Research Journal of Applied Sciences, Engineering and Technology 12(6): 650-657, 2016
DOI:10.19026/rjaset.12.2713
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: July 7, 2015 Accepted: November 4, 2015 Published: March 15, 2016

Research Article

Link Quality Based Error Correction Technique for Self-healing Wireless Sensor Networks

[1]B.R. Tapas Bapu and [2]L.C. Siddanna Gowd
[1]Research Scholar, ECE Department, S.A. Engineering College, St. Peters University, Chennai,
[2]Faculty of Electronics and Communication Engineering, AMS Engineering College, Namakkal, India

Abstract: In this study, we introduce a link quality based error correction technique for the self-healing WSN. Using the link adaptation algorithm the link quality is measured. And the relay nodes is selected by using the Link Quality Index (LQI) value, such that if the LQI value of a node is above the threshold value it will be chosen as a Relay node. These Relay nodes collect the data from the sensor nodes and apply Forward Error Correction (FEC) by partially decoding the incoming channel-coded data using lesser number of iterations. The FEC provides reliability with lesser transmission power. The quantity of FEC encoding is adaptively adjusted based on the measured link quality values. Multi-path routing is used in order to avoid data loss during the data transmission. With this, the data loss due to faulty path is avoided.

Keywords: Forward error correction, link adaptation, link quality index, multi-path routing, self-healing, wireless sensor networks

INTRODUCTION

Self-healing sensor network: Autonomic computing brings together different disciplines of computer science to promote self-managing systems that adapt to their operating environment and user needs. To this end, different systems exhibit different degrees of adaptation to dynamic environments without manual administration. Autonomic computing is defined by its properties like self-configuration, self-healing, self-protection and self-optimization, also referred as self-attributes (Bourdenas, 2011).

The system makes decisions on its own, using high-level policies; it will constantly check and optimize its status and automatically adapt itself to changing conditions. An autonomic computing framework is composed of Autonomic Components (AC) interacting with each other. An AC can be modeled in terms of two main control loops (local and global) with sensors (for self-monitoring), effectors (for self-adjustment), knowledge and planner/adapter for exploiting policies based on self- and environment awareness.

Advances in microchip and communication technologies have enabled mass production of small and cheap devices called sensor nodes that are capable of sensing the environment and interact with each other. These nodes interact over the radio channel to form Wireless Sensor Networks (WSNs). Each node can operate autonomously to monitor and collect data and send the data packet over the wireless network via multi-hop routing protocols.

Autonomic self-healing involves detection of faulty devices and reaction by means of masking or isolating the faults, where possible making use of redundancy. While faults in most distributed systems are not very common, they occur more regularly in WSNs so a holistic approach to self-healing that can compensate for faults at various levels is needed (Bourdenas and Sloman, 2009).

General issues:

Routing issue: In Self Healing Routing, nodes do not maintain knowledge of neighbors' states to make routing decisions. Instead, packets are freely broadcast to all neighbors and they autonomously decide whether to forward packets further toward a destination based on some cost metric. Broadcasting to all the neighbor nodes which increase the energy utilization and routing cost.

Hardware constraint: In self-healing sensor network the sensing, processing and computation are done in each sensor node. So the memory usage and the resource usage will be increased when the processing tasks are increased.

Overhead issue: In cluster based self-healing sensor network, the Cluster Head collects all the data from the sensor nodes, in this data gathering phase lot of route

Corresponding Author: B.R. Tapas Bapu, ECE Department, S.A. Engineering College, St. Peters University, Chennai, India

request packets will be collected because of the broadcasting nature of the self-healing sensor nodes. This will increase the congestion in the Cluster Head (Shantilal, 2013).

Security: Self-healing sensor network has two unique characteristics define with term secrecy. Secrecy divides in to two parts called forward secrecy and backward secrecy.

Forward secrecy: preventing nodes from decrypting any secret messages after they left the network.

Backward secrecy: preventing joining nodes from decrypting any previously transmitted secret message (Shantilal, 2013).

Security issues: The sensor nodes have some security issues such as, key management, privacy, authentication, secure routing and intrusion detection (Pietro *et al*., 2008).

The sensor nodes have some unsolved problems such as the shortcomings of connectivity and flexibility. Specifically, for example, there are remote sensors that cannot be connected to any other nodes in Wireless Sensor Networks and there are many useless pre-distribution key materials in nodes' memory. Also, many key materials may be disclosed after sensors being compromised by attackers.

