A Secured Routing Technique for Wireless Sensor Networks

Helen Samuel, Sharnee Kaul
Electronics and Communication Engineering
K.C.G College of Technology
Chennai, India

Jose Anand
Electronics and Communication Engineering
K.C.G College of Technology
Chennai, India

***Abstract*—Wireless Sensor Networks (WSNs) are networks which sense the data from a remote region and collect it before transmission. The collected information is transmitted to the sink node. Hence the information needs to be passed in an energy efficient and secured manner. Many of the existing routing protocols do not guarantee the optimal selection of cluster heads. The cluster head selection does not necessarily take into account the remaining energy of the nodes. Hence the protocol which takes into account the remaining energy of the nodes for cluster head election is analyzed. The Adaptive Energy-efficient Routing Protocol (AECRP) considers the remaining energy of the nodes and provides an energy-efficient network. Further the data is encrypted using the RSA algorithm to provide a secure and reliable data delivery. This paper involves the analysis of the energy consumption of Low Energy Adaptive Clustering Hierarchy (LEACH) and AECRP. The comparison of LEACH and AECRP in terms of end –to-end delay , throughput, energy consumed, and packet delivery ratio with and without encryption are analyzed.**

Keywords— Cluster, Energy-efficient, routing protocol, security

I. INTRODUCTION

WSNs consist of large number of sensor nodes which sense the information from a remote terrain, collect the information and transmit it to the sink node. The energy consumed for sensing the data is less than that required for the transmission of the data to the sink node. Many of the applications involving WSNs require the transmission of the data to the sink node and hence it consumes more energy. The data transmitted also have chances of undergoing an attack by an adversary and hence it is important to protect the data from an external attack. The secure routing of the data to the destination is an important requirement in improving the performance of a network. In order to protect the information, we use encryption and decryption technique.

Energy consumption of the network can be reduced by making use of the hierarchical routing protocols. The most popular and efficient protocol which was used to provide better energy-efficient network is the LEACH protocol. LEACH protocol is a cluster based protocol where the information is transmitted to the sink node via the cluster heads (CH). The CH collects the information from the nodes that are the members of that cluster. Each of the CH transmits the information to the CH which is nearby the sink node. The drawback of LEACH protocol is that it randomly selects the CH without considering the remaining energy of the nodes using the Random Inertia Weight (RIW) strategy. Hence this protocol reduces the lifetime of the network.
Node and to overcome this drawback of the LEACH protocol the AECRP protocol is made use of.

The AECRP protocol is a combination of particle swarm clustering algorithm and inter-clustering algorithm. The network clustering is a kind of Neighbor Position (NP) problem and this is overcome by the particle swarm clustering algorithm. Since the convergence speed of this is slow, the Particle Swarm Optimization (PSO) is used which considers the remaining energy of the nodes, the distribution within a cluster and the distribution among clusters. The inter-clustering algorithm makes use of both single-hop and multi-hop communication to reduce the communication distance between the CH and the sink node. The AECRP protocol uses the Decreasing Inertia Weight (DIW) algorithm which sets priority to the nodes based on the remaining energy of the nodes.

Moreover the information that is transmitted via the relay nodes in the network needs to be protected and unchanged when it reaches the destination. Hence the RSA algorithm is used to encrypt the data at the sender side and decrypt the data at the destination. This process of encryption and decryption assures the reliable delivery of data and provides an added security to the network thereby increasing the performance of the network.

II. LEACH

LEACH (Low-Energy Adaptive Clustering Hierarchy) is a clustering-based routing protocol that utilizes randomized rotation of cluster heads to distribute the energy load evenly among the sensors in the network. LEACH uses localized coordination to enable scalability and robustness for dynamic networks, and imbibes data aggregation into the routing protocol to reduce the amount of information being transmitted to the base station. LEACH is a self-organizing, adaptive clustering protocol that uses randomization to distribute the energy load evenly among the sensors in the network. The operation of LEACH is divided into rounds. Each round begins with a setup phase when the clusters are organized, followed by a steady-state phase when data are transferred from the nodes to the cluster head and on to the Base Station (BS).

