International Journal of Engineering Research and General Science Volume 4, Issue 2, March-April, 2016
ISSN 2091-2730

A survey on secure and energy efficient LEACH protocol

Rashim Rana Er. Anoopa Arya
(Pursuing M. Tech, CSE) (Assistant Professor, CSE)
Maharishi Ved Vyas Engineering College, Kurukshetra University

rashimrana02@gmail.com, +91-8572088409

Abstract— WSN is a network in which sensor nodes are placed in an area so that physical information like military surveillances, transport monitoring, habitat monitoring, etc can be gathered. These sensor nodes sense the data and send it to the B for evaluation for which the data aggregation is done. The data aggregation is achieved by using LEACH routing protocol. LEACH protocol is clustering algorithm which is self organizing in nature and form clusters on the basis of the signal strength of the sensors. In this paper, the WSN and security requirements for secure data aggregation are studied. Also the LEACH protocol with its phases and various attacks on LEACH are studied. In this paper techniques for energy efficieny is also apply. Thus, the research in this paper is based on WSN, its security requirements,its energy efficieny , LEACH, LEACH attacks and its effect on WSN.

Keywords— Wireless sensor network, base station, Low-Energy Adaptive Clustering Hierarchy, Time division multiple access, Cluster head, carrier sensing multiple access, medium access control.

INTRODUCTION

The Wireless sensor networks is an infrastructureless and highly distributed network in which small lightweight wireless nodes are present. In this sensor nodes are independent and power limited sensing devices which are deployed in the region to sense different types of physical information from the environment[9].

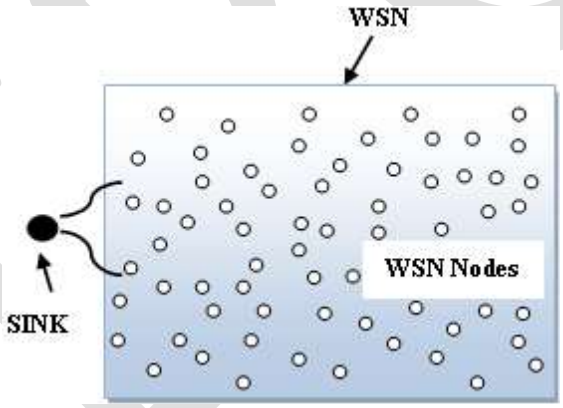

Figure 1: Illustration of WSN Network [8]

Sensors are having the ability to communicate through wireless channels and the energy computational power and memory are constrained in the sensors. The environmental data is monitor by the WSN this is the major application of the WSN. WSN transmit this data to the central node which is called as the sink node. The sink node initiate some specific action on the basis of analyzed data. The sink node analyse the data and compute the minimum or maximum or computation of average. Either sink node or network analyse the data. Every sensed data is transmitted to the sink node if analysis is carried out at that node.The required aggregate is computed by sink node when it received the data from all the node. This method is used for aggregating the data and it is called All-Node data aggregation scheme. In this approach if the amount of transmitted data increases then the consumption of energy also increases. The over all lifetime of WSN increases the aggregated data amount in the network.

In data aggregation scheme the neighboring node send the information to the aggregator node which compute the aggregate and send the aggregated data to the sink node. The number of transmission reduces and the bandwidth and energy utilization is improving by the the data aggregation.There are some security issue are present. The security in data aggregation is achieve by the secure data aggregation[2]

Sensor node energy consumption is affected by the routing protocol. Three routing protocols of wireless sensor network are :
a). Flat Based Routing Protocol:

The same role and functionality in transmitting and receiving data is play by all the nodes. In this the selection of specific set of sensor nodes to be queried is very typical due to lack of global identification with random deployment of sensor nodes. The query is send to different part of the field by base station and wait for result data from only selected parts of field. This method is called data centric routing.

b). Hierarchical Routing Protocol:

Different roles are assign to the node in this network like members of cluster, cluster head etc.This routing is mainly consider as two layer architecture in this one layer responsible for cluster head selection and other for the routing.

c). Location Based Routing Protocol:

The location tell the address of the sensor node. The signal strength give the estimate about the distance between the nodes. In this some location based scheme demand that the nodes go to the sleep mode if they are not doing any activity for saving the energy.