As the wireless sensor nodes could be placed in a region where an adversary can capture them, it is likely that it could extract the secret key and therefore would be able to monitor all communication in the network (Shantilal, 2013).

Another one Problem is setting the pair-wise keys between the sensor nodes before deployment. If there were N wireless sensor nodes in the network then each wireless sensor node would have to store N keys in its persistent memory. In a resource, constrained device this would be a problem as storing the keys would use too much memory.

Problem identification and objectives: Kyasanur and Vaidya (2006), both node adaptation and link adaptation algorithms are vulnerable to security attacks such as denial of service attack and deny of sleep attack. In their proposed approach when the network density increases the energy consumption ratio also increases in linear fashion.

The authors in Lim *et al*. (2012) proposed an integrated immune-inspired Interference Detection and Recovery System (IDRS). This is to allow individual nodes to detect, diagnose and make decision as to how to response to network failure due to radio interference. However, in this study they didn't give any information about the faulty path error correction which is the major drawback.

Hence the main objective of the proposed work is to provide a suitable error correction method for self-healing WSN using the link quality information with reliable failure-free routing.

To overcome the above problems, we propose a link quality based error correction technique for self-healing WSN in which link quality of the nodes are evaluated. The link quality is measured by using the link adaptation algorithm (Diongue and Thiare, 2015). The LQI value of a node which is above the threshold value will be chosen as a Relay node. The Relay nodes are used to collect the data from the sensor nodes. The relay nodes will do the forward error correction and partially decode the incoming channel-coded data using lesser number of iterations. The Forward Error Correction (FEC) method can provide reliability with lesser transmission power. The quantity of FEC encoding is adaptively adjusted based on the measured link quality values. In order to avoid data loss during the data transmission multi-path routing strategy will be used. So the data loss due to faulty path will be avoided. Our proposed method includes both network decode and multi-path routing strategy. This will decrease the packet loss, end-to-end delay and improves the packet delivery ratio (Qaisar and Radha, 2007; Marinkovic and Popovici, 2009).

LITERATURE REVIEW

Diongue and Thiare (2015) have proposed an energy efficient self-healing mechanism for Wireless Sensor Networks. Their proposed solution is based on probabilistic sentinel scheme. To reduce energy consumption while maintaining good connectivity between sentinel nodes, they composed their solution on two main Concepts, node adaptation and link adaptation. The first algorithm uses node adaptation technique and permits to distributive schedule nodes activities and selects a minimum subset of active nodes (sentry) to monitor the interest region. And secondly, they introduced a link control algorithm to ensure better connectivity between sentinel nodes while avoiding outlier's appearance. Without increasing control messages overhead. In their proposed approach when the network density increases the energy consumption ratio also increases in linear fashion.

Song *et al*. (2012) have proposed a new method to improve the reliability of sensor network. Their research paper adopted a hardware to implement bionic reconfigurable of wireless sensor network nodes, so as to the nodes have able to change their structure and behavior autonomously and dynamically, in the cases of the part hardware are failure and the nodes can realize bionic self-healing. Secondly, Markov state diagram and probability analysis method are adopted to realize solution of functional model for reliability, establish the relationship between reliability and characteristic parameters for sink nodes, analyze sink nodes reliability model, so as to determine the reasonable parameters of the model and ensure reliability of sink nodes. In this study the authors didn't tell any think about the hardware failures of the Sink and the sink is a battery power constrain device. In this study the energy consumption for sink's processing energy and sleep energy consumption are not considered.

Babbitt *et al*. (2008) have presented a novel wireless sensor routing protocol, Self-Selecting Reliable Paths (SRP) for Wireless Sensor Network (WSN) routing, that addresses both challenges at once. That protocol evolved from the Self-Selecting Routing (SSR) protocol which is essentially memory-less. In the first generation of SSR protocol each packet selects the forwarding node at each hop on its path from the source to destination. The protocol has taken advantage of broadcast communication commonly used in WSNs as a communication primitive. That uses a prioritized transmission back-off delay to uniquely identify the neighbor of the forwarder that will forward the packet. As a result, the protocol is resistant to node or link failures as long as an alternative path exists from the current forwarder to the destination. The second generation of SSR protocols, called Self-Healing Routing (SHR) added the route repair procedure, invoked when no neighbor of the forwarder closer to the destination is alive. In a series of transmissions, a packet trapped at the current forwarder by failures of its neighbors is capable of backing off towards the source to find an alternative route, if such exists, to the destination. In the proposed method packet drop during fault path correction is not considered and the energy usage due to stable reliable path or excessive retransmission is a major drawbacks.

