

# Survey on Energy Efficient Clustering and Routing Protocols of Wireless Sensor Network

**Priyanka Dubey**

Dept. of Computer Science & Engg.  
Rabindranath Tagore University  
Bhopal, Madhya Pradesh, India  
Priyankathapak07@gmail.com

**Dr. S. Veenadhar**

Dept. of Computer Science & Engg  
Rabindranath Tagore University  
Bhopal, Madhya Pradesh, India

**Dr. Sanjeev Gupta**

Dept. of Computer Science & Engg  
Rabindranath Tagore University  
Bhopal, Madhya Pradesh, India

**Abstract** - The past few years have witnessed increased interest in the potential use of wireless sensor networks (WSNs) in a wide range of applications and it has become a hot research area. However, the resource constrained nature of sensors raises the problem of energy. This paper focus on the detailed survey on major clustering techniques LEACH, PEGASIS, and TEEN. This article strongly examines about the advantages and limitations of different routing protocol with its recent research issues. Here research work carried out by different researcher in this field of WSN is also detailed. This paper summarizes all set of routing algorithms with comparison of on the basis advantage and disadvantages of each algorithm.

**Index Terms**- Cloud Computing, Load balancing, Machine Learning, Soft Computing, Virtual machines.

## I. INTRODUCTION

A sensor network is defined as being composed of a large number of nodes with sensing, processing and communication facilities which are deployed either inside the phenomenon or very close to it. Each of these nodes collects data and route this information back to a sink. The network must possess self-organizing capabilities since the positions of individual nodes are not predetermined. Cooperation among nodes is the dominant feature of this type of network, where groups of nodes cooperate to disseminate the information gathered in their vicinity to the user [1] as shown in fig 1. As it is shown here there are several sensor nodes scattered randomly and the data content of individual sensor nodes gets collected in the sink. Then through internet the user can view the data collected by the network.

A sensor node is made up of four basic components as shown in the figure a sensing unit, including one or more sensors for data acquisition [2], a processing unit, a transceiver unit and a power unit. They may also have application dependent additional components such as a location finding system, a power generator and a mobilizer. Sensing units are usually composed of two subunits: sensors and analog to digital converters (ADCs). The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed into the processing unit. The processing unit, which is generally associated with a small storage unit, manages the procedures. A transceiver unit connects the node to the network. One of the most important components of a sensor node is the power unit. Power units may be supported by a power scavenging unit such as solar cells.

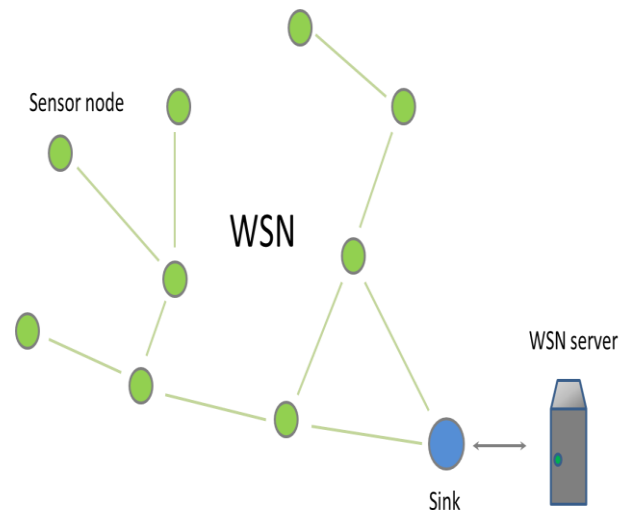


Figure 1 an example of a WSN.

## II. WIRELESS SENSOR NETWORK ROUTING ISSUES

The design of routing protocols in WSNs is influenced by many challenging factors. These factors must be overcome before efficient communication can be achieved in WSNs. In the following, we summarize some of the routing challenges and design issues that affect routing process in WSNs.

**1. Node deployment-** Node deployment in WSNs is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths. However, in random node deployment, the sensor nodes are scattered randomly

creating an infrastructure in an ad hoc manner. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation. Inter-sensor communication is normally within short transmission ranges due to energy and bandwidth limitations. Therefore, it is most likely that a route will consist of multiple wireless hops.

