



# ENERGY CONSUMPTION AND DATA AGGREGATION IN WIRELESS SENSOR NETWORK USING NS-2 SIMULATION

**Mohan Raj. C.R\***

PG Scholar - M.Sc. Information Technology  
Annamalai University, Chidambaram, Tamil Nadu, INDIA.

[crmohanraj35@gmail.com](mailto:crmohanraj35@gmail.com)

**Hashvant Vijay. B,**

UG Scholar - Department of Computer Science Engineering  
Rajalakshmi Engineering College, Chennai

[Karthivijay11@gmail.com](mailto:Karthivijay11@gmail.com)

**Haritha. R**

UG Scholar - Department of Computer Science Engineering  
Rajalakshmi Engineering College, Chennai

[harithanethra@gmail.com](mailto:harithanethra@gmail.com)

**Sumathy. V**

Assistant Professor (SG)- Department of Computer Science Engineering  
Rajalakshmi Engineering College, Chennai.

[sumathy.v@rajalakshmi.edu.in](mailto:sumathy.v@rajalakshmi.edu.in)

## Manuscript History

Number: IRJCS/RS/Vol.06/Issue07/JLCS10080

Received: 02, July 2019

Final Correction: 11, July 2019

Final Accepted: 20, July 2019

Published: July 2019

**Citation:** Mohan, Hashvant, Haritha & Sumathy (2019). Energy Consumption and data aggregation in Wireless Sensor Network Using NS-2 Simulation. IRJCS:: International Research Journal of Computer Science, Volume VI, 659-667. doi://10.26562/IRJCS.2019.JLCS10080

**Editor:** Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Copyright: ©2019 This is an open access article distributed under the terms of the Creative Commons Attribution License, Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited

**Abstract** - Energy consumption is a vital role in the resource constraint Wireless Sensor Network (WSN). To reduce energy consumption in WSN, duty cycle, energy optimized schedule, energy-aware routing and data aggregation are widely used. In this paper addresses the data aggregation during routing, to transmit data required single 32-bit computation. A proposed RSA cryptography algorithm is proposed for data aggregation and data security in WSN. The performance is analysed in terms of End to End Delay, Dropped Data Packet, Normalised Routing Load (NRL0, Packet Delivered Ratio (PDR) and Throughput. The RSA algorithm is used for encryption and decryption for data security. Here, a network simulation tool is used to simulate wireless network is NS-2 platform. Overall the simulation is analysed in the result obtained and values are tabulated at the end of this paper.

**Keywords** - Wireless Sensor Network (WSN); Base Station (BS); Cluster Head (CH); Data Aggregation; Energy Consumption;

## I. INTRODUCTION

A Wireless Sensor Network (WSN) is comprised of several sensor nodes. The function of every sensor node is to sense the atmospheric conditions and also send the sensed data to a Base Station (BS). A large number of sensor nodes consume more power from the batteries but limited power can be stored in the batteries. So energy consumption is one of the main considerable factors in the sensor nodes [1] & [2]. To reduce energy consumption, the data aggregation and clustering approaches have been used widely [5]. In this approach, all sensor nodes are divided into clusters. For each cluster, there is one representative node and is called as Cluster Head (CH). It aggregates all the data within the cluster and sends the information to the Base Station (BS).

The representative node or CH node only transmits long distance through multi-hop, but other nodes only send data to CH via single-hop. In this way, a lot of energy can be able to consume [7]. Sensor device measures the physical parameters such as pressure, temperature, air humidity, moisture level, noise and so on. When a sensor is placed within the transmission range of other, it forms a network. Its tasks are sensing, computation and forwarding. It has some limitations such as range, memory and energy consumption. The reduction of data packet size or distance between the nodes can help to save energy in a sufficient amount. Routing algorithms will help to find a minimal path in the path establishment and transfer data [11], [13]. Data aggregation approach will correlate the sensor data are widely used and in this paper also an implementation of this approach is done using Network Simulator (NS-2). The architecture of Wireless Sensor Network (WSN) is shown in the Fig.1.