Hierarchical-based routing protocols are avoid redundancy and they are the best. In this network energy is used efficiently and lifetime and scalability is enhanced. In this protocol, nodes are making the clusters in which higher energy nodes are used to process and forward the data, while other nodes can be used to sense the data. Data aggregation and fusion for reducing the size of transmitted message for the base station is done by cluster head[8]

Security Requirements

In this section of secure data aggregation two types of confidentiality requirements are considered.

1. Generic Confidentiality : The content of data is not access by the sensor node and they are not participate in the data aggregation.
2. End-to-End confidentiality : Sensors actively participating to the aggregation mechanism do not access the data that is already aggregated.

Network Model

In this we consider a network which consist of small devices and a sink node.The two type of nodes are present in this sensor nodes (SN-nodes) they senses the actual data and Aggregator nodes (AG-nodes) they are responsible for sending queries and combining answers which are send by the children and a message is forward to the parent which contains the intermediate aggregation result of the queries and their answers.The organization of nodes in the form of m-ary tree. The tree structure is as shown in fig. 1 In Fig.1. S0,S1. . . S2m are sensing nodes and SGl−1 . . . SGl−m are aggregating nodes, where l is the level of the node in the tree. The root of the tree is calles sink node[2].

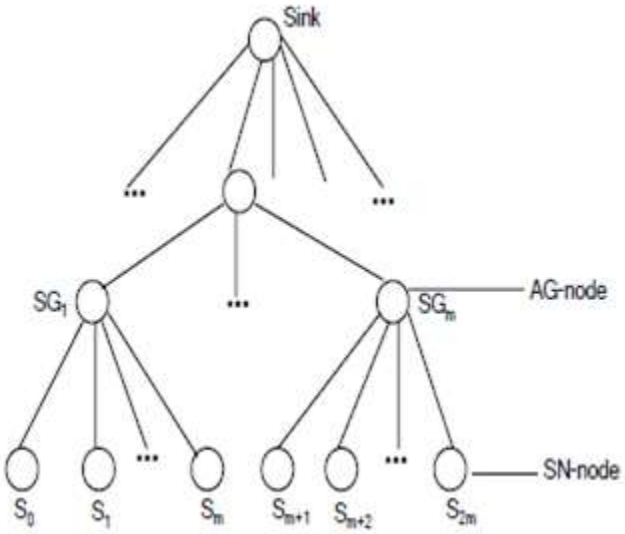

Figure 2: Tree structure of nodes in the network. In each level K nodes are present. Nodes of leaf level are sensing nodes(SN-N odes) and others are aggregated nodes(AG-Nodes).

LEACH (Low-Energy Adaptive Clustering Hierarchy)

A dynamic hierarchical clustering algorithm for sensor networks is called Low Energy Adaptive Clustering Hierarchy (LEACH) is introduced by Heinzelman, *et al*. This is a protocol, which is cluster based and in which distributed cluster formation is done. LEACH selects some sensor nodes as cluster-heads randomly and this role is rotated for equal distribution of the energy load among the sensors in the network. In LEACH the data is compressed by the cluster head which is upcoming from nodes of the same cluster and an aggregated packet is send to the BS by the cluster head for reducing the amount of information that is send to the BS. TDMA/Code division multiple access MAC is used for reducing inter-cluster and intra-cluster collisions. Randomized rotation of cluster head is conducted after a given interval of time for obtaining uniform energy dissipation in the sensor network.[10]

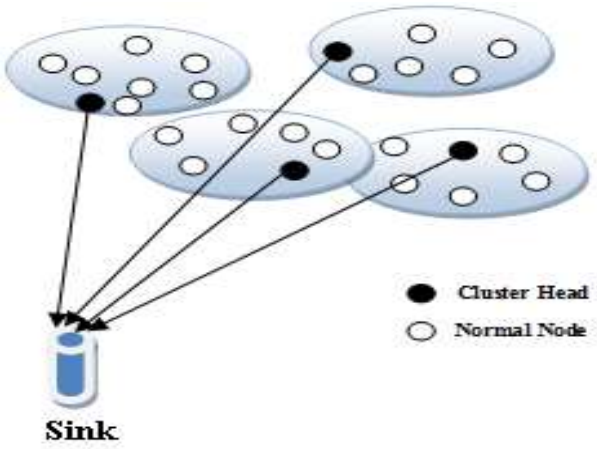

Figure 3: LEACH Routing Topology[8]