**2. Energy consumption without losing accuracy-** sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. As such, energy conserving forms of communication and computation are essential. Sensor node lifetime shows a strong dependence on the battery lifetime [1]. In a multi hop WSN, each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

**3. Fault Tolerance-** Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. If many nodes fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection base stations. This may require actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption, or rerouting packets through regions of the network where more energy is available. Therefore, multiple levels of redundancy may be needed in a fault-tolerant sensor network.

**4. Scalability-** The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more. Any routing scheme must be able to work with this huge number of sensor nodes. In addition, sensor network routing protocols should be scalable enough to respond to events in the environment. Until an event occurs, most of the sensors can remain in the sleep state, with data from the few remaining sensors providing a coarse quality.

**5. Network Dynamics-** Most of the network architectures assume that sensor nodes are stationary. However, mobility of both BS's or sensor nodes is sometimes necessary in many applications [19]. Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, in addition to energy, bandwidth etc. Moreover, the sensed phenomenon can be either dynamic or static depending on the application, e.g., it is dynamic in a target detection/tracking application, while it is static in forest monitoring for early fire prevention.

**6. Transmission Media-** In a multi-hop sensor network, communicating nodes are linked by a wireless medium. The traditional problems associated with a wireless channel (e.g., fading, high error rate) may also affect the operation of the sensor network. In general, the required bandwidth of sensor data will be low, on the order of 1-100 kb/s. Related to the transmission media is the design of medium access control (MAC). One approach of MAC design for sensor networks is to use TDMA based protocols that conserve more energy compared to contention based protocols like CSMA (e.g., IEEE 802.11). Bluetooth technology [32] can also be used.

**7. Connectivity-** High node density in sensor networks precludes them from being completely isolated from each other. Therefore, sensor nodes are expected to be highly connected. This, however, may not prevent the network topology from being variable and the network size from being shrinking due to sensor node failures. In addition, connectivity depends on the, possibly random, distribution of nodes. • Coverage: In WSNs, each sensor node obtains a certain view of the environment. A given sensor's view of the environment is limited both in range and in accuracy; it can only cover a limited physical area of the environment. Hence, area coverage is also an important design parameter in WSNs.

### III. RELATED WORK

In this literature, different techniques about WSN are studied. Earlier research has tried up to a certain extent to overcome the problem of energy consumption and network stability using energy efficient techniques. However, still, energy consumption and network stability is the primary challenging issue in Wireless Sensor Network. Therefore, this work propose a technique of energy harvesting in clustering based Wireless Sensor Network to prolong network lifetime and network stability

LEACH is a well-known clustering based protocol [2]. In LEACH sensor nodes are organized into the cluster. Each cluster has cluster head and member nodes. Cluster heads in each cluster are selected randomly. The main disadvantage of LEACH is that if a sensor node with less residual energy is selected as cluster head would die quickly; ultimately the whole cluster would become non-functional. LEACH performs local processing to reduce the amount of data being transmitted to the BS, therefore reducing energy consumption and improving network lifetime.

In [3] this study, a game theory-based dispersed Energy Harvesting-Aware (EHA) algorithm is proposed, which represents the behaviors of sensors as a game. This effort analyses the energy expenditure rate and energy-harvesting rate of every sensor node at different times. In this approach, the high harvesting energy sensor nodes

assist with the low harvesting energy sensor nodes to keep the connectivity of the sensor network. The proposed algorithm first builds a beginning topology based on the Directed Local Spanning Sub graph (DLSS) algorithm. Then every sensor node tries to and an adjacent node that covers up the remote neighbor of sensor node by adjusting the communication power stepwise.

In this paper [4] Audit-based Misbehavior Detection (AMD) can construct paths consisting of highly trusted nodes, subject to a desired path length constraint. When paths contain misbehaving nodes, these nodes are efficiently located by a behavioral audit process. AMD detects selective dropping behaviors by allowing the source to perform matching against any desired selective dropping patterns. This is particularly important when end to end traffic is encrypted. In the latter scenario, only the source and destination have access to the contents of the packets and can detect selective dropping.

