

Energy Optimised Data Encrypted Design for Wireless Sensor Node

Sneha Bele

Dept of electronics & Telecommunication,
Ballarpur Institute of technology, Bamni
Gondwana University, Gadchiroli

Sunil Kuntawar

Dept of electronics & Telecommunication,
Ballarpur Institute of technology, Bamni
Gondwana University, Gadchiroli

ABSTRACT

Due to large increased populations of wireless connected nodes, capable of computation, communication and sensing constitute wireless sensor networks (WSNs). Energy optimization has become a major research point in this field to consume large power and save energy. To optimise energy both at node level and network level data encrypted design is designed with proper hardware requirements and routing techniques. This will consume more energy in wireless sensor node. Implementation is done in hardware using various components and experimental result is calculated at each node and plotted on graph. With the help of graph compared with power level reading of each node normal with Huffman reading. It is observed that using Huffman coding and multipath routing algorithm data packets are encrypted and power is saved.

General Term

Analysis, algorithm, microcontroller. Wireless sensor nodes

Keywords

Energy Aware Multipath routing, Energy Consumption, Delivery Packet Ratio, RF2.4G.

1. INTRODUCTION

The rapid growth in mechatronics, digital electronics and wireless communication technology have enabled the development of distributed networks of small, inexpensive nodes that are capable of sensing, computation, and wireless communication. They are designed to be deployed for a broad range of environmental sensing applications from vehicle tracking to habitat monitoring. Sensors are connected in node in wirelessly in large network which consumes more energy. Thus energy optimization has become a major obstacles. Many prior researchers have studied various approaches such as sleep wake up periodic scheme, low duty cycle etc. Sensors are having batteries which can be charged through solar batteries using solar harvesting techniques. The traffic-adaptive medium access protocol has been designed to reduce energy consumption by allowing sensor nodes to assume a low-power idle state whenever they are not working in transmission or receiving mode. Many researchers have previously researched in this field and introduces various schemes. They introduced duty cycle, sleep wake period and all. For energy-efficient data acquisition, an adaptive sampling algorithm consisting of duty cycling and adaptive sampling is proposed to reduce energy consumption in a sensor network. In this way, the energy consumption for communication decreases as the data to be transmitted decrease. For energy-efficient data acquisition, an adaptive sampling algorithm consisting of duty cycling and adaptive sampling is proposed to reduce energy consumption in a sensor network. To have better result we have implemented such a hardware

methodology in which four nodes are placed in certain distance to get uniqueness in result and used high performance hardware components to save large amount of energy both at node level and network level.

2. LITERATURE REVIEW

As energy optimization has become a major topic in the field of wireless sensor node so to design such hardware is major task. Many prior research and papers are published. The ongoing research on multipath routing tries to cope up with fault tolerance and resource limitations of the low power sensor nodes through concurrent data forwarding over multiple paths. This section introduces some of the recent research in this area.

Jelena Mirković Gregory Prier (2002) [1] Distributed denial-of-service (DDoS) attacks present an Internet-wide threat. They proposed D-WARD, a DDoS defense system deployed at source-end networks that autonomously detects and stops attacks originating from these networks.

Santhosh Simon, K Paulose Jacob (October 2013) [2] The evolution of wireless sensor network technology has enabled us to develop advanced systems for real time monitoring. This paper also discusses a protocol that can be adopted for increasing the security of the transmitted data.

Pratik Agarwal (2013) [3] Wireless Sensor Networks (WSNs) are made of sensor nodes with restricted battery life and transmission capability. In this work we propose an energy efficient multipath routing algorithm in WSN. This protocol is designed to improve the latency, resiliency and efficiency through discovering multiple paths from the source to the destination.

ReshmaPatil, Prof.S.M.Shinde (Aug 2014) [4] Wireless sensor network is autonomous and infrastructure less network. In this paper they introduce new approach for WSN security, we propose Secure Energy Efficient Routing (SEER) scheme that consider cost of providing security and effects on energy efficiency.

