ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Vol. 4, Issue 8, August 2016

# An Implementation of Key Management Scheme for Securing Transmission over WSNs

Er. Gaikwad Priyanka Kiran[1], Er. Samarth Kapoor[2], Er. Avinash Bansal[3]

M.Tech Student, Dept. of C.S.E, SDDIET (Barwala), Kurukshetra University, Haryana, India

Asst. Professor, Dept. of C.S.E, SDDIET (Barwala), Kurukshetra University, Haryana, India

Asst. Professor, Dept of C.S.E, GNIT (Mullana), Kurukeshetra University, Haryana India

**ABSTRACT:** Leach was the first most routing protocol used clustering concept in wireless sensor networks (WSN). Leach algorithm re-clustering process play vital role to gather data in cycles known as round. During each round a specific percentage of total nodes are elected as cluster heads (CHs). Each node gets chance to become CH according to their probability in particular round. The proposed routing protocol increases the lifetime of network and allow CHs to transmit their gathered data to the Base Station (BS).The proposed routing protocol decreases energy dissipated per round, increases energy efficiency increases number of packet send to the base station and decreases cluster head elected per round. A key management scheme applied on proposed routing protocol so the proposed protocol is more secure.

**KEYWORDS:** Base Station(BS),Cluster Head(CH),Genetic Algorithm(GA), Wireless Sensor Network(WSN).

## I. INTRODUCTION

The name wireless sensor network (WSN) consists of three words wireless + sensor + network. Wireless having no wired connection, using wireless media for communication. Sensor device having some sensing capability, like sensing the humidity, temperature, movement etc. Network is a collection of nodes. Types of nodes like sensor, routers, printers etc. A WSN consists of a large number of sensor nodes in hundreds or thousands. Each sensor node consists of different components which work together to act like as sensor and can sense for some particular application. These units are:

**a) Sensing unit:** Which sense the events occurring around it.
**b) Processing unit:** Which computes the results based on the sensed information by sensing unit.
**c) Transmission unit:** Transmits the computed results to the base station.
**d) Mobility monitoring unit:** Monitors the mobility of node to check whether it is mobile or stationary.
**e) Position finding unit:** Finds the position of each node, which helps each node to calculate the distance from its neighbors.
**f) Power Supply unit:** Provide the energy to all other components of the sensor node.
**g) ADC:** Converts the alternate voltage to direct voltage.

To improve the quality of service each sensor node can communicate and coordinate with each other. Each sensor node has sensing, computation and communicational capabilities. Each sensor node has information which it sense and provided by its neighbors. The quality of result which is produced by the sensor node depends upon the above said utilities. The calculated result is then supplied to all its neighbors or to the base station. Base Station is a node which queries for data to sensor node and collects the result from the sensor node. A base station can be mobile or fixed.

## II. ROUTING PROTOCOL FOR WSNS

Routing techniques are required for sending data between the sensor nodes and base station for the communication. Different routing protocols are proposed for wireless sensor networks. Conventional routing protocols do not compatible with the present WSN requirements: Sensors have low battery power, limited memory. The routing tables rise up with the network size and don't support diffusion communication. [1]

**Characteristics of Routing Protocols**

- It should be specific to the application.
- It should be data centric.
- It should be capable to perform data aggregation function.
- It must optimally use network resources such as bandwidth, computation power, and battery power etc.
- It should be capable of providing certain level of QoS as application demanded by network.
- End to end delay must be less.
- The number of packets collisions should be minimum.

## III. CLASSIFICATION OF ROUTING PROTOCOLS

Three main classifications of routing protocols are:

1) **Proactive:** In the proactive routing protocol the routes from each node to the base station are predefined.

2) **Reactive:** Routes from each node to the base station are defined when there is a demand for the route.

3) **Hybrid:** Some routes are predefined and some are defined after the demand is raised.

Other general classifications are: Based on the structure of the network and Based on the operation of the protocols.

**1.1 Network Structure Based Protocols:** The network structure can play significant role in the operation of the routing protocol in WSNs. Most of the protocols that fall below network structure based category.

