International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

To Evaluate the Performance of Security Mechanism through LEACH and THVRG in WSN

Priyanka Sharma

GCET, Greater Noida, India

Abstract: ***A Wireless Sensor Network is a network, that is made up of an immense number of little sensors and observes particularize parameter(s) with bounded energy. Normally, a routing protocol is needed to deal with delay, energy efficiency, low computation, scalability and communication overhead. This work uses two protocols i.e. THVRG and LEACH and differentiates these protocols on the basis of Characteristics using OPNET simulation tool. The central point of this survey is on routing protocols that are used to deal with complexity, energy consumption, delay, communication overhead and scalability. This survey has examined data routing and classified the protocols in wireless sensor networks into five notable classes i.e. Hierarchical, data aggregation, address-centric, QoS-aware and data-centric.***

Keywords: WSN, THVRG, LEACH, Nodes, Routing protocols, Sensor networks, Sensor node, OPNET

1. Introduction

One of the recently used technologies during, this century is a Wireless sensor network. There are many applications in WSN and one of the recent technologies is sensing application which is used for the growth of devices with less cost and power. The improved quality of handling WSN consists of sensors, analysis, processing are grouped in environments. [1]. Sensor node consist transmitting data, processing and sensing skill that is made up of group of sensor nodes. Algorithm of sensor network and protocols owns the self-organizing skill. The attribute of sensor node is that they worked jointly i.e. they are cooperative. In this easy calculations are used for managing the capabilities [2]. The sensed data transmit to a cluster head when sensor network are data-centric. Given the correlation between the data in a dense cluster accessed by sensors, and the collection of the data is performed locally. Gathering of data increase accuracy and reduced redundancy of data. Robustness, low consumption of power, scalability access them a network hierarchy and clustering of nodes. Reliability, cost effectiveness, edibility, and ease of deployment are basic purpose [3].Each node on a sensor network is contoured with many devices. WSN have many applications in which battery and energy both plays a significant role.

There are numerous routing protocols i.e. LEACH, PAMA. LEACH is taken as the most famous routing protocol that uses routing rely on cluster for decreasing the consumption of energy [4]. In this paper, author introduced an improvement of LEACH and consumption of energy. Leach Protocol upgrade consumption of power; and show the results with respect to terms of nodes.

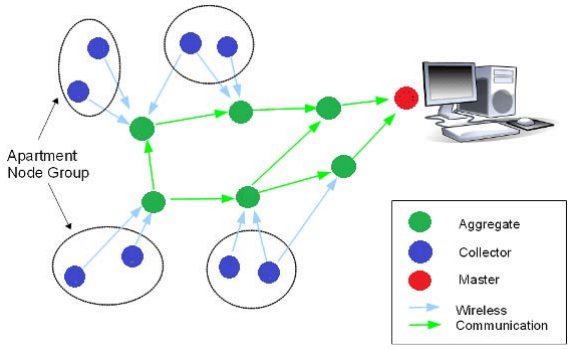

Figure 1: wireless sensor network

Types of Sensor Networks

a) Terrestrial WSNs: In this type of sensor network, nodes are issued to a particular area in a two different manner that is either by ad-hoc manner or by a pre-planned manner [5]. After all battery, power is limited, and it cannot be reenergized, terrestrial sensor nodes must be provided with a maximum power source such as solar cells.

b) Underground WSNs: In this network, sensor nodes are hidden in a cave or mine so that they can easily monitors the undercover conditions [7]. Sink nodes are deployed on the ground to forward the collected information to the base station from the sensor nodes. These are more costly than the terrestrial sensor networks because in such a type of network, genuine nodes are to be selected that can simply be in touch through mineral contents.

c) Underwater WSNs: In this network, sensor nodes and vehicles are located underwater. Independent vehicles are used for collecting the data from the sensor nodes [6]. In this network, Sparse/infrequent deployment of nodes is done. Main problems that come under this while communicating are long propagation delay, signal fading issue, and limited bandwidth [8].

d) Multimedia WSNs: In this type of network, low-cost sensor nodes are equipped with microphones and cameras [11]. These nodes are placed in a pre-planned way to guarantee coverage. Issues in these networks are the demand

of high-energy consumption, quality of service provisioning, high bandwidth, cross-layer design and data processing and compression techniques [10].

