into several areas, these areas are regards as cluster [15].

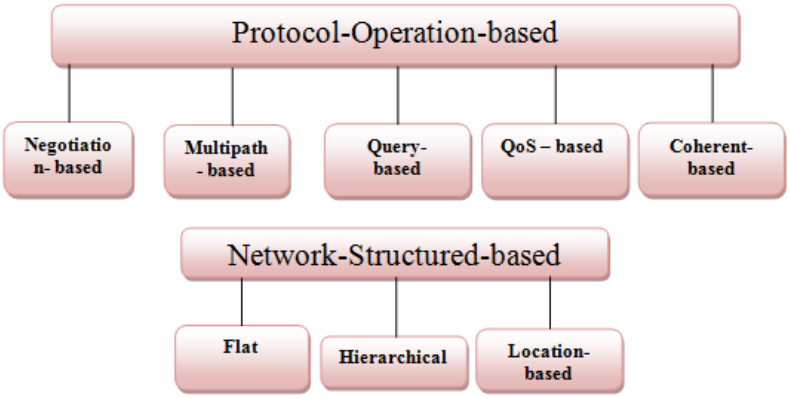

Figure2. Routing Protocols in WSNs

Based on the underlying network there are three protocol categories:

1.Flat based routing protocol: In flat routing protocols, nodes play the same role and have similar functionality in transmitting and receiving data. In this type of network,assignment of global identifier to each node is impossible due to large number of nodes. Therefore,queries are sent to different part of the field by base station where it waits for the data from sensors in selected parts of the field. This approach is also known as data centric routing.

2.Hierarchical routing protocol: In this type of network, nodes are assigned different roles in the network like members of clusters, cluster heads, etc. Processing and communication is carried by some nodes, while other nodes are employed for sensing the target area. Hierarchical routing is mainly considered as two layer architecture where one layer is engaged in cluster head selection and the other layer is responsible for routing.

Cluster head in hierarchical routing is the node which is responsible for collecting data from other nodes in the cluster, aggregating all data and sending the aggregated data to the base station. Creation of clusters and employing cluster heads for communication task contributes to a more scalable and energy efficient network. Hierarchical-based routing protocols are also known as cluster based routing protocols. In order to avoid redundancy, hierarchical routing protocols are the best.

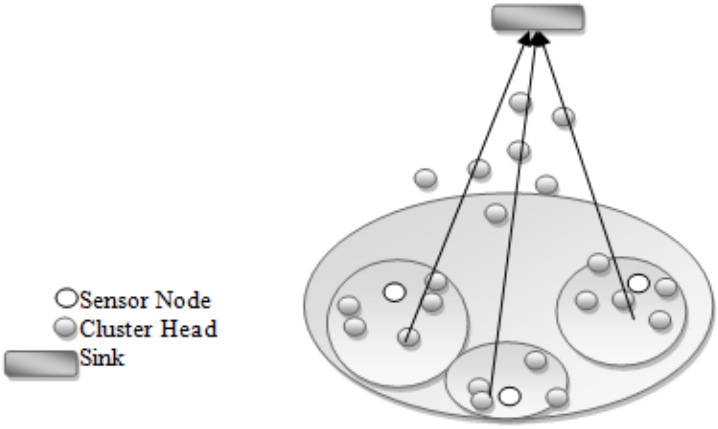

Figure 3. Model of Clustered Network [15]

Clustered WSNs were first proposed for various reasons including scalability and energy efficiency. Those with rotating CHs, like LEACH (Low Energy Adaptive Clustering Hierarchy), are also interested in terms of security, as their routers (the CHs), which are more prominent targets for adversaries because of their role in routing; rotate from one node to another periodically. This rotation helps in security, as an adversary finds it difficult to identify the routing elements and compromise them.

3.Location-based: Sensor nodes are addressed by means of their locations. The incoming signal strengths are used to calculate the distance between neighbouring nodes. The estimation of relative coordinates of neighbouring nodes is done by exchanging such information between neighbours or by communicating with a satellite using GPS.

