Reliable Energy Efficient Routing in Wireless Ad Hoc Network by Considering the Residual Energy and Data Security

Ravitheja .S, Prof Chayapathi A.R
Department of Information Technology Engineering
Acharya institute of Technology, Soldevanahalli, Bangalore – 560107, Karnataka

Abstract—Here we have implemented a unique energy-aware routing algorithm for ad hoc networks in wireless medium, entitled reliable minimum energy cost routing (RMECR) and reliable minimum energy routing (RMER), also the data confidentiality is increased by adding security for the data transmitted. Here in RMECR, threesignificantnecessities of ad hoc networks are addressed: reliability, extending network lifetime and energy-efficiency [2]. The main idea in achieving these three important requirements is by considering the residual energy in battery, the links quality and the energy intake of the nodes; hence this results in the operative period of the nodes. Whereas on other hand RMER reduces the total energy obligatory for the end to end packet traversal is also another energy efficient routing algorithm. RMECR and RMER implemented here is for the network in which reliability is ensured for either end to end or the hop by hop retransmission. By the simulation output data we can analyze that both RMER and RMECR is able to find the reliable and the energy efficient routes thus increasing the network lifetime. But RMECR is a well-designed solution because in this we consider all the tiny specifics such as restricted number of retransmission, the energy consumed by processing elements of the transceivers, packet size and the packets impact of the acknowledgement for increasing the reliability, energy competence and lifetime of the wireless ad hoc network. Along with this well efficient working off the algorithm the security can again increase the durability and making it one of the best algorithms compared with all the existing.

Index terms*: Energy-aware routing, battery-aware routing, end-to-end and hop-by-hop retransmission, reliability, wireless ad hocnetworks,*

1. INTRODUCTION

The recent development in the MES (Micro electro Mechanic System), compoundcohesive and low energy overriding digital electronics has given way for the progress of the micro sized sensor [1][3]. These categories of micro electronic sensors require a battery source, communication facility, and datahandling capabilities. The toil of the sensing circuit is to measure the neighboring conditions relating to the necessary sensing procedure which it’s anticipated to perform and then transform it to the electric signal; in short it will perform as a transducer. These data will be cascaded and then the sensor will transmit it by its intrinsic radio transmitter to the head (for example, sink) or through the in-between nodes (gateway) directly. Due to the lessening in cost and magnitude of these sensors, this has become athought-provoking field of apprehension due to its prospective in sensing, data assembly, handling it, later it will be synchronized and accomplished to pave path to sink for those sensed data. Hence this potential of the field has smeared the wheel of research in past decade. Ad hoc manner can be shaped for this kind of cooperatedstandard architecture of the sensors in a network by the wireless link.In applications relating to civil and military such as security, surveillance and disaster organization the networking unattended sensor nodes will have a greater significance. Actually this application will have a system which gather or pile up form many sensors to monitor proceedings in particular area of concern as in case of military, the sensor nodes applications are plentiful. For example, the need of the workers on field in circumstances of dangerous mission is abridged, also the local use of distantlymanageable landmines and stipulating the target through sensor nodes and hence evading the damaging of civilians. And also in case of a catastrophe management operation, where nodes are released from aerial ships and then rescue processes are carried to place down the survivors as its not practicable for humans to get into risky areas identical to this sensor nodes emanate in as great benefit ensuring the wellbeing of the salvage crew.

In spite of numerous advantages, sensor nodes has defects too which comprises to the bandwidth of task and power source. Also the design of sensor nodes where more number of nodes are positioned and its administration is a notable constraint. So these encounters has made us understand the sensible usage of resources i.e., energy awareness of accessible resource in the sensor in networking protocol hoard. The research is focused on system level power awareness because the difficultyrelated to the physical and link layers are mutual for the applications of sensor network, so the emphasis is on dynamic voltage scaling, energy aware of MAC protocol[6][4][5], hardware for communiqué, on board space, matters of low duty cycle, system panel. After the emphasis is averted to increasing the lifetime of the network by discovering a way by locating reliable relaying of the data and energy efficient course to sink as of sensor nodes.