LEACH protocol operation is split into two phases:

- Setup phase
- Steady phase

Setup phase

The set-up phase organize the cluster and select the cluster-heads. At the starting each node is independent of the other nodes . A number is generated by each sensor node which is called random number such that 0< random < 1 and this number is compares with a pre-defined threshold T (n). The sensor node becomes cluster-head for that round if the random < T(n). , else it becomes cluster. The threshold is given T(n) below:

$$T(n) = \begin{cases} P & \text{if } n \in G \\ \dfrac{}{1-P(r \bmod (1/P))} & \end{cases}$$

Where,
P is the probability of the node being selected as a CH.
r is the number of rounds.
G is the set of nodes that haven't been CH in the last 1/p rounds mod denotes modulo operator.

The next 1/p rounds are not select those nodes which are selected as a cluster head in the previous r rounds. When CH is selected the CH use a CSMA MAC protocol for broadcasting an advertisement message to its neighbours which are placed in the new cluster head. The join-request message which contain the IDs of the nodes is send by using CSMA for joining with the cluster which snd the strongest strength signal to the nodes. The TDMA schedule is set up by the CH for data transmission coordination in the cluster and propogate it to its cluster members.The collision is prevented between data messages by TDMA scheme and TDMA also conserves energy between non cluster head nodes. At that point all nodes know their TDMA slots and steady state phase is started.

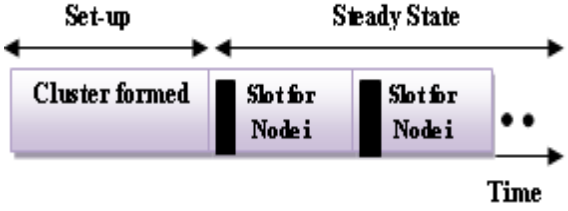

Figure 3: Period of LEACH [8]

Steady State Phase

In this phase the surrounding sense by the cluster members and sensed data is transmit to their CH on the basis of the TDMA schedule which is received in the setup phase. For saving the energy for other slots the sensor node go to the sleep mode. When all the data is received by the CH which is send by its cluster members. The CH compute the aggregated data and send this aggregated data to the BS. After some time the network is go back to the setup phase for entering to the next round. In the next round the CH selection is occure.

ATTACKS ON LEACH

Some of the Attacks on LEACH are as follows.

a). Selective forwarding attack

The message is faithfully forward to the destination by the node. Certain messages are not forward by the malicious node . The malicious node drop the message and ensure that the message is not reach to the intended destination. This attack is called selective forwarding attack.

b). Sybil attack

In a Sybil Attack, the multiple identities of a node to other nodes in the sensor networks is shown by the malicious node. By creating new false identities of the nodes or stealing identities of other nodes in the network this attack is done. In this a single node may be used many times. This attack causes many affects like consuming energy,increasing traffic,packet dropping, reducing network life time etc

c). Hello flood attack

The HELLO packets are send by the sensor nodes to the neighbours for alerting them about the attack. These packets are send only with in the transmission range. But an attacker some times sends the flood of false HELLO packets. After receiving the packets from an attacker the nodes consider that the attacker is suited inside the transmission range but in actual it is far away from the nodes. In this the nodes transmit the messages unnecessarily and reduces their energy.

LITERATURE SURVEY

Wendi B.Heinzelman.et.al(2002) When we set hundreds or thousands of cheap microsensor nodes in a network they allows users for combining the data from the individual nodes by accurately monitoring a remote environment. In this network robust wireless communication protocols are required which are energy efficient and provide low latency. In this paper, the author develop a protocol architecture called LEACH for microsensor networks that combines the idea of both media access and energy-efficient cluster-based routing with application-specific data assembling for the achievement of good performance in terms of latency, system lifetime and application-perceived quality. A new distributed cluster formation technique in LEACH is used that enables self-organization of numbers of nodes, rotating cluster head positions for even distribution of the energy load among all the nodes and algorithm for adapting cluster. Author's results show that the system lifetime improve by LEACH by an order of magnitude compared with general-purpose multihop approaches[1].