LEACH Protocol

LEACH (Low Energy Adaptive Clustering Hierarchy) is first hierarchical routing protocol proposed by Wendi B. Heinzelman of MIT. LEACH is a cluster-based routing protocol which includes cluster formation in distributed manner. In LEACH, nodes are classified into two groups: CHs and SNs. LEACH aims to reform clusters once every period of time, called a round;that rotates the role of the CH among members in a cluster. LEACH includes randomized rotation of the high-energy cluster head position such that it rotates among the several sensors nodes in order to not deplete the battery of a single sensor.

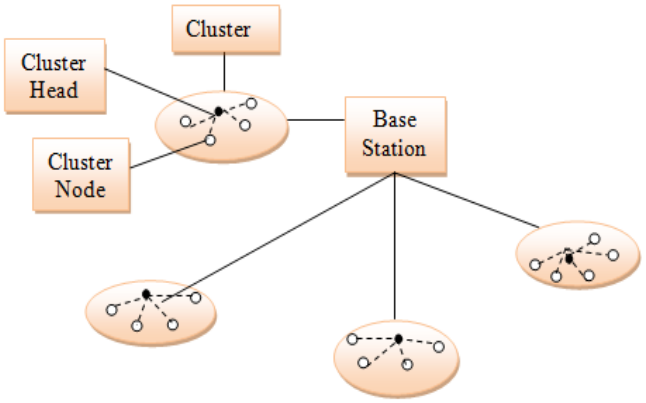

Figure 4.LEACH routing topology

Thus, LEACH incorporates randomized rotation of the high-energy cluster head position among the sensors to avoid draining the battery of any one sensor in the network. Due to this, the energy load of being a CH is evenly distributed among the nodes.
This protocol provides a conception of round. LEACH protocol runs with many rounds. Each round comprises two phases:

1. Setup Phase
2. Steady Phase

Key Management
Key management is the set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties. Key management plays a fundamental role as keys are the basis for cryptographic techniques providing data integrity,entity authentication, data origin authentication,confidentiality, and digital signatures.
Key management schemes in WSNs can be classified broadly-
-dynamic or
-static solutions, based on whether rekeying of administrative keys is enabled post network deployment.
Schemes are also classified as-
- homogeneous or
- heterogeneous schemes w.r.t the role of network nodes in the key management process.
Homogeneous schemes generally assume a flat network model, while heterogeneous schemes work for both flat and clustered networks. Key pre-distribution phase is an important starting phase where keys are distributed before the deployment of the network, i.e. during the manufacturing time of node. This is followed by the key establishment phase which refers to how nodes will establish a secure session. The network formation phase is then initiated. Node addition or Node deletion phase deals with establishment of secure sessions with new nodes being added or removed from the network.

III. RELATED STUDY

Nazia Majadi et. al.[1] build a wireless sensor network in which each sensor node remains inside the transmission range of CHs and therefore, the lifetime of the network is prolonged. A wireless sensor network is composed of a large number of sensor nodes that are densely deployed in a phenomenon or very close to it. The lifetime of sensor nodes shows a strong dependence on battery lifetime. Clustering provides an effective way for prolonging the lifetime of a wireless sensor network. Therefore, clustering techniques are used to distribute the energy consumption among nodes in each cluster and extend the network lifetime. LEACH (Low-Energy Adaptive Clustering Hierarchy), a clustering-based protocol that utilizes randomized rotation of Cluster-Heads (CHs) to evenly distribute the energy among the sensors in the network. But LEACH cannot select CHs uniformly throughout the network. Therefore there is the possibility that the elected CHs will be concentrated in certain area of the network. Hence, some nodes will not have any CHs in their vicinity. The proposed approach U-LEACH is an approach to address this problem.
Vikas Nandal and Deepak Nandal et. al. [2] proposed a progressive algorithm for the cluster head selection. The proposed algorithm for cluster head selection is based on residual energy, distance & reliability. LEACH (low-energy adaptive clustering hierarchy) is well-known & divides the whole network into several clusters, and the run time of network is broken into many rounds. In each round, the nodes in a cluster contend to be cluster head according to a predefined criterion. Since CHs consume more energy in aggregating and routing data, it is important to have an energy-efficient mechanism for CHs' election and rotation.
Lianshan Yan, Wei Pan, Bin Luo, et al. [3] investigated an improved energy-efficient communication protocol for wireless sensor networks (WSNs) in the presence of distributed optical fiber sensor (DFS) links located at the centre of WSN fields based on the protocol—low-energy adaptive clustering hierarchy (LEACH).They investigated a modified energy-efficient communication protocol, called O-LEACH, for wireless sensor networks that consist of DFS links and randomly scattered wireless sensor nodes. Network performances in terms of lifetime of nodes are simulated for the cases