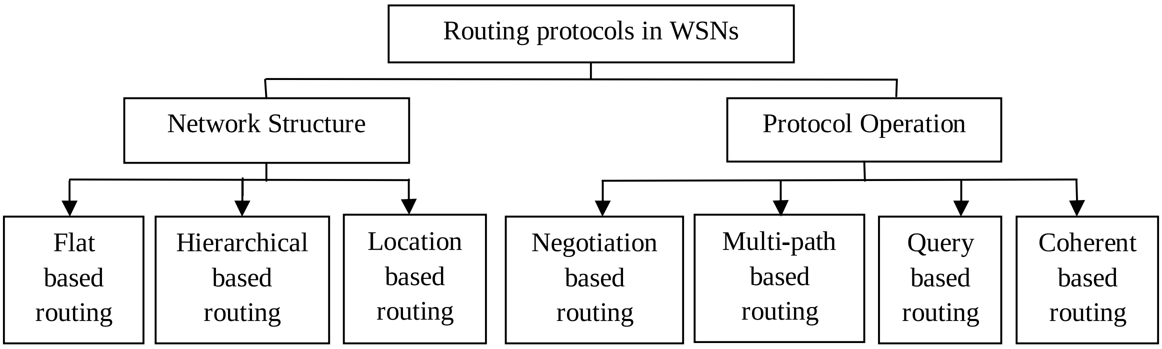


**Figure 3.1: Classification of Routing Protocol**

**3.1.1 Flat-based Protocols:** No global identification number assign to nodes due to less number of nodes present in network field. Every node plays same type of role. This protocol is also called data centric routing, the sink node transmits queries packet to certain regions and wait for reply.

**3.1.2 Hierarchical Protocols:** The main design concern for any WSN is scalability. Thousands of sensor nodes are present in the network. Sensor are not enough capable to communicate over large distance. Hierarchical routing works in two layers, first one is used for clustering and other layer used for routing. The nodes having low energy are used for sensing activity and high energy are used for processing and sending information to other nodes. It increases the network life time, energy efficiency, delay etc.

**3.1.3 Location Based Protocol:** This protocol finds the location of the sensor nodes depending upon the incoming signal strengths from source nodes. It generally tracks the location of nodes by using location of neighbor node and other is through GPS (Global positioning System).

**3.2 Routing Protocols based on Protocol Operation:** It should be noted that some of these protocols may fall below one or more of the above routing categories.

**3.2.1 Negotiation-based routing:** It is used for eliminating the redundant data transmission. This consumed more energy, battery power, communication power, memory etc. To overcome this problem negotiation based routing protocol is used, Sink or next node sends a negotiation messages before transmission begins.

**3.2.2 Multi-path based Protocols:** It uses multiple paths rather than single path for improving the WSN performance. For example the fault tolerance can be improved by maintaining multiple paths between the source and sink. It increases the cost of energy consumption and generates more traffic. The alternate paths are kept alive by sending periodic signals.

**3.2.3 Query based protocols:** The destination Sensors nodes propagate the query for data from a node through the network. A node having same data sends back reply message to the initiate's node. This sort of query used natural language and high level query language.

**3.2.4 Coherent Protocols:** The local data handling on the nodes can be differentiating between the coherent (minimum processing) and the non-coherent (full processing) routing protocols. The data is forwarded to sink node after minimum processing like time stamping, duplicate suppression etc. when all source nodes sends their data to sink at the same time, large amount of energy consumed. To overcome this problem limited number of source nodes sends data to sink node.

## IV. REVIEW OF LITERATURE

In WSN, sensor nodes are independent tiny devices. Each of them has individual battery and hardware. This leads to constraints; first one is energy and second is physical size. Once a node is deployed in a network, the battery is not rechargeable in many applications. The battery has to serve the lifetime of a node for all functions. As a result, reasonable energy consumption is very important for a sensor node and it affects the overall performance of the whole network. Then the physical size and prize of the node device decide it could not have large and expensive chips[2].

However, a sensor node built on an embedded system has three functions: sensor interface, data processing and network interface. A sensor node has to carry out all these functions with limited hardware. The processor also requires energy too. The network interfaces provide standardized functions such as passing messages, connecting and disconnecting etc [3].

In the other hand, all nodes in a WSN communicate with each other by radio channel which is open and can be accessed by anyone in the same range. This makes a great challenge for security. In addition, WSN can be deployed in different environment depend on different applications. The entire network is affected by this environment condition. Moreover, due to unreliable channel and severe environment, there are much more packet loss and fault in WSN than traditional networks. Security maintains is great challenge in the network.

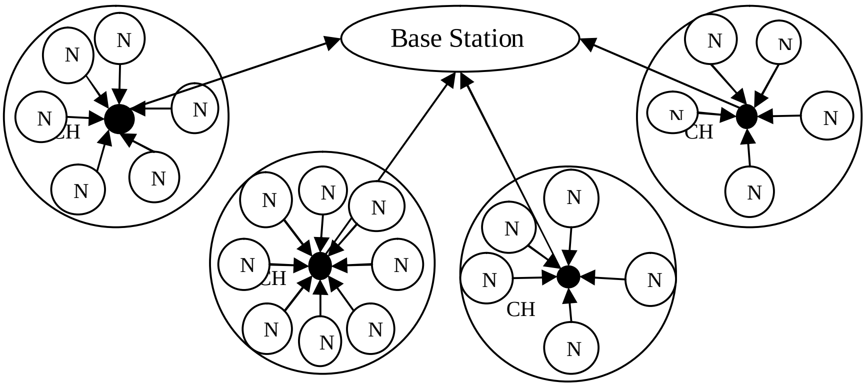


**Figure 4.1: Model of Wireless Sensor Networks**

Cryptography is the process of hiding and protecting information using encoding and decoding mechanisms. In general, there are two types of cryptosystems:

**1. Symmetric (private) key cryptosystems.**
**2. Asymmetric (public) key cryptosystems.**

**1. Symmetric (private) key cryptosystems,** a single key between two communicating parties is used for the encryption and decryption of a message. The symmetric key algorithms are having a big disadvantage that once the attacker is able to compromise a single node, he would be able to have the control of overall communication because he get the control of overall network. If the network is retried to be rekeying then it increases the cost over energy which is ultimately increases the energy dissipated in the process and makes the network objectives fail.