Lanthaler (2012) has proposed a failure detection scheme and a service management approach using the autonomic computing paradigm and some concepts of the IT Infrastructure Library (ITIL). The presented approach aims to employ self-healing services, allowing them to discover, examine, diagnose and react to malfunctions.

Lim *et al*. (2012) have proposed an immune-inspired self healing system where an individual node can detect degradations in network performance, perform diagnostic tests and provide automated immediate response to recover the network to a stable state.

Yuan *et al*. (2012) have developed a wireless sensor node with self-healing ability based on reconfigurable hardware. Two self-healing WSN node realization paradigms based on reconfigurable hardware are presented, including a redundancy-based self-healing paradigm and a whole FPAA/FPGA based self-healing paradigm. The nodes designed with the self-healing ability can dynamically change their node configurations to repair the nodes' hardware failures. Self-healing should consider both digital and analog circuits but in this study, only analog methods were discussed digital method is not explained and the speed of the self-healing process is not addressed here.

PROPOSED SOLUTION

Overview: In our study, we propose a link quality based error correction technique for the self-healing WSN. Initially the link quality is measured by using the link adaptation algorithm. Then the relay nodes is selected by using the LQI value, such that if the LQI value of a node is above the threshold value it will be chosen as a Relay node. These Relay nodes collect the data from the sensor nodes. They will do the forward error correction and partially decode the incoming channel-coded data using lesser number of iterations. The Forward Error Correction (FEC) method provides reliability with lesser transmission power. The quantity of FEC encoding is adaptively adjusted based on the measured link quality values. Multi-path routing is used in order to avoid data loss during the data transmission. With this, the data loss due to faulty path is avoided. The below Fig. 1 shows the block diagram of the link quality based error correction technique:

System model: We assume that sufficiently large number of sensor nodes is deployed in the network area with high redundancy and they are initially in sleep mode. Each sensor node had adequate autonomy to compute and control it's sleep and wake up phases (Diongue and Thiare, 2015). When they wake up, nodes will compete with their neighborhood to select a guard node which will be responsible for monitoring. If there is no guard node available in the neighborhood, it immediately assumes the role of a guard node and monitors the dedicated area.

Link quality measurement:
Estimation of Link Quality Index (LQI): Link quality is measured as the percent of packets that has attained undamaged on a link.

The network develops a link value metric which is known as Expected Transmission Time (ETT) that accounts for link quality. The ETT metric is also a factor of Packet Loss Rate (PLR) (Song *et al*., 2012):

$$E\text{TT} = (\text{ETX} * \frac{s}{b_{rate}}) \tag{1}$$

where,

ETX : Expected transmission count
s : The average packet size
b_{rate} : The data rate of the link

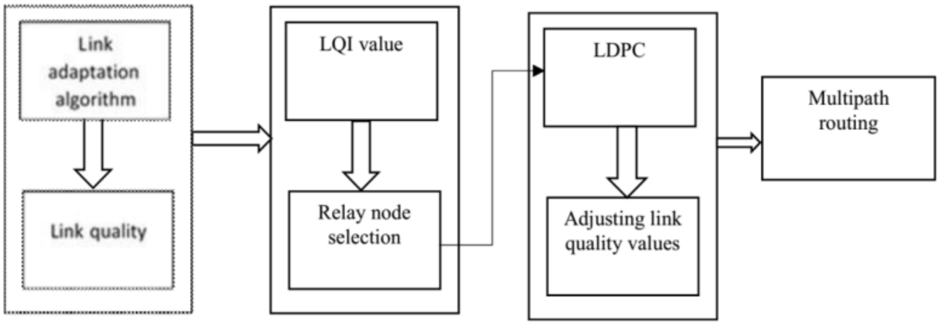

Fig. 1: Link quality based error correction technique

Here ETT is also a function of the PLR (packet loss rate). This packet loss rate considers both the PLR of forward link and PLR of reverse link. This packet loss rate is obtained by sending probe packets at the network layer