Outstanding to numerous characteristic sensor networks are reservedseparately from wireless ad hoc network in additionwith existing commutation. These compriselimitation which is actuallyneeded such as broadcast power, processing capability, storage and cautious management, broadcast power. The incapacity to design a global speakingarrangement for nodes hence for the sensor nodes standard IP based protocols cannot be applied. Next is in multiple sensor regarding the data traffic which has a significant redundancy which may generate same data within its vicinity, to increase the bandwidth and energy this redundancy must be exploited. Last in contrary to ideal communication network of almost all application the network taking sensor nodes where the sensed data from numerous regions flows to multiple regions to a specific link.

The difficulty of directing the data in the sensor network has been \revealed in many new algorithms due to these differences in the design of routing mechanism by considering the architecture and application requirements. In general the routing protocols can be generally classified into major types such as hierarchical, data- centric or position based and this can convoyed by QoS awareness or network flow establishing few changes, these grouping is centered on the core procedures of the protocol. Hierarchical protocols are those in which the nodes are gathered as clusters so that the head in the cluster will save energy by execution operations such aslessening and aggregation of data. Data centric protocols intention is reducing much redundant transmission through query and identifying of the demanding data. The previousgroup is protocols that are founded on QoSnecessities and network flow showing of the routing function. However these protocols for the wireless sensors require their sole advantages, and also matters which is under course of further exploration to increase the efficiency and the workingmotion to have improved routing protocols.

2. PRELIMINARIES

This section we present the overview about the implementation method of the routing protocol in section 2.1 and the energy parameters and the considerations made during the calculation of the minute details of the way how sender and the receiver nodes consume energy is shown in section 2.2. But the reliability is ensured only with the implementation of the retransmission method as illustrated in section 2.3 for both hop by hop and end to end system, later energy aware reliable routing and its needs also its importance is given. Finally in section 2.5 the mechanism of security used in the enhancement of security is briefed.

2.1 Network Model

In this implementation side we the topology of the wireless ad hoc networks in the graphical method as G(*W*,*E*), where *W* and *E* are the set of nodes(vertices) and links(edges), respectively. As elucidated earlier each nodes are consigned with distinctive integer identifier and these nodes are presumed to be battery powered. In order to say that battery is active then it must ensure to have a minimum threshold, but itsconsidered as zero for the simplification. The link *E* in the network is designated by *(a,b)* in which *u* and *v* are sending and receiving nodes respectively [2].

The criterion for having a link from *a*to *b*is that, only if the signal strength is above the threshold, therecould be a link form *u* to *v* and this threshold is designated in such a way that the directed link error probability is fulfilled. We represent the probability of error free reception of the packets of the length x [bit] communicated by *a* to *b* by$p_{a,b}(x)$ hence we can in short say $p_{a,b}(x)$ as packet delivery ratio (PDR) of *(a,b).*And also as a vital condition for energy-efficient routing, we adopt nodes have the provision of modifiable transmission power. The transmission power from node a to node *b* is denoted by$P_{a,b}$. $P_{a,b}$there is a fixed set of permissible transmission powers for node a,the total permissible transmission powers of node *a*. There is a discrete set in this permissible transmission and that is due to the applied contemplations that all the commercially accessible devices are preprogrammed with the conventional power settings. The considerations with respect to the power adjustment of the nodes are: (1) $P_{a,b}$ is the smallest transmission power as the permissible transmission count which satiates the targeted link error probability (2) the rate of the physical link will not change by adjusting the transmission power.