Rakesh V, Sarala S M (June, 2015) [5] Wireless sensor networks (WSN) has been increased day by day to measure and monitor physical characteristics. They compare how much energy is optimized by different compression and encryption techniques.

3. METHODOLOGY

3.1 Path Construction

No. of components in multipath routing protocol are required to construct path which makes it highly dependent on ability of proposed protocol and construct better quality of reliable path.

3.1.1 Path Discovery

Data transmissions in wsn are done in number of hops by choosing some intermediate to create multiple path from source to destination. Disjointedness is main criteria for all protocols which is of three types i.e node disjoint, link disjoint and partially disjoint. Node disjoint has no common nodes, link disjoint path has several node in common but no shared link. Partially disjoint has several links or nodes between paths.

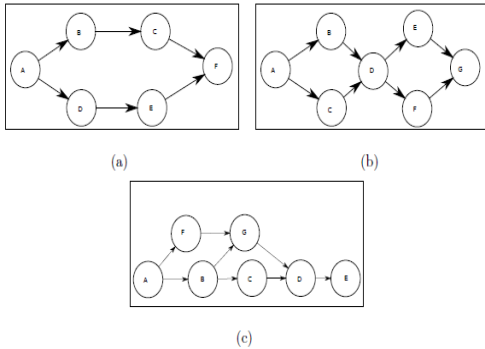


Figure 1 : Path Discovery

3.1.2 Path Selection and Traffic Distribution

After path discovery it has become very important part to find path and detect traffic distribution in network..Some algorithm provides no. of path at a time its important to find best path to have fast transmission and keep backup at each level for recovery. Some criteria must be followed to detect best neighbouring path. The main criteria to set path is path disjointness. But due to its time varying property it leads to low quality paths. To overcome this problem we add another routing algorithm with disjointness to have better quality path that increased battery level, high speed, less delay and better quality path. This routing is less expensive.

3.1.3 Path Maintenance

To reduce performance degradation some path mechanism is to be developed which gives high dynamics of low power links and highly error prone.. The path discovery can start in three different situations,

1. When an active path has failed.
2. When all active paths have failed.
3. When certain number of paths have failed.

The proposed protocol named Energy Aware Multipath Routing in RF2.4G based Wireless Sensor Networks is based on the multipath scheme where multiple route exist between each source and the sink. In the following section we discuss system model and assumptions for the proposed protocol and working principle of the proposed protocol.

3.2 Network Model and System Assumption

No of sensors nodes and sink nodes are taken in anetwork. A sink node is taken at middle which has better battery, memory space and unlimited computation. Each nodes knows their position and sink nodes has unique ID and location of source node innetwork. All nodes broadcast message to each other at same time and each nodes has its different transmission range.

3.3 Energy Aware Multipath Routing

This paper proposed a multipath routing algorithm which avoid collision and conserve energy. We construct route between source and sink to avoid tolerance. We can use proactive routing but its broadcast message to all nodes and if

any topology fails its difficult to update. So route is placed in between it.It mainly consist of three phases i.e Neighbor Discovery, Multiple Path Construction and Data Transmission.

3.3.1 Neighbor Discovery

Here every node broadcast message with unique ID, residual energy and location. Each node broadcast message to naighboring node and by repeating makes a big broadcasting network.

