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

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Vol. 3, Issue 4, April 2015

# Security for Wireless Sensor Network with Spin Protocol

Kunal M Pattani[1], Palak J Chauhan[2]

Professor, C.U.Shah College of Engineering and Technology, Wadhwan City, Gujarat, India[1]

M.E. (E.C.) Student, Dept. of Electronics & Communication Engineering, C.U.Shah College of Engineering and Technology, Wadhwan City, Gujarat, India[2]

**ABSTRACT :** In the recent past, Wireless Sensor Networks have been introduced to use in many application. Wireless Sensor Networks provides a way of information sensing, processing, communicating and transfer of information. To designs the networks, the factors needed to be considered are the coverage area, mobility, power consumptions, communication capabilities, etc. Wireless Sensor Networks have limited energy has hence efficient of protocol has a significant impact on network's lifetime. Security is a main concern everything, whether it is for Wired based networks or wireless based networks. Security is a fundamental requirement of Wireless Sensor Networks. Security in Wireless Sensor Network plays an important role in node communication. For Wireless Sensor Networks has lots of security protocol available but some have limitations. SPIN (Sensor Protocol for Information via Negotiation) has contained three messages which have given security and energy efficiency to Wireless Sensor Network. SPIN protocol is based on data centric approach which efficiently propagates information between sensor nodes in energy constrained mode. SPIN protocol solves the problem of flooding and gossiping. In this documentation we had implement SPIN protocol in NS2 and energy efficient for nodes. We have implement SPIN protocol in Network Simulator. After implementation of SPIN protocol, we had optimized SPIN-I which has given sufficient energy of three stages.

**KEYWORDS**: SPIN, Energy, Routing protocol, Security, WSN.

## I. INTRODUCTION

Wireless sensor network is a group of dense sensor nodes which sends and receives the important information from source to destination. Wireless sensor network is a family of number of small sensors which has some energy. These sensors are very small in size but have a very good sensing computation power.

Wireless sensor network is popularly increasing day by day. It has several applications such as in military, environment, home, health and industry etc. In a wireless sensor network if we have to increase the lifetime of the network then we should take care of battery life of nodes and its load balancing capabilities. For the past few decades a number of Routing protocols have been introduced, but very less number of protocols was up to the mark for energy constraint network, For example flooding is a technique in which one node broadcasts the data packet to all of its neighbours without gossiping with each other, this process repeats till the packet has reached to its destination. But this technique has some problems like implosion and collision.

In WSN [1] the routing protocol can be divided into different families of protocols like location based routing protocol, data centric based routing protocol and multipath based routing protocol, etc. There are a number of data centric protocols [2] i.e. Directed diffusion, Rumor protocol, SPIN protocol etc. But In the data centric routing scheme, data are retrieved through querying. Querying of data is dependent upon the values of their attributes. SPIN (Sensor Protocol for Information via Negotiation) is the first data centric protocol [3] and if we compare the SPIN with Directed protocol then we can point out that they have almost similar characteristics [4] [6]. Its primary work is to reduce Energy consumption and then Reduces redundancy of data. The data centric scheme is one of the different schemes for routing the data and of energy constraints.

10.15680/ijircce.2015.0304129

In this paper, we will introduce and explain SPIN protocol and its energy consumption. In section 2, we have discussed about Security threats in WSN. In section 3, we have discussed about SPIN protocol. In section 4, we have discussed about NS2. In section 5, we have discussed about simulation of SPIN and energy consumption in SPIN.

## II. SECURITY THREATS IN WSN

Security and privacy issues become very important because wireless sensor networks are usually used for very critical applications.

### a. Security Threats in WSNs

WSN is used in the several critical applications. A WSN consists of several number of tiny and resource-constrained sensor nodes. These sensor nodes are spatially distributed and deployed to collect security-sensitive information in uncontrollable environment. In a basic WSNscenario, resource constraint, wireless communication, security sensitive data, uncontrollable environment, and distributed deployment are all defenceless and these defenceless make WSNs suffer from number of security threats. There is several numbers of threats in different layer of network [5] [6].

### 1.2 Physical Layer Threats

In physical layer, there may be several threats to the wireless sensor network, due to the no tamper-resistant WSN nodes and the broadcasting nature of wireless transmission. Security threats to WSN are always added than traditional networks. Types of attacks in the physical layer include physical layer jamming and the subversion of a node.