2.2 Energy consumption for the packet transmission over wireless links

As shown earlier the packet transmitted over the physical link be of size *x* bit and the energy consumed by transmitting node *u* to receiving node *v* of length *x* [bit] through physical link *(a,b)* be $\varepsilon_{a,b}$[J]. And correspondingly the energy used up by the receiving node *b* to receive from the sender node *a* and process the packet of length x [bit] be $\omega_{a,b}$ [J]. The energy spent by the nodes during the packet transmission might be abstracted into two distinct parts. Firstly the energy consumed by the power amplifier to produce the necessary output power for data transmission through the medium, here it is air. Likewise, the energy consumed by a node to accept a packet might be abstracted by merely one portion, this is the energy consumed by the receiving circuit comprising the low noise amplifier (LNA) of the receiver.Secondly the energy spent by the transmission circuit exclusive of the power amplifier of the transmitter. Let $A_a$be the power necessary to course the processing circuit of the transmitter of the node a, $P_{a,b}$be the transmission power to the node a from the node b. the power efficiency of the power amplifier node b, be $0 < k_a \leq 1$. The power needed to run the receiving circuit of the wireless crossing point be B_b at the node b, and the data rate of the physical link be r[bit/s]. The energy consumed by the transmitting node ai.e. $\varepsilon_{a,b}$ is calculated as

$$\varepsilon_{a,b}(x) = \left(A_u + \frac{P_{a,b}}{k_a}\right)\frac{x}{r}, \quad \forall x \geq 0, \forall(a,b) \in E$$

And for the receiving node the energy consumed $\omega_{u,v}$is calculated as,

$$\omega_{a,b} = \frac{B_b}{r}\,x, \quad \forall x \geq 0, \forall(a,b) \in E$$

The equation given above is taken from the reference paper [2] for the single transmission of packet. The impact of the packet retransmission will be measured well along.

2.3 Hop-by-Hop and End-to-End Retransmission Systems

In ad hoc networks the wireless links are usually susceptible to transmission inaccuracies. Hence to guarantee the reliability we integrate the use of the retransmission scheme, this can be either end to end or hop by hop retransmissions. An acknowledgement (ACK) packet is transmitted by the receiver side to the sender end every time the receiver obtains the packet, supposes if the ACK is not received by the sender then it declares that either the packet or the ACK packet is corrupt or lost.In case of end to end system, ACK are created merely at the destination side so the destination nodes send an end to end ACK packet to the source node when it obtains an ACK correctly. Suppose if the source node see to it that if the ACK is not received then the packet is retransmitted and the retransmission will happen only in amongst the end nodes.

Whereas in hop by hop system a packet that is lost in each hop is retransmitted by the sender to ensure link level consistency, if each link is reliable then the end to end path between the nodes will not be reliable. In either of the systems i.e. hop by hop and end to end, only after the expiry of the timer the retransmission happens. We take up that the timer is long enough to avoid redundant retransmission.

2.4 Energy-Aware Reliable Routing

The main motto of finding the reliable route is to minimize the cost of end to end packettraversal, also if the routes are less reliable then the possibility of packet retransmission increases. So the note making statement here is that reliability is associated to energy cost of the route. So if the retransmission occurs then the energy consumed will be increased per packet transmission. Hence we use two different ways of computing the routes energy cost, i.e. for both hop by hop and end to end systems which is Reliable minimum energy routing (RMER) and Reliable minimum energy cost routing (RECR). The minimum energy cost path is path between source and the destination where the expected energy cost of the end to end transmission is minimized in the multihop network between those two nodes. In RMER, for the end to end transmission of packet the energy cost will be the estimated amount of energy consumed by all the nodes to transfer packet. Whereas in RMECR the expected battery cost of the nodes along the path to transfer a packet from source to the destination node will be the energy cost of the path.

2.5 Securities for the Energy efficient reliable Routing

The algorithm used of providing security is very important and the one used in this is RSA for encryption of the data packet during transmission. It is based on the effort of factorizing big numbers which require 2 and only 2 factors (must be Prime numbers). The scheme works on a public and private key structure. The public key is made accessible to everybody. Through this key an operator can encode data but may not be able to decrypt it, the solitary individual who can decrypt it is the one who owns the private key. It is hypothetically probable but tremendously challenging to generate the private key as of the public key, this makes the RSA algorithm a very popular choice in data encryption. So we make use of this to improve the applications of the reliable energy routing scheme by providing security for the data packet.

