International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 5 52 - 58

Secure Data in Low Power Cluster Based WSN Using Bioinspired Routing

Ms. Dipawali Nerkar
Department of Computer Science & Engineering
Nagpur Institute of Technology
RTMNU University, Nagpur, India
deepa11879@yahoo.com,

Prof. Jagdish Pimple
Department of Computer Science & Engineering
Nagpur Institute of Technology
RTMNU University, Nagpur, India
pimplejagdish@gmail.com,

***Abstract*—**Wireless sensor networks (WSNs) created by number of sensor nodes in order to sense and sending data from its enclosing atmosphere. The sensor nodes have limited computation ability, partial power and little memory size. In these networks, sensor nodes are needy on short power batteries to give their energy. As energy is a difficult problem in these networks. We first introduce secure and efficient bioinspired Cost-Aware Secure Routing (CASER) protocol by selecting cluster head and using genetic algorithm for transferring the data in sensor network. We also provide a calculable security analysis on the proposed routing protocol. In this we introduced bioinspired CASER protocol which provides good deal between routing efficiency and energy balance, and much increases the lifetime of the sensor networks in all sides. For the random energy delivery, our analysis shows that we can increase the lifetime and the total numbers of messages that can be send many times under the same assumption. In introduced bioinspired CASER protocol, we show that it can produce a high message delivery

Keywords- *WSNs, CASER, Genetic algorithm, clustering, AES algorithm, energy, efficiency*

*****

I. INTRODUCTION

In the modern technical developments make wireless sensor network (WSNs) technically and economically reasonable to be widely used in military and resident applications. Characteristicof such networks is that each network contains large number of free and neglected sensor nodes. In that type of nodes often contain very few and non- restorable energy resources, therefore in that situation, energy is very important design issue for these networks. Less energy reduction for message delivery and have the good message delivery ratio provided by a well-designed routing protocol which increases the sensor network lifetime and also manage total sensor network energy reduction. Now a day, WSNs make advance technically and economically. In design WSNs, Routing is another very challenging task.

Another issue in WSNs is wireless communication which is done by a broadcast medium. It is very important for security. Other possible issue is jamming and traceback attack. To solve all that issue, **we** propose a bioinspired based secured and efficient cost aware secure routing protocol (CASER) for WSNs. CASER allow message to be transmitted using two strategies : random walking and deterministic routing for same framework. These strategies are implemented by using specific security requirement. Two major advantages of CASER protocol are: (I) it help to balanced energy consumption of the entire sensor network which increases the lifetime of WSNs. (II) Based on routing requirement that containing fast/slow message delivery and secure message delivery to protect routing from traceback attack and malicious traffic jamming attack in WSNs, CASER protocol support many routing strategies Most important approach of this paper can be defined as follows:

1)A secure and capable Cost-Aware Secure Routing (CASER) protocol for WSNs, helpful to maintains the message delivery requirements.

2) Clustering is the best solutions to reduces the number of network's inner transmission wireless sensor network.

3) The proposed ,genetic algorithm based on clustering which give best chance for guess to get good presentation in terms of lifetime of network in wireless sensor networks.

II. LITERATURE SURVEY

In WSNs due to the limited resources, routing is a challenging task. Geographic routing is widely used and it is very promising approaches for WSNs. To route data packets hop-by-hop from the source to the destination geographic routing protocols collect the geographic location information .The source node select the immediate neighboring node to send the message based on the direction or the distance .The distance between the neighboring nodes can be calculated by signal strengths or using GPS equipment . The relative location information of neighbor nodes can be swap between neighboring nodes.

In a geographic adaptive fidelity (GAF) routing scheme was proposed for sensor networks equipped by low power GPS receivers. In GAF, the area of network is distributed into fixed size virtual grids. In every grid, only one node is choose as the active node, at that time, the others will sleep for a period to save energy. The sensor sends the messages support on greedy geographic routing strategy. Instead of using flooding, a query based geographic and energy aware routing (GEAR) was proposed for the sink node disseminates requests with geographic attributes to the target region. Based on estimated cost and learning cost. Each node forwards messages to its neighboring nodes. The expected cost assume for the distance to the destination and the remaining energy of the sensor nodes. At that time, the learning cost helps for updating information to deal with the local minimum problem. [11]

Di Tang et al [1] were proposing CASER Protocol introduce for Wireless Sensor networks. In this method, they proposed to

increases the energy as well as lifetime of sensor nodes in the WSNs.

