International Journal of Research in Science and Technology http://www.ijrst.com

(IJRST) 2016, Vol. No. 6, Issue No. III, Jul-Sep **e-ISSN: 2249-0604, p-ISSN: 2454-180X**

A SURVEY ON ROUTING PROTOCOLS FOR WIRELESS SENSOR NETWORKS

Mohit Tandon, Amit Nayak, Bimal Patel

Department of Information & Technology,

Charotar University of Science & Technology (CHARUSAT)

ABSTRACT

Wireless sensor networks (WSNs) nowadays considered as a hot research topic because of its wide range of applications in various fields. A wireless sensor network (WSN) is a computer wireless network composed of spatially distributed and autonomous tiny nodes, smart dust sensors, motes, which cooperatively monitor physical or environmental conditions. Different protocols have been designed to increase the overall life time of the network. Also different clustering techniques are used to solve the problem of energy consumption in WSNs. Different Wireless Sensor Network (WSN) protocols show different performance under different applications. Therefore, a WSN protocol designer must be aware of the intended applications. In this paper we have reported a comprehensive survey of different challenges faced in WSN. Outline the taxonomy of routing protocol and have given overview of different routing protocols along with their comparison. Later on, we discuss various design challenges of WSN, along with their merits and demerits

INTRODUCTION

Wireless Sensor Network is collection of group of specially designed transducers which is having communication infrastructure, which can be used for monitoring, measuring or recording conditions at remote or diverse locations[4]. Generally measured parameters are temperature, pressure, speed, humidity, sound intensity, direction of wind, intensity of illumination, voltage of power line, vibration intensity, concentrations of chemicals, pollutants presence level and body functions.

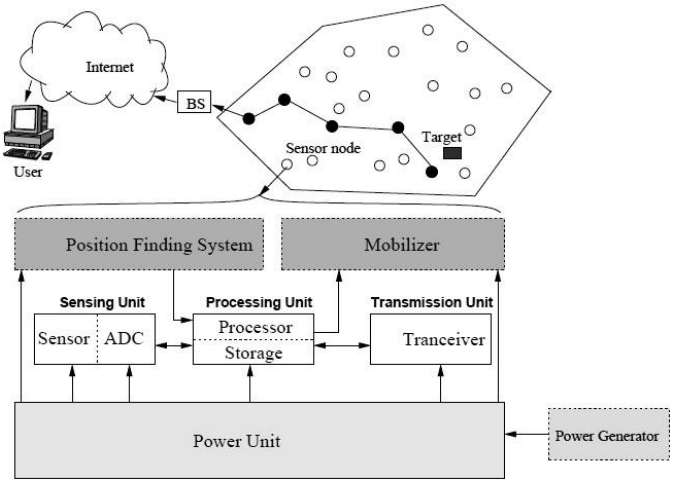

Figure 1 Sensor Node architecture[14]

WSN basically comprises of massive inexpensive, limited battery powered and small size sensor nodes[2]. Sensing unit, processing unit, power unit and communication unit are basic constituents of a sensor node.

ROUTING PROVOCATIONS AND DESIGN ISSUES IN WSNS

Advantages of WSN come with limited battery power, restricted transmission range and storage capacity[4]. Major research focuses on maximizing the lifetime of working WSN while carrying out the data communication reliably.

Some of the design issues and routing provocations are as[4] [13][14]

A. Node Deployment

Node deployment is application specific and it directly influences the capability of protocol. The deployment of stations may be in predefined or it can be random in nature. In case of predefined implementation, routing is done through already defined paths. In random implementation, the sensor stations are placed without method or conscious decision.