that two WSNs can or cannot communicate with each other. The lifetime of such sensor network with rectangular topology is further investigated. The lifetime of the situation that two WSNs are isolated is more than 20% better than that of the case where nodes inside two WSN fields are reachable to any live nodes within the whole sensor field. This can be a deployment guideline for such hybrid sensor networks.

A.S.Poornima and B.B.Amberker et. al. [4] proposed a secure data aggregation scheme which provides end-to-end data privacy. Wireless Sensor Network (WSN) consists of a large number of nodes with limited resources. In such network consisting of resource constrained nodes, data transmission is an energy-consuming operation. Hence to extend the lifetime of the network it is necessary to reduce the number of bits transmitted. The protocol uses additive homomorphic encryption method to encrypt the data. The additive homomorphic encryption allows addition of cipher texts which when decrypted results in addition of the plain text.

Mona El_Saadawy and Eman Shaaban et. al. [5] proposed MS-LEACH to enhance the security of S-LEACH by providing data confidentiality and node to cluster head (CH) authentication using pairwise keys shared between CHs and their cluster members. Developing effective security solutions for wireless sensor networks (WSN) are not easy due to limited resources of WSNs and the hazardous nature of wireless medium. The implementation of encryption/decryption algorithms which are the most essential part of the secure communication can be very intricate in WSNs since they incorporate routines that having very complex and intense computing procedures. A secure clustering protocol that achieves the desired security goals while keeping an acceptable level of energy consumption is a challenging problem in wireless sensor network. S-LEACH was the first modified version of LEACH with cryptographic protection against outsider attacks.

Jia Xu, Ning Jin, Xizhong, et al. [6] proposed a revised cluster routing algorithm named E-LEACH to enhance the hierarchical routing protocol LEACH. In the E-LEACH algorithm, the original way of the selection of the cluster heads was random and the round time for the selection was fixed. In the E-LEACH algorithm, the remnant power of the sensor nodes was considered in order to balance network load .

Meenakshi Diwakar and Sushil Kumar et. al. [7] proposed EELBCRP (Energy-Efficient Level Based Clustering Routing Protocol), a protocol for wireless sensor networks. Nowadays, advanced technology of wireless sensor networks used in many applications like health, environment, battle field etc. The sensor nodes are equipped with limited power sources. Therefore, efficiently utilizing sensor nodes energy can maintain a prolonged network lifetime. One of the major issues in sensor networks is developing an energy-efficient routing protocol to improve the lifetime of the networks.From the results of simulation, it was observed that the performance of EELBCRP was better in terms of energy consumption of CH, number of clusters and lifetime of network compared with LEACH.