### 1.3 Link Layer Threats

The responsibility of data link layer is multiplexing of data streams, data frame detection, medium access, and error control. Types of attacks can be possible in the data link layer include Data link layer jamming; Eavesdropping; Resource exhaustion and traffic analysis of wireless sensor network.

### 1.4 Network Layer Threats

In the network layer, threats mostly aim at disturbing data-centric and energy efficient multihop routing. Types of attacks and threat can be possible in the network layer contain Spoofed, altered, or replayed routing information; Sybil attack; Selective forwarding; Sinkhole attack; and flooding attack.

### 1.5 Application Layer Threats

Applications in the application layer of wireless sensor network (WSN) heavily rely on localization, time synchronization, and in network data processing to collaboratively process data. Types of attacks and threat can be possible in the network layer include False data filtering; Clock un-synchronization; False data injection.

## III. SPIN PROTOCOL

The SPIN protocol is emerged with the help of many other conventional protocols such as flooding [7]. Flooding has some strength and some drawbacks for disseminating the data in sensor network. In flooding a source node sends data to all its neighbors. Upon receiving data, it saves a copy and sends a copy to its entire neighborhood. Flooding is a protocol, which spreads data very quickly all over the network. But it has some problems which are as follows:

- Implosion*:* In this problem, nodes send the messages to its neighbor nodes without bothering about whether it has already the same data or not.

- Overlap: Sometimes nodes cover the similar geographic area for sending the data, this causes the overlapping of data and a lot of energy is wasted.
- Resource Blindness: In this problem, nodes are never concerned about how much energy is remaining in the neighbor nodes, it blindly sends the data to the sensor nodes. This conventional protocol never calculates the total energy in the sensor network.

Sensor Protocol for information via Negotiation Protocol (SPIN) can be categorized into four types: SPIN-PP, SPIN-EC, SPIN-BC, and SPIN-RL. SPIN-PP and SPIN-EC are used for point to point network and SPIN-BC and SPIN-RL are used for a broadcast network. Three deficiencies (implosion, overlap and resource blindness) which occurred in simple protocols are overcome by two main approaches i.e. negotiation and resource adaptation. Spin nodes use three types of messages to communicate[8].

- ADV - when a node has new data to advertise then it broadcasts ADV packet which contains Meta data.
- REQ – when a node needs new data then it sends the REQ packet to get the real data.
- DATA – This is an actual data which has a header named as Meta data.

Data messages are important and larger than the ADV and REQ packets. DATA packets contain real messages not the Meta data.

Meta-Data: SPIN doesn’t specify meta-data’s format which is considered to be application specific. However, if for sensor data X, x is the meta-data descriptor, the size of x in bytes ought to be lesser than size of X.

## IV. NETWORK SIMULATOR

The network simulator (NS), which is a discrete event simulator for networks, is a simulated list developed by VINT (Virtual Inter Network Tested) project group. It supports simulations of TCP and UDP, several of MAC layer protocols, different routing and multicast protocols over both wired and wireless network.

Network simulator worked on based Linux X86-64.Network simulator is a name for series of discrete event network simulators, specifically ns-1, ns-2and ns-3. Network simulator, mainly used in research and teaching. Ns-3 is free software, openly available under the GNU GPLv2 license for research, progress and use.

## V. SIMULATION

We had considered 8 nodes. As per the working of SPIN, node 0 sends advertisement to their neighbors nodes n1, n2, n3. Advertisement carried meta data which has smaller than actual data. After completion of advertisement node 2 and node 3 send request to node 0. After getting request messages node 0 send them to actual data. After getting actual data of node 3 and node 4, they had also sent advertised message to their neighbors node. Node 2 send advertised message to node 4 and node 5. Node 3 send advertised message to node 6 and node 7. After completion of advertisement node 5 and node 7 send requests to node 2 and node 3 respectively. After getting request node 2 and node 3 sends actual data to node 5 and node 7 respectively. After implementation of SPIN, we had to optimize energy of nodes which has shown in figure.