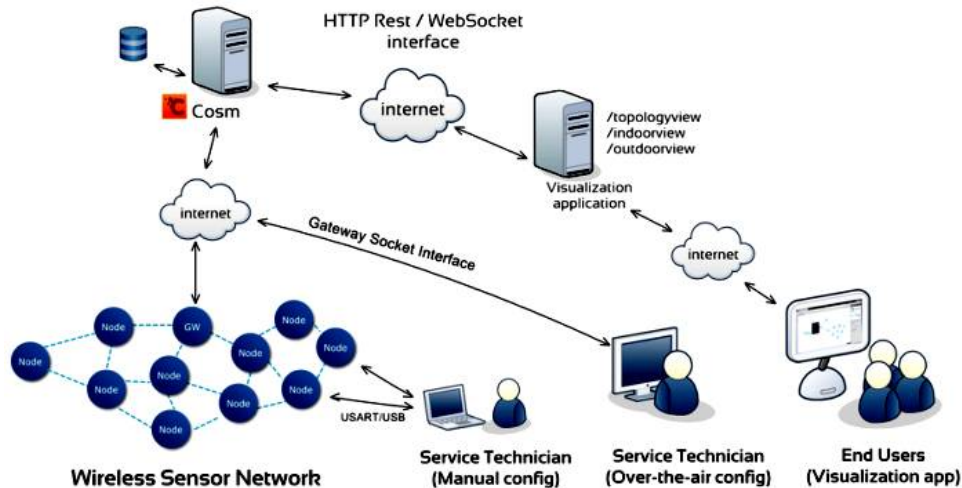


Fig.1. Architecture - Wireless Sensor Network (WSN)

## II. RELATED WORKS - A SURVEY

The researchers work to reduce the energy consumption of WSN. The reducing methods are scheduling radio, topology control, and data packet elimination control and data aggregation [9]. In order to reduce the amount of data transmission in WSN by combining the sensor data is collectively called as Data Aggregation. It is the process of gathering and routing information through a multi-hop network and processing data at intermediate nodes. It collects the critical data from the sensor nodes and transfers to the base station with minimum data potential and reduced bandwidth. The sensor gathers the information of data and performs the appropriate actions.

In case of emergency, the system should take automatic action on the basis of gathered information rather than waiting for manual involvement [10]. In emerging applications, real-time interaction, efficient and fault-tolerant communication is really essential. In real-time communication, WSN faces many challenges due to wireless nature, limited resource, reliability, architecture and dynamic network topology.

In data aggregation, there are three strategies are used [12]. They are i) In-Network aggregation [11], ii) Centralized approach, iii) Tree-based approach [8] and iv) Cluster-based approach [6].

## III. PROPOSED WORK METHODOLOGY SYSTEM

### A. Proposed Ideology

The proposed Data Aggregation RSA is mainly for data security in the wireless sensor networks. The ideology is based on i) The concept of selection of cluster head & ii) The node which sends the information when redundant data are identified.

The feature of the MMCR protocol is not allowed to send redundant data within a cluster. These features are mainly useful for data security [4] and it also used in the proposed algorithm. In simple, redundancy node is eliminated within the same cluster. The consecutive iterations redundant data is completely eliminated.

In any cluster, same or similar data (i.e. same range data) has been presented in more than one nodes means it does not send the data in the consecutive iterations. It reduces the network bandwidth and also energy consumption can be possible.

### B. Proposed Algorithm

In RSA data aggregation, the cryptographic hash function is mainly used. The data packets are transmitted through the dynamic routing protocol, the key values are changes in time to time for security purpose. In this proposed algorithm, RSA cryptography is implemented in two ways [3]. They are: i) Encryption Key generating in Public & ii) Decryption Key generating in Private. The accurate decryption key algorithm can only decrypt encrypted messages. Each person has two own keys such as encryption and decryption keys.

By this algorithm, data aggregation can be efficiently achieved and enhance the sensor life span also possible. The proposed step by step execution process is shown in the flow chart as Fig. 2.