Fuzhe Zhao, You Xu, and Ru Li et. al. [8] proposed improved clustering protocol that performed better than the LEACH and the LEACH-C by reducing the consumption of energy. Based on the LEACH, LEACH-C also organizes the sensor nodes into clusters with each cluster a cluster head and divides a round into set-up and steady state phases. It differs from LEACH only in that it uses a high-energy base station to finish the choice of cluster heads. In the set-up phase of each round, every sensor node sends its information about energy to remote BS. Then the BS selects the cluster heads based on the energy information and broadcasts the IDs of cluster heads to other member nodes.

Yuling Li, Luwei Ding and Feng Liu et. al. [9] proposed Leach-N that performs better than LEACH in the following three aspects, the number of live nodes, energy consumption and data transmission. According to the new protocol, the problem that how to select nodes as the cluster head node depend on the residual energy of nodes in the cluster.The new protocol LEACH-N will increase calculation time of the node's threshold, but the overhead of calculation is smaller than that of the cluster head election which does not take into account the residual energy of nodes. Therefore, the set of residual energy factor is reasonable and can reduce the energy cost of network nodes to a certain extent. This strategy can guarantee the rationality during selecting head nodes.

Baiping Li and Xiaoqin Zhang et. al. [10] proposed LEACH-CC in which a chain routing between clusters is established to reduce the amount of nodes which communicate with the base station. It not only extended the lifetime of the network, but also improved the energy efficiency. Using a central control algorithm, better clusters were produced by dispersing the cluster-head nodes throughout the network. Then a chain routing between cluster-heads was established to reduce the amount of nodes which communicate with the base station.This algorithm minimizes the amount of energy the non-cluster-head nodes will have to use to transmit their data to the cluster-head, by minimizing the total sum of squared distance between all the non-cluster-heads and the closest cluster-head.

IV. PROPOSED WORK

1. To study the various key management techniques in WSN. The main goal of key management scheme is to provide secure communication between sensor to sensor, a group of sensor and sensor to base station.
2. A new key management scheme is proposed “Secure Key Pool Architecture[SKPA] For Wireless Sensor Networks.
3. Study of LEACH protocol
4. Implementation of homomorphic encryption with LEACH and simulate LEACH and LEACH_HE
5. Compare the results in NS2 using LEACH protocols with and without Homomorphic Encryption

V. RESULTS AND DISCUSSION

To compare the performance of LEACH and LEACH_HE, consider the performance metrics of energy consumed, data transmitted and number of alive nodes.

The performance comparison of LEACH_HE and LEACH is done using leach.out files of both the protocols. Two scenarios are considered for simulation-one in which simulation time is considered 500 seconds.

Performance Comparison of LEACH_HE and LEACH when Simulated For 500 Seconds

Table I: Performance comparison of LEACH_HE and LEACH when simulated for 500 seconds

Performance metrics	**LEACH_HE**	**LEACH**
Total Energy Consumed (Joules)	320.08	372.57
Total Data Transmitted (bits)	54782	49216
Number of Nodes Alive	35	29
Lifetime(seconds)	500	500

1. Energy Consumed

The table depicts the result when homomorphic encryption is introduced in LEACH and the graph is compared with the normal working protocol LEACH so as to observe the energy consumed during simulation.