A.S.Poornima. et. al (2010) In WSN large number of nodes are consist of with limited communication capabilities, sensing and computation. In such network resource constrained nodes are present and transmission of data in this is a energy-consuming operation. By reducing the number of bits transmitted on a network the lifetime of a network is increased. The data aggregation method is used for reducing the data transmission. The issues of security such as confidentiality , data integrity and freshness in data aggregation become essential When the WSN is deployed in a remote or hostile environment where sensors are prone to node failures. For achievement of security in data aggregation we use secure data aggregation schemes. In this paper the author propose a Secure Data Aggregation scheme which provides end-to-end data privacy. In this 30%-50%. of the average number of bits transmitted are reduced [2].

Abderrahim Beni Hssane.et.al(2010) In WSN for increasing the lifetime and scalability of a network we can use a clustering algorithm. In this paper, the author propose a Position-Based Clustering (PBC). algorithm in this algorithm he evaluate a distributed energy-efficient clustering algorithm for heterogeneous WSNs. PBC is an improvement of LEACH-E. The ratio between the remaining energy of network and residual energy of each node give the probabilities on the basis of that probabilities the PBC elected the cluster heads. In this 2 level hierarchy is used by selecting a intermediate node for the data transmission. Moreover, in this a new technique is used for cluster formation which not only based on the received signal strength of the cluster head's advertisement but also on its position. The lifetime of the whole network is increased by this algorithm and in performs it is better than LEACH, LEACH-E and SEP [3].

Mortaza Fahimi Khaton Abad.et.al(2011) Research on WSN has received much attentive as they offer an advantage of monitoring different kinds of environment by sensing physical phenomenon. The important application of the sensor network applications are scalability, Prolonged network lifetime and load balancing. For achieving these goals cluster sensor nodes technique is used. In this paper the author introduce an LEACH based energy efficient clustering algorithm for sensor networks.WSN uses LEACH which is the most popular cluster-based structures. TDMA and MAC both are used by LEACH for balancing the energy consumption. The proposed protocol integrated some feature to LEACH for reducing the consumption of energy in each round. The result of proposed work shows a significant reduction in network energy consumption compared to LEACH[4].

Tripti Sharma.et.al(2012) WSN is the network in which power-limited sensing devices are present these are called sensors.These sensors spread in a region for sensing different types of information which is present in the environment. The considerable amount of energy is dissipated when these sensors sense and transmit data to other sensors nodes which are present in the network. In this paper, F-MCHEL is propose which is a homogeneous energy protocol. In LEACH protocol on the basis of threshold values clusters are formed; whereas, in the proposed protocol we use fuzzy logic approach for electing the cluster-head based on two form - energy and proximity distance. The master cluster head is elected out of the previously elected cluster heads.Master cluster head is having the maximum residual energy if the energy is low so it is not called as a master cluster head. In conventional LEACH all cluster heads are send the aggregated information to the BS but in the proposed protocol only master cluster head is used for sending the information to the BS. Simulation results on MATLAB shows that this proposed protocol provides better stability period, higher energy efficiency and lower instability period as compared to LEACH protocol. Results obtained shows that an suitable Master cluster-head election can enhance the lifetime of the network and reduce the energy consumption[5].

Mona El_Saadawy.et.al(2012) Security solutions for WSN are not developed easily due to the dangerous nature of wireless medium and limited availability of resources in WSN. The encryption/decryption algorithms are the most essential part of the secure communication and their implementation is very intricate in WSNs. since they integrated routines that having very complex and intense computing procedures.In WSN the designing of a secure clustering protocol that achieves the desired security goals while keeping an acceptable level of energy consumption is a very challenging task. LEACH protocol is a basic clustering-based routing protocol for WSNs. S-LEACH is the modified version of LEACH which protect againt the outside attack by using cryptographic technique. This paper proposes MS-LEACH for enhancing the security of S-LEACH by offering data confidentiality and node to CH authentication by using pairwise keys which is shared between their cluster members and the CHs. MS-LEACH has efficient security properties and achieves all goals of the WSN security. The result shows that the protocol accomplish the in demand security goals and perform better than other protocols in terms of energy consumption, network[6].