3. ENERGY AWARE RELIABLE ROUTING IN HOP BY HOP SYSTEM

This section exhibits the details of the design of RMER in addition to the RMECR algorithms for those networks assistant to HBH retransmissions [base source]. Primarily, in Section 3.1, the energy cost of a path for transmitting a packet on the way to its destination is analyzed. Bearing in mind the influence of restricted retransmissions through every link, the dimension of data besides the ACK packets, then the reliability of E2E paths is the added value of our analysis this is been given well in the novel based approach by JavadVazifehdan, R. Venkatesha Prasad, and IgnasNiemegeers.

3.1Investigation of Energy Cost of a Path

The energy cost of a path is analyzed in four steps:
1. Examining the projected transmission count of data and ACK packets,
2. Investigating the anticipated energy cost of a link compelling to the energy cost of retransmissions,
3. Evaluating the E2E reliability of a path,
4. Conveying the energy cost of a path considering the energy cost of links and E2E reliability of the path.

3.2 Implementation

The large structures are usually disintegrated into small sub-systems which will deliver certain associated set of amenities. The primary design process of classifying these small sub-systems and then creating an outline for the small sub-system regulator and communication is understood as design style. The software system design is that the description of the output. The architectural design course is apprehensive in creating a simple fundamental structure for a system; this contains of recognizing the foremost vital modules of the system and also the interactions amongst these parts. This technique style is shown below in figure 1.

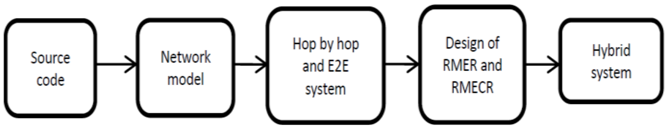

Figure 1. System design of energy efficient routing algorithm for wireless sensor network by considering the residual energy

3.3 Design of reliable minimum energy routing (RMER) and reliable minimum energy cost routing (RMECR)

In this section we present the design of RMER and RMECR algorithms for networks supporting HBH retransmissions. Before that for transferring a packet to its destination we analyze the energy cost of a path. Considering the impact of limited retransmissions across each link, the size of data and ACK packets, and the reliability of E2E paths is the added value of our analysis. Based on this in-depth analysis we design a generic routing algorithm for finding MECP between every two nodes of the network. By defining appropriate link weights, in RMER and RMECR algorithms are derived as two flavors of this generic routing algorithm. The source nodes are primarily initialized and the energy details are found where we consider the remaining power of the nodes and hence the best route is selected and the packet is transmitted to the destination.

3.4 Expected Transmission Count of Data and ACK Packets

Before proceeding to this lets make some considerations that is a node *a* is allowed to transmit a packet only limitednumber of times*N* (which includes the first transmission). A packet may be lost due to the probabilistic nature over wireless links; the same packet can be retransmitted by a random number of times and this must not greater than the (*N-1)* which is the required condition. Hence when the node *b*, a receiver node receives packet correctly, an acknowledgement ACK is sent to the transmitting node *a*. suppose if the transmitted ACK is lost, another ACK will be transmitted again for the same packet after *b*, the receiver node receives the packet correctly (may be after few attempts not crossing the maximum counts). Therefore, an ACK could be transmitted for the same data packet a random number of times not greater than *N*. It is also possible that no ACK is transmitted for a data packet, if the packet is lost in all*N* transmission attempts. In [2] itsassumed the expected number of times that sender node needs to transmit a packet to deliver it to *b* (including the first transmission), Total Energy Consumption across a link is explained well in [2]

Here $\varepsilon_{a,b}$ is the energy consumed by a during a single transmission of the packet, which is computed using
(1). Parameter $\omega_{a,b}$is the energy consumed by u during a single reception of the ACK, which is computed using
(2). the total energy consumed by the receiving node v is computed as

Here $\varepsilon_{a,b}$the energy is consumed by v during a single transmission of the ACK, and $\omega_{a,b}$ is the energy consumed by *b* during a single reception of the data packet.