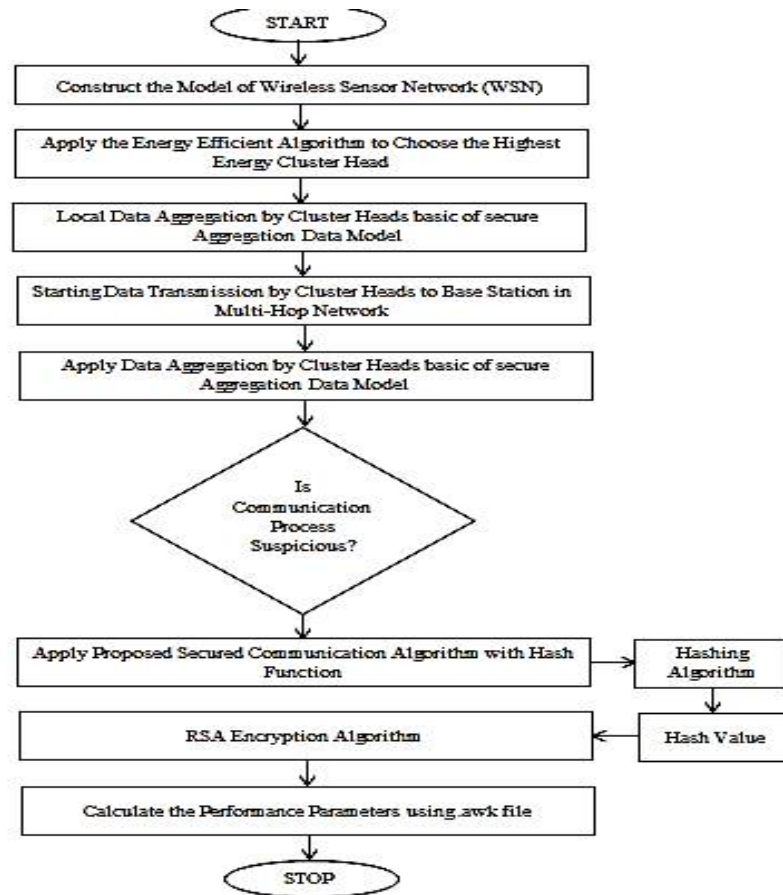


Fig.2. Proposed RSA Cryptography - Flow Chart

### Generating Own Public & Private Key for Each User:

Step 1: Randomly select two large prime i.e.  $a$  &  $b$  (Secret).

Step 2: To compute the user system modulus,  $N = a*b$  (Public). (Note:  $\phi(N) = (a-1)*(b-1)$  (Secret).

Step 3: Randomly selecting the encryption key,  $e$  (Public). Where,  $1 < e < \phi(N)$  &  $\text{GCD}\{e, \phi(N)\} = 1$ .

Step 4: To find the decryption key  $d$ , solve the equation (Secret). Encryption Key,  $e$  \* Decryption Key,  $d = 1 \text{ mod } \phi(N)$  &  $0 \leq d \leq N$ . Use the Extended Euclid's Algorithm to find the multiplicative inverse of  $e \{ \text{mod } \phi(N) \}$ .

### Publish the Public Encryption Key:

Step 1: Encryption Key,  $KU = \{e, N\}$  - Public

Step 2: To keep the Secretly Decryption Key,  $KR = \{d, a, b\}$  - Secret

Step 3: To represent each block by using an integer value. (i.e.,  $M < N$ )

Step 4: To keep the block size  $\leq \log_2 N$  bits. If the block size is  $k$  bits, then  $2K \leq N \leq 2K+1$ .

### To encrypt a message by Sender:

Step 1: Obtain the Public Key of recipient  $KU = \{e, N\}$ .

Step 2: Compute  $C = M*e \text{ mod } N$ , where  $0 \leq M < N$ .

To decrypt the cipher text  $C$  the owner:

Step 1: Use the Private Key of recipient  $KR = \{d, a, b\}$ .

Step 2: Compute  $M = C*d \text{ mod } N$ .

Note: Message  $M < \text{mod } N$ .

Hence,  $e * d = 1 + K * \phi(N)$  for some  $K$ .

By carefully chosen  $e$  and  $d$  to be inverses of  $\text{mod } \phi(N)$ .

#### IV. SIMULATION & RESULT ANALYSIS

##### A. Software Used

Network Simulator (NS-2) is a simulation tool & used to simulate the wireless communication network. It simulates discrete events and offers a better platform for Wireless Sensor Network (WSN) simulation. The square field area of 2000m x 2000m is chosen as the simulation field. The Antenna and mobility model used for simulation as Omni-directional and random waypoint respectively. The parameter used in the simulation to analyse the energy efficiency of cluster protocol in WSN is tabulated in the Table 1.

TABLE I - PARAMETERS USED IN THE SIMULATION

S.No.	Simulation Tool Used	Network Simulator (NS-2)
1	Operating System (OS)	Ubuntu 12.04
2	No. of Nodes for Testing	50, 100
3	MAC/PHY Layer	IEEE 802.11
4	Antenna Model	Omni-directional
5	Interface Queue Size	50 Packets
6	Data Payload	512 bytes
7	Pause Time (s)	10 seconds
8	Transmission Range	450 m
9	Examined Protocol	AODV
10	Interface Queue Type	Queue/ Drop Tail /Pri-Queue
11	Mobility Model	Random Way Point
12	Simulation Area	2000m x 2000m
13	Link Layer Type	LL

##### B. End to End Delay

The End to End Delay is the ratio between the sums of the individual data packet delay (i.e. Sending end to Receiving end delay) to the time taken to deliver the total data packets. In short, it is time taken to traverse the network and expressed in 'seconds s'. This delay is common due to the buffer queue, routing protocol activities transmission and delay, MAC control data exchanges.

$$\text{End to End Delay} = \frac{\text{Sum of the individual data packet delay}}{\text{Total number of Data Packet Delivered}}$$

The end to end delay (s) is compared between the base model and the proposed model is shown in Fig. 3. The delay time taken is better in the performance of the proposed RSA algorithm.