2. Literature Review

Basavaraj S. Mathapati.et.al [12]: In this paper, authors proposed a routing protocol using Kalman filters for WSNs to control the issues that increase the network for a very long time and to conserve energy in the smaller amount using some specific network resources. For evaluating the performance authors have used NS-2 as a simulation tool. For the purpose of simulation authors, have used 10, 15, 20, 25 and 30 m/s speed, 1000*1000 area size, 50 sec simulation time, 512 packet size and 75 m transmission range. The simulation result shows that the proposed works reduces the overhead and make accuracy better by position the node.

Kankaur.et.al [13]: In this paper, authors improved LEACH protocol by selecting master cluster heads to increase the network for a very long time in WSN. For evaluating the performance, authors have used MATLAB as a simulation tool. For the purpose of simulation, authors have used 100*100 m sensing areas, 100 numbers of mobile nodes, 4000 bits data packet size, 100 bits control packet size. The simulation result shows the reduction of long-way communication between cluster heads and sink nodes.

Houda Zeghilet.et.al [14]: In this paper, authors combined directed diffusion and better clustering algorithm. The objective of this is to limit passive clustering by continuing the topology to reach energy goal balancing. For evaluating the performance, authors have used NS-2 as a simulation tool. For the purpose of simulation, authors have used 1000 sec simulation run, 160*160 m2 sensors field. The simulation result gives accurate performances in network survivability and data delivery ratio.

Theodore Zahariadis.et.al [15]: In this paper, authors proposed a secure routing protocol that works with dimensions of network and depended on trusted models for the purpose of withdrawing and discovering of malicious neighbours. For evaluating the performance, authors have used JSIM as a simulation tool. For the purpose of simulation, authors have used 10 × 10 grid, IEEE 802.15.4 standard, 2 sec Beacon interval, 31 bytes of the packet and 4000 sec simulation run time. The simulation result shows that the Ambient trust sensor routing opens up malicious nodes even when they describe many attacks, presents 50% network nodes and explains existing trusted routes to the destination.

Devesh Pratap Singh.et.al [16]: In this paper, authors access the query into the network to a specific area by proposing an energy efficient routing method. For evaluating the performance, authors have used OPNET as a simulation tool. For the purpose of simulation, authors have used 1*1 km area, 180 min simulation time, 0.1 sensing duration, 1500 bits packet size and 3 routers and 1 coordinator network size. The simulation result shows that when the density of network increases by 33.33% then it shows a decrease in throughput by 22.59% and a decrease in an end to end delay by 25.55%. Future work can be done by decreasing the power required by the network.

3. Clustering Techniques

Clustering is the procedure of scheduling objects into groups whose members are same in some manner, where each cluster contains one node as a cluster head, liable for some tasks. Clustering is responsible for mutual organization of sensor nodes that is used for communication and coordination between neighboring nodes. Disturbance is decreases by this function in multiple access broadcast atmosphere [18]. Each cluster has one or more sensor nodes and a cluster head (CH). For each node in the cluster the communication with the public key is handled by the cluster head, this offer transmission quickly among cluster members, which provide straight transmission with a further node [20]. Moreover, a node without overlapping is forwarding in the exact cluster that doesn't generate any matter still it doesn't impact the cluster architecture [17]. The clustering method consist three group of nodes: the first step which is a mobile certification authority (administrator) is available at the start-up then it can free the network; master services are provided by a variety of cluster head [21]. Public and a private key is available for each node. Each cluster head in this structure is assumed as a mobile certification authority for its cluster members [19]. Resource consumption is decreases and security performance increases for manufacturing a secure WSN system which contains a variety of nodes, that are used for administration of great area and system coordination centre [22].

4. Key Pre-Loaded in Sensor Nodes

Pre-loading the secret keys into sensor node is the finest key administration prior to layout. Similarly, some secret information requires being pre-loaded into sensor nodes earlier they are deployed. One distinctive secret key is used for pre-loading sensor nodes, shared with the other sensor node in the introduced technique. Distinctive keys are used by sensor nodes which are permit to other corresponding sensor node. The other sensor nodes, generates ID during this method and charge each node with this key. The network key is used for watching ID and used in cluster formation method. Observe that each member should demonstrate their logic to the sink node. A distinctive key is used to permit the own node for each node, shared with the destination sensor node (KAB) and is removed after the first round.