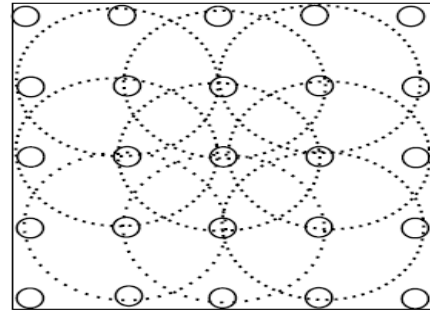


Figure 2: Path selection and traffic distribution

3.3.2 Multipath Construction

After neighboring discovery phase each node posses their neighboring information and then multipath construction starts. By assuming source node location to be known to sink and location the sink starts route request. There are two types of nodes primary and alternate. Primary node is from source to sink and madr between nearest possible path. The alternate nodes find one single path towards location factor(LF) after primary path. With minimum distance nodes are kept to find location factor. Generally primay path is choosen to avoid divergence in direction. The Next hop is given by

$$Next-hop_i = \min(LFi) \quad (3.1)$$

$$LFi = (Locsource - Locb) \delta b \ 2 \ Neighbor_i \quad (3.2)$$

where, LFi is the set of distance of all the neighbors of node i from the source.

Locsource is the location of the source node,Locb is the location of the node b,and Neighbor_i is the neighbor set of node i.

It is an incremental approach from the sink to the source. First the sink node which is itself a primary node, selects two neighbors based on the equation 3.1. Out of these two neighbor nodes one with the minimum location factor becomes the next primary node and the node with the second minimum location factor becomes the alternate node ,and with this step we initialize the multipath construction phase. A node which is associated by strong line has the base area component, means an essential hub and is in the essential way towards the source. Likewise node b is associated by dashed lines has the second least location factor is the substitute node and is the part of the alternate path towards the source node. All the intermediate nodes follow the same process as the sink node to find their corresponding neighbors till the source node is reached, this process is illustrated. Finally when the route request reaches the source node we see that one primary path and multiple alternate paths are constructed between the sink and the source node, which is shown in the figure

Input: Set of n sensor nodes randomly distributed.
Output: One primary and multiple alternate paths from source to sink.

```
repeat
if (node == sinknode) then
FindPrimaryPath();
FindAlternatePath();
else if (node == Primary) then
FindPrimaryPath();
FindAlternatePath();
else if (node == Alternate) then
FindPrimaryPath();
end if
until (node 6= Source)
procedure FindPrimaryPath()
if (node == Primary) then
Broadcast PRIMARY;
Search for the best node;
node ← Primary;
end if
if (node == Alternate) then
Broadcast ALTERNATE;
Search for the best node and prefer Primary;
if (node 6= Primary) then
node ← Alternate;
end if
end if
end procedure
procedure FindAlternatePath()
if node == primary then
Search for the next best path node accept Primary;
if ((node 6= Primary)&&(node 6= Alternate)) then
node ← Alternate;
end if
end if
if (node == Alternate) then
Exit();
end if
end procedure
```

Algorithm 1 has two procedures FindPrimaryPath() and FindAlternatePath() which are repeated till the route request reaches the source node.

FindPrimaryPath() : This function is for both primary and alternate nodes. If node is primary it broadcast its node to primary neighbor and if it is alternate then broadcast to alternate node. With minimum location factor towards the source prefer primary path. To avoid divergence it found four neighbour nodes which has two possible nodes types which are primary node or alternate node.

FindAlternatePath(): This function is called only by the Primary nodes for finding an alternate path towards the source. It finds the next best node which is called alternate node and add it in its path. In algorithm all nodes are kept at sleep node except primary node as its need all time. It saves energy as its go to sleep mode. There is only one active path between sink and source. This is done to avoid interference and avoid collision.

3.3.3 Data Transmission

After the route discovery by the multipath construction phase data transmission takes place between source and sink. The primary and alternate paths are available, but the data transmitted only over the primary path. Source utilise alternate path when primary path is not available. Rest of the nodes that are not in the active path will one to avoid collision and

interference. go to sleep mode to conserve energy. If there will be no path exist between source and sink, the process of route discovery starts.

