INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue4)
Available online at www.ijariit.com

Design and Simulation Result Analysis of Data Aggregation in NS2 for WSN with Security

Rachna Kumari
Matu Ram Institute of Engineering & Management, Haryana
rachna.azura@gmail.com

Sunil Dalal
Matu Ram Institute of Engineering & Management, Haryana
sunil1dalal@gmail.com

Abstract**: Energy efficiency is an important metric in resource constrained wireless sensor networks (WSN). Multiple approaches such as duty cycling, energy optimal scheduling, energy aware routing and data aggregation can be availed to reduce energy consumption throughout the network. This thesis addresses the data aggregation during routing since the energy expended in transmitting a single data bit is several orders of magnitude higher than it is required for a single 32-bit computation. Therefore, in the first paper, a novel nonlinear adaptive pulse coded modulation-based compression (NADPCMC) scheme is proposed for data aggregation. A rigorous analytical development of the proposed scheme is presented by using Lyapunov theory. Satisfactory performance of the proposed scheme is demonstrated when compared to the available compression schemes in the NS-2 environment through several data sets. Data aggregation is achieved by iteratively applying the proposed compression scheme at the cluster heads. The second paper, on the other hand, deals with the hardware verification of the proposed data aggregation scheme in the presence of a Multi-interface Multi-Channel Routing Protocol (MMCR). Since sensor nodes are equipped with radios that can operate on multiple non-interfering channels, bandwidth availability on each channel is used to determine the appropriate channel for data transmission, thus increasing the throughput. MMCR uses a metric defined by throughput, end-to-end delay, and energy utilization to select Multi-Point Relay (MPR) nodes to forward data packets in each channel while minimizing packet losses due to interference. Further, the proposed compression and aggregation are performed to further improve the energy savings and network lifetime. Besides this, we also applied RSA security algorithm for encryption and decryption.

Keywords: Availability, Base Station (BS), Cluster Head (CH), Data Aggregation, Data Clustering Wireless Sensor Network (WSN).

I. INTRODUCTION

A WSN consists of a large number of sensor nodes. Each sensor node senses environmental conditions and sends the sensed data to a base station (BS), which is a long way off in general. Low energy consumption is very important for sensor nodes since the sensor nodes are powered charged by limited power batteries. In order to reduce the energy consumption, a clustering and data aggregation approach have been extensively used. In this approach, sensor nodes are divided into clusters, and for each cluster, one representative node, which called cluster head (CH), aggregates all the data within the cluster and sends the data to BS [5]. Since only CH nodes need long distance transmission via multi-hop, the other simple nodes only have to send data to CH via single-hop, whereby save the energy consumption. Efficient data collection in WSN plays a key role in power conservation [7]. Sensor devices are used to measure physical parameters like pressure, temperature, humidity etc. When placed within the transmission range of each other, it forms a sensor network. It carries the task of sensing, computation, and forwarding. They have some limitations like computation, memory, and energy. Sensors deployed in applications like the agricultural field require that the batteries be operating for one cropping season. Energy in the reduction of the packet size or distance between the nodes can also help in saving sufficient amount of energy. Efficient routing algorithms will have to be incorporated to find paths which consume minimal energy during path establishment and data transfer [1-2]. Data aggregation schemes are the most popular way of using the correlation in sensor data.

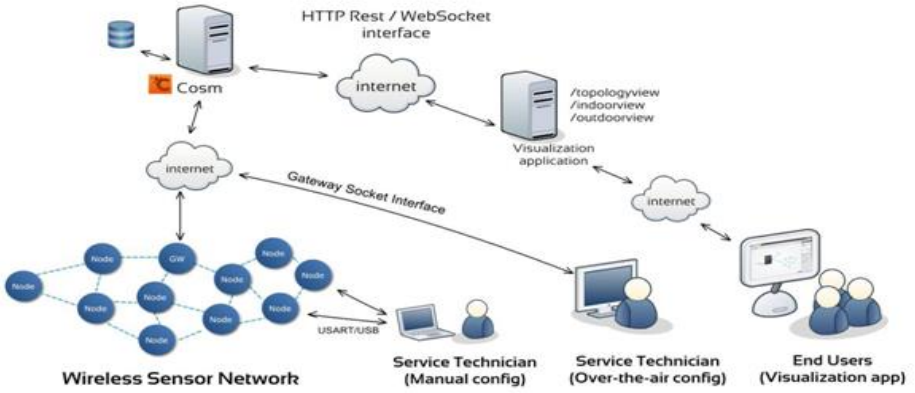


Figure1. Architecture of Wireless Sensor Network

II. LITERATURE SURVEY

There are several proposed mechanisms with the main goal to reduce the power consumption of wireless sensor networks. Mechanisms such as radio scheduling, control packet elimination, topology control, and most importantly data aggregation [8]. Data aggregation is defined as the process of summarizing and combining sensor data in order to reduce the amount of data transmission in the network. With the aim of reducing power consumption, data aggregation is the global process of gathering and routing information through a multi-hop network and processing data at intermediate nodes. It attempts to collect the most critical and important data from the sensors nodes and make it available to the Base Station in an energy efficient manner with minimum data latency and minimum possible bandwidth. The recent technological advances have to lead to the emergence of wireless sensor and actor networks. The sensors gather information regarding an event and actors perform the appropriate actions. In the case of emergency, the system should take automatic action on the basis of gathered information rather than waiting for manual intervention; therefore the role of actors is becoming very important [6-7]. The requirement of real-time, efficient and fault tolerant communication is extremely important in emerging applications. Supporting real-time communication in sensor networks faces severe challenges due to their wireless nature, limited resource, low node reliability, distributed architecture and dynamic network topology. In emerging applications based on WSN, therefore, there is a trade-off between energy efficiency and delay performance depending upon applications requirement

Data Aggregation Strategies: Centralized Approach, In-Network Aggregation, Tree-Based Approach and cluster-Based Approach are some of the existing strategies related used for data aggregation [9].

Centralized Approach: In this strategy, the node sends data to a central node via the shortest possible route. These data are aggregated by the central node (header node) to reduce the redundancy.