5. Neighbor's Public Key Distributed over CH

After the cluster establishment, the cluster head organizes and inform every cluster member. Dynamically, the sensor nodes are transmitting or hearing for a period of time and off the remainder. The sensor nodes transfer only at their scheduled time. This permits the sensor nodes to hear to the interaction in their respective clusters. It is through this passive hearing that the sensor nodes are capable of establishing trust relationships with their neighboring nodes. Nodes that constantly lost packets or which act in a selective or selfish way can be easily determined by their neighbors.

Every sensor node records and manages a trust key value of its neighboring nodes.

6. Secure Communication using Pair-Wise Keying

Pair-wise keying procedure offers basic security facilities in wireless sensor networks. That enables sensor nodes to interact securely with each other utilizing cryptographic methods. These bear sensor node compromise by restricting the scope of each key. Hence, a sensor node compromise only influences the past and future messages forwarded to or from that sensor node; other traffic is uninfluenced. Higher robustness against sensor node compromise does come at a cost, specifically in the overhead included for key management.

If a sensor node interacts with a large no. of sensor nodes, it must record several keys and choose the suitable ones when interacting. However, sensor nodes are restrained in resources this storage cost involvement can be prohibitive. This technology offers Pair-wise key establishment and management mechanisms which support in building the network secure.

7. Key Distribution and Encryption Model of the System

In our introduced technique, clustering is started by sensor nodes. Assume if any two key is a process as Node A and Node B are two interacting sensor nodes in the WSN System. MCA is a cluster head within an ad hoc network, and it is chosen to offer distributed key management centre's service. KAB is the communication pair-wise keys among nodes A and B. {M} Pub A represents the message M encryption with Public Key of node A.

Step 1 A sensor node (Node A) flood a message, which consists its ID (IDA) to its neighbors.

Step 2 Every neighbor (Node B and others) should achieve the Public Key of Node A from MCA.

Step 3 Sensor Node B utilizes Sensor Node A's public key to encrypt messages which consist its identifier (IDB) and a random number (RN1), which is utilized to determine this transaction

Step 4 Sensor Node A forwards a message to Sensor Node B encrypted with Pub B and consisting B's random no. (RN1) as well as a new random no. created by Node A (RN2).

Step 5 Sensor Node B chooses a secret key KAB and returns this and RN2, which are encrypted utilizing Pub A, to ensure A that its correspondent is B.

Step 6 The interacting parties (Sensor Nodes) are agreeing on a Pair-wise key and they can utilize this for protected communication.

8. Results and Analysis

The simulations results are examined and discussed in this chapter. The results are examined and explained in various scenarios having networks of 100 sensor nodes for monitoring applications. In introduced framework, I have utilized symmetric key cryptographic Blowfish algorithm which is suitable to all three network level. In the first scenario, there are 100 sensor nodes and the parameter throughput, delay and network load for the routing protocol LEACH and THVRG are examined. In the second scenario the no. of nodes is same. It depends on time synchronized method and some parameters are set and the performance of the protocol is examined. In the third scenario, the no. of nodes is again same. In this scenario the clustering method is utilized and in this design the cluster heads for best network performance. Eventually, in the fourth scenarios some network nodes is failed and network performance is examined by utilizing same methods which are utilized in the third scenario and the parameter throughput and delay for the routing protocol LEACH AND THVRG is examined.