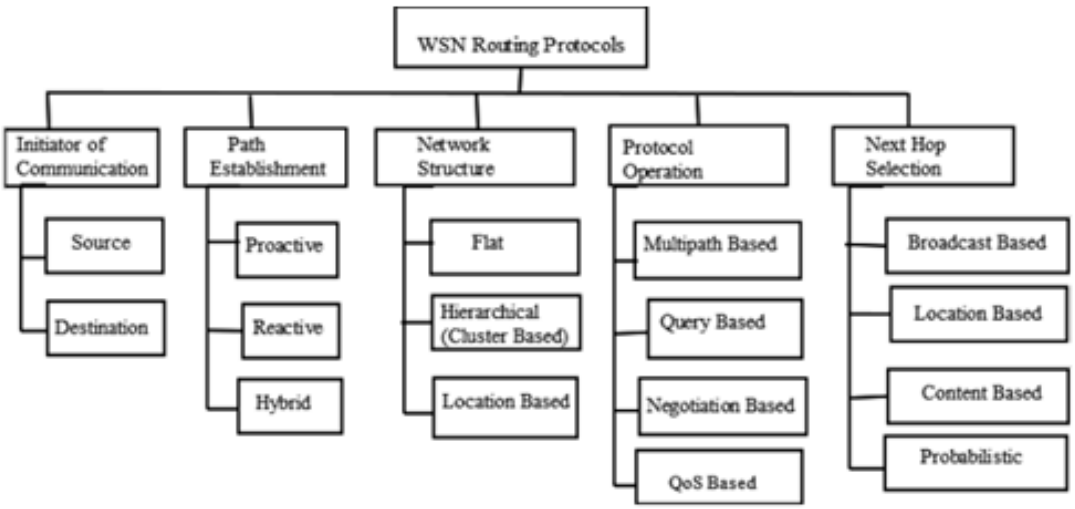

Figure 3 Classification of Routing protocols in WSN[13]

B. Energy Efficient With Precise Accuracy

Sensor nodes have only limited supply of energy for transmitting and computations of information in a wireless network. Lifetime of the node is strongly depends on its battery lifetime. If a particular node fails due to power failure then there will be significant topological changes and this will reduce reliability and data accuracy of the network.

C. Data Reporting

Sensor stations continuously percept, process data and for- wards these reports towards the sink node. This data reporting of sensor nodes may be continuous or on demand i.e. query driven. Nodes have to react any sudden or drastic changes in the data such as time critical applications.

D. Error Tolerance

During operation few of the nodes may get fail due to extreme environmental conditions, physical damage or external interference. This particular failure should not be cause failure of network. Thus routing techniques should take care of this failure node and recovery of the network after such failure. In case of node failure routing algorithm should able to establish new paths or links and data rate has to be maintained.

E. Network Scalability

The wireless sensor nodes may be in order of few to thousands or even more. So the routing technique should capable of working with such huge number of stations and it should be scalable sufficient for responding events happening in environment.

F. Mobility of Nodes

Many network architecture considers sensor nodes to be stationary, but application may demand mobility of nodes. Routing paths formation and updating such routing tree is major challenge while designing. In fixed architecture routing can be static but dynamic routing is necessary in case of movable nodes.

G. Connectivity

Nodes in sensor network precludes themselves form complete isolation from others. Thus, sensor nodes are expected connectivity on large scale. Connectivity depends on distribution of nodes.

H. Coverage

Wireless sensor networks, every node compute certain information from environment. Every node has limited scope of vision or range. It generally covers only certain limited area. Thus while designing of WSNs coverage is also one of the major parameter need to take care.

CLASSIFICATION OF ROUTING PROTOCOLS IN WSN

In WSN, the network layer is used to implement the routing of incoming data. In multi-hop network the source node cannot reach the sink node directly. So intermediate nodes have to relay their packets. The implementation of routing table gives the solution. WSN routing protocols can be classified[2][13] into five ways, according to the way of establishing the routing path, according to the network structure, according to protocols operation, according to the initiator of communications, and according to how protocols select their next hop on route of forwarding message.

The network based routing protocols are classified as [3]flat based, hierarchal based (clustering based), location based. In flat based routing all the sensor node plays the same role. While in hierarchal based some nodes act as cluster head and some act at simple sensor node to sense data. So when network scalability and efficient communication is needed, hierarchal or clustering is the best one.

Clustering Based Routing Protocols In Wireless Sensor Network

The cluster based protocol are routing efficient method in which those nodes having high energies are arbitrary selected for processing and sending data while those node having low energy are used for sensing data and sending it to cluster head (CH). This property of clustering contributes to the scalability, life time maximization. The clustering based protocols are classified into three broad [4]categories: block cluster, grid cluster and chain cluster.