### 4.1 ADV

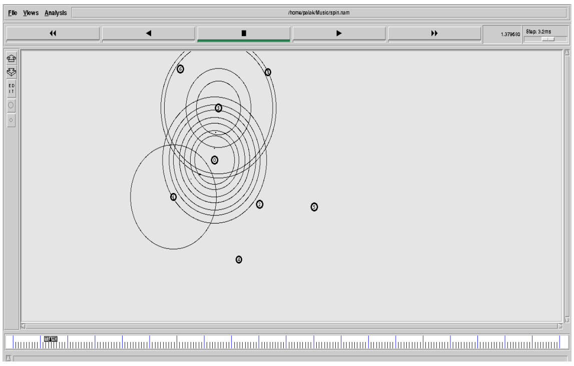

*Figure 1 Sending ADV message from node 0*

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

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Vol. 3, Issue 4, April 2015

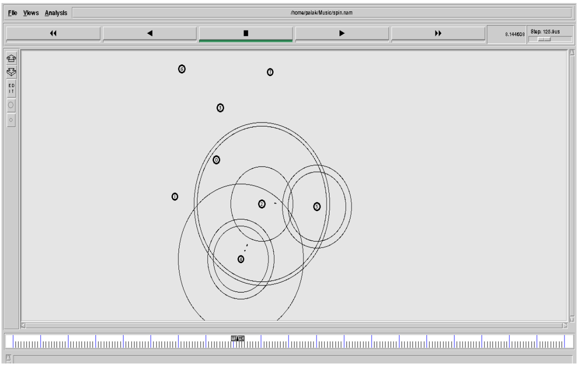

*Figure 2 Sending ADV message from node 2*

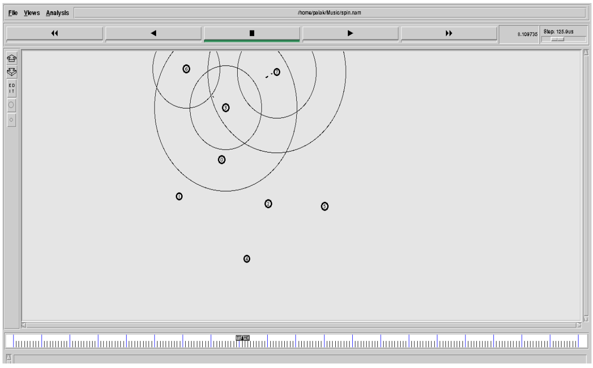

*Figure 3 Sending ADV message from node 3*

## 4.2 REQ

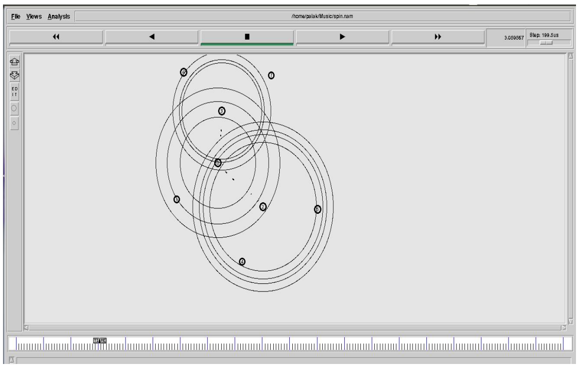

*Figure 4 sending REQ message from node2 and node 3*

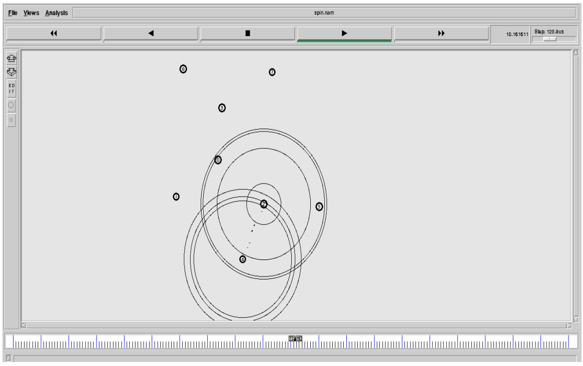

*Figure 5 Sending REQ message from node 4*

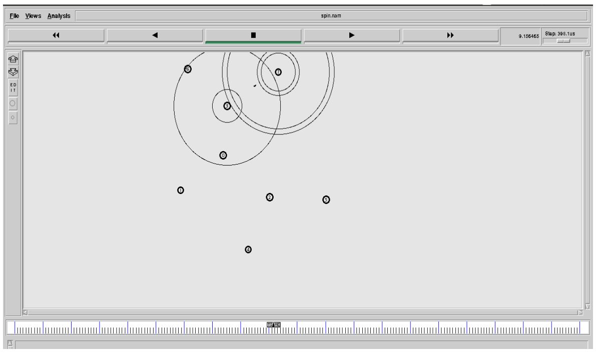

*Figure 6 Sending REQ message from node*

10.15680/ijircce.2015.0304129

### 4.3 DATA

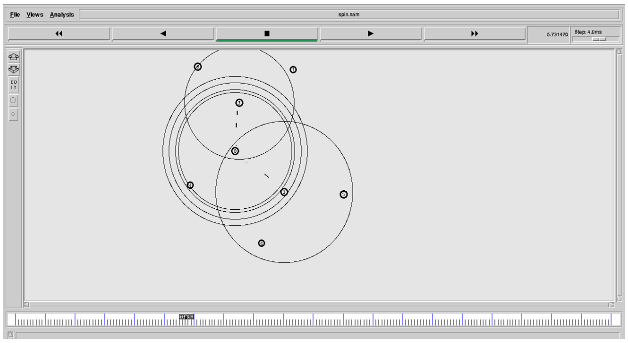

*Figure 7 Sending data frome node 0*

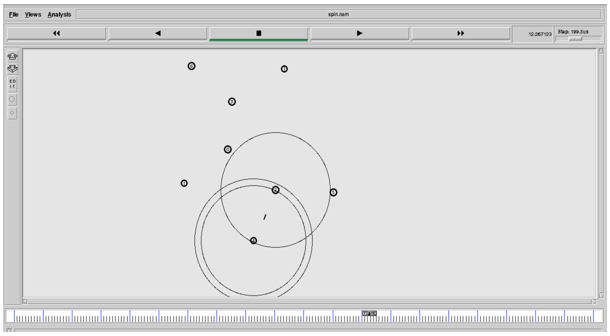

*Figure 8 Sending DATA message from node 2*

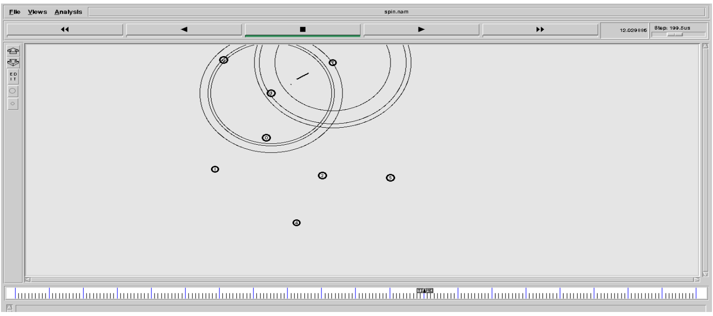

*Figure 9 Sending DATA message from node 3*

### 4.4 ENERGY

Total energy is consumed by SPIN protocol in which one node transmits the m=1500 bytes of data it receives to the neighbor node through adopting SPIN protocol. Assuming that both of ADV and REQ messages are L=500 bytes, it needs to consume Et energy to send a byte and Er energy to receive a byte. The network is distributed, no packet losses or queuing delay, and the average number of node's neighbor is N. Any node in network will forward the m bytes of data it receives to the next hop node.

1) The steps of node B forwards the m byte of data in the SPIN protocol are:
   a. Send ADV messages, energy consumption is (N-1) LEt
   b. Receive the REQ message from N-1 nodes around it, the energy consumption is L (N-1) Er
   c. Send Data + L bytes of data, consume (m + L) (N-1) Et energy

2) The steps of node B receives m bytes of data in the SPIN protocol are:
   a. Receive ADV message, consume LEr energy
   b. Send REQ message, the energy consumption is LEt
   c. Receive m bytes of data, consume (m + L) Er energy

According to the above description, in SPIN, the minimum energy consumption in process that node B receives the data and forwards the data to the next hop nodes is showed by the formal below:
ESPIN=Et(2NL+mN—m—L)+(NL+m+L)Er