Baiping Li.et.al(2012) A WSN is a group of sensor nodes which are able for monitoring different types of environments for applications that include biological detection, home security, diagnosis and machine failure. For long period of time the gathering of sensed information is an energy efficient manner is not easy in the sensor network. In WSN the amount of data transmitted between sensor nodes and the base station is reduced by the help of data fusion. The LEACH protocol is best solution for data collection problem, where formation of small number of clusters are done in a self-organized manner. On the basis of LEACH protocol, a low energy-consumption chain-based routing protocol LEACH-CC is proposed. In the new protocol each node will send information about its energy level and current location to the BS for its characterization. The simulated annealing algorithm is run for determining the clusters for that round. Then a chain routing is set between clusters for decreasing the amount of nodes which communicate with the BS. Finally, the results show that LEACH-CC performs better and it not only extends the lifetime of the network, but also improves the energy efficiency[7].

Alisha Gupta.et.al(2013) Encryption schemes which are operated over ciphertext are of extreme importance for WSN & specially in LEACH protocol. Energy is the salient limit of LEACH. Due to this limitation , the designing of a confidentiality scheme for WSN is important by doing this the sensing data can be transmitted to the receiver efficiently and securely and at the same time energy consumed must be minimum. Hence the author proposed LEACH-HE in which homomorphic encryption is added to LEACH protocol. The homomorphic encryption is the confidentiality scheme in LEACH-HE. In this encryption technique algebraically aggregation of data is occure. The decryption of data is not occure hence energy consumption is less. In this proposed work results are obtained in terms of three forms - amount of data transmitted, total energy consumed and number of nodes alive. The performance of LEACH_HE is somewhat similar to LEACH[8].

Muneer Alshowkan.et.al(2013) Working with WSN is a challenging task because in this many challenges are present such as the limited resource in processing power, energy and storage. The security maintenance in WSN is a challenging task due to presence of

limited energy. The aim of the paper is reducing the power consumption and improving the current security mechanisms in WSN. The energy routing protocol is provided by LEACH and it do not cover the security requirements. Alternatively, this paper aims to design LS-LEACH (Lightweight Secure LEACH) which is more secure and energy efficient routing protocol. Authentication algorithm is added to this for assuring authenticity, data integrity and availability. Furthermore, this paper shows the improvement over LEACH protocol which make it more secure and tell how the energy efficiency is increased [9].

Mayur S.et.al(2015) Hierarchical routing protocol is used by many application in WSN for routing of the sensed data to the sink, LEACH is one of those application and it is the first and most widely used hierarchical distributed clustering protocol in WSN. Security is the most important factor in WSN because they are prone to intrution and different types of network attack. The joining of nodes in a cluster head on the bases of Received Signal Strength (RSS) of HELLO packets which are received from CHs making it susceptible to HELLO Flood attack. HELLO Flood attack is detected by either cryptographic approach this approach is less suitable in terms of battery power and memory or non cryptography approach the packet are sending for detection which increases communication overhead as the energy needed for transmission of packet is more than the energy needed for processing. In this author proposed a detection scheme for HELLO Flood attack on the basis of cryptography and non cryptography solutions. The no. of transmission of test packets is reduced in this paper and in this location dependent key(LDK) management scheme is used which provides the security[10].

CONCLUSION OF SURVEY

The literature above reviewed can be concluded as:

Author and year	Work	Technique	Conclusion
Wendi B. Heinzelman 2002	Design Application Specific Protocol for WSN	WSN	The high performance which is needed under the tight constraints of the wireless channels are provided by LEACH
A.S.Poornima 2010	Securing the End-to-End Data Aggregation in WSN	Aggregation scheme and homomorphic encryption	In the SEEDA protocol the no. of bits which are transmitted are reduced from 30%-50%.
Abderrahim Beni Hssane 2010	Design Position-Based Clustering protocol for An Energy-Efficient Clustering Hierarchy for Heterogeneous WSN	Heterogeneous WSN model, Radio energy dissipation model, LEACH	PBC provides better use and optimization of energy dissipation in the network.
Mortaza Fahimi Khaton Abad 2011	LEACH Algorithm is modify for WSN	Clustering	The network energy of modified LEACH is high and the Dead nodes in modified LEACH is less.
Tripti Sharma 2012	Design Fuzzy Based Master Cluster Head Election Leach Protocol in Wireless Sensor Network	LEACH ,LEACH-C,CHEF	In this stability period is extended and energy is well distributed. In this the cluster are well separed from each other.
Mona El_Saadawy 2012	Security of S-LEACH is enhanced for WSN	Use cryptography with S-LEACH	MS-LEACH is better in terms of average power consumption, average work lifetime,average network throughput and average normalized routing load.
Baiping Li 2012	Study LEACH Protocol and apply add some new techniques for its improvement	LEACH, Radio Energy Model for LEACH-CC, LEACH-Centralized with Chain	In LEACH-CC the distribution of energy load among the nodes increase quality and the lifetime of the network. If the size of network increases the further improvement by LEACH-CC are shown.
Alisha Gupta 2013	Implement the LEACH protocol by using homomorphic encryption	Homomorphic encryption	In LEACH protocol if we add homomorphic encryption the protocol become more secure. The no. of bits transmitted are same in both LEACH_HE