Ameer A.Abbasi [2] offered a method for a failure of nodes may cause the network to partition into blocks. It is very effective recovery scheme to separately reposition a subset of the lead nodes to return connectivity. Recovery schemes either require high node moving overhead. To solve these problem and presents a Least-Disruptive topology Repair (LeDiR) algorithm. LeDiR relies on view of a node concerning the network to request a revival plan that relocates the least number of nodes and conform that no path between any pair of nodes is absolutely G. Wang[3] Sensor placement is a main problem in designing sensor networks. This check a distributed sensor Protocols for mobile sensors. Later than determining coverage holes the protocols calculate the location of sensors where they should shift. The protocols support high coverage within a limited placement time and limited movement. Voronoi diagrams used to find out the reporting holes and plan three movement-assisted sensor deployment protocols, VEC (VECtorbased), VOR and Minimal based on the principles of moving sensors from tightly positioned areas to lightly positioned areas.

S.Yang,[4] proposed the ability of sensor networks which depends on the coverage of the monitoring area. The good sensors placement is very important for balancing the workload of sensors. The placement of shift helped sensor deals with moving sensor deals from an unbalanced state to a balanced state. The various optimizations difficulty can be faced to reduce dissimilar parameters, plus total moving distance, total number of moves, communication cost, and meeting rate. The SMART is developed to use scan and measurement swap to get a stability state and to address a only one of its kind problem called communication holes in sensor networks. Broadly studied area in WSNs is lifetime. In a routing scheme was proposed to instead of always selecting the lowest energy path to find the secondary - best path that can expand the lifetime of the WSNs. In the introduced method, by a reactive protocol such as AODV or directed diffusion, multiple routing paths are set ahead. After that routing method will select a path based on a probabilistic method according to the remaining energy.

In Chang and Tassiulas [5] supposed that the source power level can be changed according to the distance between the source and the destination. Routing was created as a linear programming problem of neighboring node selection to maximize the network lifetime.

Then Zhang and Shen [5] examined the unbalanced energy consumption for regularly arranged data gathering sensor networks. In this proposed, the network is partition into many corona zones and each node can perform data aggregation. A localized zone-based routing scheme was suggested to stability energy consumption among nodes within each corona.
In this paper, **we** introduced a secure and efficient Cost-Aware Secure Routing (CASER) protocol that can tackle energy balance and routing security simultaneously in WSNs. In CASER protocol, each sensor node needs to remain the energy levels of its immediate neighboring grids in addition to their relative locations. From this information, every sensor node can produce varying filters based on the supposed design trade-off between securities and efficiency. In that, results shows CASER can offer brilliant energy balance and routing security and also show that the proposed secure routing can increase the message sending ratio due to decreased lifeless ends and loops in message forward. In this, **we** used Genetic algorithm and AES algorithm for design CASER protocol.

Many papers have shown the helpfulness of a Genetic Algorithm (GA) based method in sensor networks. **Our** proposed scheme assures that increases lifetime of network by using a Genetic Algorithm. **Our** work focused on finding an optimal solution to improve the lifetime of wireless sensor networks.

III. BASIC CONCEPTS OF WSN

Wireless sensor networks (WSN), is also called wireless sensor and actuator networks (WSAN).It consists of spatially allocated independent sensors to observe physical or environmental situation, such as temperature, sound, vibration, pressure, motion or impurity and to kindly pass their data through the network to a main location.

In wireless sensor networks (WSNs), all the data collected by the sensor nodes are forwarded to a sink node. Therefore, the location of the sink node has an unlimited influence on the energy consumption and lifetime of WSNs. sink node is work as a leader or base station in network.

Application of WSN:
1) Area monitoring
2) Health care monitoring
3) Environmental/Earth sensing
4) Air pollution monitoring
5) Forest fire detection
6) Landslide detection
7) Water quality monitoring

IV. MODULE

1. GENERATION OF WSN:

Sensor nodes have not only to send information to sink, but to swap data between themselves. That is why there are many method of organization of communication between sensor nodes in WSN. This is called network topologies methods. Network topologies in WSNs are: star, tree, mesh and random topology. Dissimilar WSN standards support different types of network topologies. In this model, we use 30 sensor nodes after that by applying random topology deployment of 0-29 nodes randomly in wireless sensor area.