IJERT

In LEACH, the nodes organize themselves into local clusters, with one node acting as the local base station or cluster-head. Sensors elect themselves to be local cluster-heads at any given time with a certain probability. These cluster head nodes broadcast their status to the other sensors in the network. Each sensor node determines to which cluster it wants to belong by choosing the cluster-head that requires the minimum communication energy. Once the cluster-head has all the data from the nodes in its cluster, the cluster-head node aggregates the data and then transmits the compressed data to the base station. Each Cluster Head (CH) is responsible for creating and manipulating a TDMA (Time division multiple access) schedule and sending aggregated data from nodes to the Base Station (BS). Remaining nodes are cluster members.

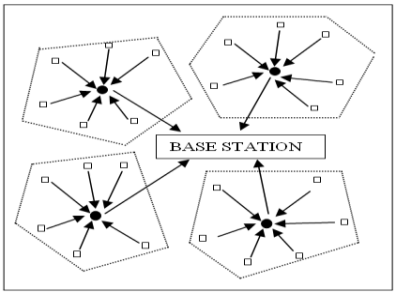

Fig.1. LEACH Protocol

Figure 1 show the process of LEACH protocol which explains the steps involving collecting the data from cluster members and the cluster head aggregating the information. The compressed information from all the cluster head finally reaches the BS. LEACH provides an energy-efficient network but it suffers from few drawbacks. The drawbacks are that the CH selection takes place in a random manner without considering the remaining energy of the node in the network. In this process the low energy nodes are also selected as cluster heads. Hence this process leads to the network performance declination as the node dies as soon as its energy drains off. Another drawback in LEACH is that it cannot cover large area. Hence a protocol which can overcome these drawbacks and make the performance better is required.

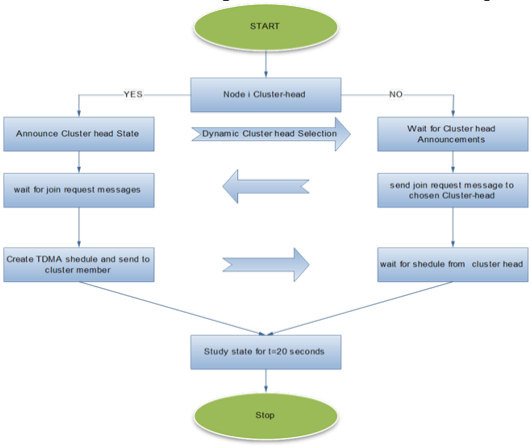

Fig.2. Architecture of LEACH Protocol

Figure 2 describes the architecture of LEACH protocol. In LEACH the election of nodes as cluster heads takes place in a random manner without considering the remaining energy of the node at that instant of time. In this process the nodes with low energy if selected as the cluster head will die soon and will cause the performance of the network to decline.

III. AECRP

To overcome these drawbacks of LEACH, a protocol that can consider and calculate the remaining energy of the nodes in order to select the cluster heads is required. Hence AECRP protocol that is a combination of the PSO and inter-clustering algorithm is analyzed. This protocol makes use of the DIW strategy. In this scheme the nodes with less amount of energy is given priority in the network. The nodes with low energy are first chosen as cluster head in each round of its operation. The nodes are arranged in their decreasing order of priority and the nodes which are first in this order are in a critical position because of the energy available in the node. If the node with low energy is selected as cluster heads in the network then the performance of the network declines as the cluster head will die as soon as the energy of the node is drained completely.

The AECRP protocol is more efficient than LEACH in terms of energy, security, throughput and delay. It provides a more secure transmission of information through the network. The time taken for the data to reach the destination node is less than the time taken in LEACH.