**2. Asymmetric (public) key cryptosystems,** which uses pairs of keys: public key and private key. In a public key encryption system, any person can encrypt a message using the public key of the receiver, but such a message can be decrypted only with the receiver's private key.

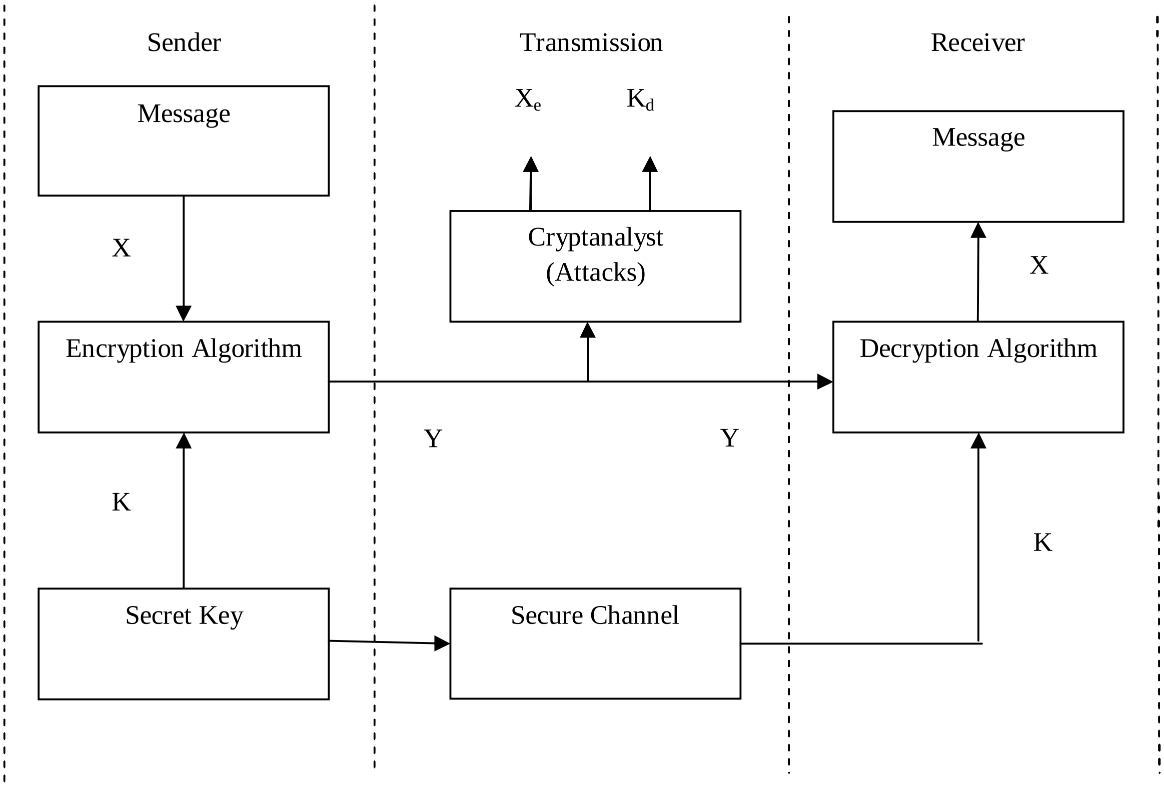


Figure 2.3: Model of symmetric encryption

**Definition and Goals of Cryptography**
Cryptography is a study of techniques (called cryptosystems) that are used to accomplish the following four goals: Confidentiality, Data Integrity, Authentication and Non-repudiation. A study of techniques used to break existing cryptosystems is called Cryptanalysis. Since cryptography and cryptanalysis are greatly dependent of each other, people refer to Cryptology as a joint study of cryptography and cryptanalysis. Four goals of cryptography:

**Principles of Encryption**
The basic idea of Encryption is to modify the message in such a way that only a legal recipient can reconstruct its content. A discrete-valued cryptosystem can be characterized by:
**A set of possible plaintexts, P.**
**A set of possible ciphertexts, C.**
**A set of possible cipher keys, K.**

DOI: 10.15680/IJIRCCE.2016. 0408054

**A set of possible encryption and decryption transformations, E and D.**

An encryption system is also called a cipher, or a cryptosystem. The message for encryption is called plaintext, and the encrypted message is called ciphertext. Denote the plaintext and the ciphertext by P and C, respectively. The encryption procedure of a cipher can be described as:

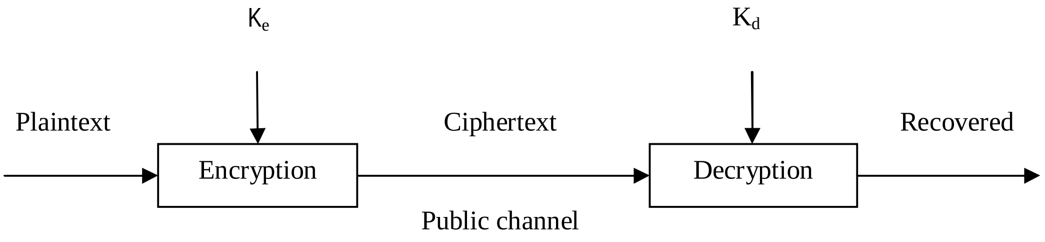


**Figure 4.2 : Encryption/decryption of a cipher**

$C = E_{Ke}(P)$

Where $K_e$ is the encryption key and E is the encryption function. Similarly, the decryption procedure is defined as:

$P = D_{Kd}(C)$

Where $K_d$ is the decryption key and D is the decryption function. The security of a cipher should only rely on the decryption key $K_d$, since adversaries can recover the plaintext from the observed ciphertext once, it gets $K_d$.

**Encryption Classification Algorithm**

Encryption algorithms, also called ciphers, can also be classified by different ways, such as with respect to the structures of the algorithms, or with respect to keys, or with respect to the approach in constructing the scheme, or with respect to the percentage of the data encrypted.

**a. Classification according to encryption structure**

Encryption algorithms can be classified according to encryption structure into block ciphers and stream ciphers. A block cipher is a type of symmetric-key encryption algorithm that transforms a fixed-length block of plaintext data into a block of ciphertext data of the same length. The fixed length is called the block size, and for many block ciphers, the block size is 64 or 128 bits. The larger the block size, the more secure the cipher, but the more complex encipher and decipher algorithms and devices. Typical block ciphers include DES, Triple TDES, RC5, RC6, Blowfish, IDEA and Rijndael. Some of them have become standard cipher lately. Modern block ciphers have the following features:

1. Variable key length.
2. Mixed arithmetic operations, this can provide non-linearity.
3. Data-dependent rotations and key-dependent rotations.
4. Lengthy key schedule algorithm.
5. Variable plaintext/ciphertext blocks length and variable number of rounds.

**b. Classification according to keys**

According to keys, there are two kinds of ciphers following the relationship of $K_e$ and $K_d$. When Ke¼$K_d$, the cipher is called a private-key cipher or a symmetric cipher. For private-key ciphers, the encryption/decryption key must be transmitted from the sender to the receiver via a separate secret channel. When $K_e$ 6¼$K_d$, the cipher is called a public-key cipher or asymmetric cipher. For public-key ciphers, the encryption key $K_e$ is published and decryption key $K_d$ is kept to private for which no additional secret channel
is needed for key transfer.

### Genetic Algorithm

In GA nodes initialize as pollution by opting genetic behavior, best fitness function result is considered as best pollution, to calculate fitness value three steps (crossover, mutation, selection) are repeated for particular number of generations to find  local solution. It is best in case when we have two options for a solution.

### Basic terminology used in Genetic Algorithm

- **Chromosome:** It is a set of genes that contains the solution in the form of genes. For e.g. 98150 is a chromosome value then 9,8,1,5 and 0 are its genes.
- **Population:** The total number of individuals or chromosome with same number of genes.
- **Fitness:** It is a value that assigned to an individual based on readiness of an individual to provide solution. Greater the fitness value, more appropriate solution will obtained.
- **Fitness function:** It is an application oriented objective function which assigns fitness value to the individual.
- **Crossover:** Taking two fit individuals and then performs process to generate new two individuals.
- **Mutation:** It is a process of changing random genes in an individual value.
- **Selection:** The process of selecting individual to generate the new generation.

### Fitness function computed from following equation

$$F_{ij}^{d} = G(t)\left(\frac{M_{pi}(t)*M_{aj}(t)}{R_{ij}(t)+\epsilon}\right)\left(x_j^d(t) - x_i^d(t)\right)$$

$F_{ij}^{d}(t)$is the force acting on agent i from agent j at$d^{th}$ dimension and $t^{th}$ iteration. $(t)$ is the computed gravitational constant at the same iteration while ∈ is a small constant.$R_{ij}(t)$is the Euclidian distance between two agents i and j at iteration t.