Clustering

- Gateway: A gateway is a network point that acts as an entrance to another network.
- Cluster: A group of sensor node is called cluster.
- Cluster head: Cluster head is a node whose energy is maximum than all other node

By using a Genetic algorithm, the CASER protocol become superior and also increasing lifetime of network we used clustering method in genetic algorithm. In clustering method, sensor nodes are divided into many clusters and among of them two node is selected as cluster head which node has high energy in every cluster. Selection of a right cluster head improve the network life time. The node is stand for bit of a chromosome. The cluster head and ordinary nodes are signifying as 1s and 0s, in that order. In a population, there are consists of a number of chromosomes and the greatest chromosome is apply to produce the after that population which is based on the survival fitness. At first, every fitness parameter is giving a random weight; but after every creation, the fittest chromosome is calculated and the weights of every fitness parameter are updated as a result. The GA result recognizes suitable clusters for the network. The numbers of cluster heads are connected with each cluster head, and the number of communication is done. All the sensor nodes get the packets transmitted by the BS and clusters are generated as a result; thus implementation the cluster creation stage. This is go after by the data transfer stage by applying Genetic algorithm.

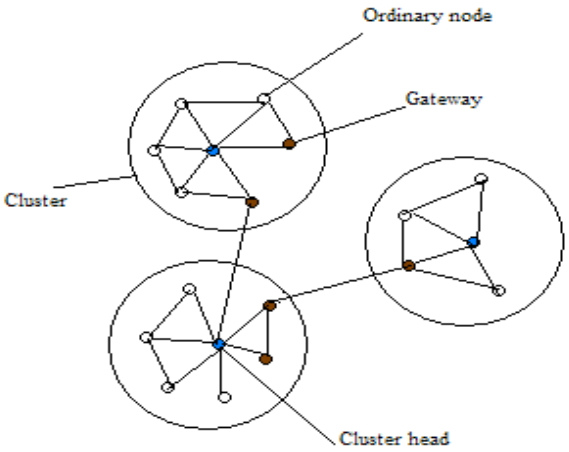

Fig.2. Clustered Architecture

By using this formula, **we** find out the cluster head, Cluster head will be the node whose energy is maximum than all other node. Every node has energy. Max function is used to find out maximum energy node from each cluster.

$$\text{Emax} = \max(\text{E1}, \text{E2} \ldots \text{E10}) \quad (1)$$

Where E1, E2…E10 has 10 node in one cluster with its energy.

2. IMPLEMENTATION OF GENETIC ALGORITHM:

Genetic algorithm (GA) is an arbitrary search and optimization technique which is broadly applies for solving optimization problems in which huge number of promising solutions. GA is supported survival of fittest theory. GA has a set of promising result called initial population which is generated randomly. Every individual solution is called chromosome. Each chromosome Length must be same. A fitness function calculates fitness value for each chromosome. Optimal solution is closer to chromosome high fitness value. For crossover two parent chromosomes are selected to produce two offspring. Mutation is used to randomly choose chromosome to get an improved solution. Crossover and mutation produce next population. In new generation, population selected little greatest fitness value of chromosome than previous population which selected value guarantee that the new generation is better fit as the previous. This entire process is repeated until some stopping criteria are not matched. Small energy efficiency in network which decreased generally lifetime of network .It is very huge and difficult task. We have to generate combinational method to improve and advance in the existing technique. To propose the genetic algorithm which provide the number of solution for packet delivery and giving data security.

Genetic algorithm operation:
Following operation is performed by genetic algorithm to find the path for sending packet on the basis of fitness survival theory.

i) Population Generation:
The WSN nodes are signifying as bits of a chromosome. Cluster Head and ordinary nodes are shows as 1s and 0s, respectively. Chromosome fitness is found by several parameters such as node density and energy consumption. A population made of several chromosomes and to generate the next population the best chromosome is used. For the first population, a huge number of arbitrary cluster heads are selected on the basis of survival fitness, the population make over into the upcoming generation.