3.4 Energy Model

Energy modeling in WSN is based on the theoretical energy consumption not on practical of the existing platforms. We have considered three modes of energy consumption, first the energy consumed due to transmission of packets (Eq 3.3), secondly, energy consumed due to reception of packets (Eq 3.4), third, energy spent by nodes in the idle mode (Eq 3.5) and finally the energy consumed by the nodes in processing.

$$\text{EnergyTransmission} = \text{EnergyXT} \times t(\text{bits}) + \text{EXP}(d2) \quad (3.3)$$

$$\text{EnergyReceiving} = \text{EXR} \times t(\text{bits}) \quad (3.4)$$

$$\text{EnergySleep} = \text{EXS} \times t(\text{sec}) \quad (3.5)$$

$$\text{TotalEnergy} = \text{EnergyTransmission} + \text{EnergyReceiving} + \text{EnergySleep} \quad (3.6)$$

In Equations 3.3, 3.4 and 3.5 EnergyXT refers to energy consumed per bit for transmission, EXR is the energy consumed per bit for receiving, and EXS is the energy consumed per second in idle mode and EXP(d2) is the energy consumed in finding the next hop neighbor.

3.5. Rf2.4g-A Overview

In our work RF2.4G pretends to be interlinking wireless technology to operate remote device via serially received data from PC. This section explain general aspects of RF2.4G regarding what is RF2.4G, how it works in general environment & why RF2.4G is selected for our work:-

3.5.1 Why RF2.4G:

The RF2.4G used due because:

- Low cost
- Secure
- Reliable and self healing
- Flexible and extendable
- Low power consumption
- Easy and inexpensive to deploy
- Global with use of unlicensed radio bands
- Integrated intelligence for network set-up and message routing

3.5.2. What is RF2.4G?

RF2.4G is the only standards-based technology that addresses the unique needs of most remote monitoring and control sensory network applications. RF2.4G technology is a low data rate, low power consumption, low cost, wireless networking protocol targeted towards automation and remote control applications. IEEE 802.15.4 committee started working on a low data rate standard a short while later. Then the RF2.4G Alliance and the IEEE decided to join forces and RF2.4G is the commercial name for this technology. RF2.4G is expected to provide low cost and low power connectivity for equipment that needs battery life as long as several months to several years but does not require data transfer rates as high as those enabled by Bluetooth. In addition, RF2.4G can be implemented in mesh networks larger than is possible with Bluetooth. RF2.4G compliant wireless devices are expected to transmit 10-75 meters, depending on the RF environment and the power output consumption required for a given application, and will operate in the unlicensed RF worldwide (2.4GHz global, 915MHz Americas or 868 MHz Europe). The data rate is 250kbps at 2.4GHz, 40kbps at 915MHz and

20kbps at 868MHz. IEEE and RF2.4G Alliance have been working closely to specify the entire protocol stack. IEEE 802.15.4 focuses on the specification of the lower two layers of the protocol (physical and data link layer). On the other hand, RF2.4G Alliance aims to provide the upper layers of the protocol stack (from network to the application layer) for interoperable data networking, security services and a range of wireless home and building control solutions, provide interoperability compliance testing, marketing of the standard, advanced engineering for the evolution of the standard.. A unique feature of RF2.4G network layer is communication redundancy eliminating single point of failure in mesh networks. Key features of PHY include energy and link quality detection, clear channel assessment for improved coexistence with other wireless networks.

4. IMPLEMENTATION

This project is designed to optimize energy and encrypt data in wireless sensor node by implementing it with hardware using software.

4.1 Hardware Implementation

The figure below represents the complete hardware block of the system

4.1.1 Designed Hardware

The hardware is designed using different electronics components such as microcontroller PIC18F252, VANET Node (WM) ,LED's ,LCD ,Power Supply Regulators 7805, Temp. Sensor LM35. In this four nodes are wireless connected with each other in which two are analog and two are digital. These nodes are kept at particular distance from each other using RF2.4G. In the middle central monitoring unit is placed where all the data of four nodes have and power required for each node is displayed on LCD screen.. When power supply is on , nodes broadcast messages through RF2.4G the power required for each node is displayed on screen and by using energy multipath routing algorithm and energy aware model data is encrypted using Huffman coding. It is found that by designing this model the power required at normal mode is greater as compared to Huffman power. Due to this energy is optimized and data is encrypted. The hardware power level are set in it from 1 to 30 level which calculate energy required for different node.