The ETX of a link depends on the forward packet loss rate from S to D on edge (e_f) and the reverse packet loss rate from D to S on edge (e_r):

$$PL = 1-[(1 - LR_f) * (1-LR_r)] \tag{2}$$

where,

PL : The packet loss,
LR_f : The forward packet loss on edge e_f
LR_r : The reverse packet loss on edge e_r

After the computation of the packet loss considering both the forward packet loss and reverse packet loss on the edge e, ETX is successfully given by:

$$ETX = \frac{1}{1 - PL} \tag{3}$$

So the Link Quality Index (LQI) of a link can be represented in terms of ETT as:

$$LQI = ETT+C(e) \tag{4}$$

where, C(e) is the cost of an edge e.

Link adaptation algorithm: The link adaptation algorithm (Diongue and Thiare, 2015) is applied in order to avoid the coverage holes appearance between guard nodes.

The guard nodes use the connectivity message to estimate the link quality between them. Each guard node randomly shot a timer and when it expires, it sends connectivity message to other guard nodes. When they receive the connectivity message, they send back (by unicast) a reply.

The guard node measures the link quality based on the obtained LQI (defined in Eq. (4). If the measured LQI value is below a given threshold, node will adjust its communication power strength in to maintain a good connectivity with other guard nodes. Otherwise, it ignores the message and prepares itself for another connectivity check round. Figure 2 shows the process of link adaptation and connectivity adjustment.

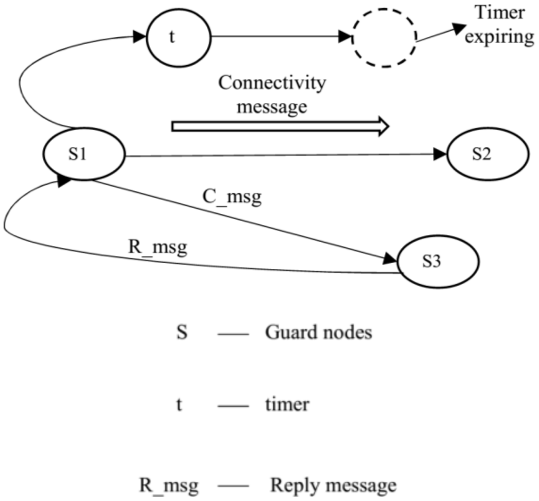

Fig. 2: Connectivity adjustment

Algorithm:

```
t_c ≠ 0, linkstate = {S,W}
status = Active, connectionMsg = Wrong
if (t_c expires) then  connectivity message is send if
(connection Msg = Received) then
    check the LQI value from the received message
    if (linkstate == Good) then
        set timer t_c
  else
      alter the link parameters
        set timer t_c
    end if
  end if
end if
```

Relay node selection: Using the LQI value, relay node are selected. The LQI value of the node, which is above the threshold value, is selected as relay nodes:

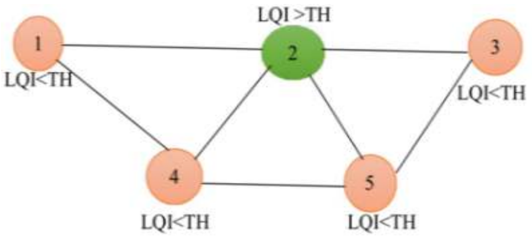

Fig. 3: Relay node selection

$LQI>LQI_{th}$

The Relay nodes collect the data from the sensor nodes. They will do the forward error correction and partially decode the incoming channel-coded data using lesser number of iterations. Figure 3 shows the process of relay node selection.

Error correction encoding: Using the relay nodes forward error correction and partial decoding of the incoming channel-coded data using lesser number of iterations is performed.

Channel error probability: Relay nodes were allowed to process the entire incoming information. In order to obtain the channel error probability, the signal to Interference Noise Ratio (SINR) is calculated at the node n_j for the transmission from node n_i and is given by:

$$SINR = \frac{\frac{P_t}{d(n_i, n_j)\alpha}}{P_A + \sum_{t \in T, t \neq i} \frac{P_t}{d(n_t, n_j)^{\alpha}}} \tag{5}$$

where,

$d(n_i, n_j)$: The distance between n_i and n_j
P_A : The ambient noise power
P_t : The transmit power of each node

Then the channel error probability ε is given by:

$$\varepsilon\,(n_i) = Q * (2 * SINR\,(n_i))^{½} \tag{6}$$

Decoding process: Low Density Parity Check (LDPC) codes are systematic block codes which have gained considerable attention due to their near capacity performance.