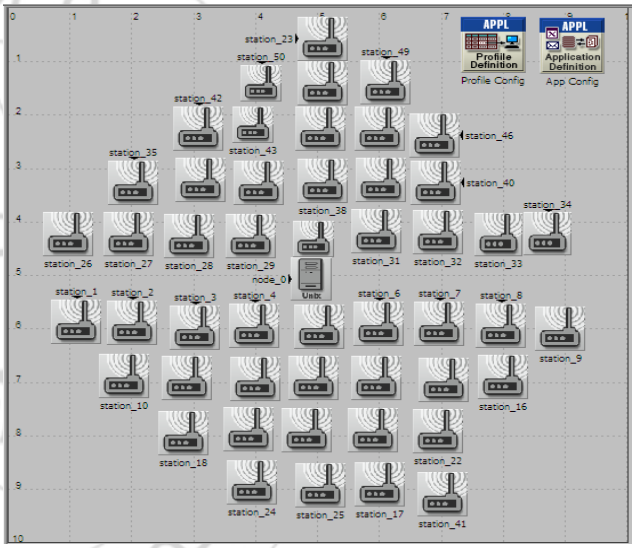

Figure 2: Simple Wireless Sensor Network

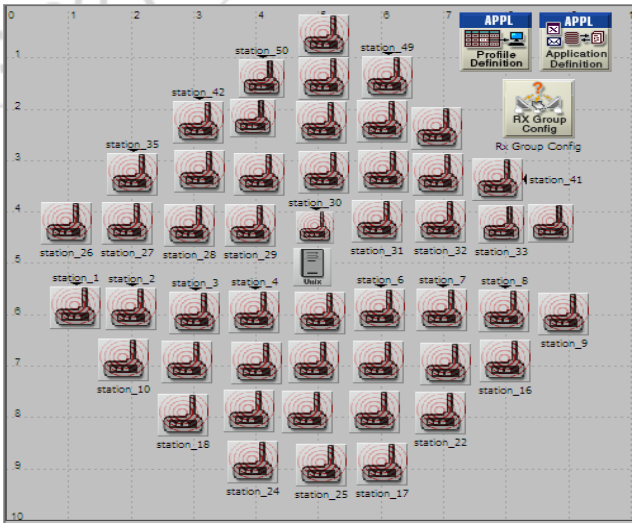

Figure 3: Wireless Sensor Network using Time

Synchronization Technique through LEACH and THVRG

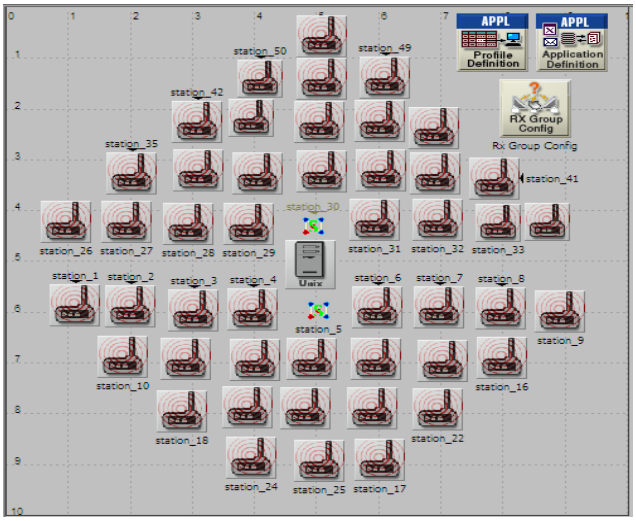

Figure 4: Wireless Sensor Network using clustering Technique through LEACH and THVRG

7.1 Delay

In fig. 5 no mechanism is used on mobile nodes in a provided scenario. During simulation, the delay is detected at different intervals. In representing graph x-axis indicates the time and y-axis presents the delay in term of seconds. The Maximum delay is detected at 0.0023 sec.

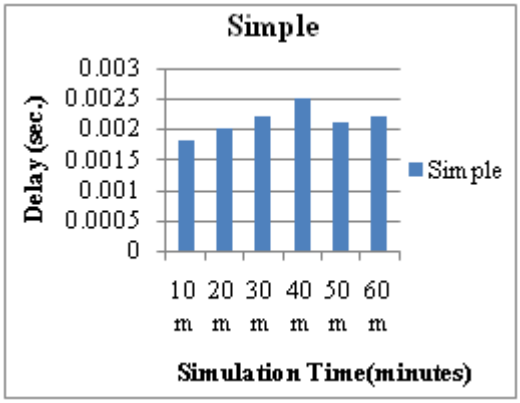

Figure 5: Delay of Simple scenario through LEACH and THVRG

The delay value reduces slowly till 0.0018 sec. Delay value increases and reduces slowly throughout the simulation procedure. It is concluded that during simulation for the delay there is more fluctuation, and determine more delay when there has no mechanism used.