Fitness Parameters
Chromosome fitness is proposed to reduce the energy use and to increases the network lifetime. Some fitness parameters are explained in this part.

a) Cluster Distance (C):
The sum of the distances from the nodes to the cluster head and the distance is cluster distance(C). For each cluster with k member nodes, the cluster distance C is defined
as follows:

$$\mathbf{C} = \sqrt{(\mathbf{x_2} - \mathbf{x_1})^2 + (\mathbf{y_2} - \mathbf{y_1})^2} (2)$$

Where x1, x2 is distance between node to cluster head in x direction and y1, y2 distance between nodes to cluster head in y direction. The cluster distance will be higher thus the energy consumption will be higher. For compact energy consumption, C should not be too high. This metric will control the size of the clusters.

b) Fitness Function:
In nature, a person's fitness is its capability to pass on its genetic material. This capability consists of quality that allows it to survive and further reproduce. In a GA, fitness is calculated by the function defining the problem. The chance of an individual chromosome depends on the fitness value. The possibility of survival is higher for improved fitness values. The chromosome fitness, F, is a function of all the above fitness parameters, this is defined as

$$F = \sum_{m=l}^{k-1} \frac{X * y}{C(m, m+1)}$$

Where m is node no, l is source node, k is destination node, x width and y is height.

ii) Selection:
In selection process, **we** decided which chromosomes from the current population will be crossover to make new chromosomes. These new chromosomes link with the surviving population. This collective population will be the beginning for the next selection. The individuals (chromosomes) with improved fitness values have more chances of selection. There are several selections methods, such as: roulette-wheel selection, rank selection and tournament selection. We used Rank selection, method in this paper. One chromosome is chosen at random from the population which has less fitness value as compared to mean fitness value.

iii) Crossover:
The most important step for generating a new generation is the crossover process. In fact, it is a recreation of the sexual reproductive procedure in that the inheritance attribute are obviously transferred into the new population. To produce new children, crossover process chooses a pair of individuals as parents .a children have some attribute from individuals parents. For all the solution where fitness value is less than mean fitness value, carry them forward for next iteration (population) this is called crossover.

iv) Mutation:
After crossover, discard all population whose fitness value is more than mean fitness values and replace them with other random population this is called mutation find out all iteration. At the end of kth iteration select the solution which has minimum fitness value. After that send the data though that path.

3. AES ALGORITHM MODULE:

AES is used for encryption as well as decryption. That always performed same steps for to complete both encryption and decryption in reverse order. AES is a private key symmetric block cipher algorithem.it is very fast and strong. Number of rounds depends on the key length.

Key length	Rounds
128	10
192	12
256	14

Table 1

i) Structure of AES:
AES encrypts all 128 bits of data in one round and each round consists of four layer.
1) Byte Substitution
2) Shift Row
3) Mix Column
4) Add Round Key

Last round does not have the mix column layer

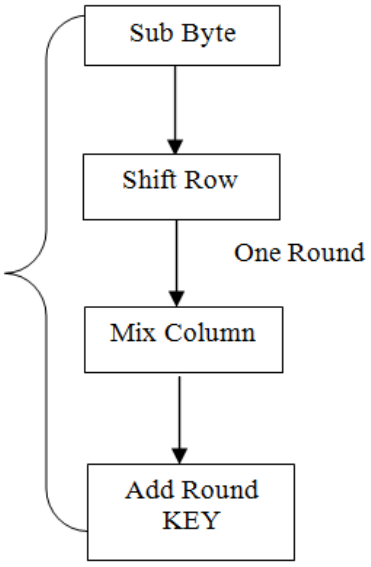

Fig 1. Details of each round

a) Byte substitution:
Each byte of a simple substitution provide a confusion

- A permutation containing 256 8-bit values which is used for one S-box of 16x16 bytes.
- By row (left 4-bits) & column (right 4-bits),each byte of state is replaced by byte indexed
- eg. Byte {31} is replaced by byte in row 3 column 1 which has value {C7}.
- S-box constructed using defined transformation of values in Galois Field- GF(2^8).

b) Shift Row:
Shifting, which permutes the bytes. A circular byte shift in each

- 1st row is unaffected
- 2nd row does circular shift to left by 1 byte
- 3rd row does circular shift to left by 2 byte
- 4th row does circular shift to left by 3 byte

The transformation is called ShiftRows, in the encryption,
The transformation is called InvShiftRows and the shifting is to the right, in the decryption.