3.6 Link and Path Reliability

Its defines in [2] the reliability of (*a*,*b*) for packets of size L_d bits. The reliability of a link is the probability that a packet is successfully delivered to the receiving node within the number of allowed transmissions. In the HBH system, link reliability is related to the PDR of the link as[2]. We must notice that the reliability of a link is not affected by the probability of losing the ACK. If the packet is received correctly but its ACK is lost, the packet will be retransmitted after expiration of a timer. If the retransmitted packet is received correctly too, there will be a duplicate packet at the receiver. Duplicate packets are usually discarded silently at the MAC layer, but ACKs are sent for them. This, however, affects the energy consumption of the transmitting and the receiving nodes.

3.7 Design of a Routing Algorithm for Finding MECP

Here, we design a generic routing algorithm for finding MECP between every two nodes in the network. Since energy cost is an additive metric, it may seem that the Dijkstra's shortest path routing algorithm could be used to find MECP in the HBH system. However, we show that the Dijkstra's shortest path routing algorithm is only a heuristic solution for finding MECP, but under some circumstances it could be the optimal solution.[7]

According to the Dijkstra's algorithm, the cost of a path from s to v is calculated in a recursive way as

$$\left(P(n_1, n_{h+1})\right) = C\left(P(s,a)\right) + W\ (a,b)$$

Where*a* precedes *b* in *P(s,b)* and *W(a,b)* is the weight of *(a,b)* .To find out whether the Dijkstra's shortest path routing algorithm could be used to find MECP in the HBH system.

3.8 Link weightage in RMECR and RMER Algorithm

To formulate the link weight in RMCER, let B_a be the remaining battery energy of*a* andC_b be the remaining battery energy of b. As introduced in Section 3.5, the energy consumed by *u* to deliver a packet to *b* is defined , and the energy consumed by *b* for receiving the packet is defineded too as in[2] Considering the definition of the battery cost of a link in RMECR, the link weight in this algorithm is$W(a,b)$ as in [2]. The link weight in RMECR captures the impact of the quality of the links, the energy consumption parameters of the nodes and the remaining battery energy of the node.The general approach used to define other variations of energy aware routing algorithms by defining other formulations for energy cost of the link is just the total amount of energy consumed by the transmitting and the receiving nodes to exchange the packet; we can devise an energy efficient routing algorithm. This if we define the energy cost associated to a link *(a,b)* as in [2]. Hence the result algorithm is named as the RMER, this is an energy efficient routing algorithm minimizing the total amount of energy consumed to route a packet to the destination node form the source node. The security for the data transmitted is the enhancement done in this algorithm, so the packet transmitted from the sender node will be encrypted and then sent so that only the authenticated user will have permission to access the data and not the intermediate nodes which will forward the packets.

4. HYBRID SYSTEM FOR THE PROPOSED ALGORITHM

Up to now we have comprehended the performance of the RMER algorithm when either hop-by-hop or end to end retransmissions is held. So both the RMER and RMECR has its own prominence and downsides so we need to make use of the protocol with respect to the situation . We can say that the E2E system has the drawback of increased energy cost in the network, since the PDR of routes drop exponentially with the number of hops. E2E systems, however it can ensure E2E reliability between a source and a destination. So we define a hybrid model where the source nodes will be guided by the hybrid model and then see the system performance by the selected protocol and path and to come to conclusion which is best , this is shown in figure (2).