### Best fitness function computed as follow

Minimization Problems

$best(t)$= $min fit_j(t)$ $j\epsilon(1 \ldots \ldots \ldots N)$
$worst(t) = max fit_j(t)$ $j\epsilon(1 \ldots \ldots \ldots N)$

Maximization problems
$best(t) = max fit_j(t)$ $j\epsilon(1 \ldots \ldots \ldots N)$
$worst(t) = min fit_j(t)$ $j\epsilon(1 \ldots \ldots \ldots N)$

$fit_j(t)$Represents the fitness values of the $j^{th}$agent at iteration t, best (t) and worst (t) represents the best and worst fitness at iteration t.

### Energy consumption model

WSN use an energy attenuation model depending on the distance value between two nodes (Sender and Receiver). The transmitter transmits k bits data to another node, d  is the meter distance between two nodes.

### The energy consumption calculation formula

$$E_{TX}(k,d) = \begin{Bmatrix} kE_{ele} + kE_{fs}d^2 & d < d_0 \\ kE_{ele} + kE_{mp}d^4 & d \geq d_0 \end{Bmatrix}$$

$$E_{RX}(k) = kE_{ele}$$

$$E_{DA}(k) = kE_{da}$$

$E_{mp}$Is multipath length energy value for transmission data,$E_{fs}$ is for fixed path length energy value for transmission, $E_{da}$is the energy consumption used to compressed data unit. $E_{TX}$is transmission energy of sender, $E_{RX}$ is received energy of the receiver, $d_0$ is the critical distance between two nodes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Vol. 4, Issue 8, August 2016

## V. RESEARCH METHODOLOGY

There are basically two types of algorithms in wireless sensor networks cluster based and non cluster based. In non cluster based protocols every node is in direct communication with the base station. Each node sense its environment for which it is deployed, compute the result and send the result to base station based on the query which is broadcasted by the base station. On the other hand, in cluster based algorithms, the network is divided into clusters, and nodes elect the cluster heads, every non cluster head node is responsible for sensing and computation, after computation the result is send to the cluster head. [4]

### 5.1 Proposed Algorithm

1. Generate the Initial Population.
2. Initialize the iteration variables.
3. Key pre-distribution phase.
4. Authentication and key establishment scheme based on Diffie-Hellman algorithm.
5. Compute the fitness function f(x) for each cluster selected to communicate.
6. Finding the best nodes having the best fitness value.
7. Denote these best nodes as cluster heads and start the communication.
8. After the completion of the communication cycle, go to step 6. This process continues till the entire network nodes die or all nodes have zero power.
9. Plot the result graphs from the generated data by the sensor node performance parameters and data information collected during the simulation.
10. The following parameters are compared:
    i. Network lifetime.
    ii. Security Analysis and comparison with the existing technique.
    iii. Number of nodes died vs. time.
    iv. Number of packets sent to base station.
    v. Number of cluster heads selected.
    vi. Energy consumption per second.

### 5.2 Objectives of Proposed Work

The scope and objective of this proposed research is the design and development a WSN routing protocol that can be implemented on existing WSN infrastructures and which exhibits the following criteria:

- Uses the optimization technique to optimize routing.
- Uses Diffie Hellman basic model and with Elliptic Curve method to get the best out of these.
- Energy Efficiency is achieved not only by reducing the complexity but also at the routing level.
- The assumption made for the attack used the same node compromise attack model of WSN security.

## VI. RESULTS AND DISCUSSIONS

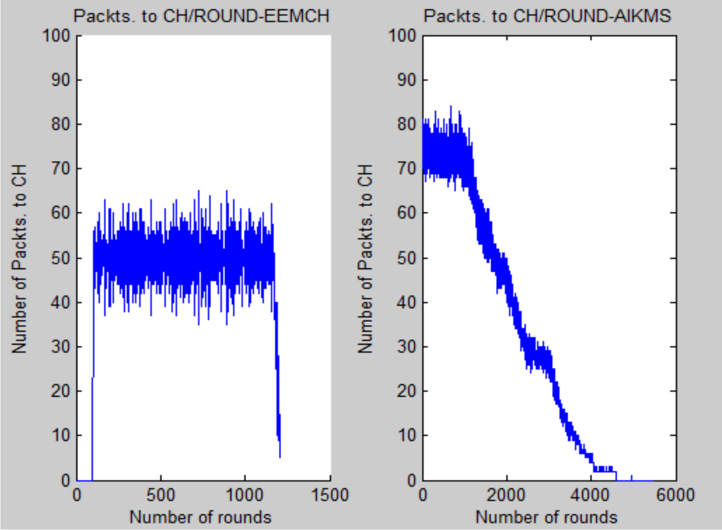
The proposed routing protocol is simulated using MATLAB tool. Experiments are performed on simulations with different numbers of sensor nodes uniformly distributed in a 100 m×100 m. Base station is located at position [50,50].