In-Network Aggregation: There are two approaches in-network aggregation [1]:

- With size reduction: each node combines and compresses the data packets received from its neighbors in order to reduce the packet length which will be transmitted towards Base Station.
- Without size reduction: is defined as the process of merging data packets received from different neighbours into a single data packet. The process merging data packets received from different neighbours into a single data packet but unlike with size reduction process, it is without processing the value of data.

Tree-Based Approach: This strategy [11] is held by constructing an aggregation tree, in which Base Station is considered as roots and sensor nodes are the leaves. Each node has a parent node whose data are forwarded. The flow of data starts from sensor nodes (leaves) up to the Base Station (roots) and the aggregation is done by parent nodes.

Cluster-Based Approach: With this approach [12] the whole network is divided into different clusters. A Cluster Head is selected in each cluster among different sensor nodes or cluster members. The nodes selected as a Cluster Heads are responsible for the aggregation process of data received from cluster members and then transmit the result to the Base Station.

III. PLANNING OF WORK/METHODOLOGY

The proposed solution called RSA (for Data Aggregation) for security. The main and most important improvement in this proposed solution is based on the concept of selection of Cluster Head and which node sends the information when redundant data are detected [11]. On the other hand, by combining features of MMCR protocols is allowed not to send the redundant data within a cluster and among different iterations, i.e. redundancy is eliminated first among nodes in the same cluster, and later from the same nodes among consecutive iterations, thus we eliminate 100% redundancy. In other words, within the same cluster, we achieve that if more than one node has the same or similar data (data in the same range), only one node sends the information, and also that if the same node yields the same or similar information among consecutive iterations, it does not send data. In this way the traffic on the network will be 100% useful, thereby reducing the bandwidth used and what is most important, energy consumption [15].

Proposed Algorithm: A cryptographic Hash Function algorithm is mainly used-RSA in data Aggregation. By using, the data packets are transferred through dynamic routing by time to time key value change securely. RSA cryptography implements two important methods: Public-key generating encryption and Private-key generating decryption. In RSA Cryptography, the encryption key is public, while the decryption key is not. The algorithm with the correct decryption key can decipher an encrypted

message. Every person has their own encryption & decryption keys. Through this method, efficient data aggregation model is achieved and the life time of sensors node are increased.

•Every user generates own public/private key:

1. selecting 2 large prime at random -a, b (secret)
2. computing their system modulus N=a.b (public)
   –note ø(N)=(a-1)(b-1) (secret)
3. Selecting at random the encryption key e
   (public)
   – where 1<e<ø(N), gcd(e,ø(N))=1
4. solve equation to find decryption key d (secret)

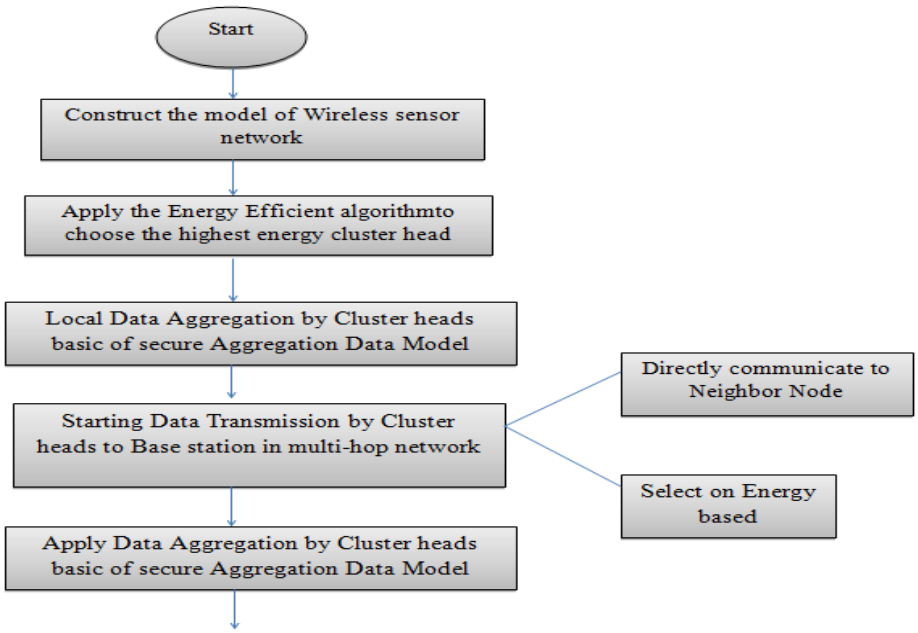
e.d=1 mod ø(N) and 0 ≤d≤N

Use the extended Euclid's algorithm to find the multiplicative inverse of e (mod ø(N))

Publish their public encryption key: KU={e,N}

- keep Secret private decryption key: KR={d,a,b}.
- Each block are represented an integer number
- Each block has a value M less than N
- The block size is <= log2(N) bits
- If the block size is k bits then
- 2k<= N <= 2K+1
- to encrypt a message M the sender:
- obtains the public key of recipient KU={e, N}
- computes: C=Memod N, where 0≤M<N
- to decrypt the ciphertext C the owner:
- use private key KR={d,a,b}
- computes: M=Cdmod N
- note that the message M must be smaller than the modulus N (block if needed)
- because of Euler's Theorem:
- aø(n)mod N = 1
- where gcd(h,N)=1
- in RSA have:
- N=p.q

- ø(N)=(a-1)(b-1)
- carefully chosen e & d to be inverses mod ø(N)
- hence e.d=1+k.ø(N) for some k



