Grenze International Journal of Engineering and Technology, July 2017

Optimized Implementation of Energy Efficient Spherical Grid Routing Protocol to Monitor Fast Moving Object

Jai Prakash Prasad[1] and Dr. Suresh Chandra Mohan[2]
[1]Department of ECE, DBIT, Bangalore, India
Email: jaiaasu@gmail.com
[2]Deptarment of ECE, BIET, Davangere, India
Email: drcmohan@rediffmail.com

***Abstract*—Wireless Sensor Networks (WSN) is composed of a several number of sensor nodes which is scattered over a particular field to ensure node communication connectivity and intra or inter cluster broadcasting. Due to resource constrained nature, WSN faces many unattended challenging issues. In this paper we propose spherical based grid routing framework for long range communication. The proposed routing algorithm also implements elliptic curves cryptography for more storage and secured network. The secure routing protocol offers security benefits of authentication and confidentiality to the network. The authors present the proposed optimized implementation of Energy Efficient Spherical Grid Routing Protocol [EESGRP] to monitor fast moving object to improve network lifespan. We evaluated the performance of EESGRP on NS-2 simulation platform and its result is compared with LEACH and TTDD algorithm.**

***Index Terms*— Wireless Sensor Network, Network Life span, Inter-cluster, Intra-cluster, authentication and Confidentiality.**

I. INTRODUCTION

Wireless sensor networks are deployed over an area with several number of sensor nodes where each node is equipped with sensors that perform a collaborative measurement process in order to perform a monitoring activity. There is different types of routing algorithm exist in practice, which are able to communicate efficiently with optimized path over the network with different region of interest and is suitable for several applications. Wireless sensor networks is basically consists of main elements as nodes (Autonomous sensor-equipped device with a processor), sensors, battery and a trans-receiver module, data collections and external systems for data storing and managing center. The purpose of our work is to model a secured routing architecture to optimize communication path and to secure delivery of data using wireless sensor networks to provide authentication, confidentiality.

In order to achieve less data redundancy and control on network structure scalability sensor nodes can be divided in to number of clusters. Clustering approaches are best suitable for managing the network more effectively and therefore it improves overall network life span. Clustering in WSN has a Cluster Head (CH)

Grenze ID: 01.GIJET.3.3.10

and number of group members. The cluster heads task is to perform sensing from the environment and also provides data aggregation.
The main contribution of EESGRP is as follows. The moment EESGRP generates fresh clusters, the set of nodes are used to form different spherical routing link involving the sensor node without any packet collisions. Therefore, using EESGRP communication delay is reduced and communication process becomes faster.

II. Performance Metrics

There are various performance factors which can be used to evaluate and analyze the performance of EESGRP such as average end to end delay, packet delivery ratio, normalized overall load etc. and they are defined as follows:
Average End to End Delay- It is calculated based on the node that are finally reaches to the destination. When node starts transmitting or receiving the packets it has to come across few performance degrading factors such as queuing delay, retransmission delay, route search delay, requesting delay, broadcasting delay and so on. The proposed algorithm mainly focuses on to reduce overall processing delay of the network. The EESGRP is tasted using NS-2 simulator and hence outcome of the result has given some useful findings.
Packet Delivery Ratio (PDR) - Every packet delivery consumes some energy and delay due to processing by node before it reaches to the destination. It delivery of packet from source to destination may take different route and time because every time situation keeps on changing. Therefore is important to compute the packet delivery ratio that gives the ratio of total number of transmitted packets to total number of received packets. More the values of packet delivery ratio results in to lower value of loss of packets which guarantees better quality of service by the network.

$$PDR = \frac{\text{Total No. of received packets}}{\text{Total no. of transmitted packets}} \quad (1)$$

Normalized Overhead load (NOL) – The network involves many packets while processing the link formation and maintenance of link. The overhead for each packet in the process uses some specific message format such as RREQ and RREP for discovery of link. Nodes keep on sending information about packet to neighboring nodes to obtain the route status. NOL is the ratio between the overall routing packet to the overall received packets. Overhead gives the packet involvement in link finding using request message.