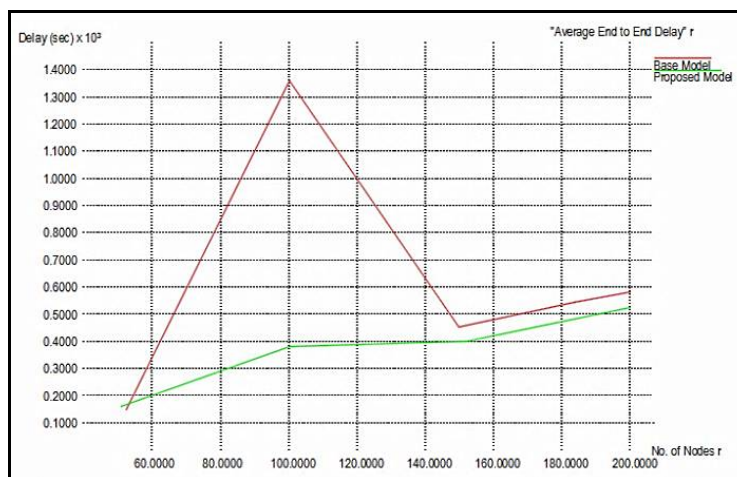


Fig.3. End to End Delay – Comparison

##### C. Dropped Data Packets

During the data transmission from the source to destination, some data are failed to reach the destination is called as dropped data packets. In Fig. 4 shows the comparison between dropped data in the base model with the proposed algorithm.

$$\text{Packet Drop Ratio} = \frac{\text{Data Packet Send} - \text{Data Packet Received}}{\text{Data Packet Send}}$$

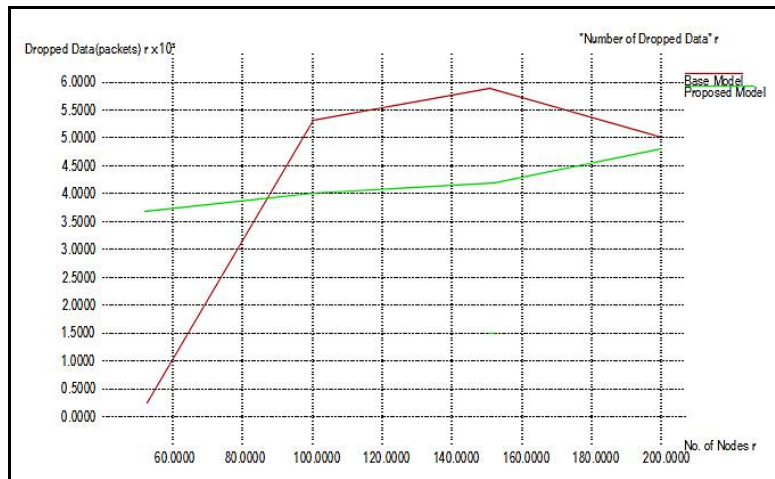


Fig.4. Dropped Data Packets – Comparison

In base model, For 50 nodes, Packet Drop Ratio = 401 – 360 = 41  
For 100 nodes, Packet Drop Ratio = 10877 – 6326 = 4551

In Proposed model, For 50 nodes, Packet Drop Ratio = 10877 – 7196 = 3681  
For 100 nodes, Packet Drop Ratio = 10877 – 8813 = 2064

#### D. Energy Consumption

The term 'Energy' is the product of the power consumed by the mobile nodes in WSN and time taken in's'.