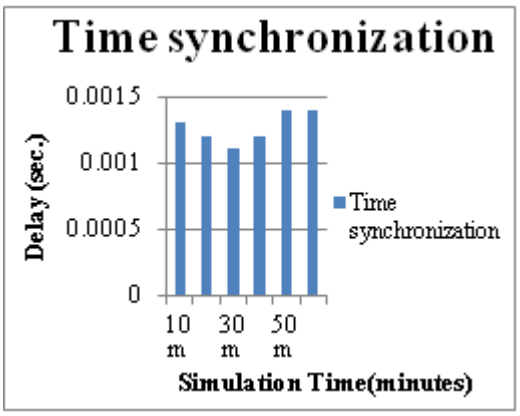

Figure 6: Delay using Time Synchronization technique

In fig. 6 time synchronization mechanism is used on mobile nodes in a provided scenario. During simulation, the delay is determined at different intervals. The maximum delay is detected at 0.0015 sec. The delay value reduces slowly till 0.0013 sec. It is concluded that during simulation for the delay there is less fluctuation, and determine less delay when there has time synchronization method used in the comparison of the first scenario.

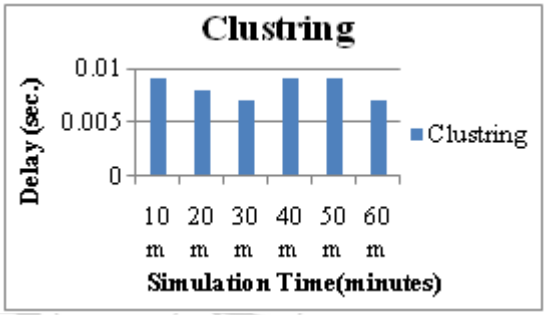

Figure 7: Delay using clustering technique

In fig. 7 clustering mechanism is used on mobile nodes in a provided scenario. During simulation, there is no delay change by employing clustering technique as indicated in fig. It is concluded that during simulation for the delay there is no fluctuation, and detect no delay when there has clustering mechanism used in the comparison of the second scenario.

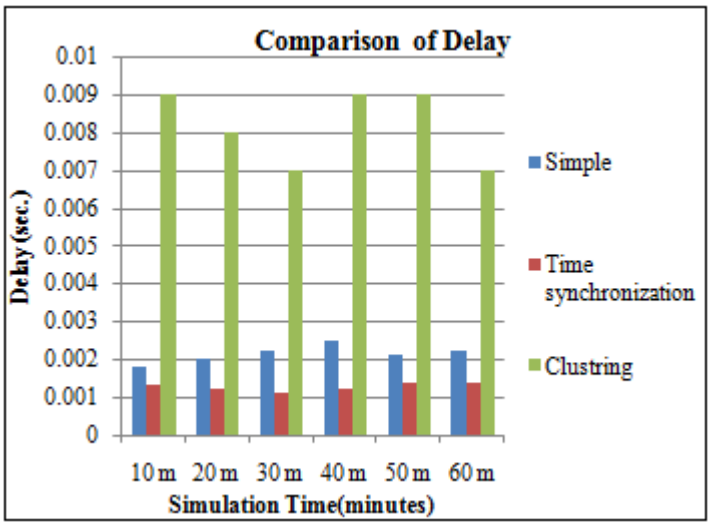

Figure 8: Comparison of Delay

So according to the simulation the performance analysis of clustering mechanism is better in terms of delay.

7.2 Throughput

In fig. 9 there is no technique used on mobile nodes in a provided scenario. Highest throughput is detecting at 7500 sec. Throughput value increases and reduces slowly throughout the simulation procedure.