On the other hand, a HBH system with limited number of retransmissions in each hop may fail to provide, E2E reliability, since packets might be lost in each hop. Here, we consider a situation in which both HBH and E2E retransmissions are supported (henceforth called the hybrid system). In the hybrid system, each link supports a limited number of HBH retransmissions while unlimited number of E2E retransmissions ensures complete reliability between the source and the destination. An immediate question that arises is, which of the RMER algorithms should be used to find energy-efficient routes for the hybrid system: 1) the RMER algorithm designed for the HBH system, or 2) the RMER algorithm designed for the E2E system based on heuristic solution, or 3) the RMER algorithm designed for the E2E system based on heuristic solution.

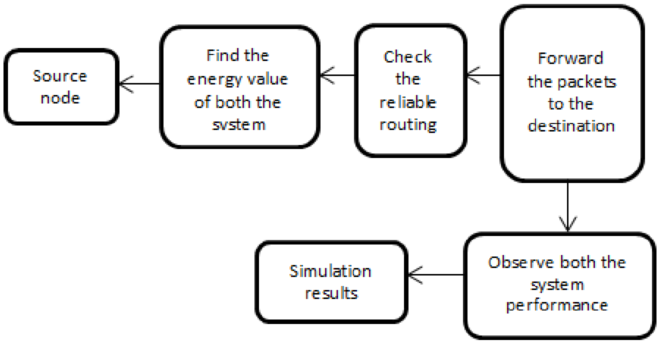
Source node
Find the energy value of both the system
Check the reliable routing
Forward the packets to the destination
Observe both the system performance
Simulation results

Figure 2. Hybrid system

The energy cost and reliability of routes discovered by variants of RMER algorithm for the hybrid system shows that RMER-HBH finds more energy-efficient and more reliable routes for the hybrid system. However, if links are of good quality (on the average), RMER-E2E algorithms perform similar to the RMER-HBH algorithm. This is carried out as shown in the figure 2.

5. PERFORMANCE

The Graph is plotted for the output values of the simulation results and it's given in this section.Also the comparison of protocol with the other routing algorithm is given here in this section. Figure3.