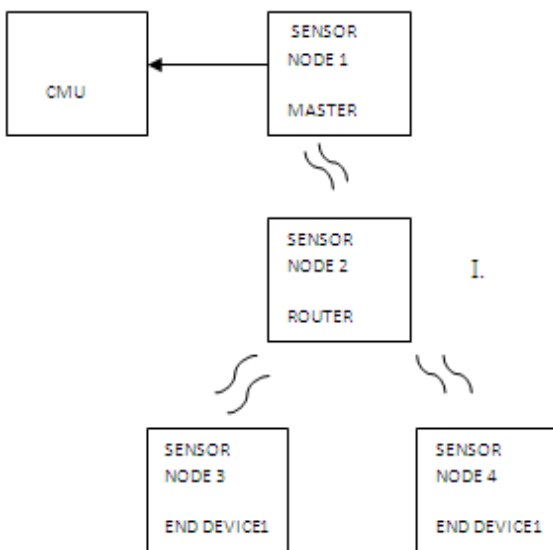


Figure 4.1 Block Diagram



Figure 4.2: Designed Hardware

4.2 Software

For microcontroller development MPLAB IDE software brings an ease of software development previously unseen in the 8/16-bit microcontroller market. The MPLAB IDE is a Windows® based application.

5. RESULT & ANALYSIS

5.1 FROM HARDWARE MODELING

The readings obtained from hardware such as transmitted power, received power and power loss at normal and Huffman power is plotted in table as follows

		Node 1		Node 2		Node 3		Node 4	
		Normal	Huffman	Normal	Huffman	Normal	Huffman	Normal	Huffman
power level 000	Power (mW)	168	109	201	87	149	75	117	58
	Send Packet	21	16	21	16	21	16	21	16
	Received Packet	16	15	16	15	16	15	16	15
	Power loss	5	1	5	1	5	1	5	1
power level 001	Power (mW)	169	109	202	87	150	76	118	59
	Send Packet	21	16	21	16	21	16	21	16
	Received Packet	16	15	16	15	16	15	16	15
	Power loss	5	1	5	1	5	1	5	1
power level 002	Power (mW)	169	109	202	87	150	76	118	59
	Send Packet	21	16	21	16	21	16	21	16
	Received Packet	16	15	16	15	16	15	16	15
	Power loss	5	1	5	1	5	1	5	1
power level 003	Power (mW)	169	109	202	87	150	76	118	59
	Send Packet	21	16	21	16	21	16	21	16
	Received Packet	16	15	16	15	16	15	16	15
	Power loss	5	1	5	1	5	1	5	1
power level 004	Power (mW)	170	110	204	88	151	76	119	59
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 005	Power (mW)	170	110	204	88	151	76	119	59
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 006	Power (mW)	170	110	204	88	151	76	119	59
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 007	Power (mW)	171	111	205	88	152	76	119	59
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 008	Power (mW)	171	111	205	88	152	76	119	59
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 009	Power (mW)	171	111	205	88	152	76	119	59
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 010	Power (mW)	172	111	206	89	153	77	120	60
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2