$$NOL = \frac{\text{Overall Routing Packets}}{\text{Overall Received Packets}} \quad (2)$$

III. Energy Efficient Spherical Grid Routing Protocol [Eesgrp]

In this paper we propose a model for fast moving object and a sink is moving around the network region. When each entity finishes a round completely around the network then the next outer limit of an area or object movement is very near to the centre which forms spherical movement in the network. When sink is very close to the centre of the network and if its find no further link to reduce its peripheral movement, then it initiates to move around the network with increase in distance from centre after every round trip in the network. Since the routing path is altered after every tour in the peripheral, therefore it do not cause overhead on any node on the link nodes and it optimize load balancing in the network. The optimized path formation process by the sink in the EESGRP process is shown in Fig. 1.

A. Authentication and Confidentiality Scheme

Elliptic curve cryptography: Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the mathematic proprieties of elliptic curves. Elliptic curves are suitable for encryption, digital signatures, and other security aspects. We have implemented the properties of elliptic curves in EESGRP to ensure the security of data sent by the sensors nodes and communication among sensor nodes which provides confidentiality and authentication to users.

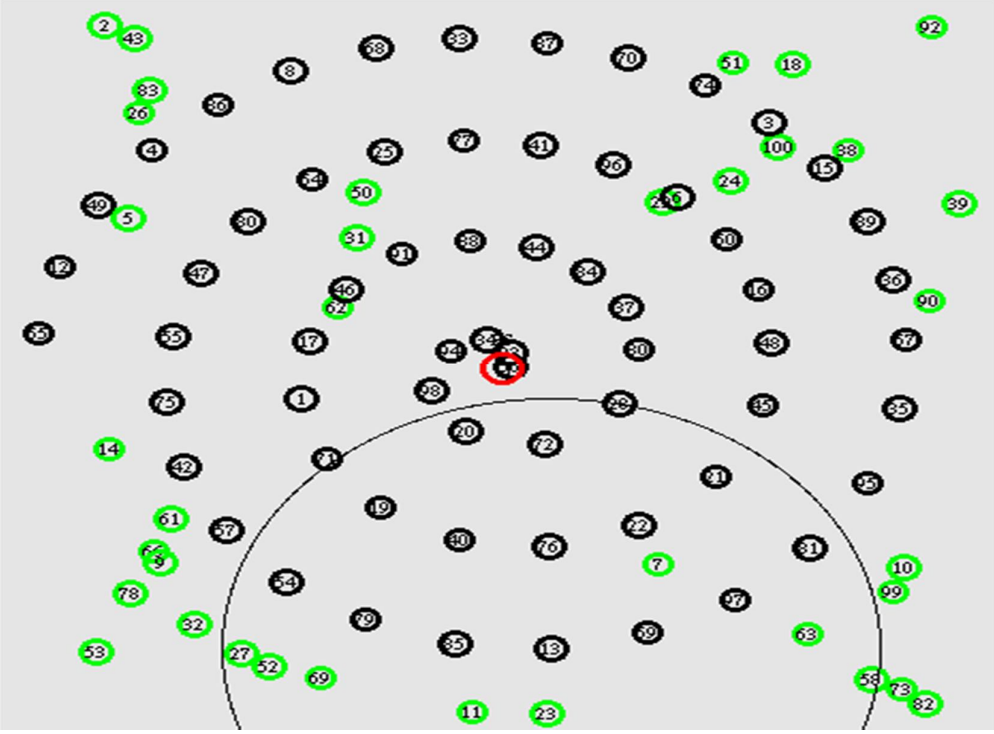

Fig. 1: Energy Efficient Spherical Grid Routing Protocol

IV. Simulation Results

We conduct the simulation in terms of average end to end delay, packet delivery ration and normalized overhead load using NS-2 for different data rate of EESGRP model and LEACH protocol. Comparison is made for both the routing protocols in terms of their performance metrics and the result obtained is shown with the help of graph in Fig. 2 to Fig. 4.