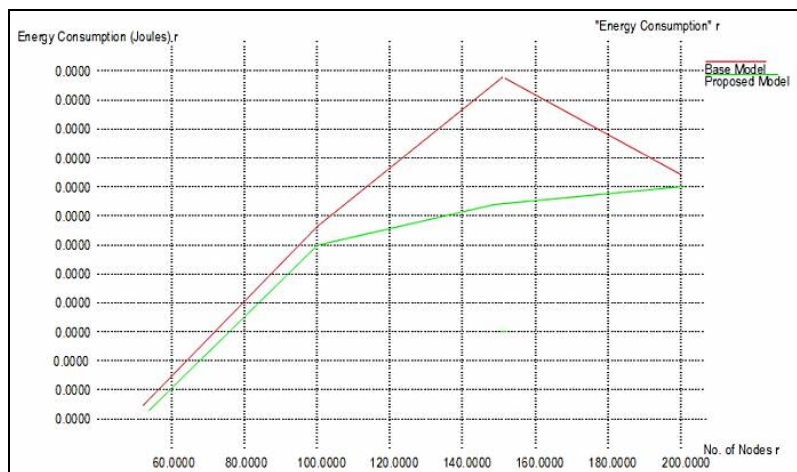


Fig.5. Energy Consumption – Comparison

It is expressed in Joule per second, J/s. In the base model, the AODV protocol consumed more energy than the proposed routing protocol and is shown in Fig.5.

$$\text{Energy Consumption} = \frac{\text{Sum of Energy Expended by each node}}{\text{Total number of Data Packet Delivered}}$$

#### E. Normalized Routing Load

Normalized Routing Load (NRL) is the ratio of the total routing packets to the received packets. It is expressed in kbps. It can be calculated as,  $\text{NRL} = \text{Routing Packet} - \text{Received Packet}$

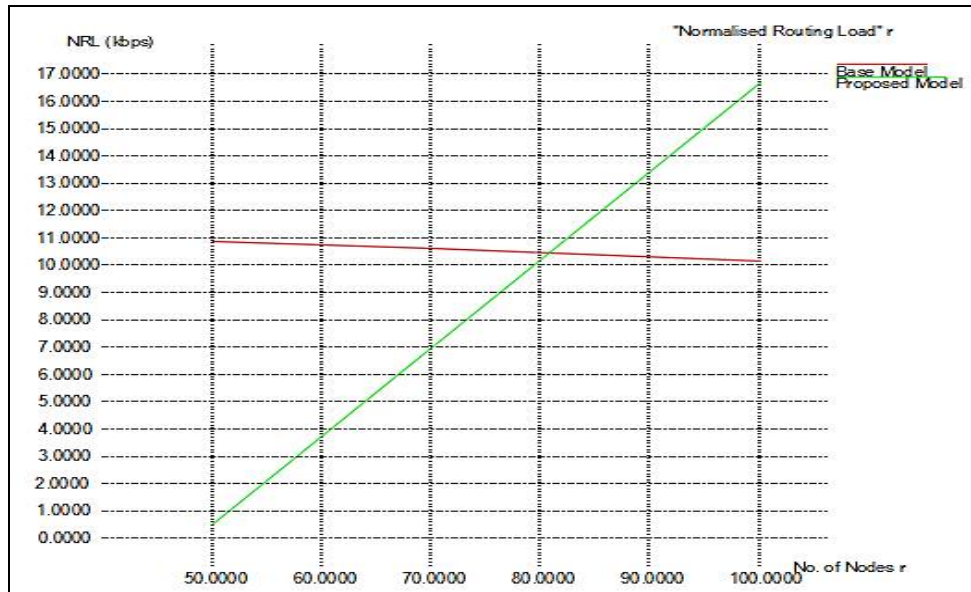


Fig.6. Normalized Routing Load - Comparison

### F. Packet Delivery Ratio

Packet Delivery Ratio (PDR) is the data packets received at the destination to data packets generated at the sending end. It is normally expressed in %. It denoted the maximum throughput can achieve by WSN.

$$PDR = \frac{\text{Received Packet}}{\text{Packets generated}} * 100$$

The simulation result analysis of the existing and proposed algorithm for 50 & 100 nodes, the performance can be analysed in the terms of Energy consumption, PDR, NRL and dropped packet values are tabulated in Table II.

TABLE III - RESULT ANALYSIS OF EXISTING & PROPOSED ALGORITHM

Nodes	Existing Model		Proposed Algorithm	
	50	100	50	100
Energy (Joule)	136.38	1367.23	229.43	379.36
PDR (%)	16.96	58.16	66.16	81.02
Delay (seconds)	136.38	1367.23	229.43	379.36
NRL (kbps)	10.53	10.24	0.55	16.53
Send Packet	401.00	10877.00	10877.00	10877.00
Receive Packet	360.00	6326.00	7196.00	8813.00
Dropped Packet	41	4551	3681	2064

The Packet Delivery Ratio and Throughput analysis are shown in Fig. 7 & 8 respectively.