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

### 4.4.1 TRANSMITTING ENERGY

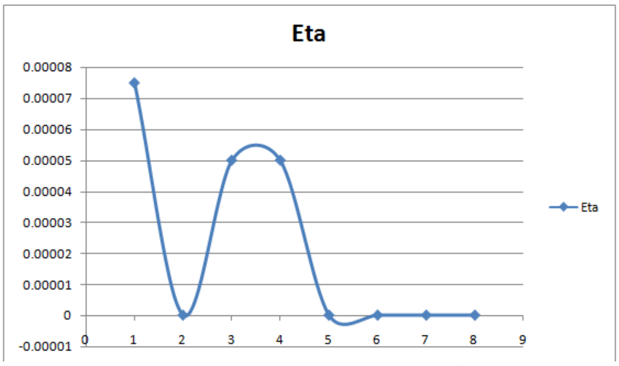

*Figure 10 Transmitting Energy of ADV*

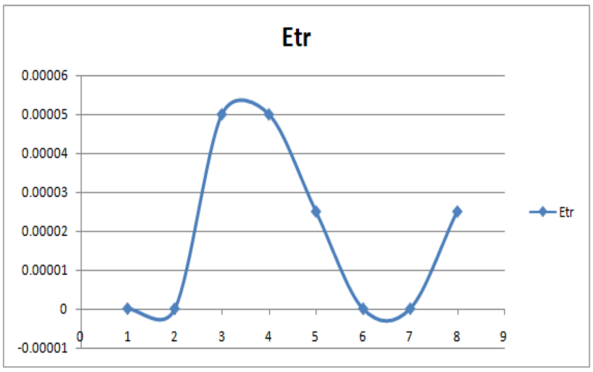

*Figure 11 Transmitting Energy of REQ*

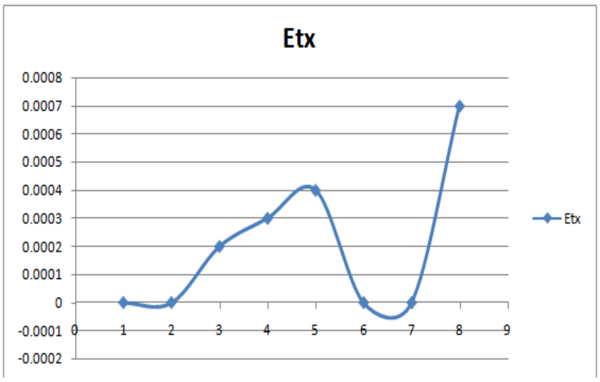

*Figure 12 Transmitting Energy of DATA*

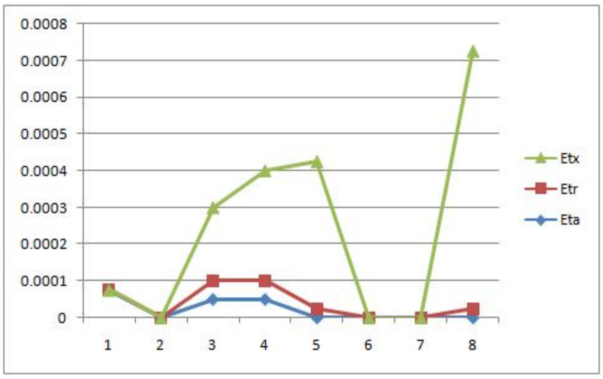

*Figure 13 Transmitting Energy*

### 4.2.2 RECIVING ENERGY

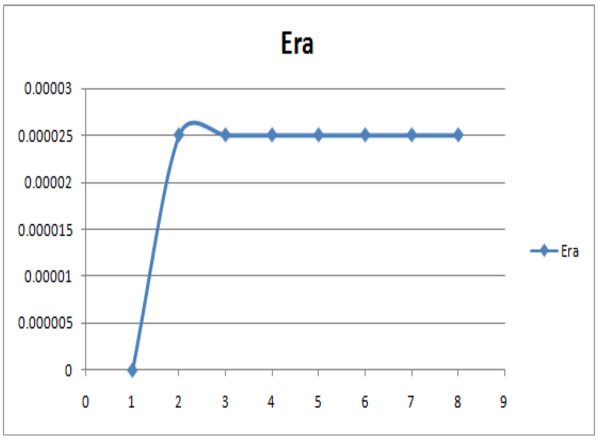

*Figure 14 Receiving Energy of ADV*

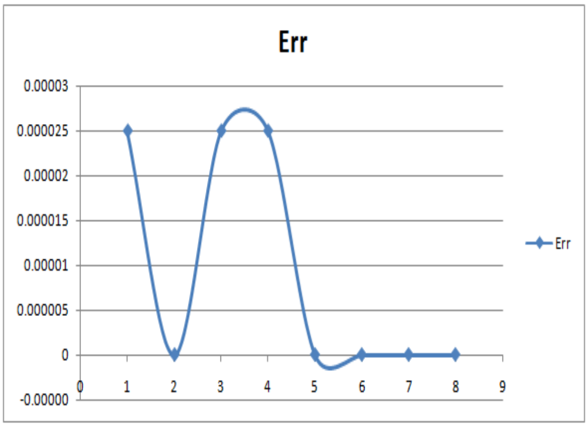

*Figure 15 Receiving Energy of REQ*

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

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Vol. 3, Issue 4, April 2015

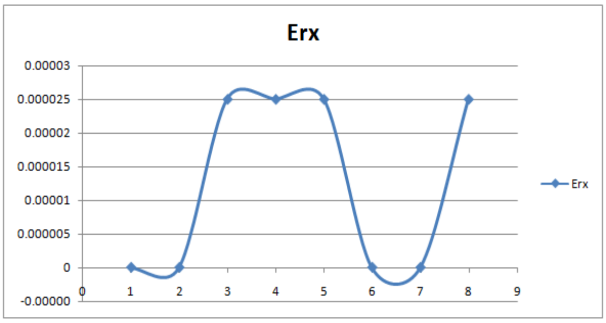

*Figure 16 Receiving Energy of DATA*

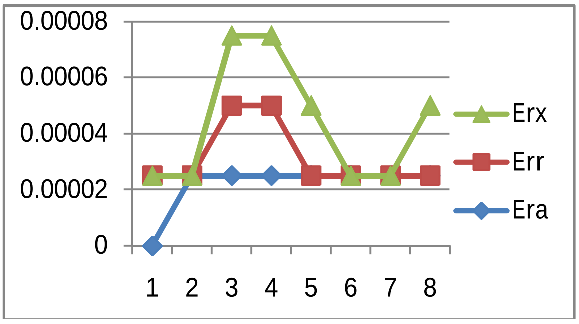

*Figure 17 Receiving Energy*

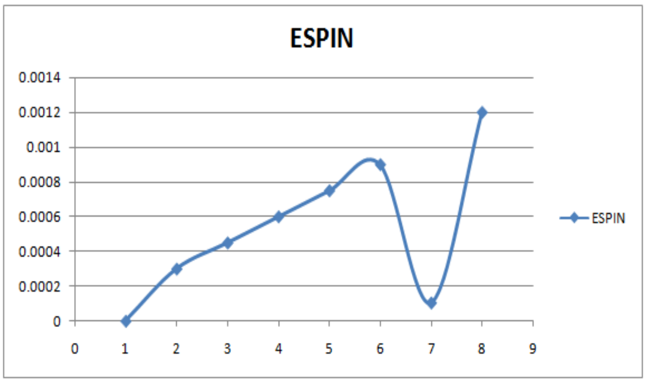

*Figure 18 Total Energy of SPIN*

## VI. CONCLUSION

The simulation result portrayed with the help of NS2, shows source node sends ADV message to neighbours nodes, REQ sent for requesting data and DATA is the actual data which has transmitted after receiving request. Also shown that the energy consume in ADV, REQ and DATA. In future work, concept of energy optimization and distance discovery also the concept of sending data directly to the sink are implemented which better result for Wireless Sensor Networks.

