International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 6
ISSN: 2454-4248
17– 21

Enhanced EQSR based QoS Mechanism for Wireless Sensor Networks

Beula Darling T
Department of Computer Science
Women's Christian College
Nagercoil, India
beulark@gmail.com

Dr. G. Suganthi G
Associate Professor, Department of Computer Science
Women's Christian College
Nagercoil, India
dr_suganthi_wcc@yahoo.co.in

***Abstract*—** Wireless sensor networks are widely used in real-time applications. Due to the resource limited nature of sensor networks providing Quality of Service (QoS) is quiet interesting and challenging task for the researchers in recent years. The QoS based schemes require to cope up with the energy constrained smaller devices. Therefore, allowing QoS applications in sensor networks mandate it to implement in separate layers. In this work an enhanced version of Energy Efficient Quality of Service Routing (EQSR) is offered. The enhanced EQSR maximizes the task of the application in mixed delay sensitive and delay tolerant applications. The scheme balances the energy by distributing the traffic in a disperse manner that guaranties the delay sensitive packets to be forwarded on time within the tolerable delay. By conducting simulations with varying scenarios the performance of the protocol is evaluated and compared with the base EQSR. The simulation results have proven that the enhanced EQSR works better by lowering the energy and increasing the packet delivery ratio.

Keywords*-sensor networks; Quality of Service; delay sensitive; multipath routing; trust computing*

*****

I. INTRODUCTION

Wireless sensor networks consist of large number of tiny wireless devices, low powered capable of sensing and monitoring environment. The applications of sensor networks include but not limited to military surveillance, health care, transportation and logistics and smart buildings. The work in this paper addresses the problem of routing real-time data such as video and imaging though maintaining the quality of service (QoS) of the application. QoS defines the overall performance measurement of a network that satisfies the objectives of a sensor network application.

On the other hand, with the specific properties of sensor network devices such as limited power, stringent computational capability, high network density, and scalability pose unique challenges in designing and managing sensor networks. These challenges demand energy aware QoS based design protocols [1]. Recently most of the researches discourses efficient utilization of sensor's energy and maximizing its lifetime. However, real-time sensor network applications may contain delay sensitive and delay tolerant data. For example, the data that caries the information about an indication of fire should be reported to the user within time limits. Any delay in routing the data may causes fail to take corrective actions and the damage will be heavy. Therefore, QoS routing is most important aspect of research community more recently.

In this paper, an enhanced version of EQSR protocol is presented that prioritizes real-time and non-real-time data and achieves node balancing through dispersion of traffic widely with the help of a trust based neighbors. Any excessive delay in forwarding the packets is avoided by not selecting the node that delivers the data not within the time limits. The major contribution of the paper is the offer of an enhanced version of EQSR, that support real-time and non-real-time applications while maintaining the energy consumption and delay lower than the other methods and also increasing the packet delivery ratio considerably.

The rest of the paper is organized as follows: In section 2 some of the related works are described. Section 3 briefly details the enhanced version of the EQSR. Performance evaluation and simulation scenario is presented in section 4 and section 5 concludes the paper.

II. RELATED WORK

Trust Computing has been widely used in recent years in sensor networks. The trust computing plays a vital role in assessing the reliability of a sensor node based on the past communication experiences.

Trust aware routing is wireless sensor networks arises due to motivation for tracking the problem from the highly resource constrained wireless devices. So a reputation based systems are used where the approach requires to continuously monitoring the environment to detect the malfunctioned needs. The authors [1] proposed a reputation based system for trust aware routing by implementing a monitoring procedure in a reputation System (EMPIRE). EMPIRE Approach tries to reduce the monitoring activity of a node without compromising the ability to detect attacks.

Scalable Cluster based hierarchical trust management protocol for wireless Sensor Networks was developed[2] to deal with Selfish or malicious nodes . Here the authors considered multidimensional trust attribute derived from communication and social networks to evaluate the trust of node. Here the authors considered multidimensional trust

 ISSN: 2454-4248
17– 21

attributes derived from communication and social networks to evaluate the trust of a node. H and Hierarchical trust management protocol is analyzed for heterogeneous sensor network with different social and Qos behaviors by applying to protocol to geographic based rating. The results indicate that the authors is able to achieve the ideal performance level by flooding based rating message delivery ratio and message delay without increasing the message overhead.