I. Data Aggregation

The most prominent technique for optimization of routing task is achieved by using available computational strength through the routing paths. This is known as in-network data aggregation. Aggregation simply means combination. In simple words, data aggregation is simply the combination of data which is originated from different sources. Main function of data aggregation is to suppress the duplication.

In this technique a number of sensor nodes act as a group which collects data or information from target region. Traditionally nodes send data individually when base station demands for network. Instead of that there is a special node called as aggregator which collects statistics from its neighbouring stations, adds them and forwards that combined information to base station in multi hop pattern. By aggregation we reduces number of transmission and thus improves network and bandwidth utilization.

J. Simple Periodic Aggregation

This is the simple timing strategy for data aggregation. In this strategy, each node waits for particular fixed time periods then aggregates all received data packets. Then it forwards that data packets converting in a single packet which in turns results aggregation

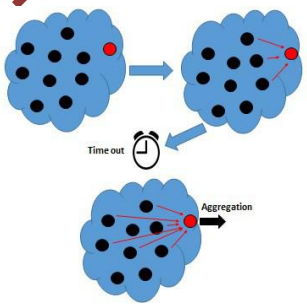

Figure 2 Simple Periodic Aggregation

K. Per-Hop Periodic Aggregation

This is same as previously defined strategy. In this the central or coordinator node waits for certain time till all of his children send data to him. This technique needs each parent to have knowledge of its total children. In case of failure of particular child, timeout can be used to maintain link.

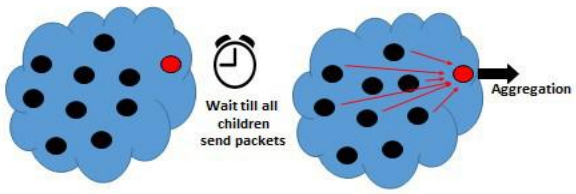

Figure 4 Per-Hop Periodic Aggregation

L. Adjusted per-hop periodic aggregation

In this strategy, time period is adjusted in accordance of the node position in the network tree. Thus transmission time of node gets changed according to the position in the gathering tree.

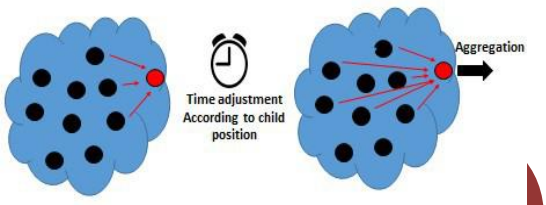

Figure 5 Adjusted per-hop periodic aggregation

SURVEY OF PROTOCOLS

M. SPIN

The SPIN (Sensor Protocols for Information via Negotiation) is a family of protocols used to disseminate individual sensor observations to all the nodes in the network[3]. SPIN tries to solve three problems associated with classic flooding: implosion, overlap, and resource-blindness.

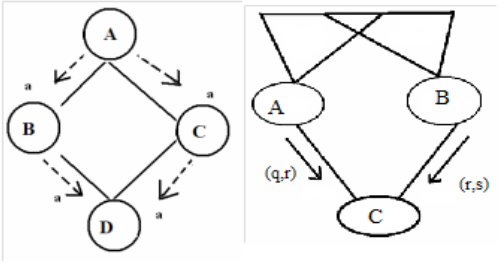

Fig 6 Implosion and overlapping

The implosion problem occur when a node D receives two copies of the same data from two neighbours B and C, as shown in Fig. Since sensors cover overlapping geographical areas, they gather overlapped pieces of sensed data, as illustrated in Fig. Finally, in classic flooding is resource-

blind, i.e., nodes don't modify their activities supported the offered energy. SPIN uses application-specific meta-data to call the perceived knowledge

SPIN uses three types of [5]data: ADV for advertising new data, REQ for requesting data, and DATA for a data message. SPIN-1 starts once a node has new data. It sends out an ADV message, containing meta-data about the new data, to all its neighbours. If a neighbour is curious about these data, it sends out an REQ message to the broadcasting node, which then sends the DATA to the interesting node. This process is repeated at every node that gets new data. In SPIN-2, if a node gets new data or receives an ADV message, it'll not participate in the protocol if it does not have enough energy. In classic flooding, a node sends out its data to all its neighbours. When a node receives new data, it sends it to all its neighbours except the one it received it from. SPIN solves the implosion, overlap, and resource-blindness problems. Each node needs to how about its neighbours only and it consumes little energy in computation.