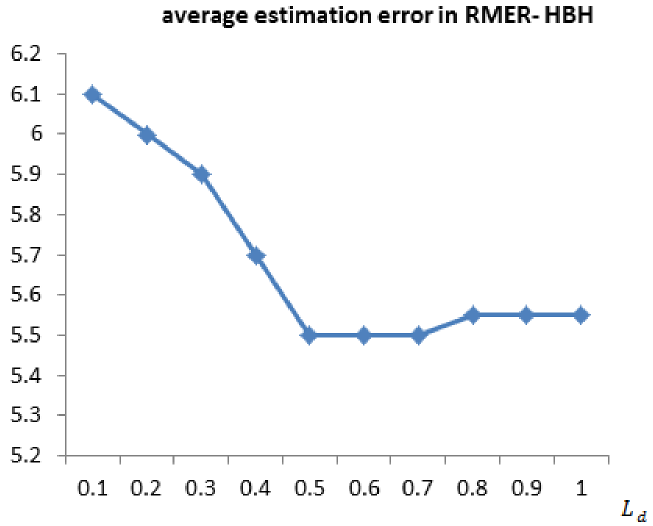

Figure 3

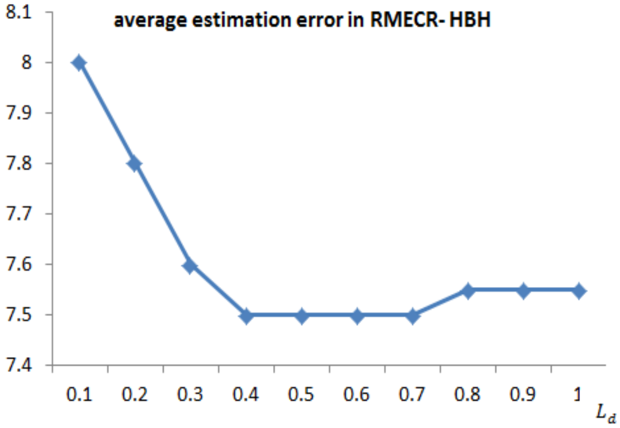

Figure 4

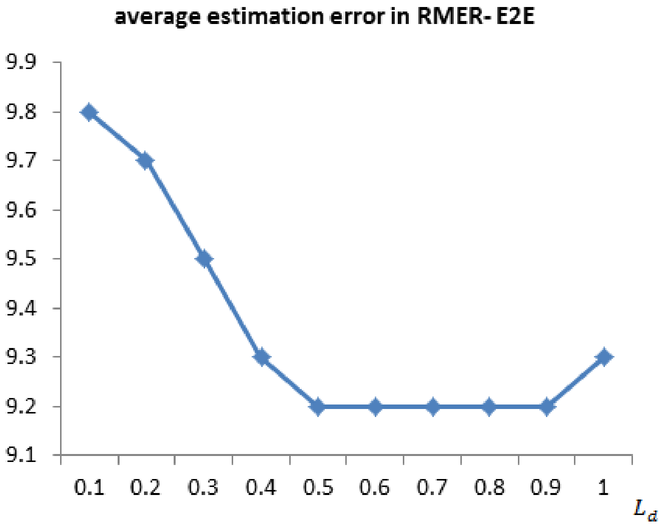

Figure 5

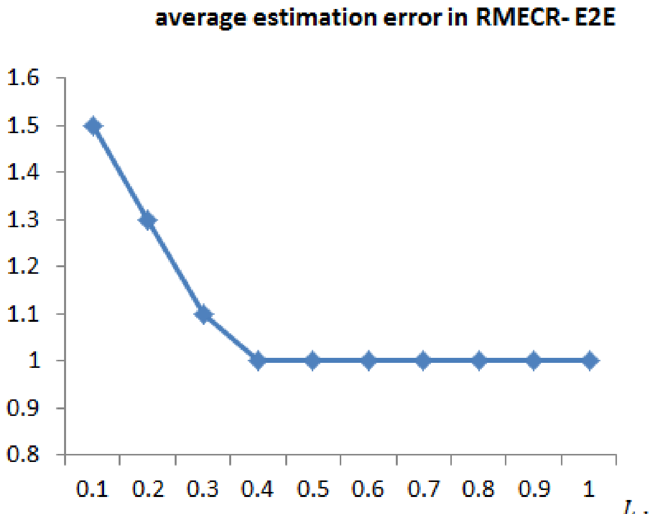

Figure 6

The average estimation error for the data packet transmission among the 36 nodes is plotted in order to know the transmission efficiency in the protocols, this is shown in figure 3,4, for RMECR HBH, RMER HBH respectively and 5,6 for RMER E2E , RMECR E2E respectively.Then the comparison of three protocols is done to know the goodness of the RMECR and RMER as plotted in 7 for mean reliability and 8 for network lifetime. We can derive at the solution that RMECR has always an upper hand over RMER by looking at the graphs plot of average estimation error. also the packet delivery ration along with the network lifetime is good in RMECR. The performance is tested for 36 nodes and the graph data is plotted.