| Max_Round | No of Max Round | 5498 |
|---|---|---|
| $E_0$ | Initial energy of each node | 0.5 nJ |
| $E_{TX}$ | Energy for transferring of each bit (ETX) | 50 nJ/bit |
| $E_{RX}$ | Energy for receiving of each bit(ERX) | 50 nJ/bit |
| $E_{fs}$ | Energy of free space model | 10e-12 J/bit |
| $E_{mp}$ | Energy of multi path model | 1.3e-15J/bit |
| $E_{DA}$ | Data aggregation energy | 5e-9 J/bit |

**Table 6.1: Simulation Parameters**

### 6.1 Packets to Cluster Head per Round

Each non cluster head nodes send data in the form of tiny packets. The graph (fig 6.1 (a)) represents in EEMCH scheme at 1000 rounds approximate 60 packets sends to cluster head but in proposed AIKMS scheme at 1000 rounds approximate 75 packets sends to cluster head after that proposed graph is stable up to the 4500 rounds so the lifetime of network is increases. We can see this value in fig 6.1(b).

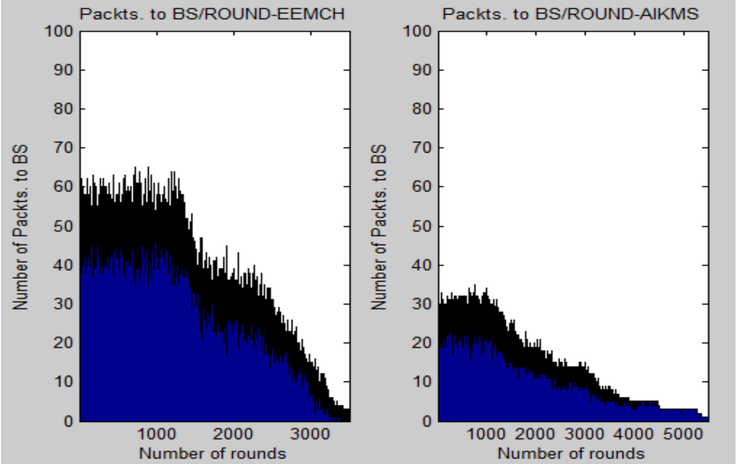


6.1(a) 6.1(b)

Figure 6.1 Packets to cluster heads

### 6.2 Packets Send to Base Station per Round

After all non cluster head nodes have send their data to the cluster head nodes. A node should transmit maximum number of packets to BS before energy of all nodes goes down. The graph (fig 6.2 (a)) represents in EEMCH scheme at 1000 rounds approximate 60 packets sends to base station but in proposed AIKMS scheme at 1000 rounds approximate 30 packets sends to base station but in figure 6.1(a) represent the network live is just up to 3000 rounds but in proposed AIKMS scheme network live up to 5000 rounds.



6.2(a) 6.2(b)

Figure 6.2: Packets sent to base station

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

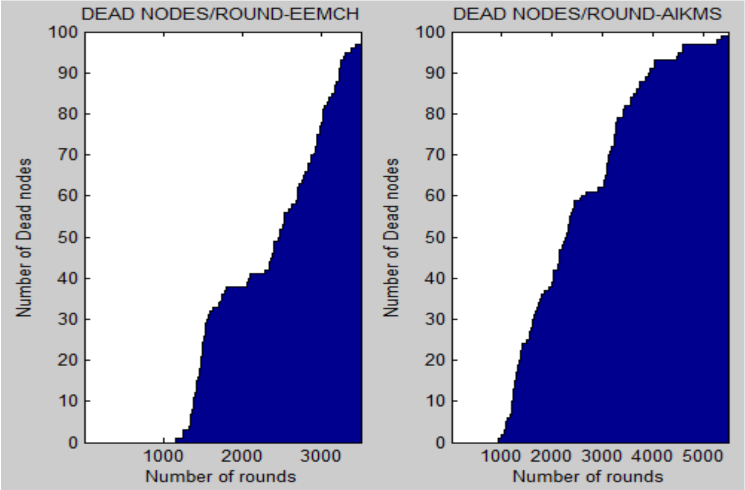
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

### 6.3 Number of Dead Nodes per Round

Thetime from beginning of transmission to first node dies is the stability period of the network and time when all nodes have died describes the overall lifetime of the network. The graph (fig 6.3 (a)) represents in EEMCH scheme at 1000 rounds approximate 40 dead node andin proposed AIKMS scheme at 1000 rounds approximate 38 dead node. Figure 6.3(a) represent the network live is just up to 3000 rounds but in proposed AIKMS scheme network live up to 5000 rounds.