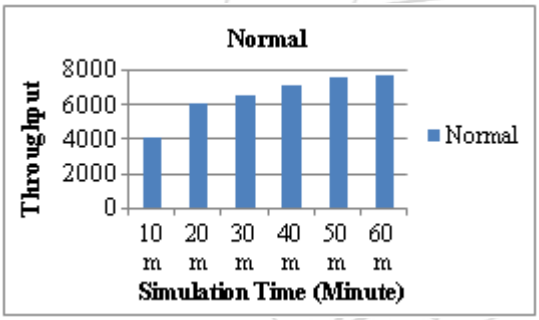

Figure 9: Throughput of Simple Scenario through LEACH and THVRG

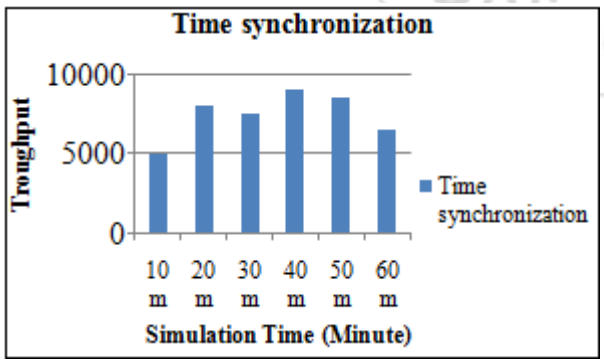

Figure 10: Throughput using Time Synchronization Technique through LEACH and THVRG

In fig. 10 there is time synchronization mechanism is used on mobile nodes in a provided fig. highest throughput is detecting at 9000 sec. Throughput value increases and reduces slowly throughout the simulation procedure. It is concluded that during simulation for throughput there is more throughput when there has time synchronization method used in the comparison of the first scenario.

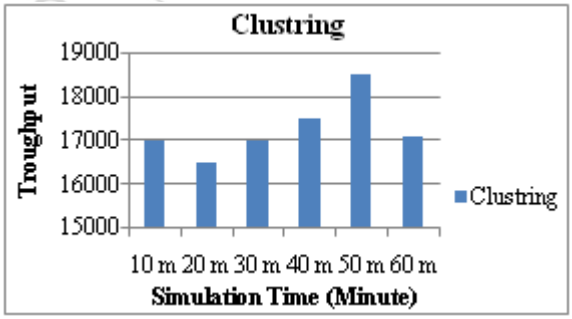

Figure 11: Throughput using Clustering Technique through LEACH and THVRG

In fig. 12 there is clustering technique is used on mobile nodes in a provided scenario. Highest throughput is determining at 21000 sec. It is concluded that during simulation there is an increase in throughput in comparison of other techniques when there has clustering technique is used.

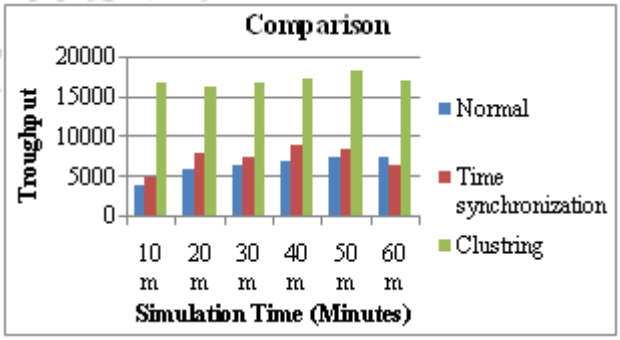

Figure 12: Comparison of Throughput through LEACH and THVRG

9. Conclusion

This thesis talks about and measures the performance of several techniques in various scenarios for WSN by utilizing LEACH and THVRG routing protocol for monitoring of serious conditions with the support of significant metrics i.e. throughput, delay, and network load. So according to the

simulation the performance analysis of clustering mechanism is better in terms of throughput and delay for mobile nodes in WSN. Based on results obtained from simulation a conclusion is drawn on the comparison among these various techniques with parameters i.e. throughput, delay and conclude that clustering method is better for the energy efficiency.

References

[1] S.K. Singh, M.P. Singh, and D.K. Singh, "A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.

[2] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[3] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient Communication Protocol for Wireless microsensor Networks", in IEEE Computer Society Proceedings of the Thirty Third Hawaii International Conference on System Sciences (HICSS '00), Washington, DC, USA, Jan. 2000, vol. 8, pp. 8020.