The source node n_0 generates k message bits which are encoded using a rate R code. The subsequent code word is transmitted over the first relay with the channel error probability ε_1. Node n_1 performs l_1 Low Density Parity Check Codes (LDPC) decoding iterations and is given by:

$$\varepsilon_1' = f(\varepsilon_1, l_1) \tag{7}$$

After the partial processing at the second relay the error rate is given by:

$$\varepsilon_2' = f(\varepsilon_2, l_2) * \varepsilon_1' \tag{8}$$

where, $\varepsilon_1 * \varepsilon_2 = \varepsilon_2(1-\varepsilon_1) + \varepsilon_1(1-\varepsilon_2)$.

The total number of decoding iterations $\Gamma(\bar{l})$ in the entire network is given by:

$$\Gamma(\bar{l}) = \sum_{j=1}^{N-1} l_j \tag{9}$$

where, l_j is the number of iterations at node n_j.

The relationship between the estimated bit error rate $\hat{f}$ for a given channel error probability and the number of decoding iterations is given by:

$$\hat{f}(\varepsilon_{ind}, l) = \alpha(\varepsilon_{ind})e^{\beta(\varepsilon_{ind})l} + \gamma(\varepsilon) \tag{10}$$

The quantity of FEC encoding is adaptively adjusted based on the measured link quality values

Multipath routing: Multi-path routing is the technique of using alternative paths over a network. Here we are using this in order to avoid data loss during the data transmission. With this, the data loss due to faulty path is avoided.

This multipath routing protocol is an on-demand reactive multipath routing protocol that makes use of path tables at the sensor nodes (Maimour, 2008). Each sensor is able to create, maintain and update a path table that records the different paths to the sink. It contains an entry for each path with the following fields:

- P is the path id, corresponds to the last crossed sensor in this path from the source to the sink.
- Nn, is the next hop towards the sink on this path,
- Qm, an estimation of the associated link quality metric for this path which is calculated based on LQI.
- F_{iu} is a flag when set which indicates that the corresponding path is currently in use.

The sink node Sn floods the network with a request (SREQ) until the source having the requested data is reached.

SREQ contains the following fields:

- A request sequence number that gives the rank of the currently built path for this session, (ReqS)
- A path id that corresponds to the first crossed sensor from the sink by this request, (Pid)
- The last crossed node id, (Lp)

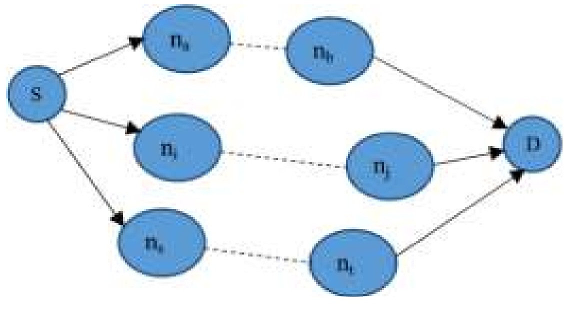

Fig. 4: Multipath route discovery

- Till this node path quality metric. (PQm)
- A flag called R_{path} is set when a path has to be repaired (the currently built path is to replace a broken one) (Kyasanur and Vaidya, 2006).

Algorithm for route discovery:

```
1.  Initially all nodes are in active state.
2.  Sink Sn floods the SREQ to towards the source.
3.  On receiving SREQ, the node Nj checks the path id
    Fp.
4.  If Fp is not in path table of Nj, then
        Creates a new path entry in its table
    Else
5.   If $Q_m$ of new $P_{id}$>$Q_m$ of previous $P_{id}$
        New $P_{id}$ of is stored in path table of Nj.
    Else
            $P_{id}$ of new node is ignored.
        End if
6.  End if
```

Three nodes, the current node, previous node and next node are active. Hence these three can establish the best paths for data transmission. An additional path is initiated by the sink which is based upon the application provided. This path is initiated when the first primary path is failed. The multipath route discovery is shown in Fig. 4.