N. LEACH

The LEACH (Low-Energy Adaptive Clustering Hierarchy) algorithm is non-energy-aware and assumes a continuously-operating model. [3][11]LEACH is a popular algorithm not only because of its clarity and efficiency, but also for its introduction of the CHs rotation theory. Rotation of CHs addresses the need for load balancing among the network sensors. In the LEACH algorithm, the lifetime is divided into a number of rounds. Each round contains set-up and stable phases. In the set-up phase, the CHs are elected and the clusters are shaped. In stable phases meanwhile, events are sensed by sensors and are sent to the sink via CHs. [7][8]The procedure of CH election is conducted in an ad-hoc manner, using random number generation in each sensor. In the LEACH algorithm, each CH advertises its role to all of the other sensors and the other sensors join to the closest CH using the received signal strength. In the LEACH algorithm, the
CHs[7] aggregate the collected data in order to decrease the amount of transmitting data and the consequent energy cost.

In LEACH-C[5][8], base station should guarantee uniform distribution of energy among all the clusters. To this end the algorithm defines a threshold for energy and each node that has more energy than the threshold will be candidate for being clusters head.

Merits[2]

- ✓ Each node has equal chance to become the cluster head.CH are not selected in sequence. So load is shared between the nodes.
- ✓ Leach uses TDMA so it keeps CHs from unnecessary collision.

Demerits[2]

- ✓ Use single hop communication so cannot be use in large. Each node has equal chance to become the cluster head.CH are not selected in sequence. So load is shared between the nodes

CH is selected on the basis of probability so uniform distribution cannot be ensured and cannot provide local balancing

O. PEGASIS

PEGASIS is a hierarchical protocol and it is an appendage of LEACH protocol. In this protocol, a chain is formed where one node can communicate with only one neighbour node. There is no cluster formation in this protocol. Only one node sends and receives data with sink. [3]Eventually, all data are aggregated in one node and only one node transmits the aggregated data to the sink using long-distance transmission. All nodes are aware of network knowledge. Whenever any node fails due to energy loss, a new chain is formed using some greedy algorithm excluding failed node. A random node is selected for aggregated data transmission to the base station in every round.

PEGASIS[5][7][11] is centred on two ideas: chaining and data fusion. To construct a chain, nodes employ the greedy algorithm starting with the farthest node from the BS. In each round, a node is chosen randomly to be a leader. This leader node initiates a control token to start data transmission from the ends of the chain. Each node fuses its neighbour's data packet with its own to generate a single packet of the same length and then transmits that to its other neighbour. This is repeated till all the sensed data are collected at the leader node, which then transmits one data packet to the BS through direct communication. If nodes can communicate only with neighbours, the leader node can start a multi-hop routing to the BS.

Merit[2]

- ✓ Energy load is distributed uniformly.
- ✓ Reduce overhead due to dynamic cluster formation.
- ✓ Decrease number of data transmission.

Demerit[2]

- ✓ The main problem with PEGASIS is the long latency, which is at the order of N, where N is the number of nodes
- ✓ Network is not stable and not good for time varying topology.

P. TEEN

This algorithm is one of hierarchical algorithms which were introduced for the reactive sensor network and is based on LEACH algorithm. The clustering process use two thresholds named soft and hard threshold. [5]The aim of this threshold is reducing transmitted amount of data between nodes. Hard threshold is one of the rules for transmitting. If the value obtained from a sensor is greater than this threshold, the data will be sent. [8]Otherwise, information is not sent to the base station. Soft threshold is a threshold that gives the algorithm more flexibility. In one scenario if the

value of one node is less than the hard threshold but the difference between two recently values of the node is more than the Soft threshold, data will sent to the base station.