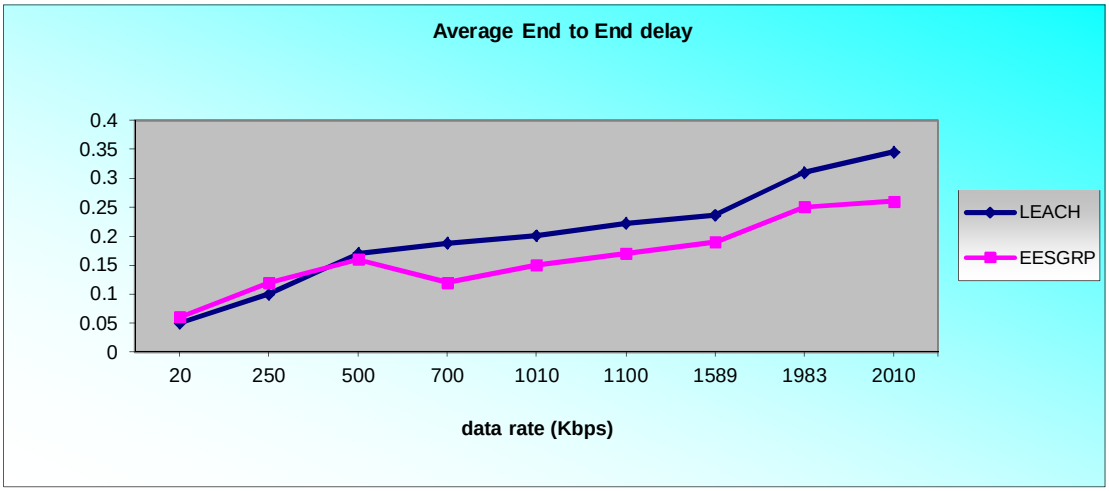

Fig. 2: Average end to end delay for different data rates

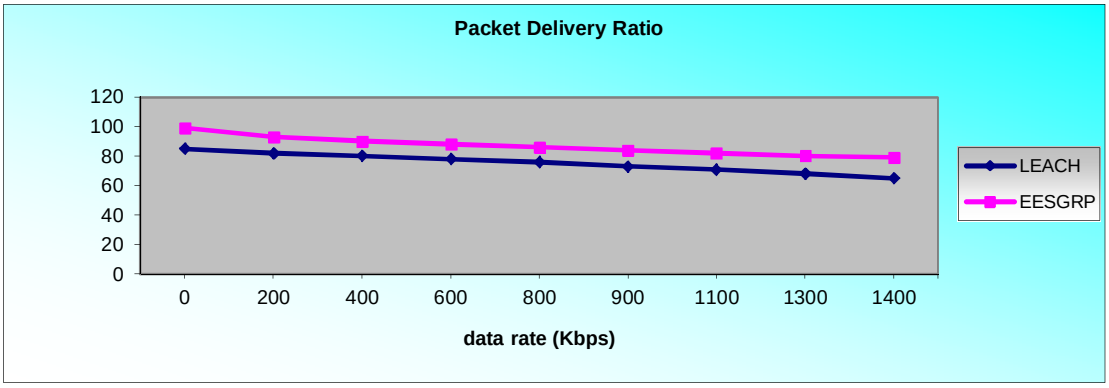

Fig. 3: Packet delivery Ratio for different data rates

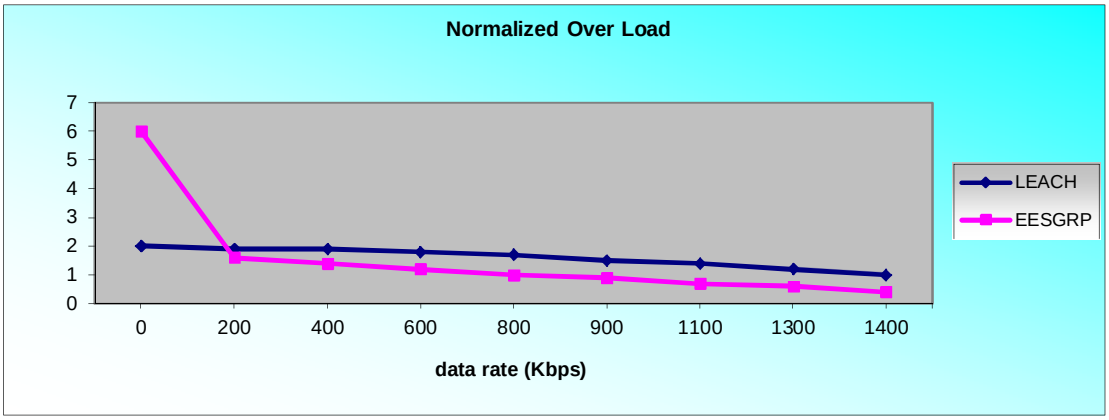

Fig. 4: Normalized overhead load for different data rates

V. Conclusion

From the above simulation outcome we have noticed that EESGRP routing protocol performs better in real time traffic application in terms of packet delivery ratio or other parameters which is discussed in the previous section. In some value of data rates the NOL is reduced in EESGRP compared to LEACH. The packet which arrives to the destination very late needed to be dropped because there is no use of such packets in real-time applications. In EESGRP the source node initiates broadcasting when there is selection of proper link between source and destination that guarantees sufficient data rate is present so that message can arrive to the destination in time. Finally we conclude that in real time application EESGRP is very much suitable when traffic load is more therefore EESGRP ensures the packet transmission over network in time.

References

[1] Cheng-Lung Yang, WernhuarTarng, Kuen-Rong Hsieh and Mingteh Chen. 2010. A Security Mechanism for Clustered Wireless Sensor Networks Based on Elliptic Curve Cryptography. Intelligent Internet Systems.

[2] AshmitaDebnath, PradheepkumarSingaravelu, ShekharVerma. 2014. Privacy in wireless sensor networks using ring signature.Journal of King Saud University – Computer and Information Sciences.