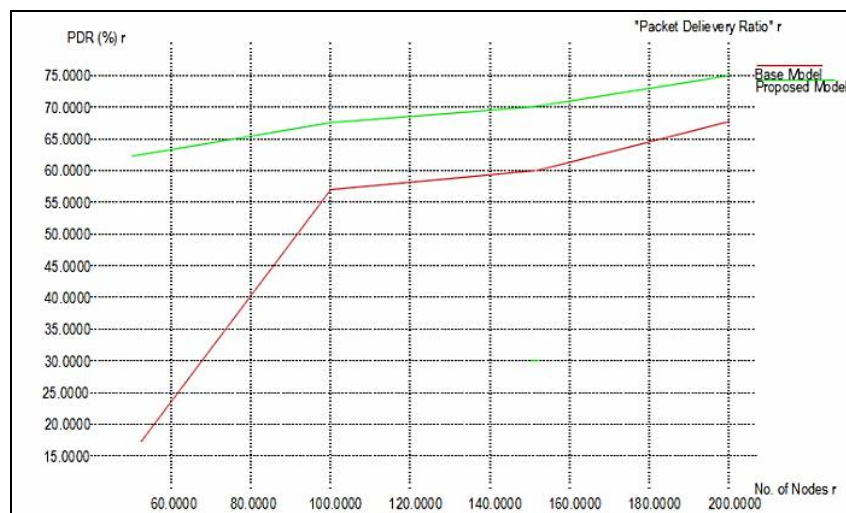


Fig.7. Packet Delivery Ratio - Comparison

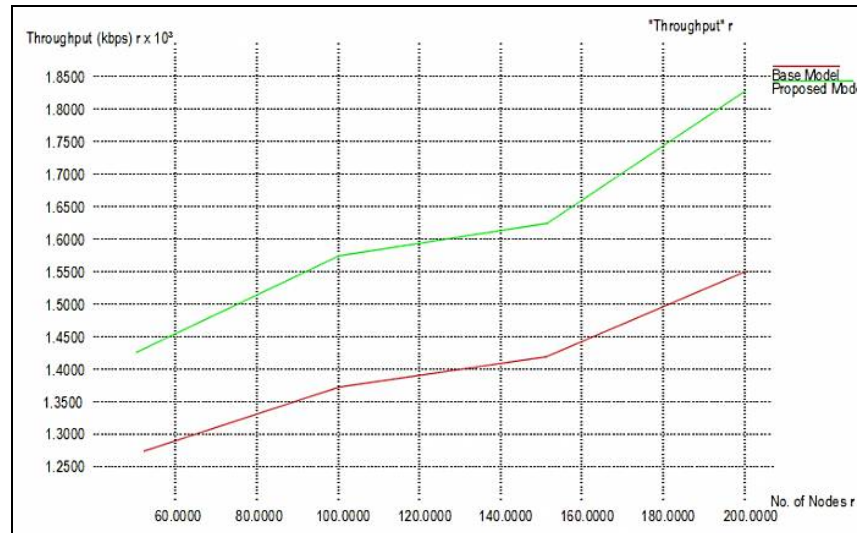


Fig.8. Throughput – Comparison

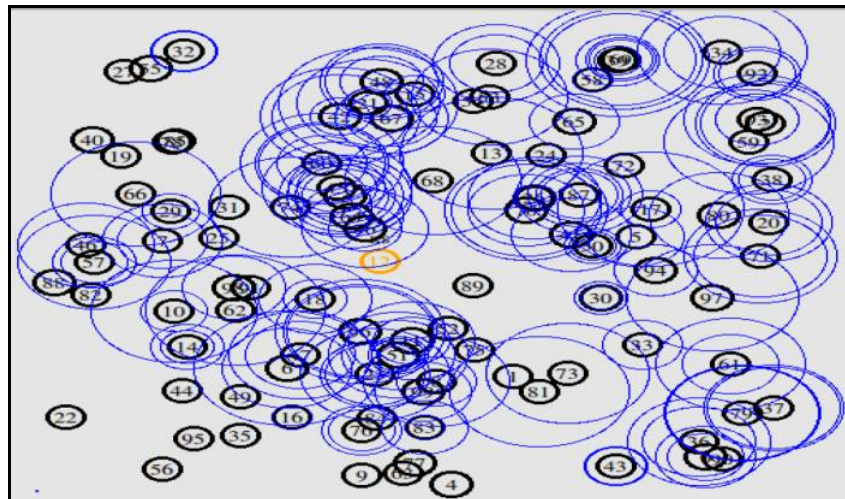


Fig.9. 1<sup>st</sup> Level Data Aggregation to access Network

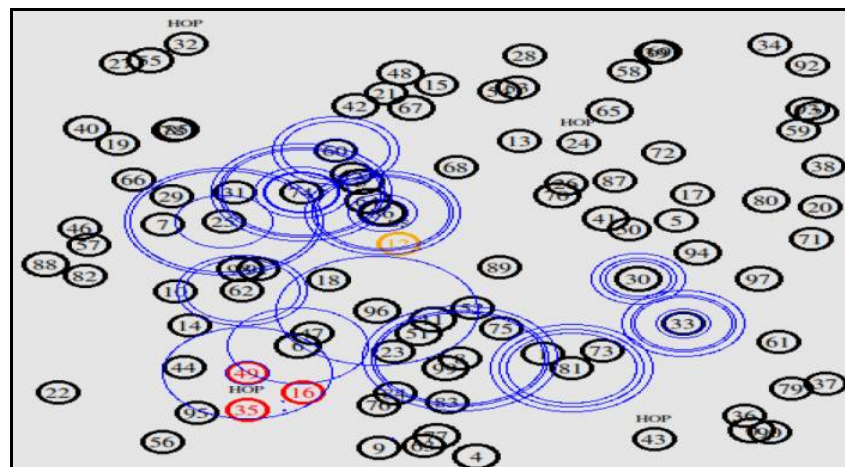