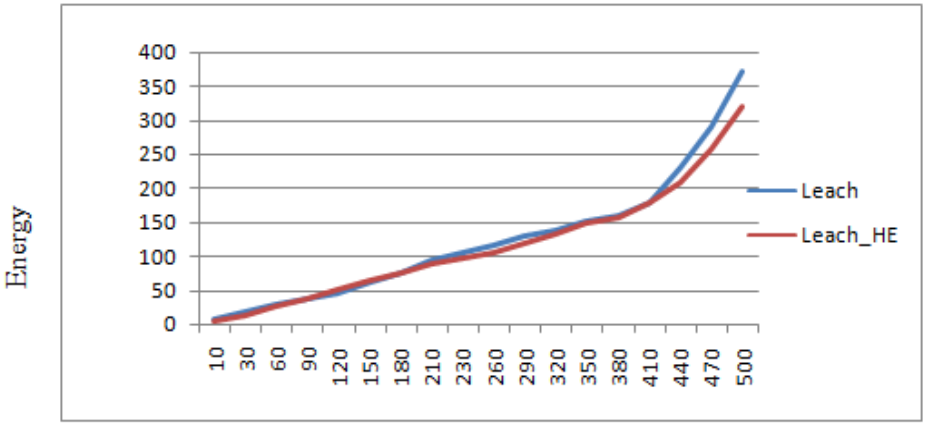

Figure 5. Energy Consumed vs. Time

The graph shows that LEACH_HE consumes somewhat equal energy as compared to LEACH. Since homomorphic encryption reduces the task of decryption at CHs hence no extra energy consumption and hence LEACH_HE consumes almost equal energy as consumed by LEACH.

2. Data Transmitted

Figure 5 compares the number of bits transmitted by LEACH and LEACH_HE for each time period during the simulation period of 500 seconds. This result is carried out when homomorphic encryption is introduced in LEACH and the graph is compared with the normal working protocol LEACH so as to observe number of bits transmitted during simulation.

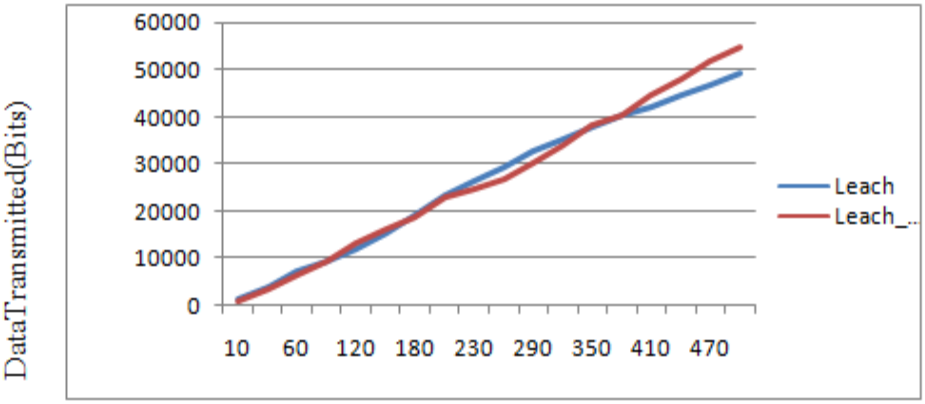

Figure 6. Data Transmitted (bits) vs. Time

This clearly depicts that addition of homomorphic encryption in LEACH doesn't degrades its performance.

3. Number of Alive Nodes

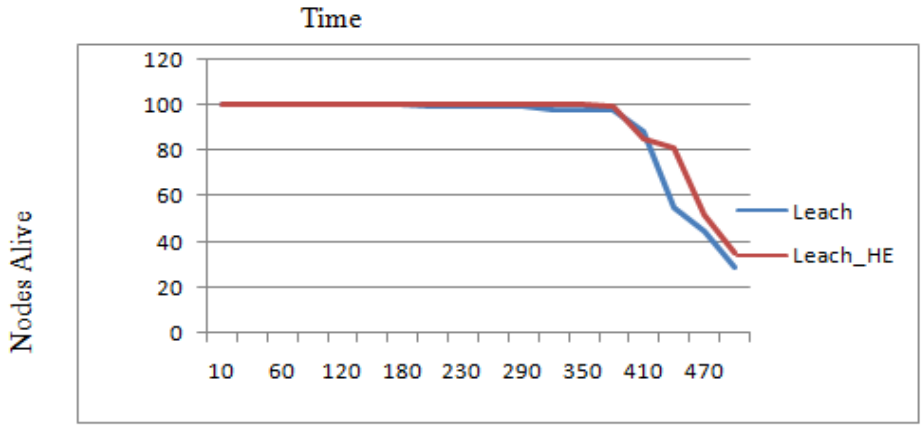

Figure 7. Nodes Alive vs. Time

This graph shows that numbers of nodes alive in LEACH_HE are more as compared to LEACH initially but at the end of simulation time both have equal number of nodes alive. Hence it shows that LEACH_HE performance is similar to LEACH.