An active detection based security and security rating known as active trust[3], actively create a number of ratio and detects to obtain the trust values to overcome the black hole attack. Active trust can also be used to rate messages through non hotspot areas to achieve the desired energy efficiency. The active trust scheme effectively improves the success probability ratio against the black hole attacks.

To overcome the energy consumption of Trust and Energy aware routing protocol the authors [4] include a composite rating function that are trust residual energy and hop count in making rating decisions. Moreover TERP is built on a distributed trust model which helpful to overcome the single point of failure in isolating misbehaving and faulty nodes.

To defined against the adversaries misdirecting the multihop rating. Trust Aware Rating Framework (TARF) [5] defined against harmful attacks without using geographic information. The authors [5] also demonstrated that the application function well against ant detection mechanism.

By using clustering algorithm, Light weight and Dependable trust system(LDTS) [6] for sensor networks cancel the feedback mechanism between cluster members and cluster heads, to improve the energy efficiency LDTS also considered the communication between cluster heads to improve the efficiency and the detection of malicious nodes.

Intrusion –tolerant protocol for wireless sensor networks (INSENS) [7] aims to protect the sensor network against the intruder, who is capable of compromising sensor node with the intention of modifying or blocking the data packets. INSENS is adoptable to the characteristic of WSN and also remove the complexity from the sensor node to rescue rich bare station.

Energy efficient QoS assurance routing based on cluster hierarchy (EEQAR) [8] achieves energy efficiency with the quality of service requirement. EEQAR adopts cellular based topology and form a cluster structure. The energy consumption is balanced by structure movement within the cellular.

III. ENHANCED EQSR PROTOCOL

This section describes the enhanced version y EQSR, then the working of the enhanced EQSR, as well as the data allocation and transmission of data to the sink.

A. Route Discovery Phase

There are several methods to route discovery phase that enable to create a list of neighbors that is used to forward to the sink. This work focuses on using multipath that enables the forwarding of data packets which helps efficient utilization of available network resources.

The route discovery procedure is executed according to the following phases.

1) Initialization

Soon after the deployment of sensor node, the sink node broadcast a control packet that represent to initiation of the route discovery process. The control message structure is illustrated in fig 1. The source- node represent the node initiated the control manage. The Hop-count field is to number of hops requires to traverse the message to the source – node.

2) Neighbor Discovery

The control message initiated by the sink is flooded to the neighbors present within the transmission range. The neighboring nodes that receive the control message copy the value of those fields present in the control message to its neighbor- table. In the next step, the node replaces the source node field as its own node-id, increase the hop count by one and node- location is also updated accordingly.

Source-node	Hop-count	Node-location

Figure 1 Neighbor discovery routing data structure

After updating the control packet the node broadcast the packet to its neighbors. All the nodes present in the network receives this control message and eventually the neighbor-table is updated with the neighboring nodes details. The nodes are allowed to broadcast the control packet only once so that the looping of control message is prevented there by removing redundant information in the neighbor table.

3) Route refreshment

In order to preserve the energy of the sensor network and perform seamless task of the application periodically the nodes self-evaluate its residual energy, link quality. If the residual energy is minimal and the link quality is degraded over the period of time the node send a message to its neighbors, so that the node's entries will be removed by neighboring node's neighbor_ table. This prevents that the node from participating in data forwarding process.

B. NEXT HOP SELECTION

After the process of route discovery phase, to next phase involves the next hop selection process. The next hop selection is to select a set of nodes from the available neighbor table that is used to transfer the traffic from the source to destination. The problem here is to select a next hop from out of N available neighbors from the neighbor table. Now out of the available N nodes, the protocol picks out a separate set of node for real

 ISSN: 2454-4248
17– 21

time traffic as well as for non-real time or regular traffic. The techniques for creating separate neighbor list are as follows.

1) Trust model

Each sensor nodes maintain a value that is called as a trust value. The trust value is a measure of the level of trust on a particular neighbor for which a level of QOS can be achieved. The trust model and the evaluation is followed by the work done in [2]

Let Trust $i_{(j)}$ denote the level of trust that can be achieved by node i on a neighbor node j. The values of Trust $i_{(j)}$ ranges from 0 to 1. Which is directly proportional to the level of trust that the node i can rely on node j. Trust $i_{(j)}$ is calculated as the weighted average of two components as given in Equation 1.

$$\text{Trust } i_{(j)} = \alpha \text{ Trust}(self)_{(j)} + \beta \text{ Trust}(\text{ neighbor})_{(j)} \quad (1)$$

Trust (self)(j) represent the trust o node i on node j. Trust$(self)_{(j)}$ is obtained by either monitoring the traffic of node j or by receiving periodic reports of delay and QOS values received from node j. The entire work is assumed that to Trust$(self)_{(j)}$ is computed based on the periodic reports received from node j.