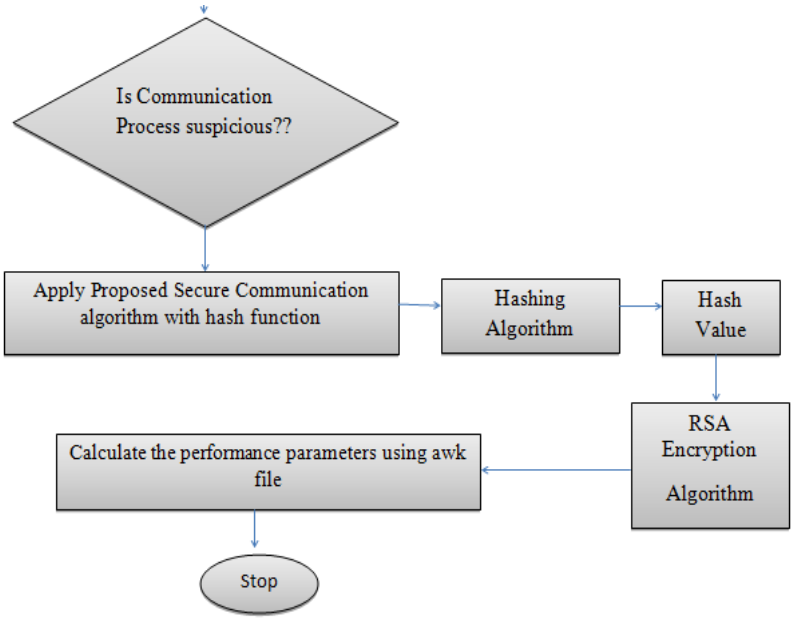


Figure2. RSA Encryption Flow chart.

IV. SOFTWARE USED AND SIMULATION RESULT

Software NS-2

We use NS-2 (v-2.35), a network simulation tool to simulate wireless communication network. NS2 is discrete event simulator developed. It provides a good platform for wsn simulation. The random way point model is selected as a mobility model in a rectangular field (2000 x 2000 m2). AODV is used for simulation at the network layer. Nodes send constant bit rate (CBR) traffic at varying rates.

The performance of Energy Efficient based Cluster Protocol in Wireless Sensor Network (WSN) is being estimated with the help of simulation on network simulator-2.

Simulation Setup

Table I: Simulation parameters in NS2

Simulation Tool	NS-2.35
Operating System	Ubuntu 12.04
No. of Nodes	50,100,150,200
MAC/PHY layer	IEEE 802.11
Antenna model	Omni directional
Interface queue size	50 packets
Data payload	512 bytes
Pause time	10 seconds
Transmission range	450m
Examined protocol	AODV
Interface Queue Type	Queue/DropTail/PriQueue
Mobility model	Random way point
Simulation area	2000M*2000M
Link Layer Type	LL

Table II Comparative Analysis of Result Table

Existing Model	Energy(Joule)	PDR (%)	Delay(sec)	NRL(Kbits/sec)	Send Packet	Receive Packet	Dropped Packet
50 Nodes	136.38	16.96	136.38	10.53	401.00	68.00	41
100 Nodes	1367.23	58.16	1367.23	10.24	10877.00	6326.00	5354
Proposed Algorithm	Energy(Joule)	PDR (%)	Delay(sec)	NRL(Kbits/sec)	Send Packet	Receive Packet	Dropped Packet
50 Nodes	229.43	66.16	229.43	0.55	10877.00	7196.00	3686
100 Nodes	379.36	81.02	379.36	16.53	10877.00	8813.00	4122
150 Nodes	392.43	85.12	389.20	21.34	10877.00	9814.00	4231
200 Nodes	398.27	88.23	395.12	24.56	10877.00	9927.00	4346

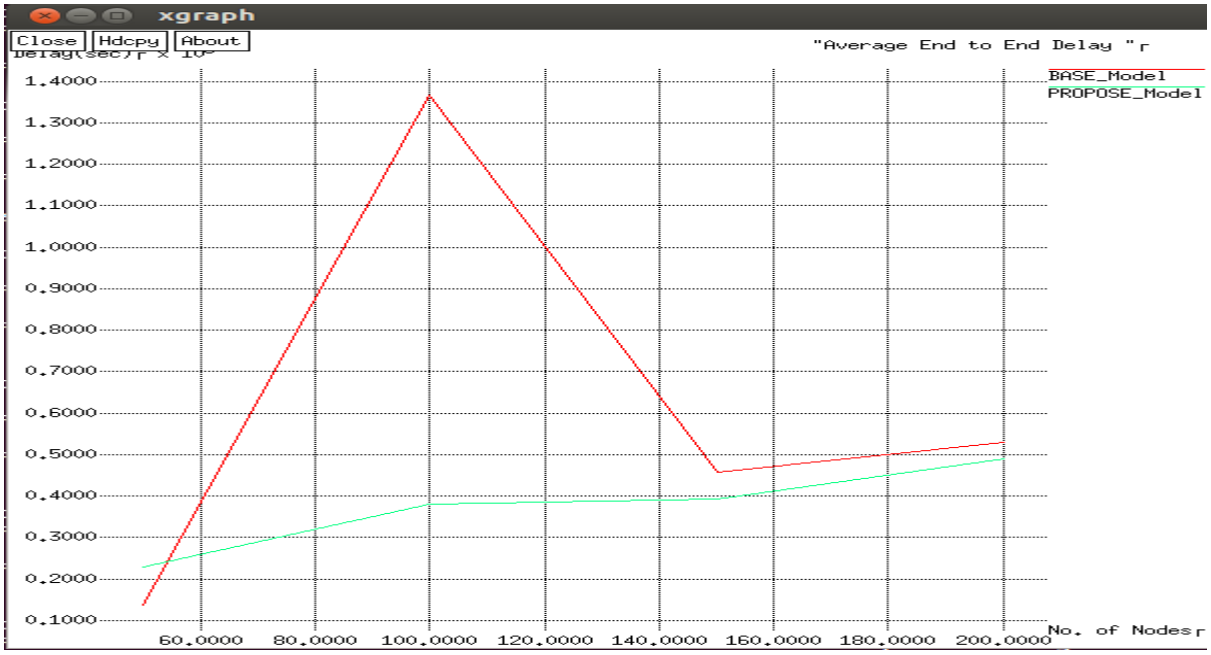


Figure 3 Comparison of average end-to-end delay

Average End-to-End Delay –The average time packets take to traverse the network. This is the time from the generation of the packet by the sender up to send at the destination application layer and expressed in second. It, therefore, includes all the delay in the network such as buffer Queue, transmission, and delay induced by routing protocol activities and MAC control data exchanges. Figure shows that the less delay in proposed protocol