			and LEACH. Hence by these performance parameters we conclude that adding homomorphic encryption to LEACH donot degrades the performance.
Muneer Alshowkan 2013	Design a new secure and Energy Efficient Routing Protocol for WSN	LEACH, clustering and data aggregation	The, network life time, system throughput and the total energy consumption of the network become better after improving the LEACH protocol.
Mayur S 2015	Security of LEACH Protocol is enhanced from HELLO Flood Attack in WSN Using LDK Scheme	Location Dependent key	The performance of the network is improved by the proposed work.In this detection time and energy for detection are less used. In this work LEACH function smoothly in the HELLO Flood Attack.

CONCLUSION

In this paper the WSNs are studied and the various security concerns related to WSNs are also studied. The LEACH protocol and attacks on this are studied. The methods of security on LEACH are studied. The alternative solutions for security and energy efficiency are : In LEACH protocol if we add homomorphic encryption the protocol become more secure and this technique donot degrades the performance. The position based clustering protocol provides better use and optimization of energy dissipation in the network.The network energy of modified LEACH is high and the Dead nodes in this is less. For making the networking more secure and energy efficient we can use any of the given techniques as given in the paper and some other techniques are also available we use these as per the requirement.

REFERENCES:

[1] Wendi B. Heinzelman, "An Application- specific Protocol Architecture for Wireless Microsensor Networks" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 1, NO. 4, OCTOBER 2002.

[2] A.S.Poornima, B.B.Amberker, "SEEDA : Secure End-to-End Data Aggregation in Wireless Sensor Networks" IEEE 2010.

[3] Abderrahim Beni Hssane, Moulay Lahcen HASNAOUI, Mostafa SAADI, "Position-Based Clustering: An Energy-Efficient Clustering Hierarchy for Heterogeneous Wireless Sensor Networks" International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010.

[4] Mortaza Fahimi Khaton Abad , Mohammad Ali Jabraeil Jamali, "Modify LEACH Algorithm for Wireless Sensor Network" International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, September 2011 ISSN (Online): 1694-0814

[5] Tripti Sharma , Brijesh Kumar, " F-MCHEL: Fuzzy Based Master Cluster Head Election Leach Protocol in Wireless Sensor Network" International Journal of Computer Science and Telecommunications Vol. 3, Issue 10, October 2012.

[6] Mona El_Saadawy, Eman Shaaban, " Enhancing S-LEACH Security for Wireless Sensor Networks" IEEE 2012

[7] Baiping Li, Xiaoqin Zhang, "Research and Improvement of LEACH Protocol for Wireless Sensor Network" International Conference on Information Engineering Lecture Notes in Information Technology, Vol.25, 2012

[8] Alisha Gupta , Vivek Sharma, " Implementation of LEACH Protocol using Homomorphic Encryption" International Academy of science, Engineering and technology

[9] Muneer Alshowkan, Khaled Elleithy, Hussain AlHassan, "LS-LEACH: A New Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks" 17th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications.

[10] Mayur S, Ranjith H.D, "Security Enhancment on LEACH Protocol From HELLO Flood Attack in WSN Using LDK Scheme" International Journal of Innovative Research in Science, Engineering and Technology *(*An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 3, March 2015

[11] Vikas Nandal and Deepak Nandal, "Maximizing Lifetime of Cluster-based WSN through Energy-Efficient Clustering Method": IJCSMS Vol. 12, Issue 03, September 2012

[12] Meenakshi Diwakar and Sushil Kumar., "Energy Efficient Level Based Clustering Routing Protocol For Wireless Sensor Networks" IJASSN, Vol 2, No.2, April 2012