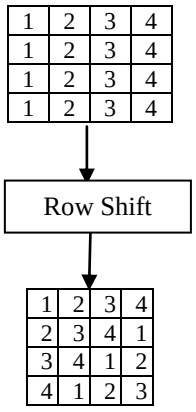

Fig 2: Shift Row

c) Mix column:
Shift Rows and Mix Columns provide diffusion to the cipher Each column is processed separately. A value dependent on all 4 bytes in the column replaced by each byte. Effectively a matrix multiplication in GF(2^8) using prime poly

$M(x) = x^8+x^4+x^3+x+1$

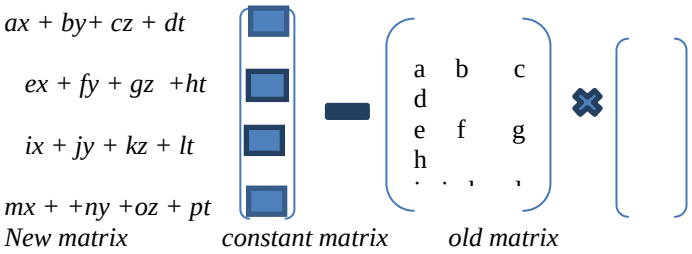

fig3. Mixing bytes using matrix multiplication

d) Add Round Key:
At a time one column is proceed in addroundkey. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition. The Add Round Key transformation is the inverse of itself.

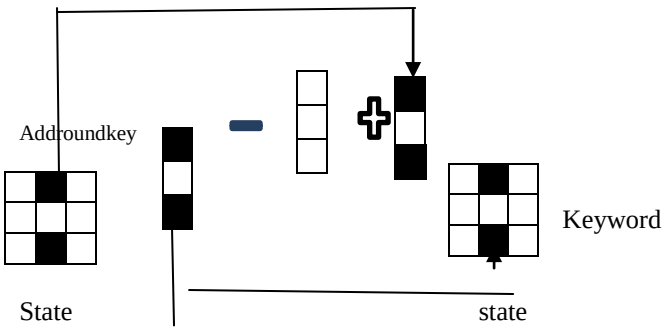

Fig.4.Add Round Key transformation

IV) INTEGRATION OF GENETIC ALGORITHM WITH AES MODULE:
In this module, we combine the genetic algorithm with AES Module for cost aware secure routing. Genetic algorithm find out secure path for sending data with increasing lifetime of network and AES algorithm sending and receiving data securely and reduces jamming and trace back attack

V.CONCLUSION AND FUTURE WORK

In this paper, we introduced a bioinspired cost aware secure routing protocol for wireless sensor network for stability of the energy consumption and raises network natural life. CASER has given to support routing method in message forwarding to enhance the lifetime at the same time as extending routing security. CASER shows that brilliant routing presentation in terms of energy balance and routing path sharing for routing path security. We also introduced an uneven energy position method to extend the sensor network lifetime. Our analysis and reproduction results show that enhance the lifetime and the many messages that can be forward under the uneven energy placement by other than four moments in times.
Future Scope:
1. To implement the system in real time with real nodes
2. To design the system for a specific application like military

VI.SIMULATION RESULT:

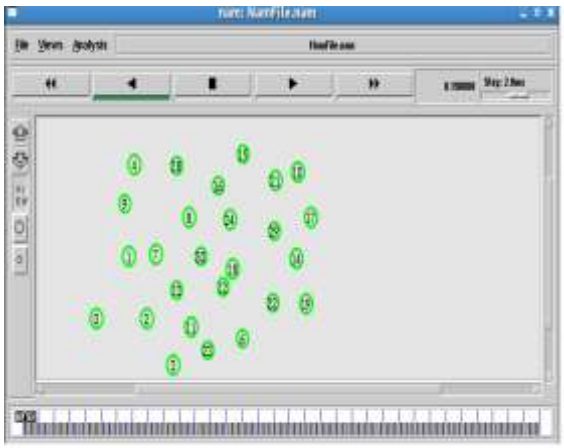

FIG 8.1: SCATTERED NODES IN THE NETWORK

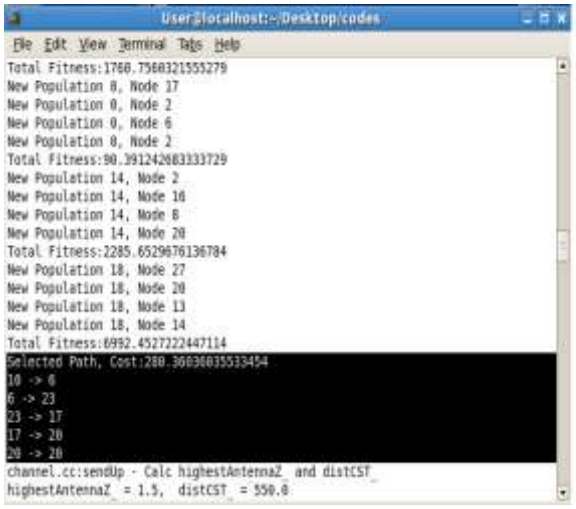

FIG 8.2:SELECTED PATH FOR COMMUNICATION

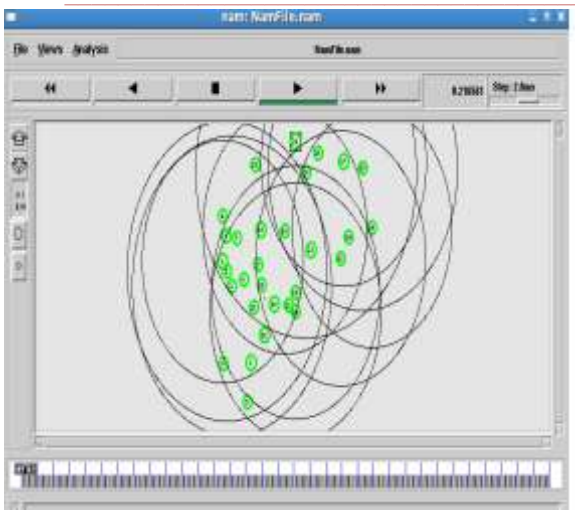

FIG 8.3: PATH SEARCHING FOR COMMUNICATION.