Merits[2]

- ✓ Data transmission can be controlled by varying the threshold value.
- ✓ Well suited for time critical application.

Demerits[2]

- ✓ Whenever the threshold do not satisfy the condition data transmission is not possible.
- ✓ Data may be lost if CHs are not able to communicate with each other.

Q. DD

Directed diffusion is a communication paradigm for information dissemination in sensor networks based on data-centric routing. In data-centric routing, all the interest is in the data, not the location of the node. Data-centric muting is to find routes from multiple sources to a single destination that allows in-network consolidation.

Directed diffusion[3] utilizes the query-response operation model. A query (interest), is like give me periodic reports about any interest. Periodically, the sink broadcasts the interest to all its neighbours but with lower data rate than specified. When the interest reaches the nodes within react, each node has an interest cache to store the interest in. The interest entry has a timestamp field and several fields for gradients. A gradient specifies the required data rate and the direction to the interested node. When a neighbour receives the interest, it checks if it exists in its cache. If no entry is found, one is created. When a node in region reacts senses an event, it sends out the response to all the interested nodes. After receiving the initial data, the sink reinforces one of its neighbours by re-sending the interest hut with a higher data rate. Then, reinforcement propagates till it reaches the source.
Simulation results showed that directed diffusion performs better than both flooding and omniscient multicast in terms of energy dissipated. Directed diffusion is robust and fault tolerant. However, the low-data rate paths and the periodic broadcast of the interest reduce network lifetime. The few nodes that are within the radio range of the BS may die quickly, reducing network lifetime too.

SECURITY ATTACKS IN SENSOR NETWORK

After Wireless Sensor Networks have the main factor which makes the network vulnerable is its broadcast nature of transmission. WSNs are susceptible to broad range of security attacks due to wireless nature of communication. Because of broadcast nature of communication always there is threat of attacks. Furthermore, as sensor nodes are often placed in open environment so there is bonus threat of physical or natural attacks, because they are not physically protected. Attacks in WSN are follows:

R. Sinkhole Attack[6],[12]

Sinkhole attack is basically the attack within which opponents attempt to attract the entire traffic of the actual network. It takes place by once a compromised node creates centre of attraction for different nodes and attracts whole traffic. This takes place only with the assistance of a compromised node.

S. Selective forwarding[6],[12]

In selective forwarding attack the compromised node forward only selected data packets not all to the receiver.

T. Wormhole Attack[6],[12]

In wormhole attack the wrongdoer records information packets in one location then stores those information packets in another location in order to transmit them later within the network.

U. Hello flood attack[6],[12]

In hello flood attack the wrongdoer sends a hello packet to the receiver nodes, that is a trial to create fool to the sensing nodes that this hello message is send by the base station. This hello packet works as a weapon to persuade alternative sensing element nodes.

V. Sybil Attack[6],[12]

In Sybil attack a node itself presents in several duplicate identities. This attack primarily goals to fault tolerant schemes like multi-path routing and topology maintenance and distributed storage.

W. Message corruption[6],[12]

In this attack the wrongdoer will modification within the message throughout the transmission, this disturbs the integrity of the network.

X. Denial of Service Attack [6],[12]

Denial of Service Attack (DoS) could be a clear effort to forestall the genuine user of a service or information. The standard technique of attack involves overloading the target system with requests, in order that it cannot service to real traffic. This attack stops services for real users. The samples of attack are: electronic jamming, Tapering, collision, homing, flooding, etc

Y. Node malfunction[6],[12]

If a data-aggregating node such as a cluster leader is a malfunction node then it will produce the inaccurate data that can harm the integrity of sensor network.

Z. Node Outage[6],[12]

The situation when a node stops operating is understood as node outage. it should be a great problem harmful if the victim node is the master node within the network.