End to End delay = [(Sum of Individual data packet delay) / (Total number of data Packets delivered)]

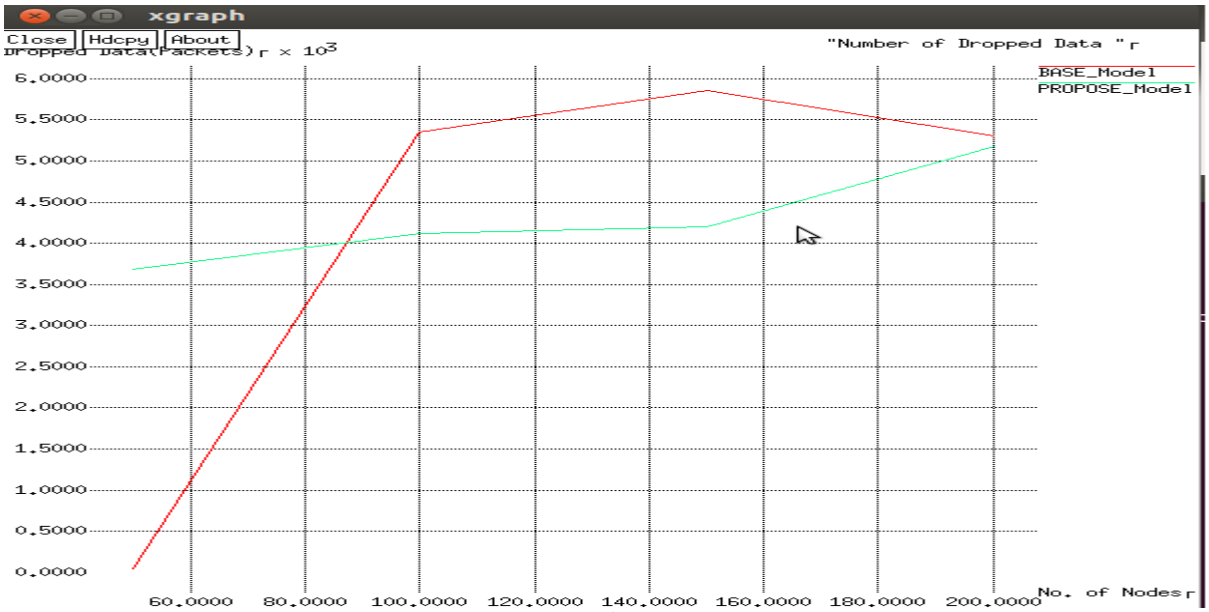


Figure 4 Comparison of dropped data packets

Total Packet Dropped – The failure of one or more transmitted packets to arrive at their destination is called as Total Packet Dropped. The figure shows that in term of drop packet AODV gives the better performance compared to proposed protocol.

Packet Drop Ratio = Data packets sent – Data packets received

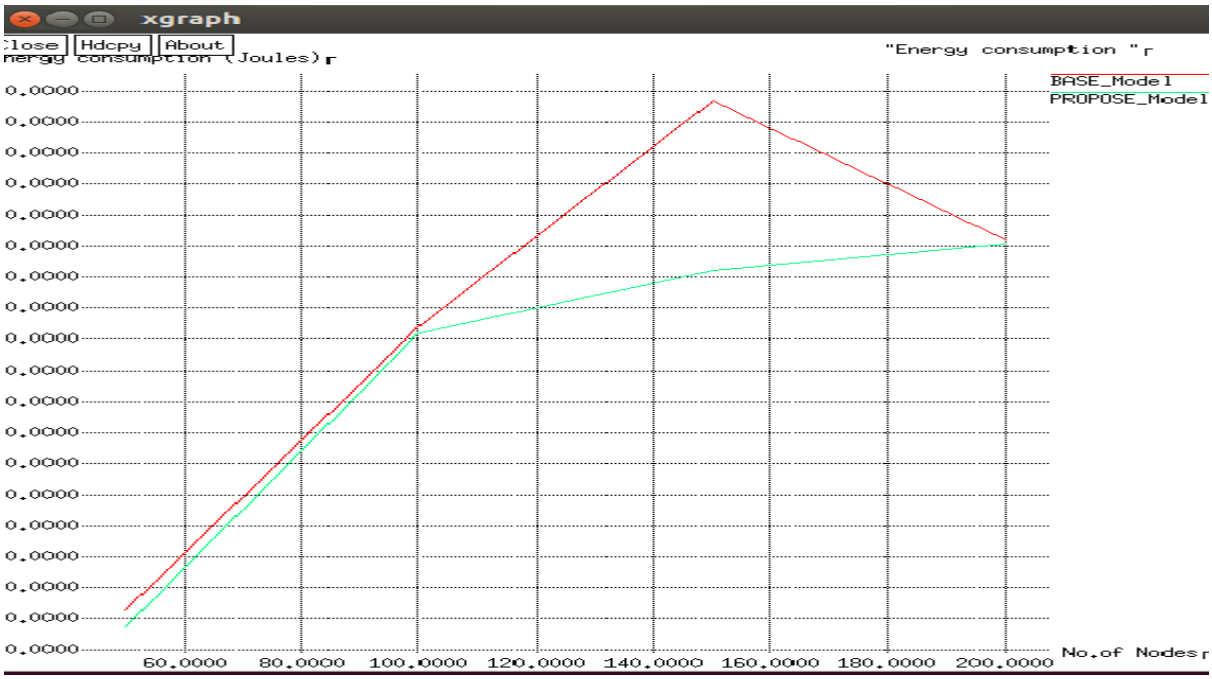


Figure5. Comparison of Energy Consumption

Energy Consumption – Energy is converted in joules by multiplying power with time. The graph below shows the energy consumed by mobile nodes in WSN. Energy consumption represented in Joule per Second. The figure shows that the AODV routing protocol consuming more energy compared to Proposed Routing Protocol.