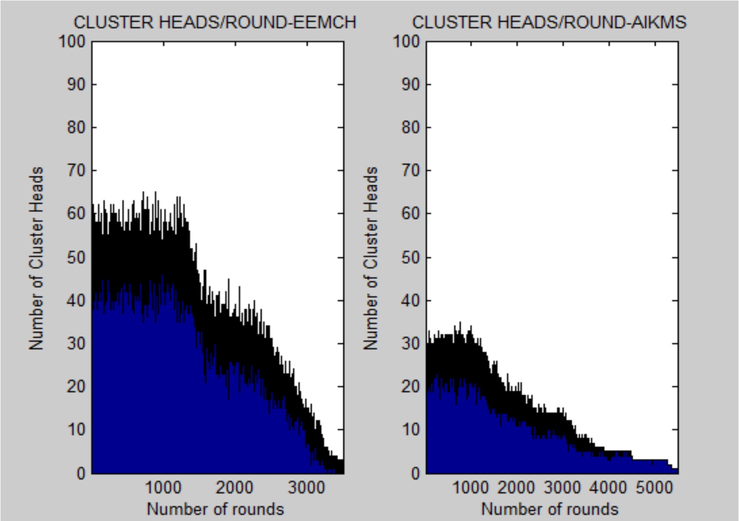


6.3(a) 6.3(b)

Figure 6.3 Number of dead nodes

### 6.4 Number of Cluster Heads Elected per Round

When the new round begins new cluster heads are elected. If number of cluster heads is large more energy will be consumed. The graph (fig 6.4 (a)) represents in EEMCH scheme at 1000 rounds approximate 60 cluster head elected but in proposed AIKMS scheme at 1000 rounds approximate 30 cluster head elected. So the proposed routing protocol increases enegy efficiency. So we can see this value in figure 6.4(b).



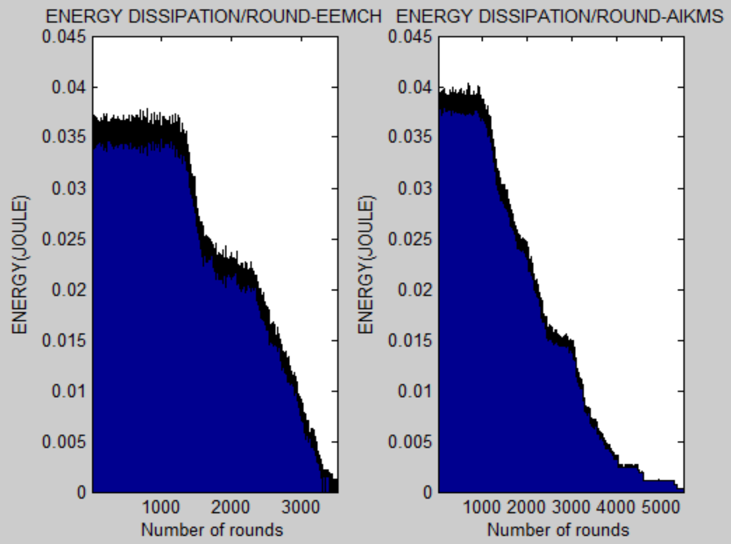
6.4(a) 6.4(b)

Figure 6.4: Number of Cluster heads

DOI: 10.15680/IJIRCCE.2016. 0408054

### 6.5 Energy Dissipated Per Round

Energy dissipation is an important factor in determining the performances of the network.The graph (fig 6.5 a)) represents in EEMCH scheme at 2000 rounds approximate 0.0225J energy dissipated but in proposed AIKMS scheme at 2000 rounds approximate 0.0205J energy dissipated. So the proposed routing protocol decreases enegy dissipated per. So we can see this value in figure 6.5(b).



6.5(a) 6.5(b)
Figure6.5:Energy Dissipated Per Round

## V. CONCLUSION

Simulation results are studied and analyzed and provides us the information about the performance comparisons of the proposed protocol is an implementation of key management scheme (AIKMS) with the base paper protocol is energy efficient key management scheme for clustered hierarchical(EEMCH). During the simulation firstly the number of nodes are not fixed, i.e. simulation can be done in the limits provided by the Matlab programming for the number of elements in an array. For lower number of nodes the partitions cannot be obtained because, in these cases the Matlab generates an error. The scenario replicates the communication pattern of actual wireless sensor network. The authentication check step is done at the time of selection of cluster heads, if the nodes have the desired key only then it is allowed to be a cluster head. Only cluster heads take the data to the base station which saves the energy of other nodes. At a time, multiple nodes communicate through multiple paths. The energies confirm the hardware standards set for the wireless sensor which helps to have the nearly same results of simulations as that of hardware. Due to random election each node goes through the selection process. No fix area or number of cluster heads. Network lifetime is increased up to desired levels. The proposed routing protocol increases the energy efficiency.

## VI. FUTURE WORK

Wireless sensor network is build with the nodes with limited energy resources, which limits the lifetime of the network, and a major constrain to WSN. To cope up with such types of constrains researchers put many effort to design protocols for WSN which helps to increase the lifetime of the network and increase the stability period of the network. The protocols discussed in this paper are also proposed by means to increase the energy capacity of the network, but these protocols can be further improved to maximize the packet transfer rate.