power level 011	Power (mW)	172	111	206	89	153	77	120	60
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 012	Power (mW)	172	111	206	89	153	77	120	60
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 013	Power (mW)	173	112	207	89	153	77	121	60
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 014	Power (mW)	173	112	207	89	153	77	121	60
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 015	Power (mW)	173	112	207	89	153	77	121	60
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 016	Power (mW)	174	113	208	90	154	78	121	60
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 017	Power (mW)	174	113	208	90	154	78	121	60
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 018	Power (mW)	174	113	208	90	154	78	121	60
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 019	Power (mW)	175	113	210	91	155	78	122	61
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 020	Power (mW)	175	113	210	91	155	78	122	61
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 021	Power (mW)	175	113	210	91	155	78	122	61
	Send Packet	21	17	21	17	21	17	21	17
	Received Packet	17	15	17	15	17	15	17	15
	Power loss	4	2	4	2	4	2	4	2
power level 022	Power (mW)	176	114	211	91	156	79	123	61
	Send Packet	22	17	22	17	22	17	22	17
	Received Packet	17	16	17	16	17	16	17	16
	Power loss	5	1	5	1	5	1	5	1

power level 023	Power (mW)	176	114	211	91	156	79	123	61	
	Send Packet	22	17	22	17	22	17	22	17	
	Received Packet	17	16	17	16	17	16	17	16	
	Power loss	5	1	5	1	5	1	5	1	
power level 024	Power (mW)	176	114	211	91	156	79	123	61	
	Send Packet	22	17	22	17	22	17	22	17	
	Received Packet	17	16	17	16	17	16	17	16	
	Power loss	5	1	5	1	5	1	5	1	
power level 025	Power (mW)	177	115	212	92	157	79	123	61	
	Send Packet	22	17	22	17	22	17	22	17	
	Received Packet	17	16	17	16	17	16	17	16	
	Power loss	5	1	5	1	5	1	5	1	
power level 026	Power (mW)	177	115	212	92	157	79	123	61	
	Send Packet	22	17	22	17	22	17	22	17	
	Received Packet	17	16	17	16	17	16	17	16	
	Power loss	5	1	5	1	5	1	5	1	
power level 027	Power (mW)	177	115	212	92	157	79	123	61	
	Send Packet	22	17	22	17	22	17	22	17	
	Received Packet	17	16	17	16	17	16	17	16	
	Power loss	5	1	5	1	5	1	5	1	
power level 028	Power (mW)	178	115	213	92	158	80	124	62	
	Send Packet	22	17	22	17	22	17	22	17	
	Received Packet	17	16	17	16	17	16	17	16	
	Power loss	5	1	5	1	5	1	5	1	
power level 029	Power (mW)	178	115	213	92	158	80	124	62	
	Send Packet	22	17	22	17	22	17	22	17	
	Received Packet	17	16	17	16	17	16	17	16	
	Power loss	5	1	5	1	5	1	5	1	
power level 030	Power (mW)	178	115	213	92	158	80	124	62	
	Send Packet	22	17	22	17	22	17	22	17	
	Received Packet	17	16	17	16	17	16	17	16	
	Power loss	5	1	5	1	5	1	5	1	
Percentage		64.73		43.17		50.42		49.75		
Overall Percentage		52.02								

Table 5.1 given above shows the packet delivery ratio which is given by

$$P=R/S$$

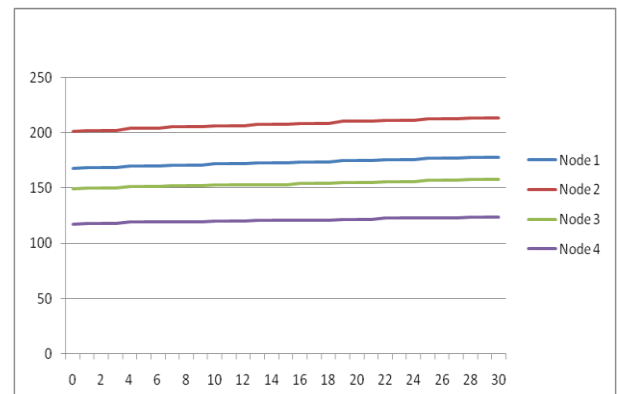
Where P is the packet delivery ratio, R is receiving packet, S is sending packet. Also it gives percentage compression without Huffman encoding & with Huffman encoding, which is given as