In this paper [5], source node verifies the authenticity of node that initiates RREP by finding more than one route to the destination. The source node waits for RREP packet to arrive from more than two nodes. In ad hoc networks, the redundant paths in most of the time have some shared hops or nodes. When source node receives RREPs, if routes to destination shared hops, source node can recognize the safe route to destination. But, this method can cause the routing delay. Since a node has to wait for RREP packet to arrive from more than two nodes. Therefore, a method that can prevent the attack without increasing the routing overhead and the routing delay is required.

Deng et. al. [6] has proposed an algorithm to prevent black hole attacks in ad hoc networks. According to the algorithm, any node on receiving a RREP packet, crosschecks with the next hop on the route to the destination from an alternate path. If the next hop either does not have a link to the node that sent the RREP or does not have a route to the destination then the node that sent the RREP is considered as malicious. This solution cannot prevent cooperative black hole attacks. Apart of that there are many techniques which are used for the security of AODV.

In this paper [7], they proposed a method uses Intrusion Detection using Anomaly Detection (IDAD) to defend against black hole attacks established by both single and multiple black hole nodes. It proved the specific result increases network performance by reducing formation of control (routing) packets including effectively defend black hole attacks opposed to mobile ad-hoc networks.

In this paper [8], they proposed a method uses promiscuous mode to find malicious node and transmit the

data of malicious node to every some other nodes in the network. The efficiency of suggested mechanism as throughput of the network does not decay in existence of the black holes.

In this paper [9], they proposed two possible solutions to study black hole attack. The first solution is to study several route to the destination. The second is to apply the packet sequence number contained in any packet header. In study to AODV routing scheme, the second solution is superior and of the route to the destination rely upon on the pause time at a lowest cost of the delay in the networks.

In this paper [10], they have proposed a solution the requesting node wait and check the replies from all neighboring node to find a safe route. It is provide better performance than the conventional AODV in the existence of Black holes with smallest additional delay and overhead.

In this paper [11], they apply a reactive routing protocol called as Ad hoc On-demand Distance Vector (AODV) routing for examine of the outcome of the black hole attack when the destination sequence number is altered via simulation. Then, they determine characteristic in order to define the normal state from the character of black hole attack. They proposed training scheme for huge accuracy detection by modifying the training data in every given time intervals and adaptively specifying the normal state according to the changing network environment.

Bouachir Ons (2016) et. al [13] present that an ORP and data dissemination protocol for energy harvesting IOT (EH-IOT) depend on cross-layer constructs that allow across the layers synchronization and coordination among the routing protocol and the application layer service. The OMNET++ based extensive simulation of this protocol showed promising results in terms of meeting application requirements of handling urgent traffic and delay tolerant traffic seamlessly and ensuring energy usage efficiency.

## IV. WSN ROUTING TECHNIQUES

### 1. Data-Centric Protocols

In data-centric routing, the sink sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute based naming is necessary to specify the properties of data. SPIN is the first data-centric protocol, which considers data negotiation between nodes in order to eliminate redundant data and save energy [13]. Later, Directed Diffusion has been developed. Then, many other protocols have been proposed either based on Directed Diffusion or following a similar concept [14]. This section describes these protocols in details.

### 1.1 Sensor Protocols for Information via Negotiation

**(SPIN)** - The idea behind SPIN is to name the data using high level descriptors or meta-data. Before transmission, meta-data are exchanged among sensors via a data advertisement mechanism, which is the key feature of SPIN. Each node upon receiving new data, advertises it to its neighbors and interested neighbors, means those who do not have the data, retrieve the data by sending a request message. SPIN's meta-data negotiation solves the classic problems of flooding such as redundant information passing, overlapping of sensing areas and resource blindness thus, achieving a lot of energy efficiency.

There is no standard meta-data format and it is assumed to be application specific. There are three messages defined in SPIN to exchange data between nodes. These are: ADV message to allow a sensor to advertise a particular metadata, REQ message to request the specific data and DATA message that carry the actual data. Details of it can be studied from [13]. In SPIN, topological changes are localized since each node needs to know only its single-hop neighbors. SPIN is not used for applications such as intrusion detection, which require reliable delivery of data packets over regular intervals.