Fig.10. Four Hops Assigned & Hop 35 Choose the Nearest Node

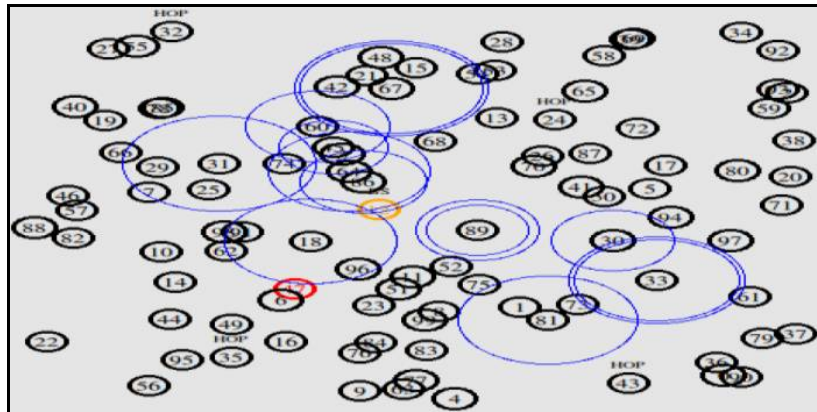


Fig.11. Selecting the Highest Energy Node & 2<sup>nd</sup> Level Data Aggregation

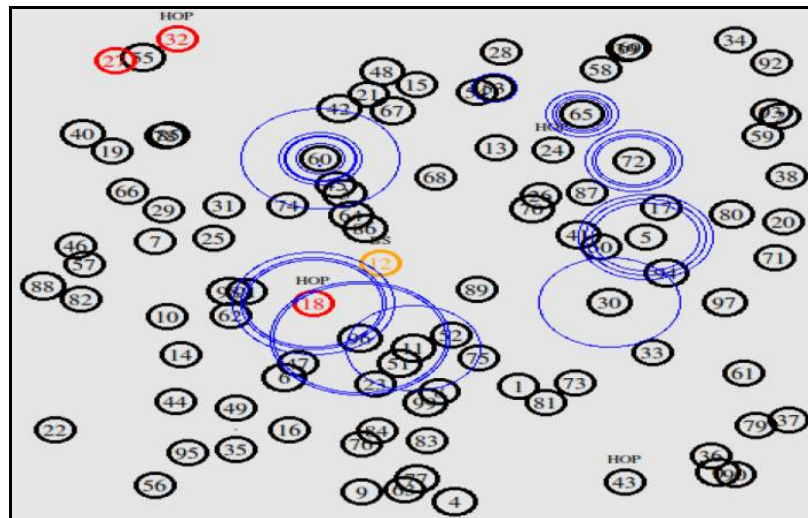


Fig.12. Sense Data and Choose the Nearest Node in 2<sup>nd</sup> Level Data Aggregation