[3] Panagiotis Sarigiannidis, Eirini Karapistoli, Anastasios A. Economides. 2015. Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information, Expert Systems with Applications 42, 7560–7572.

[4] Ahmed Lounisa, AbdelkrimHadjidja, AbdelmadjidBouabdallaha, YacineChallala. 2015.Healing on the Cloud: Secure Cloud Architecture for Medical Wireless Sensor Networks.Future Generation Computer Systems.

[5] Farrukh Aslam Khan, Aftab Alia, HaiderAbbasb, Nur Al Hasan Haldarc. 2014. A Cloud-based Healthcare Framework for Security and Patients Data Privacy Using Wireless Body Area Networks. The 9th International Conference on Future Networks and Communications (FNC'14)/The 11th International Conference on Mobile Systems and Pervasive Computing (MobiSPC'14)/Affiliated Workshops, Volume 34, 511–517.

[6] Karim ZKIK, Maha TEBAA, Said EL HAJJI. 2015. New Homomorphic Platform for Authentication and Downloading Data in MCC.Proceedings of the World Congress on Engineering 2015 Vol I WCE2015, London, U.K.
[7] Don Johnson, Alfred Menezes and Scott Vanstone.2001. The Elliptic Curve Digital Signature Algorithm (ECDSA).
[8] Nigel P. Smart.1997.The Discrete Logarithm Problem on Elliptic Curves of Trace One.HP Laboratories Bristol, 97-128.
[9] J. JPC Rodrigues, I. de la Torre, G. Fern´andez, M. L´opez- Coronado. 2013.Analysis of the security and privacy requirements of cloud-based electronic health records systems. J Med Internet Res 15 (8).