**1.2 Directed Diffusion (DD)**- DD is an important milestone in the data-centric routing research of sensor networks. The idea aims at diffusing data through sensor nodes by using a naming scheme for the data. DD suggests the use of attribute-value pairs for the data and queries the sensors in an on demand basis by using those pairs. In order to create a query, an interest is defined using a list of attribute-value pairs such as name of objects, interval, duration, geographical area, etc. The interest is broadcast by a sink through its neighbors. Each node receiving the interest can do caching for later use. The nodes also have the ability to do in-network data aggregation. The interests in the caches are then used to compare the received data with the values in the interests.

The interest entry also contains several gradient fields. A gradient is a reply link to a neighbor from which the interest was received. Hence, by utilizing interest and gradients, paths are established between sink and sources. Several paths can be established so that one of them is selected by reinforcement. DD is highly energy efficient since it is on demand and there is no need for maintaining global network topology. However, DD cannot be applied to all sensor network applications since it is based on a query-driven data delivery model. Details of DD can be studied from [13].

**1.3 Rumor Routing (RR)**- RR is a compromise between flooding queries and flooding event notifications. The main idea of this protocol is to create paths that lead to each event. Unlike event flooding which creates a network-

wide gradient field. Thus, in case that a query is generated it can be then sent on a random walk until it finds the event path, instead of flooding it throughout the network. As soon as the event path is discovered it can be further routed directly to the event. On the other hand, if the path cannot be found, the application can try re-submitting the query or flooding it. The RR can be a good method for delivering queries to events in large networks [12].

### 2. Location-Based Protocols

In this section, location-based protocols for WSNs, is presented. They are based on two principal assumptions [12]:

- It is assumed that every node knows its own network neighbors positions.
- The source of a message is assumed to be informed about the position of the destination.

#### 2.1 Distance Routing Effect Algorithm for Mobility

**(DREAM)**-It is a proactive protocol and each Mobile Node (MN) maintains a location table for all other nodes in the network [12]. To maintain the table, each MN transmits location packets to nearby MNs in the sensor network at a given frequency and to far away MNs in the sensor network at another lower frequency. Since far away MNs appear to move more slowly than nearby MNs, it is not necessary for a MN to maintain up-to-date location information for far away MNs. Thus, by differentiating between nearby and far away MNs, DREAM attempts to limit the overhead of location packets.

#### 2.2 Geographic and Energy Aware Routing (GEAR):

Unlike previous geographic routing protocols, GEAR does not use greedy algorithms to forward the packet to the destination [18]. Thus, it differs in how they handle communication holes. The GEAR uses energy aware and geographically informed neighbor selection heuristics to route a packet towards the target region.

#### 2.3 Minimum Energy Relay Routing (MERR) –

**Location**-It is based on the idea that the distance between two nodes that transmit data is very important [19]. This distance is closely related to the energy consumed on the entire path, from the source to the base station. Thus, in MERR each sensor seeks locally for the downstream node within its maximum transmission range whose distance is closest to the characteristic distance.

As soon as a sensor has decided to use the next hop, it adjusts its transmission power to the lowest possible level such that the radio signal can just be received by the respective node. This can minimize the energy consumption. If the distances between each pair of sensors are all greater than the characteristic distance, each sensor will select its direct downstream neighbor as the next hop node.

Table 1 Comparison of various techniques of WSN node clustering.

Protocol		
LEACH [16]	Data collection is centralized	LEACH ignores residual energy LEACH is not suitable for large networks.
SPIN [17]	Eliminates the redundancy of data [17].	It cannot guarantee the delivery of data [15].
GEAR [15]	Energy consumption is balanced. [15]	The routing table exchange periodically [15]
MWE[15]	Each sensor node in the network has a set of minimum energy path to each source node	More delay Larger overhead Less scalability.
TAG [17]	It reduces the amount of traffic transmitted in the sensor network.	Overhead increases.

## V. WSN CLUSTERING TECHNIQUES

### 1. Greedy Hierarchical Virtual Protocol (HVP)

Greedy Forwarding with Hierarchical Virtual Position (HVP) [23] algorithm uses the combination of all K-level virtual positions ( $K \geq 1$ ) and the geographic positions of nodes in a down-hill fashion. HVP requires nodes to store the geographic positions as well as all the K-level virtual positions of itself and its direct neighbors. A flag level is added to the packets to indicate the current level of virtual position. The down-hill process is uni-directional to ensure that HVP is loop-free. HVP fails if the lowest level virtual position (the geographic position) is already used and there is no neighbor to make further progress towards the destination of a packet. The down-hill process does not need to have a fixed decrement of 1. When using larger decrements, less levels of virtual position are needed, that implies less information storage on nodes. Dynamic decrements can be used when certain level of virtual position is missing.