Let $r_1, r_2, \ldots\ldots r_n$ be the neighbors of node i and also the neighbors of node j. Then the Trust$(neighbor)_{(j)}$ is calculated as

$$\text{Trust}_i \text{ (neighbor)}_{(j)} = \frac{1}{n} \sum_{a=1}^{n} Trust\, r_{a\,(j)} \quad (2)$$

2) Trust estimation

In the previous section, the trust values of any node are evaluated based on the information present in the periodic reports broadcasted by the neighboring node. For simplicity and case of implementation purpose the periodic reports are broadcasted on a basis of regular interval. Each sensor node maintains a periodic timer and an expiry of an interval to node broadcast its report.

For each node the protocol maintains the following data structure a) Forwarded –in- delay and b) Forwarded- packets. The forwarded- in-delay represents the number of packets forwarded to the receiver or to sink node within the window of D_i. Here D_i is to acceptable amount of delay bearable to any packets. D_i is the user configurable value that can be used to achieve the delivery of packets within the tolerable delay. Forwarded – packets represents the total number of packets forwarded to the sink within a particular time interval. Now the trust is calculated as given in Equation 3.

$$\text{Trusti (j)} = \frac{forwarded-in-delay}{forwarded\,packets} \quad (3)$$

Thus Trusti$_{(j)}$ is the ratio of the number of packets forwarded within the given delay to the total number of forwarded packets.

3) Selection of neighbor list

Now the average of all the trust values of neighbors is calculated as in Equation 4.

$$\text{Trust\_ th (self)} = \frac{1}{n} \sum_{a=1}^{n} Trust \text{ (ra)} \quad (4)$$

All the neighbors with trust value greater than Trust_th(self) is separated as *real_traffic* other nodes are *non_real* traffic. While receiving any real time traffic packets the node select the next hop from the real traffic list and for non- real time traffic the node select the next hop from the non_real_traffic list.

4) Data transmission

After the selection of the neighbor list for the real-time traffic the next hop is selected from list realtim_traffic and for non-realtime traffic the next hop is selected from the non_realtime list. The received neighbornode repeat the process and eventually the packet will be received by the sink.

IV. IMPLIMENTATION

The performance is evaluated in terms of network related parameters. The simulation is carried out in OmNet++ based Castalia sensor network simulator. Castalia framework is a discrete event based simulation framework specific to sensor network.

The simulation environment consists of 300 sensor nodes deployed in a square field of 500 X 500 m. All the sensor nodes are capable of sensing an event within the radius 5m. The sink node is located in the left bottom corner of the sensor network. For every Δ seconds a timer triggers an event that initiates the sensor node to sense for any event. If any event is detected the node acts as a source node and initiates the data transmission process. Else the node enters into a sleep state for the next Δ seconds. The simulation experiment lasts for 1000s and Δ value is seta s 30 s. The simulation results are averaged over several simulation runs. The enhanced EQSR is implemented using multi-hop network topology.

V. PERFORMANCE EVALUATION

The average end-to-end delay, packet delivery ratio, average energy consumption and the impact of node-failure-probability are evaluated.

A. Average end-to-end delay

End-to-End delay is defined as the time taken for the packet to be transmitted from the source node to the destination. The