Energy Consumption = [(Sum of Energy expended by each node) / (Total number of data packets delivered)]

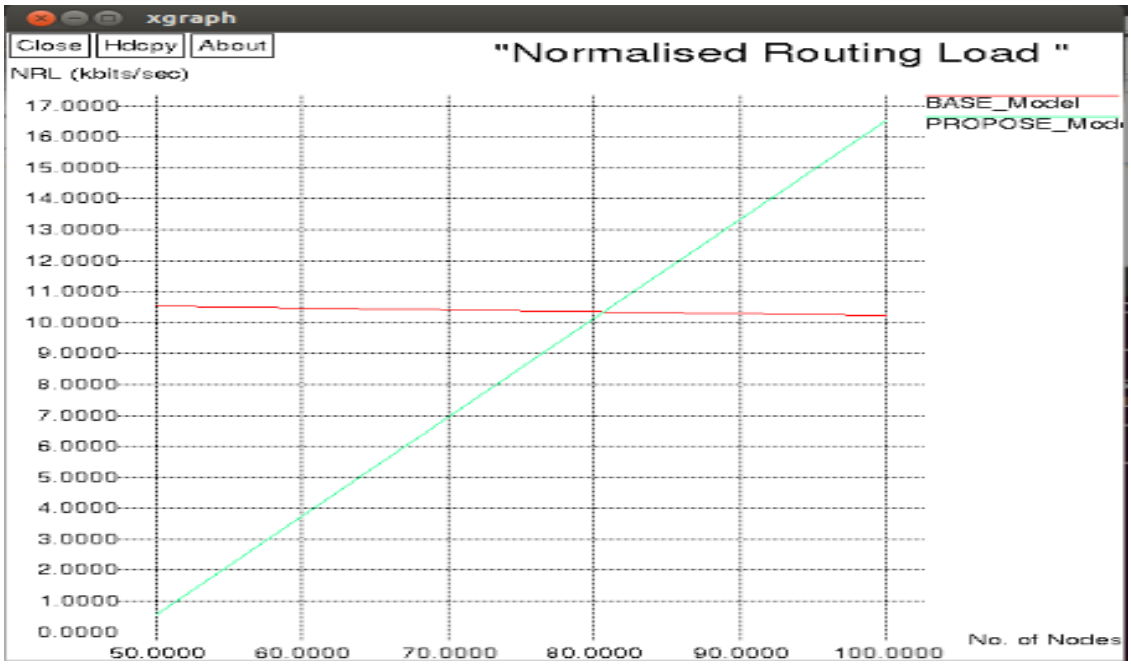


Figure6. Comparison of Normalized Load

Normalized Routing Load (Normalized Routing Load) – It is defined as the total number of routing packet transmitted kilo bits per data packet. It is calculated by dividing the total no. of routing packets sent (includes forwarded routing packets) by the total number of data packets received.

NRL = Routing packets/received packets

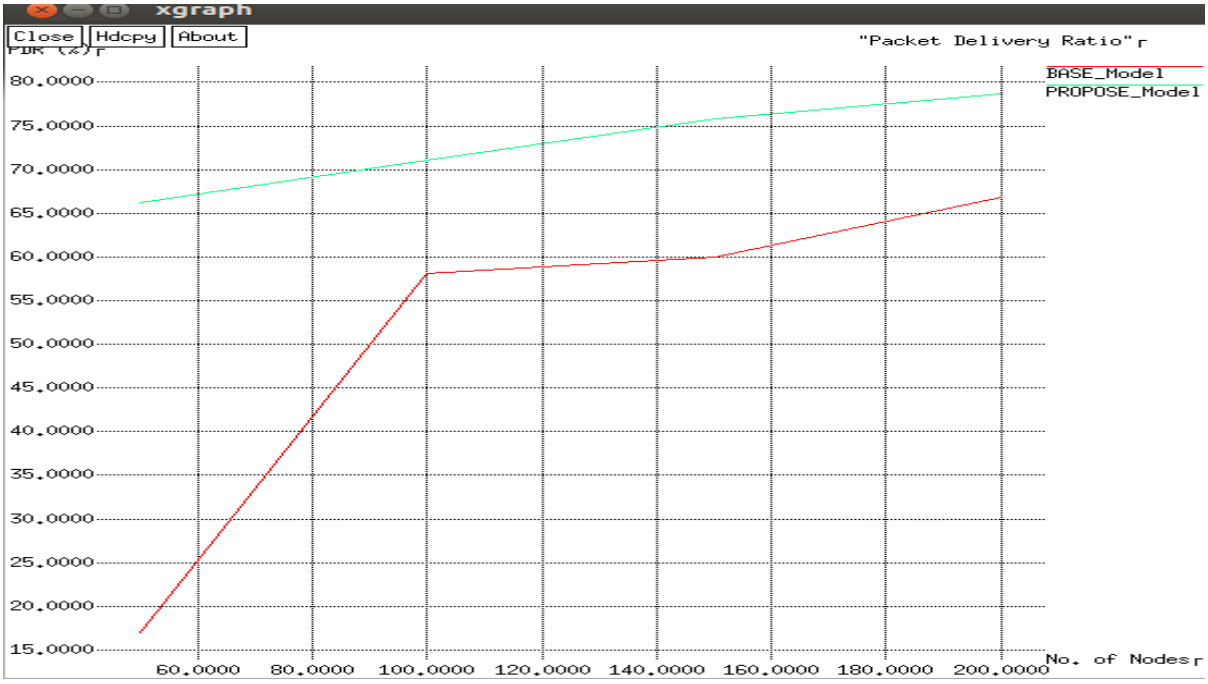


Figure 7 Comparison of PDR between base paper and proposed

Packet Delivery Ratio (PDR) – The ratio between the numbers of packets delivered to the receiver to the number of packets sent by the source is called as Packet Delivery Ratio. It denotes the maximum throughput a network can achieve. A high average packet delivery ratio is desired in the network