Overall algorithm:

- Initially the link quality is measured using the link adaptation algorithm.
- The guard nodes measure the link quality value from the acquired LQI value.
- From the obtained LQI value, the relay nodes are selected for which the LQI is above a threshold.
- The relay nodes are used for the forward error correction and partial decoding for the incoming data.
- Lastly, multipath routing is made in order to avoid data loss.

SIMULATION RESULTS

Simulation model and parameters: We used the NS-2 Network Simulator (http://www.isi.edu/nsnam/ns) to simulate our proposed Link Quality Based Error Correction Technique (LQBECT) based routing protocol. We use the Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

Table 1: Performance metrics

No. of nodes	20,40,60,80 and 100.
Area size	500×500m
Mac	802.11
Routing protocol	LQBECT
Radio range	250m
Simulation time	50 sec
Traffic source	CBR
Packet size	512 bytes
Antenna	Omni antenna
Rate	100, 200, 300, 400 and 500Kb
Initial energy	12.1 Joules

During the simulation, the packet sending rate is varied from 100 to 500 Kb and the number of nodes is varied from 20 to 100.

Our simulation settings and parameters are summarized in Table 1.

The proposed LQBECT protocol is compared with OPERA (Qaisar and Radha, 2007). We evaluate mainly the performance according to the following metrics.

Average packet delivery ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Residual energy: It is the average energy remaining for the entire network.

Packet drop: It is the total number of packets dropped.

Based on rate: In the first experiment, we vary the packet sending rate as 100, 200, 300, 400 and 500 Kb for CBR traffic.

Figure 5 to 7 show the results of delay, delivery ratio, energy and throughput for the packet sending rate 100, 200, 300, 400 and 500 in LQBECT and OPERA protocols. When comparing the performance of the two protocols, we infer that LQBECT outperforms OPERA by 86% in terms of delivery ratio, 7.18% in terms of energy and 41% in terms of drop.

Based on nodes: In the second experiment, we vary the number of nods as 20, 40, 60, 80 and 100.

Figure 8 to 10 show the results of delay, delivery ratio, energy and throughput for the number of nodes 20, 40, 60, 80 and 100 in LQBECT and OPERA protocols. When comparing the performance of the two protocols, we infer that LQBECT outperforms OPERA by 75.4% in terms of delivery ratio, 14.2% in terms of energy and 59% in terms of drop.