VI. CONCLUSION

Addition of homomorphic encryption in Leach (LEACH_HE) shows that the performance of LEACH_HE doesn't degrades. In some cases it performs better or just same as LEACH. Adding homomorphic encryption to LEACH neither reduces the network lifetime nor does it consume extra energy. LEACH_HE consumes almost same energy as consumed by LEACH. LEACH_HE transmits almost same number of bits as compared to LEACH. LEACH_HE lifetime is somewhat similar to LEACH. Hence these performance parameters depicts that adding homomorphic encryption to LEACH doesn't degrades the performance. It works similar to simple Leach protocol with security applied to the data communication between sensor nodes and the cluster heads.

REFERENCES

[1] Nazia Majadi. U-LEACH, "A Routing Protocol for Prolonging Lifetime of Wireless Sensor Networks, " (IJERA) Vol. 2, Issue4, July-August 2012
[2] Vikas Nandal and Deepak Nandal , "Maximizing Lifetime of Cluster-based WSN through Energy-Efficient Clustering Method," IJCSMS Vol. 12, Issue 03, September 2012
[3] Lianshan Yan and Wei Pan, " Modified Energy-Efficient Protocol for Wireless Sensor Networks in the Presence of Distributed Optical Fiber Senor Link,"IEEE SENSORS JOURNAL, VOL. 11, NO. 9, SEPTEMBER 2011
[4] A.S.Poornima and B.B.Amberker, "SEEDA : Secure End-to-End Data Aggregation in Wireless Sensor Networks," IEEE 2010
[5] Mona El_Saadawy,et al, "Enhancing S-LEACH Security for Wireless Sensor Networks," IEEE 2012
[6] Jia Xu,et al, "Improvement of LEACH protocol for WSN," 2012 IEEE
[7] Meenakshi Diwakar and Sushil Kumar, "An Energy Efficient Level Based Clustering Routing Protocol For Wireless Sensor Networks," IJASSN, Vol 2, No.2, April 2012
[8] Fuzhe Zhao, You Xu, and Ru Li , "Improved LEACH Routing Communication Protocol for a Wireless Sensor Network," Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2012
[9] Yuling Li, Luwei Ding ,FengLiu, "The Improvement of LEACH Protocol in WSN," IEEE International Conference on Computer Science and Network Technology 2011
[10] Baiping Li1 and Xiaoqin Zhang, "Research and Improvement of LEACH Protocol for Wireless Sensor Network," 2012 International Conference on Information Engineering, Vol.25
[11] Abderrahim Beni Hssane, Moulay Lahcen, "Position-Based Clustering: An Energy-Efficient Clustering Hierarchy for Heterogeneous Wireless Sensor Networks," (IJCSE) Vol. 02, No. 09, 201
[12] Salem Hadim and Nader Mohamed. Middleware Challenges and Approaches for Wireless Sensor Networks. IEEE Computer Society, IEEE DS Online Exclusive Content, 2007
[13] Joao Girao, Dirk Westhoff, Einar Mykletun, and Toshinori Araki. Tinypeds: Tiny persistent encrypted data storage in asynchronous wireless sensor networks,2005
[14] Wikipedia. Wireless Sensor Network, 2007
[15] Yi Liu, Shan Zhong, Licai You, Bu Lv, Lin Du, "A Low Energy Uneven Cluster Protocol Design for Wireless Sensor Network," Int. J. Communications, Network and System Sciences, 2012
[16] Zhuang Jun, Qiang Chun-Xia and Feng Wan-li, "Research Of Cross-Layer And Multi-Hops Algorithm Based On Energy And Location" 2012 International Conference on Industrial Control and Electronics Engineering