AA. Node Subversion[6],[12]

If the node is captured by an wrongdoer then there's threat of revelation of some secret information like crypto logic keys and so compromise the complete sensor network. Any sensor

	Classification	Mobility	Position Awareness	Power Usage	Negotiation based	Data Aggregation	Localization	QoS	State Complexity	Scalability	Multipath	Query based
SPIN	Flat	Possible	No	Limited	Yes	Yes	No	No	Low	Limited	Yes	Yes
Directed Diffusion	Flat	Limited	No	Limited	Yes	Yes	Yes	No	Low	Limited	Yes	Yes
Rumor Routing	Flat	Very Limited	No	N/A	No	Yes	No	No	Low	Good	No	Yes
GBR	Flat	Limited	No	N/A	No	Yes	No	No	Low	Limited	No	Yes
MCFA	Flat	No	No	N/A	No	No	No	No	Low	Good	No	No
CADR	Flat	No	No	Limited	No	Yes	No	No	Low	Limited	No	No
COUGAR	Flat	No	No	Limited	No	Yes	No	No	Low	Limited	No	Yes
ACQUIRE	Flat	Limited	No	N/A	No	Yes	No	No	Low	Limited	No	Yes
EAR	Flat	Limited	No	N/A	No	No		No	Low	Limited	No	Yes
LEACH	Hierarchical	Fixed BS	No	Maximum	No	Yes	Yes	No	CHs	Good	No	No
TEEN & APTEEN	Hierarchical	Fixed BS	No	Maximum	No	Yes	Yes	No	CHs	Good	No	No
PEGASIS	Hierarchical	Fixed BS	No	Maximum	No	No	Yes	No	Low	Good	No	No
MECN & SMECN	Hierarchical	No	No	Maximum	No	No	No	No	Low	Low	No	No
SOP	Hierarchical	No	No	N/A	No	No	No	No	Low	Low	No	No
HPAR	Hierarchical	No	No	N/A	No	No	No	No	Low	Good	No	No
VGA	Hierarchical	No	No	N/A	Yes	Yes	Yes	No	CHs	Good	Yes	No
Sensor aggregate	Hierarchical	Limited	No	N/A	No	Yes	No	No	Low	Good	No	Possible
TTDD	Hierarchical	Yes	Yes	Limited	No	No	No	No	Moderate	Low	Possible	Possible
GAF	Location	Limited	No	Limited	No	No	No	No	Low	Good	No	No
GEAR	Location	Limited	No	Limited	No	No	No	No	Low	Limited	No	No
SPAN	Location	Limited	No	N/A	Yes	No	No	No	Low	Limited	No	No
MFR, GEDIR	Location	No	No	N/A	No	No	No	No	Low	Limited	No	No
GOAFR	Location	No	No	N/A	No	No	No		Low	Good	No	No
SAR	QoS	No	No	N/A	Yes	Yes	No	Yes	Moderate	Limited	No	Yes
SPEED	QoS	No	No	N/A	No	No	No	Yes	moderate	Limited	No	Yes

Figure 7 Comparisons of Protocols

node could be hacked, and secret info (key) accumulated thereon could be acquire by the wrongdoer.

BB. False node[6],[12]

When an wrongdoer adds an additional node in any network so as to inject malicious information, comes below the category of false node. With the assistance of this false node associate entrant could add some false information which can disturb the communication. Malicious code injected within the network with the assistance of false node may unfold to any or all nodes, which may damage whole network

CC. Pulse delay attack[6],[12]

There might arise the matter when any interloper or snoopers snoops the message transmission between 2 nodes, it's going to store the message pulses and so retransmits the message once some modifications. This downside is understood as pulse delay attack.

DD. Node Replication Attack[6],[12]

In node replication attack as name implies a replicated copy of a node is added to the network. A wrongdoer adds a replicated node in an exceedingly sensor network by repetition

node ID and alternative details associated with their identity. This malicious node could also be dangerous for the sensor network as a result of by inserting this node attacker can manipulate a particular network phase or perhaps it will destroy the network.

EE. Traffic Analysis[6],[12]

If the message that is transferred is encrypted then conjointly there's risk of malicious damage. This damage can be potential when the trespasser endlessly studies the communication pattern. This study will provide enough info to trespasser to damage the network.