$$\text{Percentage compression}=(S-R)/S*100$$

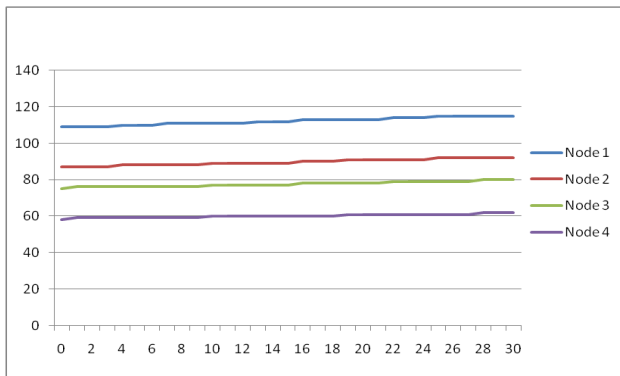
5.2 GRAPHS

From the above obtained result graphs are plotted about normal power and Huffman power for a each four node separately and compared with each other.

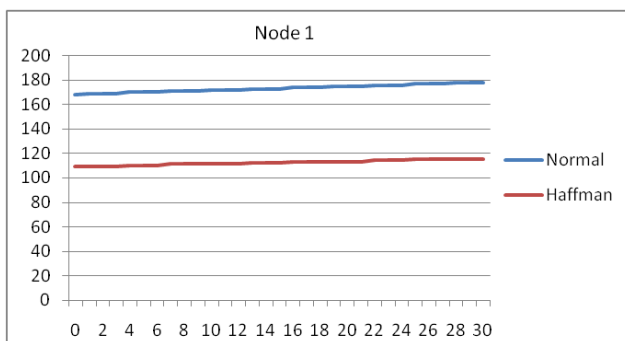
I) Normal power required for all node



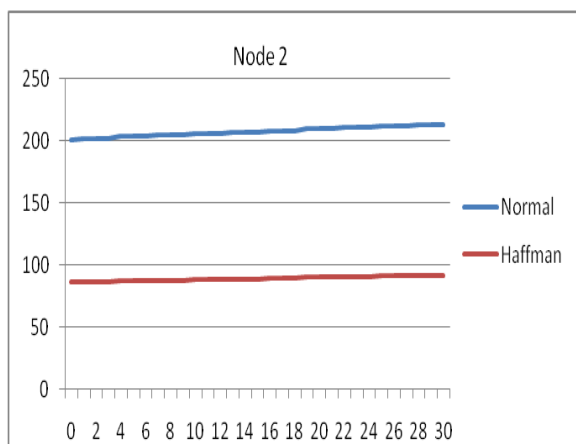
II) Haffman power required for all node



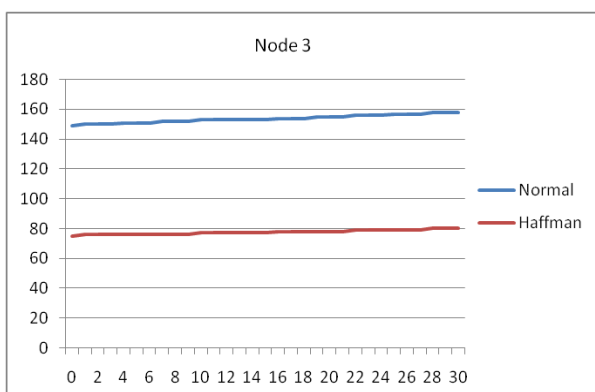
III) Power for Node 1



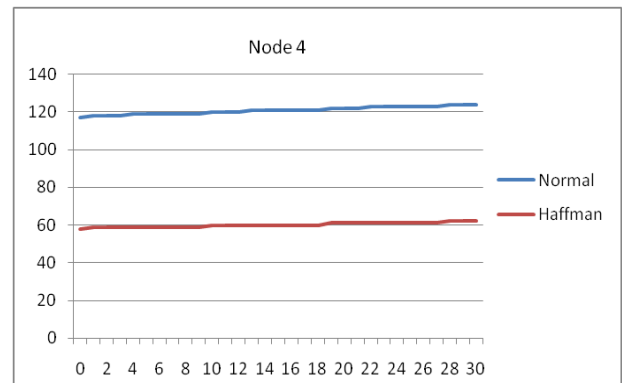
IV) Power for Node 2



V) Power for Node 3



VI) Power for Node 4



By analysing following graph we obtained that using multipath routing energy aware model the power required at Haffman mode is less as compared to normal mode. So lot of energy is saved by designing such system. It increases its battery life and consume less power for data transmission.

6. CONCLUSION

In this thesis, an energy efficient multipath routing protocol for WSN is proposed. This protocol is designed to decrease the routing overhead, improve the latency and packet delivery ratio and through discovering multiple paths from the source to the destination. It has a sink initiated Route Discovery process with the location information of the source known to the sink. There are two types of nodes which are used here one is primary and the other is alternate. The simulation result finds the latency, packet delivery ratio, average control packet over head and total energy consumed. The total normal power required is greater as compared to Haffman power. So by using energy aware model using RF2.4G energy is optimized and data is encrypted in wireless sensor nodes.

7. ACKNOWLEDGEMENT

We are very thankful to Ballarpur Institute of technology for fulfilling our requirements for this project. We express our deep gratitude guide for his unending support to carry out this work and for giving his suggestions and sharing information to improve this research work.