Packet Delivery Ratio = (Packets Received / Packets Generated) * 100

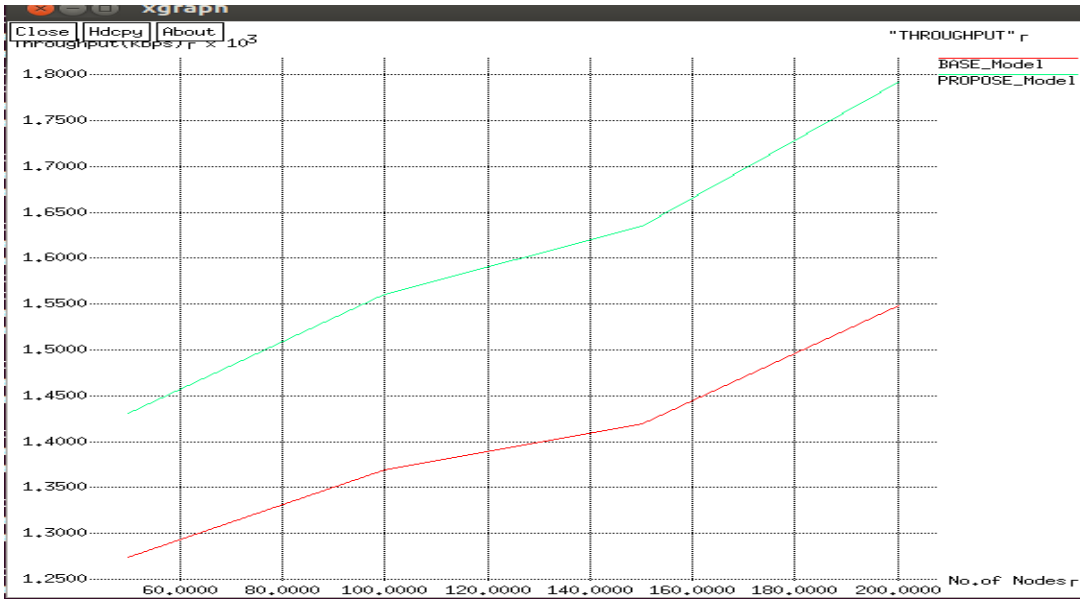


Figure 8 Comparison of Throughput between base models and proposed

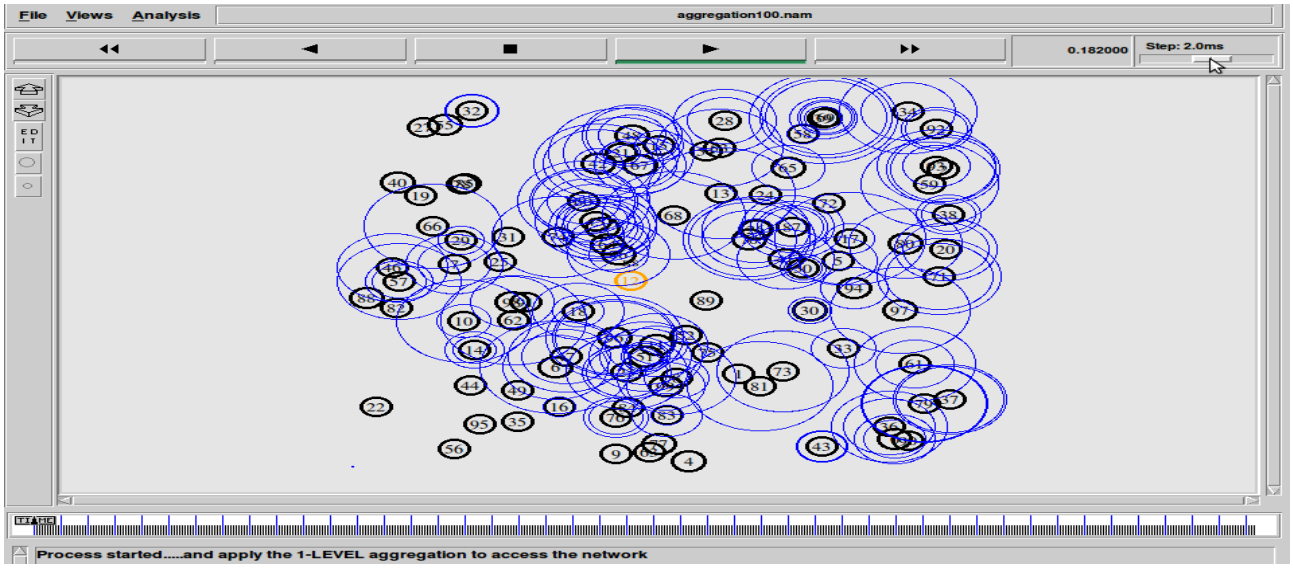


Figure 9 First level Aggregation to access network

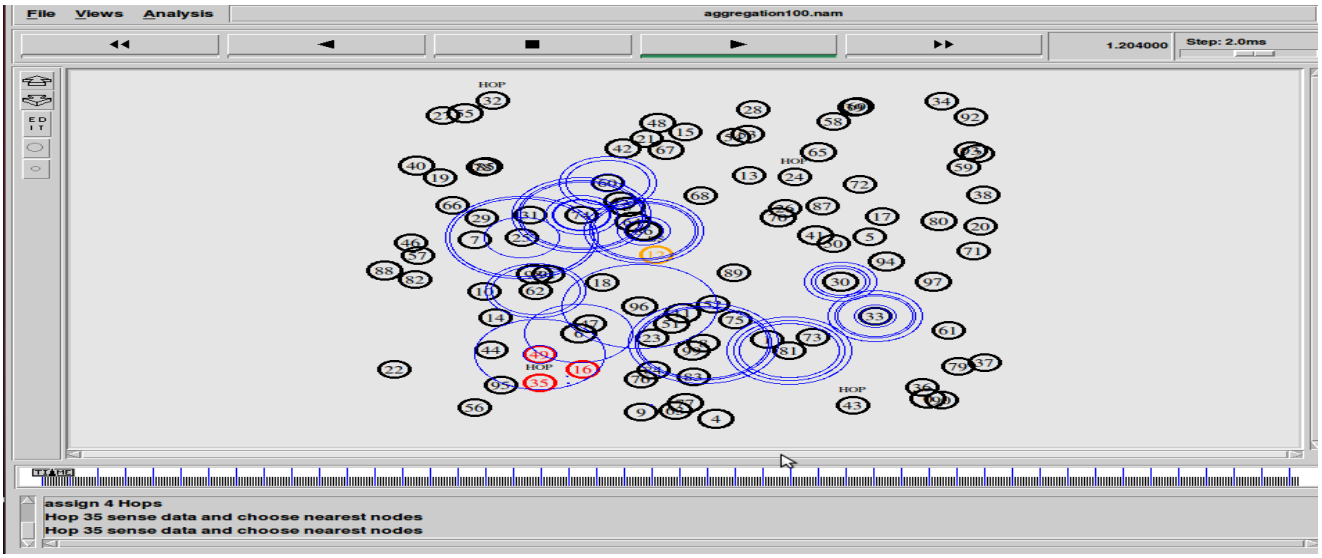


Figure 10 Four hopes are assigned and hope 35 sense data, choose the nearest node