Further efforts can be made to improve the stability period of the network, which is a period from the starting to the time when first node dies, by inhibiting the nodes to die instantly. The protocol which takes care of the time which is between the two nodes die, another stability line can be added to the graph which is near the x-axis. Energy dissipated per round can be minimized, hence more reliable protocols can be proposed.

## REFERENCES

[1]BhushanSharma,Harish Kumar Saini and AvinashBansal,"Energy Efficient A-Leach Routing Protocol","IJIRCCE" volume 4, Issue 5, May 2016.
[2] Rathna and Sivasubramanian, "Improving Energy Efficiency in Wireless Sensor Networks through Scheduling and Routing", Research Scholar, Sathyabama University, TamilNadu, India, International Journal of Advanced Smart Sensor Network Systems, vol: 2, pp: 21-27, January 2012.
[3] Honey Soni, PriyankaTripathi and Robin Singh Bhadoria, "An Investigation on Energy Efficient Routing Protocol for Wireless Sensor Network", Computational Intelligence and Communicational network, vol: 7, pp: 141-145, Sept 2013.
[4] LaveenaMahajan "Improving the Stable Period of WSN using Dynamic Stable Leach Election Protocol" Issues and Challenges in Intelligent Computing Techniques (ICICT), vol-11, pp: 393-400, 2014.
[5] S. Lindsey, C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems", published in: IEEE Aerospace Conference Proceedings, 2002, Vol: 3, pp: 1125-1130.
[6] M. Chu, H. Haussecker, and F. Zhao, "Scalable Information-Driven Sensor Querying and Routing for ad hoc Heterogeneous Sensor Networks, "published in The International Journal of High Performance Computing Applications, Aug 2002, Vol: 16, pp: 106-109.
[7] Smaragdakis. Georgios. Ibrahim Matta. And AzerBestavros. "SEP: A stable election protocol for clustered heterogeneous wireless sensor networks", Boston University Computer Science Department, pp: 223-230, 2004.
[8] Yuhua Liu Yongfeng Zhao JingjuGao "A New Clustering Mechanism Based On LEACH Protocol", International Joint Conference on Artificial Intelligence (IEEE), Hainan, pp: 715-718, April 2009.
[9] BhaskarKrishnamchari, Deborah Estrin, "Impact of Data Aggregation in WSN", IEEE Journal Selected Areas in Communications, pp: 1333-36, Aug 2009.
[10] Shio Kumar Singh, M P Singh, D K Singh, "A Survey of Energy-Efficient Hierarchical Cluster-Based Routing in Wireless Sensor Networks", International Journal.of Advanced Networking and Applications, vol: 02, pp: 570-580, 2010.
[11] Ma Chaw Mon Thein, ThandarThein "An Energy Efficient Cluster-Head Selection for Wireless Sensor Networks" , International Conference on Intelligent Systems, Modeling and Simulation (IEEE), vol: 8, pp: 287-291, Jan 2010.
[12] Linlin Wang, JieLiu, Wei Wang "An Improvement and Simulation of LEACH Protocol for Wireless Sensor Network", First International Conference on Pervasive Computing, Signal Processing and Applications (IEEE), pp: 444-447, Sept 2010.
[13] Yun Li, Nan Yu, Weiyi Zhang, Weiliang Zhao, "Enhancing the Performance of Leach Protocol for WSN", IEEE INFOCOM, pp: 223-228, 2011.
[14] VivekKatiyar, Narottam Chand, Gopal Chand Gautam, Anil Kumar "Improvement in LEACH Protocol for Large-scale Wireless Sensor Networks", (IEEE),vol: 32, pp: 1070-1075, Mar 2011.
[15] ReetikaMunjal, Bhavneesh Malik "Approach for Improvement in LEACH Protocol for Wireless Sensor Network", Second International Conference on Advanced Computing & Communication Technologies (IEEE), pp: 517-521, Jan 2012.
[16] Shijun He, Yanyan Dai, Ruyan, "A Clustering Protocol for Energy Balance of WSN based on Genetic Clustering Algorithm", International Conference on Future Supported Education, pp: 788-793, 2012.
[17] Fuzhe Zhao, You Xu, Ru Li, "Improved Leach Communication Protocol for WSN", International Conference on Control Engineering and Communication Technology, pp: 700-702, 2012.
[18] Yamunadevi, S.P, "Efficient Comparison of Multipath Routing Protocols in WSN", Computing Electronics and Electrical Technologies (ICCEET), vol: 2, pp: 807-811, Mar 2012.
[19] JiaXu, Ning Jin, Xizhong Lou, TingPeng, Qian Zhou, Yanmin Chen, "Improvement of Leach Protocol for WSN", Fuzzy System and Knowledge Discovery (FSKD), vol: 11, pp: 2174-2177, May 2012.
[20] M MIslaml, M A Matin2, T K Mondol l "Extended Stable Election Protocol (SEP) for Threelevel Hierarchical Clustered Heterogeneous WSN", (IEEE), vol: 5, pp.: l-4, June 2012.