8. REFERENCES

- [1] Jelena Mirkovi'c Gregory Prier Peter Reiher, 2002, "Attacking DDoS at the Source", Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02)1092-1648/02 \$17.00 © 2002 IEEE
- [2] Suraj Sharma, Pratik Agarwal, and Sanjay Kumar Jena. Energy Aware Multipath Routing for Wireless Sensor Networks. In Nabendu Chaki, Natarajan Meghanathan, and Dhinakaran Nagamalai, editors, Computer Networks & Communications (NetCom), volume 131 of Lecture Notes in Electrical Engineering, pages 753-760. Springer New York, 2013.
- [3] Rakesh V, Sarala S M, June 2015, "Energy Optimization In Wireless Sensor Network Using Different Compression And Encryption Techniques", International Journal of Engineering Research and General Science Volume 3, Issue 3, Part-2, May-June, 2015 ISSN 2091-2730
- [4] Dilek Karabudak, "Security Optimization and Data Classification in Wireless Sensor Networks"

- [5] M. Roseline Juliana, S.Srinivasan , Sep 2015, “seladg: secure energy efficient locationAware data gathering approach for wireless Sensor networks”
- [6] ReshmaPatil, Prof.S.M.Shinde , aug 2014, “secure energy efficient routing inWireless sensor network”, ReshmaPatil et al, Int.J.Computer Technology &Applications,Vol 5 (4),1392-1397 ISSN:2229-6093
- [7] Santhosh Simon, K Paulose Jacob, October 2013, “Energy Optimized Secure Routing Protocol for Wireless Sensor Networks”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 4, October 2013
- [8] C. Chong and S. P. Kumar, “Sensor networks: Evolution, opportunities, challenges,” Proc. IEEE, vol. 91, no. 8, pp. 1247–1256, Aug. 2003.
- [9] R. Gao and Z. Fan, “Architectural design of a sensory node controller for optimized energy utilization in sensor networks,” IEEE Trans. Instrum.Meas., vol. 55, no. 2, pp. 415–428, Apr. 2006.
- [10] Tiwari, P. Ballal, and F. L. Levis, “Energy-efficient wireless sensor network design and implementation for condition-based maintenance,”ACM Trans. Sens. Netw., vol. 3, no. 1, pp. 1–23, Mar. 2007.