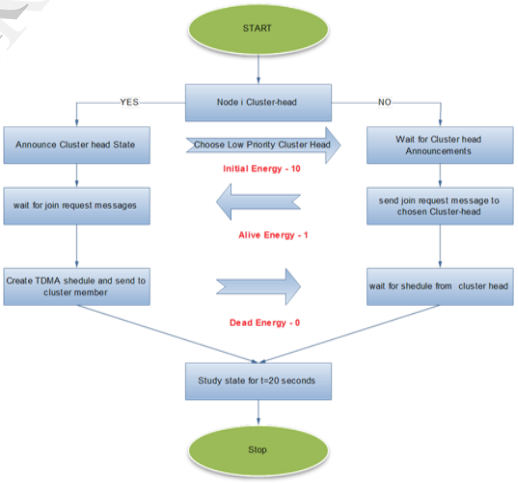

Fig. 3. Architecture of AECRP Protocol

Figure 3 shows the architecture of AECRP protocol. The protocol chooses the cluster head based on the priority. The node with low energy which has low priority is first chosen as cluster head. The initial energy of the node is taken as 10J. The cluster head then sends messages to the members to join under its cluster. If the energy of the node is greater than 1J then the node is said to be alive and can be chosen as cluster head for that round of operation. If the node is 0J then the node is said to be dead which states that it cannot be chosen as the cluster head.

AECRP is a protocol which reduces the energy consumption of the network and balances the energy throughout the lifetime of the network. It chooses the low

energy nodes as cluster heads first in the network. By doing so the lifetime of the network is increased and the energy gets distributed in a balanced manner making the performance of the network efficient.

The security feature in both LEACH and AECRP is given using the RSA algorithm. The RSA algorithm is a public key encryption technique. RSA algorithm is named after its founders, Ron Rivest, Adi Shamir and Leonard Adleman. There are two interrelated components of RSA; they are the choice of the public and the private key, the encryption and decryption algorithm. The public and private keys are chosen by considering two prime numbers. The larger the number, the more difficult it is to break RSA.

IV. RESULTS AND SIMULATIONS

A. Energy and throughput analysis of LEACH and AECRP

The important element of the routing protocol which determines the efficiency of the WSN is the energy consumed by the entire network and the throughput of the network. Hence the energy and throughput of LEACH and AECRP is analyzed. The simulation is carried out using NS-2 simulator and 100 nodes are taken with an initial energy of 10J.

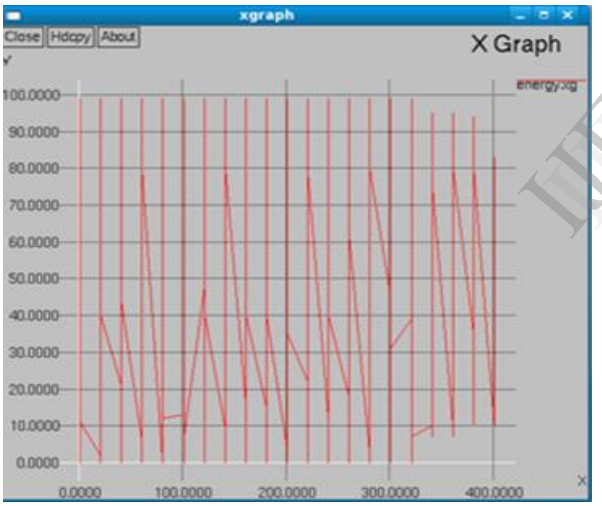

Fig.4. Energy Analysis of LEACH Protocol

Figure 4 shows the energy analysis of LEACH protocol. The graph is plotted against time in milliseconds in X-axis and energy in Joules in Y-axis. The graph explains how the energy consumed by the nodes at different time instants in the network varies. In LEACH protocol the nodes are elected as cluster heads in a random manner. Thus the energy of the low energy nodes get dropped soon thus causing the network performance to vary rapidly.