 ISSN: 2454-4248
17– 21

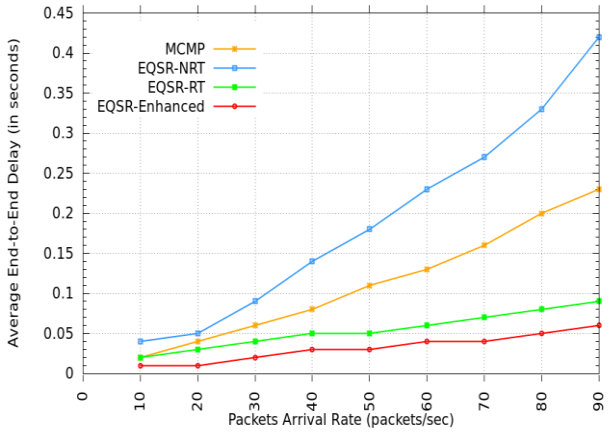

Figure 2 Average end-to-end delay

average delay of EQSR, EQSR-RT, EQSR-Enhanced are shown in Figure 2. The end-to-end delay is measured by varying the packets arrival rate at the source node. The enhanced version of EQSR in Figure represents the average of both real-time traffic and non-real-time traffic. From the results it is clearly shown that the enhanced EQSR out performs MCMP, EQSR-RT, EQSR-NRT and MCMP. It is also observed from the Figure that, as the packet arrival rate increases the average delay also increases due the overhead of queuing delay in forwarding the packets. At each sensor node the queuing delay is reduced at considerable amount of time in the enhanced version of EQSR and so it out performs all other compared techniques.

B. Packet delivery ratio

The packet delivery ratio measures the ratio of packets received by the destination to the packets transmitted by the source node. Figure 3 shows the average delivery ratio of all the techniques. As the packet arrival rate increases the packet delivery ratio drops noticeably for all the compared techniques. The average packet delivery ratio of the enhanced EQSR is high for the entire packets arrival rate thereby performing well than the compared techniques.

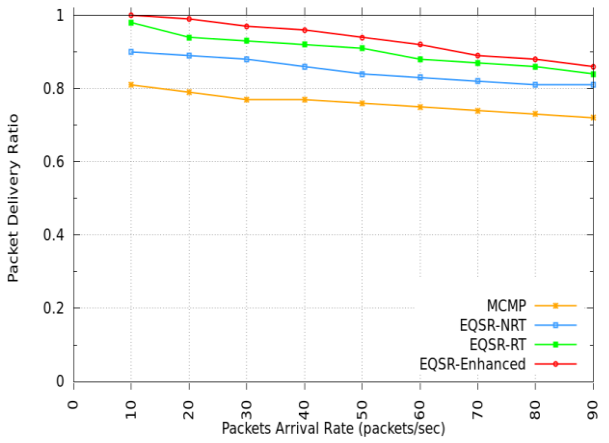

Figure 3 Packet Delivery Ratio

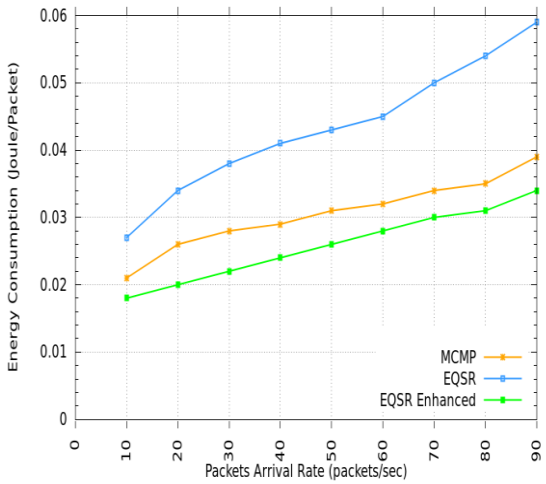

Figure 4 Average Energy Consumption

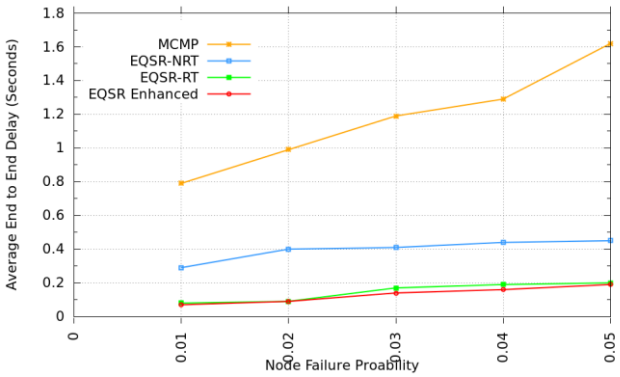

Figure 5 Average delay as node probability increases

C. Average energy consumption

Figure 4 shows the average energy consumption of MCMP, EQSR and EQSR-Enhanced. As the arrival rate of packet increases the average energy consumption also increases due to the transmission and the reception by the forwarding nodes. The energy consumption of EQSR is high when compared to MCMP due to the tradeoffs in meeting the quality of service requirement and also the computing overhead of EQSR. However, by reducing the computation overhead and changing the network conditions in forwarding packets the EQSR-enhanced reduces the average energy consumption when compared to EQSR and MCMP.