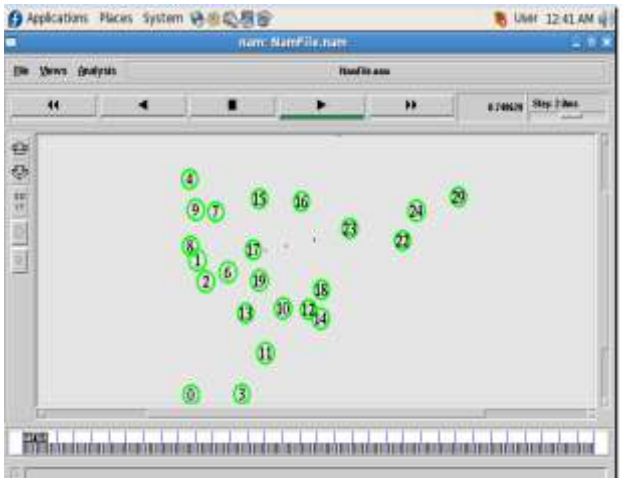

FIG8. 4: START COMMUNICATION 17 TO 23 NODES

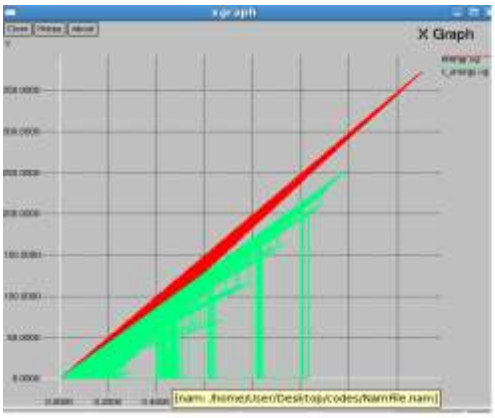

FIG.8.5 COMPARISON FOR CASER ENERGY AND WITHOUT CASER ENERGY

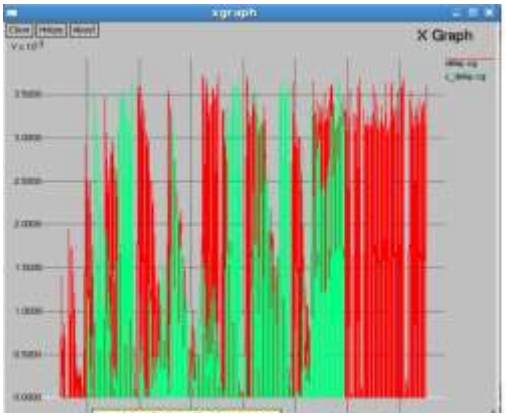

FIG.8.6 COMPARISON BETWEEN WITH CASER DELAY AND WITHOUT CASER DELAY

VII. REFERENCES

[1] Di Tang Tongtong Li Jian Ren and Jie Wu "Cost -Aware SEcure Routing (CASER) Protocol Design for Wireless Sensor Networks" IEEE Transactions on Parallel and Distributed Systems. 2015

[2] A. Abbasi, M. Youngish, and K. Akkaya,"Movement-assisted connectivity restoration in wireless sensor and actor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 9, pp. 1366-1379, Sep. 2009.

[3] G.Wang, G. Cao, and T. La Porta, "Movement-assisted sensor deployment," IEEE Trans. Mobile Comput., vol. 5, no. 6, pp. 640–652 Jun. 2006.

[4] S. Yang, M. Li, and J.Wu, "Scan-based movement-assisted sensor deployment methods in wireless sensor networks," IEEE Trans. Parallel Distrib.Syst., vol.18, no.8, pp.1108–1121, Aug.2007

[5] Z. Shen, Y. Chang, H. Jiang, Y. Wang, and Z. Yan,"A generic framework for optimal mobile sensor redeployment," IEEE Trans. Veh. Technol.,vol. 59, no. 8, pp. 4043–4057, Oct. 2010.

[6] C.V.Swathi1, Mrs.Nagarathna2, "Energy Efficient Routing Protocol with Secure Hash Algorithm for Multi Hop WSN," International Journal of Research In Science & Engineering Volume: 1 Special Issue: 2

[7] B.Sireesha1, G.TagoreSai Prasad2, "an alternative secured and efficient routing strategy for wireless sensor networks" (IJETER), vol. 3 no.6, (2015)

[8] Mrs. S. Gowsiga , Dr. P. Senthil Kumar " a review study of various routing protocols based on routing information update mechanism of mobile ad hoc networks"(IJERA) International Conference on Humming Bird (01st March 2014)

[9] Salonee Mishra and Binod Kumar Pattanayak "power aware routing in mobile ad hoc networks:a survey" vol. 8, no. 3, march 2013.

[10] Junmo Yang, Kazuya Sakai, Bonam Kim, Hiromi Okada, and Min-Te Sun "Cost-Aware Route Selection inWireless Mesh Networks"

[11] Anandhi.R, Dr.R.Manickachezian "A Review on Geographic Routing in Wireless Sensor Network" Vol. 2, Issue 7, July 2014.

[12] Roshni M. Bhave, Prof. Vijay Bagdi "Recovery of Nodes Failure in Wireless Sensor Network Using CASER Protocol and DARA:Review" Volume: 3 Issue: 2

[13] Sajid Hussain, Abdul WaseyMatin, Obidul Islam Genetic Algorithm for Hierarchical Wireless Sensor Networks" journal of networks, vol. 2, no. 5, september 2007

[14] P.D. Khambre,S.S.Sambhare, P.S. Chavan1 "Secure Data in Wireless Sensor Network via AES(Advanced Encryption Standard)" Vol. 3 (2) , 2012,3588-3592
[15] G. Hussein EkbataniFard, Reza Monsefi, Mohammad-R. Akbarzadeh-T, Mohammad H. Yaghmaee "A Multi-bjective Genetic Algorithm based Approach for Energy Efficient QoS-Routing in Two-tiered Wireless Sensor Networks" vol ,2010.
[16] Vipin Pala, Yogita, Girdhari Singh, R P Yadav , "Cluster Head Selection Optimization Based on Genetic Algorithm to Prolong Lifetime of Wireless Sensor Networks",ICRTC 2015.