### 2. LEACH (Low Energy Adaptive Clustering Hierarchy)

A proposed protocol [4] is an adaptive clustering protocol for distributing energy load among the sensor nodes in network. LEACH uses single-hop routing in which each sensor node transmits information directly to the cluster head or the sink. It works in two phase: 1) The setup phase- In the setup phase, the clusters are organized and the cluster heads are selected and each round stochastic algorithm is used by each node to determine whether it will become a cluster head. 2) The steady state phase- The data is sent to

the base station the duration of the steady state phase is longer than the duration of the setup phase in order to minimize overhead. Cluster head creates a TDMA (Time Division Multiple Access) schedule based on the number of nodes in the group. CDMA (Code Division Multiple Access) code is used for random communication inside the cluster. LEACH is not suitable for large network areas.

### 3. Particle Swarm Virtual Coordinates (PSVC)

PSVC [24] is a distributed virtual coordinate assignment algorithm that employs Particle Swarm Optimization to compute virtual coordinates for geographic routing. The selection of the reference nodes and the relaxation steps are similar to Gossiping. PSVC computes the coordinates of the reference nodes by modeling the hop counts between the reference nodes as a spatial distance in a manner similar to NoGeo. The election of each reference node floods the network, but the cost per reference node is approximately  $O(D) \approx O(\sqrt{n})$ , where D is the diameter of the network and n is the network size. PSVC uses 4 reference nodes for 2D networks and 6 reference nodes for 3D networks. PSVC converges faster, achieves a lower hop stretch, and scales well up to large networks of 3,200 nodes compared to NoGeo. Also, PSVC makes no assumptions on the network topology and can naturally be extended to three-dimensional (3D) IOT.

### 4. Ant-Based analysis

Proposed protocol [8] which is based on the Ant Colony Optimization heuristic. Initially the forward ants are sent to no specific destination node, which means that sensor nodes must communicate with each other and the routing tables of each node must contain the identification of all the sensor nodes in the neighborhood and the correspondent levels of pheromone trail. For large networks, this can be a problem since nodes would need to have big amounts of memory to save all the information about the neighboring nodes. The algorithm can be easily changed to save memory. If the forward ants are sent directly to the sink, the routing tables only need to save the neighbor nodes that are in the direction of the sink. This reduces the size of the routing tables and, in consequence, the memory needed by the nodes. The quality of a given path between a sensor node and the sink-node, should be determined not only in terms of the distance, but also in terms of the energy level of that path.

## VI. CONCLUSION

To make an energy efficient design for routing protocol in WSN is the major challenge faced now days. The main aim is to make the sensor to work for long time with less usage of energy. Generally the major energy consumption is due to data transfer and reception. Consequently, many innovative security protocols and techniques have been developed to meet this challenge. It was obtained that use of dynamic algorithm which handle real time situation

without any prior training is highly demanding. Here one has to separately work for clustering and routing as each module will improve WSN life span. Use of hierarchal routing algorithm leads to packet loss which ultimately require extra energy to transfer same data. In future a flawless calculation is with great component blend is wanted by investigating new load balancing calculations which adjusts the load much better and furthermore helps in green processing.