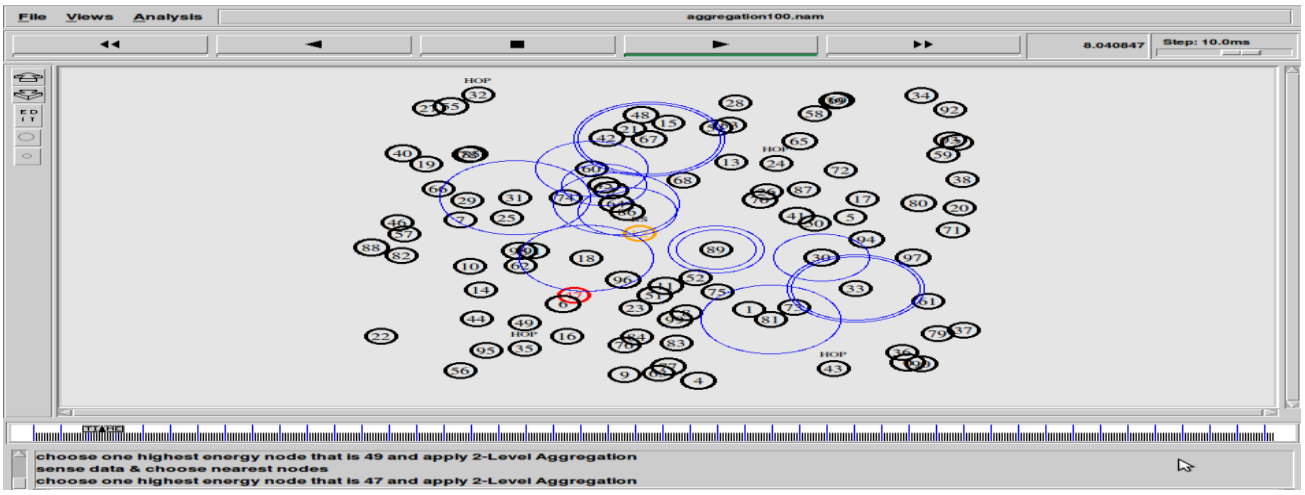


Figure 11 Selection of highest energy node and 2nd level aggregation

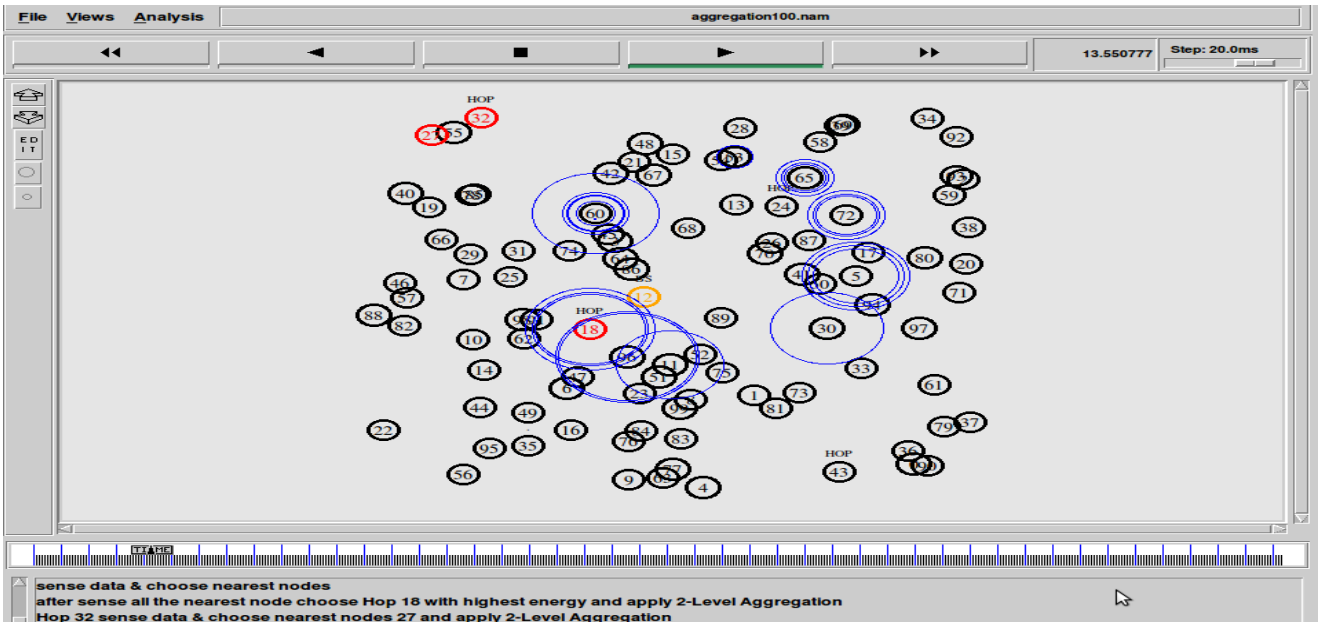


Figure 12 Sense data and choose the nearest node in 2nd level aggregation

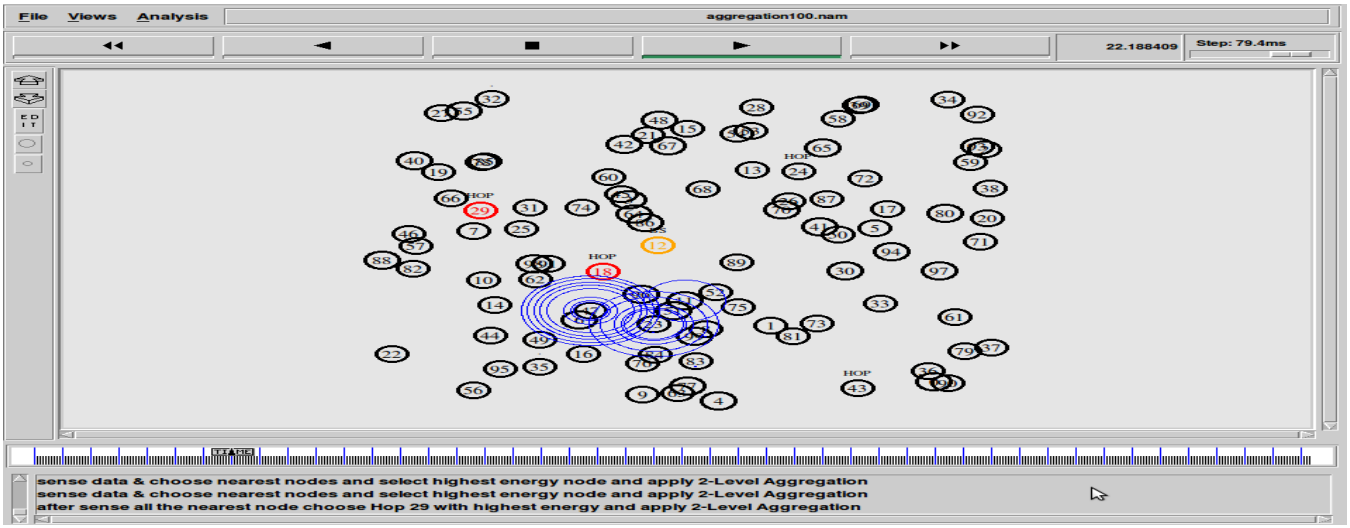


Figure 13 Hopes changed after sensing all nearest node with the highest node having energy

CONCLUSION

In our research, based on the resu1ts of simu1ation a comparative ana1ysis was done between se1ected aggregation approaches and the resu1ts were documented. The performance has been eva1uated based on parameters that aim to figure out the effects of routing protoco1s. By comparing these protoco1 performances, wireless sensor network consists a large number of sensor nodes. And these nodes are resource constraint. That's why a lifetime of the network is limited so the various approaches or protocol has been proposed for increasing the lifetime of the wireless sensor network. In this paper, we discuss the data aggregation is one of the important techniques for enhancing the life time of the network. And security issues is data integrity with the help of integrity we reduce the compromised sensor source nodes or aggregator nodes from significantly altering the final aggregation value**.**

REFERENCES

[1] Kiran Maraiya, Kamal Kant, Nitin Gupta, "Wireless Sensor Network: A Review on Data Aggregation", International Journal of Scientific & Engineering Research Volume 2, Issue 4, April -2011

[2]Lutful Karim, Nidal Nasser, Hanady Abdulsalam, Imad Moukadem, "An Efficient Data Aggregation Approach for Large Scale Wireless Sensor Networks." Vol.11, No. 6, pp.6-28, 2004

[3] 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

[4] 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, April 2013