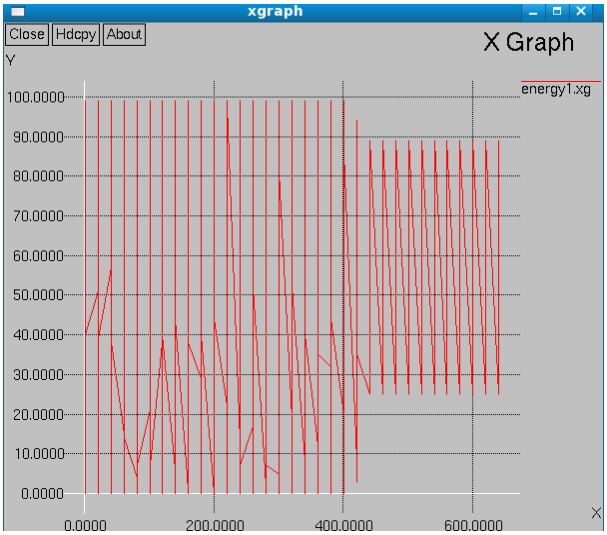

Fig.5. Energy Analysis of AECRP Protocol

Figure 5 explains the energy variations in AECRP protocol. AECRP protocol uses the DIW strategy. The graph is plotted against time in millisecond s in X-axis and Energy consumed in Joules in Y-axis. The analysis shows that due to the priority wise selection of nodes as cluster heads based on remaining energy of the nodes, the energy of the network is balanced till the lifetime of the network and thus increases the performance.

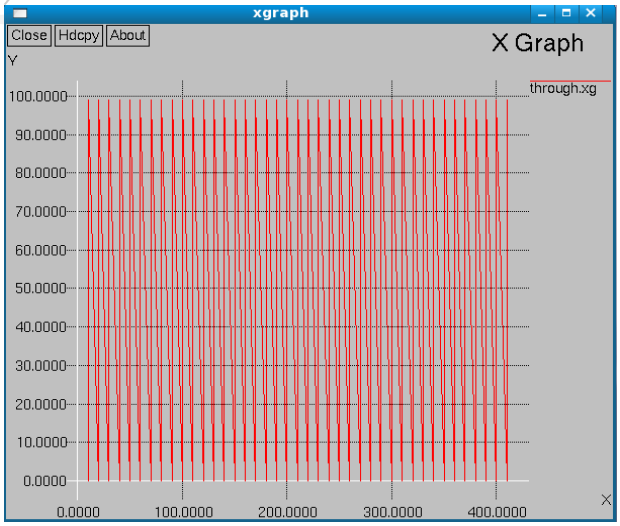

Fig.6. Throughput Analysis of LEACH protocol

Figure 6 shows the throughput analysis of LEACH protocol. As discussed above due to the random selection of nodes as cluster head without considering the remaining energy of the nodes, we obtain a low throughput percentage of the network. The graph is plotted against time in milliseconds in X-axis and throughput in percentage in Y-axis.

IJERT

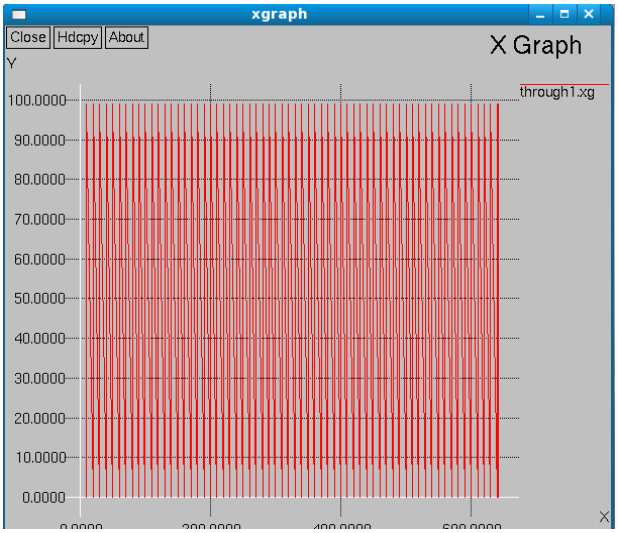

Fig.7. Throughput Analysis of AECRP

In figure 7 the throughput analysis of AECRP protocol is analyzed. The graph is plotted against time in milliseconds in X-axis and throughput in percentage in Y-axis. As discussed due to the priority wise selection of nodes as cluster heads based on the remaining energy of the nodes, the throughput percentage of the network is high and hence this improves the performance of the network.