D. Impact of node failure probability

Node failure is an increasing risk factor for any kind of sensor network applications. In this work the behavior of the protocol is studied by simulating node failures. The probability of node failure is changed from 0 to 0.05. The packet arrival rate is fixed at constant rate at 50 packets per second. The average end-to-end delay and the packet delivery ratio are assessed in the presence of node failures. The result is shown in Figure 5.

E. Average delay

Figure indicates the node failure probability of MCMP, EQSR and EQSR-enhanced. The average delay for MCMP is

 ISSN: 2454-4248
17– 21

significantly higher for different node failure probabilities when compared to EQSR and EQSR enhanced. The enhanced EQSR reduces the average delay when compared to MCMP and EQSR. Also, the delay is not increased further when the node failure probability increases.

The average packet delivery ratio for all the techniques is illustrated in Figure . Visibly the enhanced EQSR delivers more packets when compared to EQSR and MCMP. The trust based routing offers a better connectivity between the forwarding nodes and hence in this work the enhanced EQSR is able to deliver more packets than the compared representative methods. The next section concludes the paper.

VI. CONCLUSION

Energy efficient and quality of service aware method that improves the network performance is presented in this paper. The technique is specifically tailored to sensor networks with preserving resources in mind. The enhanced EQSR technique in this work uses trust based computing technique that enables the forwarding nodes to select next hop efficiently in forwarding the packets to the destination, thereby improving quality of service parameters.

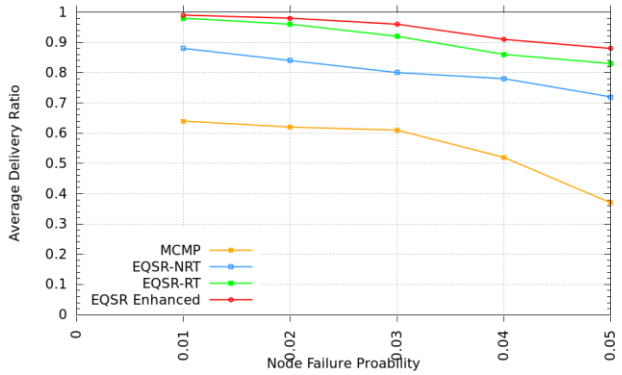

Figure 6 Avearge packet delivery ratio as node failure increases

Through simulation, the method is studied and the performance is compared with MCMP and EQSR techniques. The simulated results show that the enhanced EQSR lowers the packets delay and increases the packet delivery ratio with lesser energy consumption. As a future work, the performance of the work can be further intended to analyze based on machine learning techniques.

REFERENCES

[1] Maarouf, I. Baroudi, U. and Naseer, A.R.: 'Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks', IET Communications, 2009,vol. 3, no. 5, pp. 846-858.

[2] F. Bao, I. R. Chen, M. Chang and J. H. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," in IEEE Transactions on Network and Service Management, vol. 9, no. 2, pp. 169-183, June 2012.

[3] Y. Liu, M. Dong, K. Ota and A. Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2013-2027, Sept. 2016.

[4] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb and A. W. Khan, "TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network," in IEEE Sensors Journal, vol. 15, no. 12, pp. 6962-6972, Dec. 2015.

[5] G. Zhan, W. Shi and J. Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 184-197, March-April 2012.

[6] .X. Li, F. Zhou and J. Du, "LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 6, pp. 924-935, June 2013.

[7] Jing Deng, Richard Han, Shivakant Mishra, INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications, Vol. 29, pp. 216-230, Jan. 2006.

[8] K. Lin, J. J. P. C. Rodrigues, H. Ge, N. Xiong and X. Liang, "Energy Efficiency QoS Assurance Routing in Wireless Multimedia Sensor Networks," in IEEE Systems Journal, vol. 5, no. 4, pp. 495-505, Dec. 2011.

[9] .OMNET. (2017) INET Framework. [Online]. http://inet. omnetpp. org/

[10] Castalia: A simulator for WSN, [online] Available: http://castalia.npc.nicta.au.