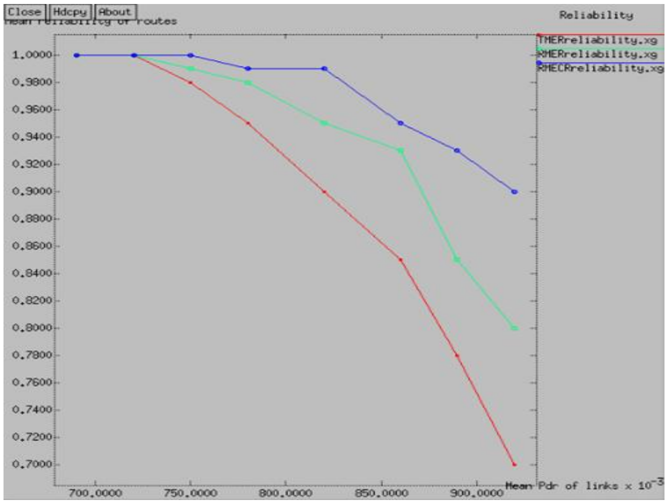

Figure7mean reliability of routes

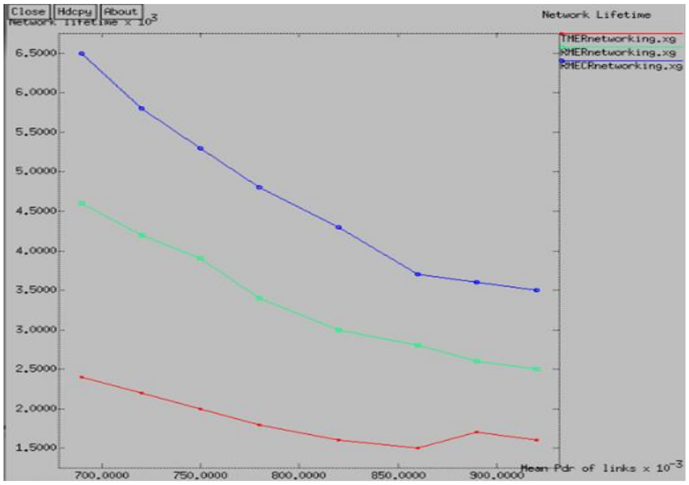

Figure 8network lifetime

6. CONCLUSION

RMECR will increase the operational time period of the network by means of energy-efficient and reliable routes. Within the style of RMECR, we have a tendency to use an in depth energy consumption model for packet transfer in wireless unplanned networks. RMECR was designed for 2 styles of networks: those during which hop-by-hop retransmissions guarantee responsibleness and people during which the actual end-to-end retransmission guranteeresponsibleness. The overall approach that we have a tendency to utilized in the planning of RMECR was accustomed additionally devise a progressiveenergy-efficient routing formula for wireless sensor networks. RMECR additionally extends the network time period by leading the traffic to nodes having the additional quantity of battery energy. Also along with the energy efficiency and the reliability we provide the security for the data packet for the high end applications.

7. FUTURE WORKS

The single packet size will actually estimate the quality of the links;these packets can be either ACK or else the data packet. The encryption provided will be for 256 byte of data. So the reliability can be made available even for bigger packet size and also the data packet transmitted can be increased (i.e. >256Bytes).

REFERENCES

[1]. D.S.J. De Couto, D. Aguayo, J. Bicket, and R. Morris, ―A HighThroughput Path Metric for Multi-Hop Wireless Routing,‖ Proc.ACMMobiCom, pp. 134-146, 2003.

[2]. Energy-Efficient Reliable Routing Considering Residual Energy in Wireless Ad Hoc Networks JavadVazifehdan, R. Venkatesha Prasad, and IgnasNiemegeers

[3]. S. Singh and C. Raghavendra, ―PAMAS—Power Aware MultiAccess Protocol with Signalling for Ad Hoc Networks,‖ ACM Computer Comm. Rev., vol. 28, pp. 5-26, 1999.

[4]. X. Li, H. Chen, Y. Shu, X. Chu, and Y.-W. Wu, ―Energy Efficient Routing with Unreliable Links in Wireless Networks,‖ Proc. IEEE Int‗l Conf. Mobile Adhoc and Sensor Systems (MASS '06), pp. 160-169, 2006.

[5]I. F. Akyildiz et al., ―Wireless sensor networks: a survey‖, Computer Networks, Vol. 38, pp. 393-422, March 2002.

[6] R. Min, et al., "Low Power Wireless Sensor Networks", in the Proceedings of Internation Conference on VLSI Design, Bangalore, India, January 2001.

[7] T.H. Cormen and C.S. Charles, E. Leiserson, and R.L. Rivets,Introduction to Algorithms, second ed. MIT Press, 2001.