B. Comparison of LEACH and AECRP

LEACH and AECRP protocols are compared in terms of throughput, energy consumed, end-to-end delay and the packet delivery ratio. The simulations are carried out using NS-2 simulator and 50 nodes are taken for comparison.

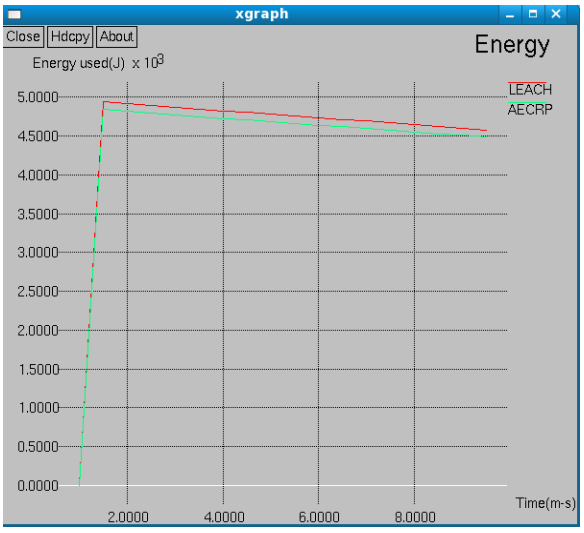

Fig.8. Energy comparison of LEACH and AECRP protocol

Figure 8 shows the comparison of energy consumed. The graph is plotted against time in milliseconds in X-axis and energy in Joules in Y-axis. The comparison shows that AECRP consumes less energy than LEACH and this is due to the DIW strategy used in the AECRP protocol thereby making it an energy-efficient routing protocol.

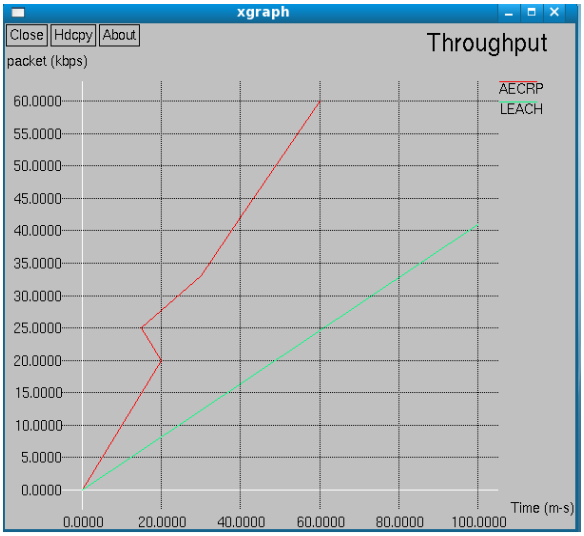

Fig.9. Throughput Comparisons of LEACH and AECRP

Figure 9 shows the throughput comparison of LEACH and AECRP. The graph is plotted against time in milliseconds in X-axis and the number of packets in kbps in Y-axis. The plot shows that throughput of AECRP is higher than LEACH. As discussed in the throughput analysis graph, AECRP has high throughput than LEACH due to the DIW strategy used.