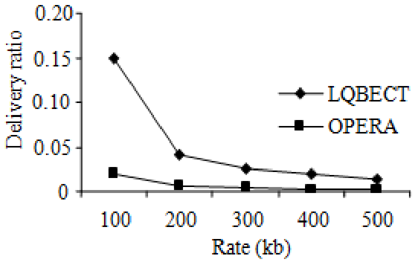

Fig. 5: Rate vs delivery ratio

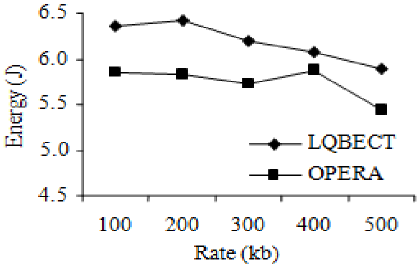

Fig. 6: Rate vs energy

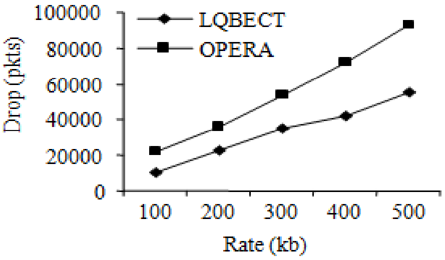

Fig.7: Rate vs drop

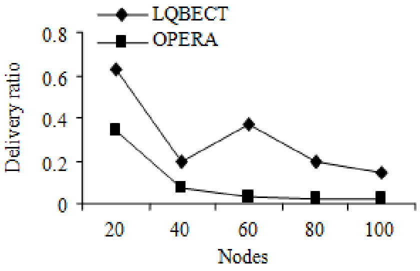

Fig. 8: Nodes vs delivery ratio

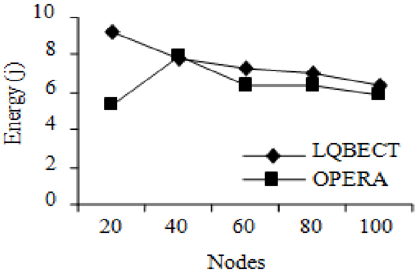

Fig. 9: Nodes vs residual energy

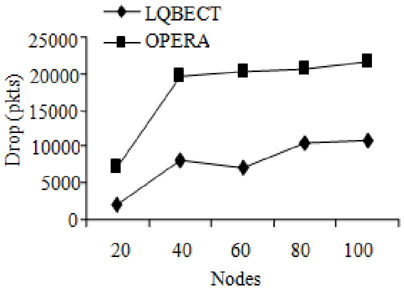

Fig. 10: Nodes vs packet drop

CONCLUSION

In our study we have used the link adaptation algorithm and the link quality is measured. The relay nodes are selected by using the LQI value, such that if the LQI value of a node is above the threshold value it will be chosen as a Relay node. These Relay nodes collect the data from the sensor nodes and fix the forward error correction by partially decoding the incoming channel-coded data using lesser number of iterations. The Forward Error Correction (FEC) method provides reliability with lesser transmission power. The quantity of FEC encoding is adaptively adjusted based on the measured link quality values. Multi-path routing is used in order to avoid data loss during the data transmission. With this, the data loss due to faulty path is avoided.

REFERENCES

Babbitt, T.A., C. Morrell and B.K. Szymanski and J.W. Branch, 2008. Self-selecting reliable paths for wireless sensor network routing. Comput. Commun. J., 31(16): 3799-3809.

Bourdenas, T., 2011. Self-healing in wireless sensor networks. Ph.D. Thesis, Imperial College London Faculty of Engineering Department of Computing, London.

Bourdenas, T. and M. Sloman, 2009. Towards self-healing in wireless sensor networks. Proceeding of the 6th International Workshop on Wearable and Implantable Body Sensor Networks, pp: 15-20, ISBN: 978-0-7695-3644-6.

Diongue, D. and O. Thiare, 2015. An Energy Efficient Self-healing Mechanism for Long Life Wireless Sensor Networks. In: Sobh, T. and K. Elleithy (Eds.), Innovations and Advances in Computing, Information, System, Sciences, Networking and Engineering, Lectures Notes in Electrical Engineering (LNEE), Springer International Publishing, Switzerland, 313: 599-605.

Kyasanur, P. and N.H. Vaidya, 2006. Routing and link-layer protocols for multi-channel multi-interface ad hoc wireless networks. ACM SIGMOBILE Mob. Comput. Commun. Rev., 10(1): 31-43.

Lanthaler, M., 2012. Self-healing Wireless Sensor Networks. Retrieved from: https://www.cs.helsinki.fi/u/niklande/opetus/SemK07/paper/lanthaler.pdf.

Lim, T.H., H.K. Lau, J. Timmis and I. Bate, 2012. Immune-inspired Self Healing in Wireless Sensor Networks. In: Coello, Coello, C.A. *et al*. (Eds.), ICARIS, 2012. Artificial Immune Systems. Springer-Verlag, Berlin, Heidelberg, 7597: 42-56.

Maimour, M., 2008. Maximally radio-disjoint multipath routing for wireless multimedia sensor networks. Proceeding of 4th ACM International Workshop on Wireless Multimedia Networking and Performance Modeling (WMuNeP'08), Vancouver, Canada.

Marinkovic, S. and E. Popovici, 2009. Network coding for efficient error recovery in wireless sensor networks for medical applications. Proceeding of the 1st International Conference on Emerging Network Intelligence, pp: 15-20.

Pietro, R.D., D. Ma, C. Soriente and G. Tsudik, 2008. POSH: Proactive co-operative self-healing in unattended wireless sensor networks. Proceeding of the IEEE Symposium on Reliable Distributed Systems (SRDS'08), pp: 185-194.

Qaisar, S.B. and H. Radha, 2007. OPERA: An optimal progressive error recovery algorithm for wireless sensor networks. Proceeding of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '07), pp: 344-352.

Shantilal, P.J.K., 2013. Self-healing sensor network key distribution scheme for secure communication. Res. J. Recent Sci., 2(ISC-2012): 158-161.

Song, Y., T. Chen, J. Ma, Y. Feng and X. Zhang, 2012. Design and analysis for reliability of wireless sensor network. J. Netw., 7(12).

Yuan, S., L. Qiu, S. Gao, Y. Tong and W. Yang, 2012. Providing self-healing ability for wireless sensor node by using reconfigurable hardware. Sensors, 12(11): 14570-14591.