FF. Camouflages Adversaries[6],[12]

Any wrongdoer will insert a malicious node within the network or will compromise a node so as to attract the information packets of the network and so these packets can be misrouted or can be altered.

GG. Monitoring & Eavesdropping[6],[12]

This is the foremost well known assault to protection. Snooping is that the method by which, the opponent will simply get the message contents. Some times when nodes are communicating data concerning controls then eavesdropping is extremely harmful.

COMPARISION OF PROTOCOLS

To make wireless sensor networks practically useful, we need to develop network protocols for them that meet several unique requirements and constraints. Among those come the low power consumption, small size, fault tolerance, long lifetime, adaptively, scalability, robustness, and low latency. We have surveyed some of the recent work on network protocols for sensor networks. We have covered design goals, assumptions, operation models, energy models, and performance metrics used in these protocols in some depth. Moreover, we have highlighted the advantages and drawbacks of each protocol and pointed out possible improvement.

Due to application centric utility of WSN, we can't establish the superiority of any specific protocol over another. Instead we could compare them based on some parameters only. Table shows the comparison of the discussed protocols of Wireless Sensor Network.

REFERENCES

1) Manal Abdullah, Hend Nour Eldin, Tahani Al-Moshadak, Rawan Alshaik, Inas Al Anesi “Density Grid-Based Clustering for Wireless Sensors Networks ” International Conference on Communication, Management and Information Technology (ICCMIT 2015) Science Direct

2) Santar Pal Singh, S.C.Sharma ” A survey on cluster based Routing Protocol in Wireless sensor network “” International Conference on Communication, Management and Information Technology (ICCMIT 2015) Science Direct

3) Ahmed A. Ahmed, Hongchi Shi, Yi Shang "A SURVERY ON NETWORK PROTOCOLS FOR WIRELESS SENSOR NETWORKS" 0-7803-77249103617.000 2003 IEEE International Conference on Computing for Sustainable Global Development (INDIACom)

4) Ajay. K. Talele, Suraj G. Patil, Nilkanth. B. Chopade "A Survey on Data Routing and Aggregation Techniques for Wireless Sensor Networks" 2015 International Conference on Pervasive Computing (ICPC) 978-1-4799-6272-3/15(c)2015 IEEE

5) Jyoti Kumari, Prachi "A Comprehensive Survey of Routing Protocols in Wireless Sensor Networks" 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) 978-9-3805-4416-8/15/$31.00_c 2015 IEEE

6) Rajshree Purohit, Navjot Sidhu "Wireless Sensor Network: Routing Protocols and Attacks- A survey" 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) 978-9-3805-4416-8/15 2015 IEEE

7) Morteza M. Zanjireh and Hadi Larijani "A Survey on Centralised and Distributed Clustering Routing Algorithms for WSNs" 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) 978-1-4799-8088-8/15 ©2015 IEEE

8) Shahrzad Dehghania, Mohammad Pourzaferanib, Behrang Barekatain "Comparison on energy-efficient cluster based routing algorithms in wireless sensor network" Information Systems International Conference (ISICO2015) ScienceDirect

9) M. Aslam, N. Javaid, A. Rahim, U. Nazir, A. Bibi, Z. A. Khan "Survey of Extended LEACH-Based Clustering Routing Protocols for Wireless Sensor Networks" IEEE June 2012

10) Bhakti Parmar, Jayesh Munjani, Jemish Meisuria, Ajay Singh " A Survey of routing protocol LEACH forWSN" International Journal of Scientific and Research Publications, Volume 4, Issue 1, January 2014

11) Ishu Sharma, Rajvir Singh, Meenu Khurana "Comparative Study of LEACH, LEACH-C and PEGASIS Routing Protocols for Wireless Sensor Network" 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA)

12) Suraj Sharma, Sanjay Kumar Jena "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks" *ICCCS'11* February 12-14, 2011, Rourkela, Odisha, India
Copyright_c 2011 ACM 978-1-4503-0464-1/11/02

13) Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados, Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013

14)Santar Pal Singh, S.C.Sharma, A Survey on Cluster based Routing Protocol in Wireless Sensor Network International Conference on Advance Computing Technologies and Applications (ICACTA-2015)