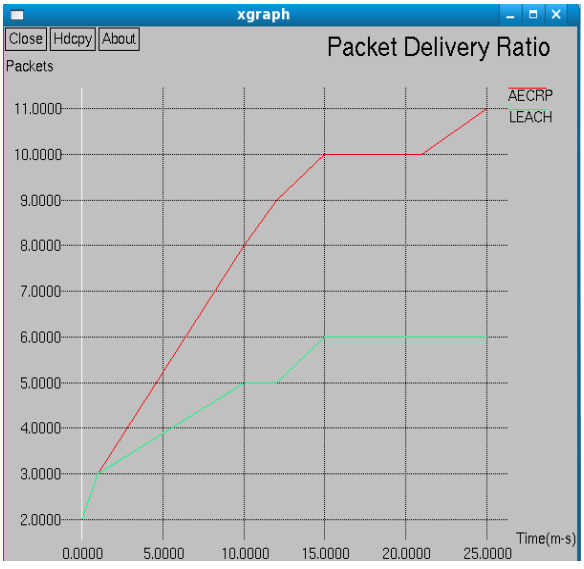

Fig.10. Packet delivery ratio comparisons of LEACH and AECRP before encryption and decryption

Figure 10 shows the comparison of packet delivery ratios of LEACH and AECRP. Packet delivery ratio is defined as the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination. The greater value of packet delivery ratio means the better performance of the protocol. This graph considers the ratio before adding the cryptographic technique to add the security feature to the data.

IJERT

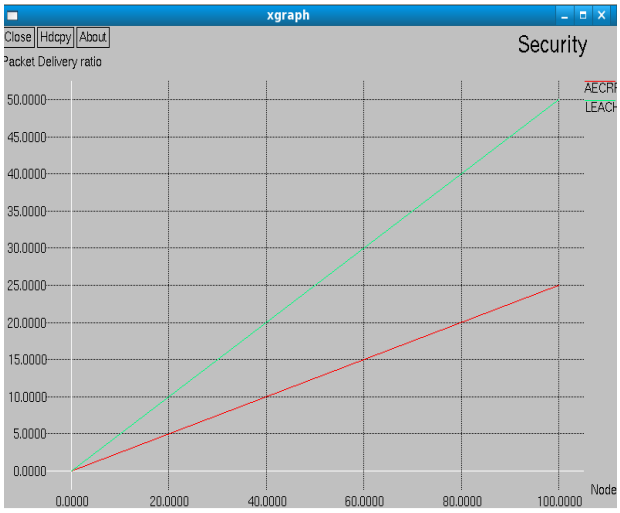

Fig. 11. Comparison of packet delivery ratio of LEACH and AECRP after encryption and decryption

Figure 11 shows the comparison of packet delivery ratio of LEACH and AECRP after invoking the security feature. The information is encrypted in the sender side using the RSA algorithm and it is decrypted at the receiver side. This security feature increases the number of packets delivered. If the figure 10 is observed the number of packets delivered without security in AECRP is 11 whereas after securing it 100 packets are delivered. Thus security feature in AECRP increases the data reliability in a WSN.

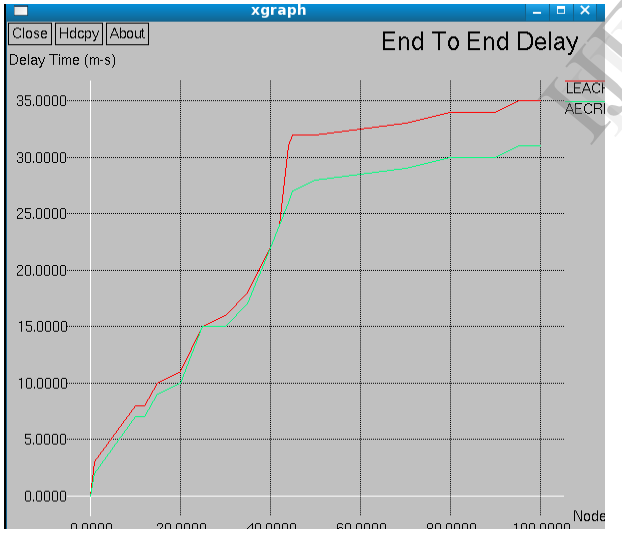

Fig. 12. End-to-end delay comparisons of LEACH and AECRP

In figure 12 the end to end delay of LEACH and AECRP is compared. The graph is plotted against time in X-axis and delay time in Y-axis, both are taken in milliseconds. End-to-end delay is defined as the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that are successfully delivered to destinations are counted. The lower value of end-to-end delay means better performance of the protocol.