[5] Neeraj Kumar Mishra, Vikram Jain, Sandeep Sahu, "Survey on Recent Clustering Algorithms in Wireless Sensor Networks", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013

[6] Karim Seada, Marco Zuniga, Ahmed Helmy, Bhaskar Krishnamachari, "Energy Efficient Forwarding Strategies for Geographic Routing in Lossy Wireless Sensor Networks" IPSN, pp. 124 – 133, Apr 2004

[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] Gyanendra Prasad Joshi, Seung Yeob Nam and Sung Won Kim, "Cognitive Radio Wireless Sensor Networks: Applications, Challenges and Research Trends." vol. 3 no.4, pp. 366–379, 2004

[9] Koutsonikola, D., Das, S., Charlie, H.Y. and Stojmenovic, I. (2010) „Hierarchical Geographic multicast routing for wireless sensor networks", Wireless Networks, Vol. 16, No. 2, pp.449–466.

[10] Wei Ye, John Heidemann, Deborah Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks"

[11] 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

[12]C. Lu, B. M. Blum, T. F. Abdelzaher, J. A. Stankovic and T. He. "RAP: A Real Time Communication Architecture for Large-Scale Wireless Sensor Networks," in Eighth IEEE Real-Time and Embedded Technology and Applications Symposium, pp. 55-66, 2002. doi: 10.1109/RTTAS.2002.1137381

[13]T. He, J.A. Stankovic, C. Lu, T. Abdelzaher. "SPEED: A Stateless Protocol for Real-Time Communication in Sensor Networks". Proceedings of 23rd International Conference on Distributed Computing Systems, Providence, Rhode Island, USA, pp. 46-55, May 19-22, 2003. doi: 10.1109/ICDCS.2003.1203451

[14]Emad Felemban, Chang-Gun Lee, Eylem Ekici, Ryan Boder and SMMCRr Vural, "Probabilistic QoS Guarantee in Reliability and Timeliness Domains in Wireless Sensor Networks" Proceedings of IEEE INFOCOM 2005, vol. 4, pp. 2646- 2657, March 13-17, 2005. doi: 10.1109/INFCOM.2005.1498548

[15] 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, APRIL 2013