## REFERENCES

1. Satoshi Kurosawa<sup>1</sup>, Hidehisa Nakayama<sup>1</sup>, Nei Kato<sup>1</sup>, Abbas Jamalipour<sup>2</sup>, and Yoshiaki Nemoto," Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, November 2007.
2. Maria Sebastian and Arun Raj Kumar P, "A Novel Solution for Discriminating Wormhole Attacks in MANETs from Congested Traffic using RTT and Transitory Buffer" International Journal of Computer Network and Information Security, pp. 28-38, 2013.
3. Imad Aad, Jean-Pierre Hubaux and Edward W. Knight "Impact of Denial of Service Attacks on Ad Hoc Networks" IEEE/ACM Transactions on Networking, Vol. 16, No. 4, pp. 791- 802, August 2008.
4. Yu Zhang, Loukas Lazos and William Jr. Kozma "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks" IEEE Transactions On Mobile Computing (Article in Press), 2012.
5. M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE'04), pp. 96-97, April 2004.
6. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, vol.40, pp. 70-75, 2002.
7. Yibeltal Fantahun Alem Zhao Cheng Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection" IEEE 2nd International Conference on Future Computer and Communication (ICFCC), pp.V3-672 - V3-676, 21 to 24 MAY 2010.
8. Pramod K. Singh and Govind Sharma, "An Efficient Prevention of black hole problem in AODV routing protocol in MANET," 2012 IEEE 11<sup>th</sup> International Conference on Trust ,Security and Privacy in Computing and Communications, pp. 902-905.
9. Ms Nidhi Sharma, Mr Alok Sharma "The Black-hole node attack in MANET" 2012 Second International Conference on Advanced Computing & Communication technologies, 546-550 2012 IEEE.
10. Latha Tamilselvan, Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", In Proceedings of IEEE 2<sup>nd</sup> International Conference on Communications, IEEE 2007.
11. Faheem khan, Sohail abbas, Samiullah khan, An Efficient and Reliable Core-Assisted Multicast Routing Protocol in Mobile Ad-Hoc Network, International Journal of Advanced Computer Science and Applications, vol7:5, 2016.
12. Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey by Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados, Senior Member, IEEE, 2012
13. A Survey on Routing Protocols for Wireless Sensor Networks by Kemal Akkaya and Mohamed Younis Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County Baltimore, MD 21250
14. R. Shah and J. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks", in the Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Orlando, FL, March 2002.
15. N.A.Pantazis,Stefanos A. Nikolidakis, Dimitro D. Vergados"Energy Efficient routing protocols in wireless sensor network: A survey", IEEE communications and tutorials, vol.15 no. 3, 2013, pp. 551-589
16. Neha Rathi, Jyoti Saraswat, P.P Bhattacharya,"A review on routing protocols for applications in wireless sensor networks" International Journal of Distributed and Parallel System vol. 3, no. 5, 2012, pp. 39-58.
17. Parul Khurana and Inderdeep Aulakh,"Wireless sensor network routing protocols: a survey", International Journal of Computer Applications, vol. 75, no. 15,2013, pp. 17-25
18. Y. Yu, R. Govindan, D. Estrin, "Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," UCLA Computer Science Department Technical Report, 2001, pp. 1-11.
19. M. Zimmerling, W. Dargie, J.M. Reason, "Energy Efficient Routing in Linear Wireless Sensor Networks," In Proc. 4th IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS 2007), Italy, Pisa, 2007, pp. 1-3.
20. Suraj Sharma, Deepak Puthal, Sabah Tazeen, Mukesh Prasad, And Albert Y. Zomaya. MSGR: A Mode-Switched Grid-Based Sustainable Routing Protocol for Wireless Sensor Networks.Digital Object Identifier 10.1109/ ACCESS October 12, 2017.
21. Ram Murthy Garimella, Damodar Reddy Edla, Venkatanareash babu Kuppili. "Energy Efficient Design of Wireless Sensor Network: Clustering". Centre for Communications International Institute of Information Technology Hyderabad - 500 032, INDIA February 2018.
22. G.S. Mamatha and Dr. S. C. Sharma "A Highly Secured Approach against Attacks in MANETS",

- International Journal of Computer Theory and Engineering, Vol. 2, No. 5, 1793-8201, October, 2010.
23. R. V. Biradar, S. R. Sawant, R. R. Mudholkar and V. C. Patil, "Inter-Intra Cluster Multihop-LEACH Routing in Self-Organizing Wireless Sensor Networks", International Journal of Research and Reviews in Computer Science (IJRRCS), vol. 2, no. 1, (2011)
  24. J. Zhou, Y. Chen, B. Leong and B. Feng, "Practical Virtual Coordinates for Large Wireless Sensor Networks", Proceedings of IEEE International Conference on Network Protocol (ICNP), Kyoto, Japan, (2010) October 5- 8.