V. CONCLUSION

WSNs require high amount of energy in order to transmit the data to the base station .Clustering techniques is a useful and efficient method to reduce the consumption of energy in the network. This technique reduces the communication overhead and exploits data aggregation in WSNs. Clustering has been shown to improve network lifetime, a primary metric for evaluating the performance of a sensor network. Although there is no unified definition of "network lifetime," common definitions include the time until the first/last node in the network depletes its energy and the time until anode is disconnected from the base station. Hence it is proved in this paper that AECRP is an energy-efficient routing protocol which delays the death time of the node and provides better packet delivery ratio using the encryption and decryption technique.

REFERENCES

[1] Al-Karaki, A. Kamal, "Routing Techniques in Wireless Sensor networks: A Survey," Security and Networks, 2004, Vol. 11, Issue 6, pp. 6-28.
[2] B. Naik, S. Swetanisha, D.K. Behera, S. Mahapatra, B.K. Padhi. "Cooperative swarm based clustering algorithm based on PSO and k-means to 6find optimal cluster centroids", 2012 National Conference on Computing and Communication Systems (NCCCS), 1-5, 2012.
[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Proc. of IEEE SNPA 2003, 2003.
[4] Chi-Tsun Cheng, C.K. Tse, F.C.M. Lau. "A Delay-Aware Data Collection Network Structure for Wireless Sensor Networks", IEEE Sensors Journal, Vol.11, No.3, 699-710, 2011.
[5] C. Li, M. Ye, G. Chen, J. Wu, "An energy-efficient unequal clustering mechanism for wireless sensor networks", Proceedings of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems MASS'05, 2005.
[6] D. A. Vidhate, A. K. Patil, S. S. Pophale, "Performance Evaluation of Low Energy Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," In Proc. International Conference and Workshop on Emerging Trends in Technology (ICWET 2010)TCET, Mumbai, India, 2010, pp. 59-63.
[7] J. Kennedy, R. Eberhart. "Particle swarm optimization", IEEE International Conference on Neural Networks, Vol.4, 1942-1948, 1995.
[8] K. Latif, M. Jaffar, N. Javaid, M.N. Saqib, U. Qasim, Z.A. Khan. "Performance Analysis of Hierarchical Routing Protocols in Wireless Sensor Networks", 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), 620-625, 2012.
[9] L. Qing, Q. Zhu, M. Wang, "Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks". ELSEVIER, Computer Communications 29, pp 2230-2237, 2006.
[10] M. J. Handy, M. Haase, D. Timmermann, "Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection," In Proc. 4th International Workshop on Mobile and Wireless Communications Network, USA, 2002, Vol. 1, pp. 368-372.
[11] NS-2 Network Simulator. http://www.isi.edu/nsnam/ns/.
[12] R.V. Kulkarni, G.K. Venayagamoorthy. "Particle Swarm Optimization in Wireless-Sensor Networks: A Brief Survey", IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol.41, No.2, 262-267, 2011.
[13] Xia Li, Wang Gang, Liu Zongqi, Zhang Yanyan , "An energy-efficient routing protocol based on particle swarm clustering algorithm and inter-cluster routing algorithm for WSN", 978-1-4673-5534-6/13/$31.00, c 2013 IEEE.
[13] Y. Shi, R.C. Eberhart. Empirical study of particle swarm optimization, 1999. CEC 99. Proceedings of the 1999 Congress on Evolutionary Computation, Vol.3, 1999.

IJERT