## REFERENCES

1. Shio Kumar Singh, M P Singh, and D K Singh, “Routing Protocols in Wireless Sensor Networks–A Survey”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.
2. IAkyidiz,W.Su,YSankarasubramaniam and E. Cayirici, “Wireless sensor network: A survey”, Computer Networks (Elsevier), vol 38, pp.393-422,2002.
3. Azni, A.H., Madihah Mohd, S., Azreen, A., and Ariff Syah, J., (2009), “Performance Analysis of Routing Protocol for WSN Using Data Centric Approach”, World Academy of Science, Engineering and Technology, Vol. 53.
4. Jian Wu, Paul Havinga, “Reliable Cost-based Data Centric Routing Protocol for Wireless Sensor Networks”, Proceedings of Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD’06).
5. J. Kulik, W. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks", *Wireless Networks*, vol. 8, no. 2/3, Mar.-May 2002, pp. 169-185.
6. C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks", *Proceedings ACM MobiCom'00*, Boston, MA, Aug. 2000, pp. 56-67.
7. B.Baranidharan, B.Shanthi, “A Survey on Energy Efficient Protocols for Wireless Sensor Networks”, International Journal of Computer Applications (0975 – 8887) Volume 11– No.10, December 2010.
8. Prashant Mishra, Rakesh Tripathi, “Optimum Energy Path (OEP) Protocol for Wireless Sensor Network”,978-1-4799-2494-3/14/$31.00 ©2014 IEEE.