[4] Bhoopathy, V. and R.M.S. Parvathi, "Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2, pp.466-474,Mar-Apr 2012.

[5] Karl Holger, Willig Andreas, "Protocol and Architecture for Wireless Sensor Network", John Willey and Sons Ltd, 2005

[6] Amrinder Kaur, Sunil Saini," Simulation of Low Energy Adaptive Clustering Hierarchy Protocol for Wireless Sensor Network," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue7, July 2013.

[7] I.F. Akyildiz, W. Su, et al., "Wireless sensor networks: a survey", Computer Networks 38 (4) (2002) 393–422.

[8] Akyildiz, I. F., Melodia, T. & Chowdhury, K. R. (2007). A survey on wireless multimedia sensor networks, Comput. Netw. 51(4): 921–960.

[9] K.SOHRABY,D.MINOLI,T.z NATI" WIRELESS SENSOR NETWORKS, Technology, Protocols, and Applications" Published by John Wiley & Sons, Inc., Hoboken, New Jersey. 2007

[10] L. Sun, J. Li, Y. Chen, et al., "Wireless Sensor Network", Tsinghua University Press, Beijing, China, 2005.

[11] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey", Computer Networks, Vol. 52, No. 12, 2292-2330, 2008.

[12] Basavaraj S. Mathapati , Patil Dr. Siddarama. R. , and Mytri Dr. V D. "Energy Efficient Cluster based Mobility Prediction for Wireless Sensor Networks", (IEEE (International Conference on Circuits, Power and Computing Technologies (ICCPCT)), 2013.

[13] Sachin Gajjar, Shrikant N. Pradhan, Kankar Dasgupta, "Performance Analysis of Cross Layer Protocols for Wireless Sensor Networks",

[14] Houda Zeghilet, Nadjib Badache, and Moufida Maimour, "Energy Efficient Cluster-based Routing in Wireless Sensor Networks" , IEEE symposium on computers and communication 2009, ISCC- 2009, pp. 701-704, sepember 2009.

[15] Theodore Zahariadis, Panagiotis Trakadas, Helen C. Leligou, Sotiris Maniatis and Panagiotis Karkazis, "A Novel Trust-Aware Geographical Routing Scheme for Wireless Sensor Networks", Wireless Personal Communications, Springer Nature, pp. 805-826, April 2012.

[16] Devesh Pratap Singh and R. H. Goudar, "Energy efficient clearance routing in WSN", International Journal of System Assurance Engineering and Management, Springer Science+Business Media, May 2014.

[17] Khalid Haseeb, Kamalrulnizam Abu Bakar, Abdul Hanan Abdullah and Tasneem Darwish, "Adaptive energy aware cluster-based routing protocol for wireless sensor networks", Wireless Netw, Springer Science+Business Media, April 2016.

[18] Suneet K. Gupta and Prasanta K. Jana, "Energy Efficient Clustering and Routing Algorithms for Wireless Sensor Networks: GA Based Approach", Wireless Pers Commun, Springer Science+Business Media, vol. 83, pp. 2403-2423, April 2015.

[19] E. Golden Julie, S. Tamilselvi, and Y. Harold Robinson, "Performance Analysis of Energy Efficient Virtual Back Bone Path Based Cluster Routing Protocol for WSN", Wireless Pers Commun, Springer Nature, July 2016.

[20] Hiren Kumar Deva Sarma, Avijit Kar, and Rajib Mall, "A Hierarchical and Role Based Secure Routing Protocol for Mobile Wireless Sensor Networks", Wireless Personal Communications, Springer Nature, vol. 90, pp. 1067-1103, June 2016.

[21] Md Azharuddin and Prasanta K. Jana, "PSO-based approach for energy-efficient and energy-balanced routing and clustering in wireless sensor networks", Soft Comput, Springer Nature, June 2016.

[22] S. Prabhavathi, A. Subramanyam and A. Ananda Rao, "Energy Efficient Dynamic Reconfiguration of Routing Agents for WSN Data Aggregation", Emerging Research in Computing, Information, Communication and Applications, Springer Science+Business Media, pp. 291-301, Aug 2015.