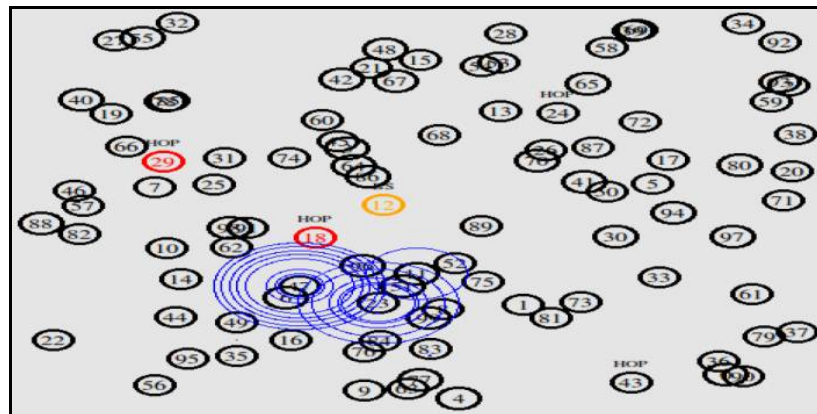


Fig.13. Hops Changed After Sensing the Nearest High Energy Node

#### IV. CONCLUSIONS

Data aggregation approach is proposed to enhance the lifetime of the wireless sensor network. Because WSN has a large number of sensor nodes and is resource constraints. It reduces the life span of the network. The performance evaluation is given through the simulation tool as Network Simulator (NS-2) and comparative analysis is made in terms of End to End delay, Dropped data packets, Energy Consumption, Normalised Routing Load, Packet Delivery Ratio, Throughputs. Overall results prove the proposed algorithm by selecting the highest energy nearer node reduces the delay and improves the performance of the network. The data security issue is also solved by the compromised sensor or aggregates nodes by changing the final aggregation values.

## REFERENCES

1. Ram Murthy Garimella, Damodar Reddy Edla, Venkatanaresh babu Kuppili, "Energy Efficient Design of Wireless Sensor Network: Clustering", International Conference on Recent Trends in Engineering Sciences, IIIT, Feb. 2018.
2. Najmesh Kamyab Pour, "Energy Efficient in Wireless Sensor Networks", A thesis for Ph.D in the Faculty of Engineering & Information technology, University of Technology Sydney, Dec. 2015.
3. Dr. K. Sheela Sobana Rani, R. Abiya Neethu, R. Aiswarya, S. Archana, M.Divya Bharathi, "A Secure RSA for Data Transmission in Wireless Sensor Networks", International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), Vol.13, Issue-4, Mar. 2015.
4. Madhumita Panda, "Security in Wireless Sensor Networks using Cryptographic Techniques", American Journal of Engineering Research (AJER), Vol.3, Issue-1, pp. 50-56, 2014.
5. Prakashgoud Patil, Umakant P Kulkarni, "Energy Efficient Aggregation With Divergent Sink Placement For Wireless Sensor Networks", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.4, No.2, Apr. 2013.
6. Neeraj Kumar Mishra, Vikram Jain, Sandeep Sahu, "Survey on Recent Clustering Algorithms in Wireless Sensor Networks", International Journal of Scientific and Research Publications, Vol. 3, Issue 4, Apr. 2013.
7. Xun Li, Geoff V Merrett, Neil M White, "Energy-efficient data acquisition for accurate signal estimation in wireless sensor networks", Journal on Wireless Communications and Networking, Vol. 12, pp. 411 – 413, 2013.
8. Mohit Saini, Rakesh Kumar Saini, "Solution of Energy-Efficiency of sensor nodes in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.
9. N. Akilandeswari, B. Santhi and B. Baranidharan, "A Survey on Energy Conservation Techniques in Wireless Sensor Networks", ARPN Journal of Engineering and Applied Sciences, VOL. 8, NO. 4, Apr. 2013.
10. Neeraj Kumar, Manoj Kumar, and R. B. Patel, "A Secure and Energy Efficient Data Dissemination Protocol for Wireless Sensor Networks", International Journal of Network Security, Vol.15, No.6, PP.490-500, Nov. 2012.
11. Kiran Maraiya, Kamal Kant, Nitin Gupta, "Wireless Sensor Network: A Review on Data Aggregation", International Journal of Scientific & Engineering Research Volume 2, Issue 4, Apr.2011.
12. Koutsonikola, D., Das, S., Charlie, H.Y. and Stojmenovic, I., "Hierarchical Geographic multicast routing for wireless sensor networks", Wireless Networks, Vol. 16, No. 2, pp.449–466, 2010.
13. Lutful Karim, Nidal Nasser, Hanady Abdulsalam, Imad Moukadem, "An Efficient Data Aggregation Approach for Large Scale Wireless Sensor Network", Vol.11, No. 6, pp.6-28, 2004.