www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-5, October 2018
Research Paper

Int. J. Sc. Res. in
Network Security
and Communication

E-ISSN:2321-3256

Combining Trust with Authentication Information for Routing in Wireless Sensor Networks

1*Annlin Jeba S.V., 2Gnana King D.R.

1Dept. of computer science & engineering, Sree buddha college of engineering, Pattoor Kerala, India
2Dept. of Electronics and Communication Engineering, Sahrdaya College of Engineering and Technology, Kodakara-680684,Thrissur, Kerala, India

Corresponding Author: sureshannlin@gmail.com

Received: 27/Aug/2018, Accepted: 16/Oct/2018, Published: 31/Oct/2018

Abstract-Demand for Wireless sensor network (WSN) applications increases due to the peculiar features owned by the sensor nodes in connecting real world with virtual world. Mission-critical services such as health monitoring and military insist for reporting sensed event information to the required authorities. But WSNs deployed in harsh environment suffer from unexpected changes in the link quality which severely affect the information in transit. To cope with these issues, it is essential to have efficient secure and reliable communication mechanisms. This study proposes a routing mechanism based on link quality, residual energy and authentication information owned by nodes involved in communication. Forwarding nodes are selected based on the stability of the link between consecutive nodes and remaining energy of the nodes along the path. In addition, the proposed scheme support to achieve security and privacy in communication with the help of link level authentication information shared between nodes. The Trust degree of the sensor node is computed based on the combined effort of the routing metrics. The performance is evaluated in terms of packet delivery ratio, delay and energy consumption. It was observed that proposed scheme perform well in high traffic, limited bandwidth and routing attacks performed through malicious nodes.

Keywords**:** residual energy, link quality, forwarding, authentication, trust, reliable.

I. INTRODUCTION

A wireless sensor is a smallest entity used in many applications such as military, civilian, health care etc. One of the primary objectives with respect to wireless sensor network applications is the design and development of secure and reliable routing protocol to perform efficient communication in WSNs [I][2]. The wireless medium used for communication and the unreliable wireless link that exist between sensor nodes lead to frequent topology changes [3].

The dynamic topology demands for frequent route determination between sensor nodes for establishing reliable communication. One of the important issues that limit the functionality of the WSNs is its lifetime. Sensor nodes are battery powered. Once the battery power gets depleted, sensor nodes die and thereby replacing batteries in such nodes is expensive. Therefore, power consumption plays a major role in the lifetime of the sensor nodes [4]. Hence it is necessary to have efficient routing protocol that is aware of the residual energy of the sensor nodes to increase network lifetime.

If a single routing metric is used for determining a route, then the same sensor nodes gets selected again and again to function as a relay node. This results in uneven distribution of traffic in WSNs. The unreliable and fluctuating link that exists between nodes may lead to packet drop [5]. In most of the WSN applications hop count is used as a metric for selecting the path towards the destination. Even if a path with minimum hop count is selected and if the selected path contains many weak links then there is chance for high packet loss rate[6][7]. This leads to packet retransmission wasting network energy and bandwidth. The poor network connection causes difficulty in differentiating honest node and an attacker. Hence, it is necessary to consider link quality or link connectivity as an important metric for route selection in resource constraint WSN[8]. Moreover, it is necessary to consider the related concepts security and reliability in achieving trustworthiness in data transmission for WSN [9] [10]. Most existing routing protocols [11][12] focus on energy efficiency of the node involved in communication. But it is necessary to consider security as an important factor or routing metric for path determination. Incorporating security as a means for selecting trusted nodes results in success of emergent sensing WSN applications

[13][14]. To specify security in routing, the proposed scheme determines the next hop based on security primitives such as authentication information.

Further, adversary can damage the packets during transmission from source to destination [15][16]. The goal of the adversary is to prevent the forwarding node from doing their expected function or to waste the resources of the forwarding node such as energy, bandwidth and memory [17][18]. In the proposed scheme residual energy and link quality are the two factors that combine to function as forwarding node selection metric towards the destination. The proposed scheme is able to achieve security by sharing authentication message between interacting nodes. Proposed routing mechanism can detect nodal trust without decreasing lifetime of the nodes and thus improve security.

A. Contributions of the proposed scheme:

The key contributions of the proposed scheme are as follows:

i) This study proposes a reliable and efficient routing scheme based on the combined effect of routing metrics energy and link quality along with link level authentication message.
ii) The mechanism followed determines the priority of the neighbour nodes to function as forwarding node.
iii) The proposed scheme maintains reliability and security of the selected path with minimum energy dissipation.

B. Notation

For the reason of clarity, the notations used throughout the study are listed in Table1.

Table: 1 Notations used in the proposed scheme

Notation	Description
TOM	Type of message
TS	Timestamp
RE	Residual Energy
LQ	Link Quality
E_{max}	Initial Energy assigned to a node
E_c	Energy Consumed by a node
E	Rate of energy consumed
W_{RE}	Weightage given for residual energy
W_{LQ}	Weightage given for link quality
$LQ_{(i,j)}$	Link quality of a node j linked with parent node i

The rest of the paper is organized as follows. Some literatures related to the proposed scheme are discussed in Section II. Section III presents the detailed description of the proposed scheme, followed by analysis and discussion in section IV Analysis through simulation in section V. The proposed mechanism is concluded in section VI.

II. RELATED WORKS

Timing Chen et.al [5] proposed a path selection based on the link quality of the intermediate nodes involved in data forwarding. In this scheme link quality is determined by a dynamic windowing concept. The window contains k bits represents the historical details about the successful and unsuccessful packet transmission within a period of time. Historical details maintained determine the link quality of a particular node. This scheme initially determines the path with minimum hops for routing then applies the link quality determination technique to select suitable links for data forwarding. The lack of energy-efficiency mechanism results in reduced lifetime of the network [19][20].

Guoxing Zhan [6] proposed a scheme to select trustable nodes for forwarding the data to reduce the impact of adversaries misdirecting the packet by modifying the packet header or modifying the content of the data. For selecting the trustable nodes this scheme considers energy efficiency and trustworthy. The performance of TARF is evaluated and determined that TARF achieves Energy efficiency and High throughput. Further TARF is scalable and adaptable for any environment.

H.C.Leligou et.al [2] proposed a scheme for routing based on trust attributes and location information. Author's derived four different types of rules to determine the trustworthiness of the nodes involved in routing thereby identify the malicious node on the path of data transfer. The performance evaluation shows that proposed scheme can provide good results when the percentage of malicious nodes is high. Even though the trust rules specify better results they cannot guarantee good security during operation.

Xufei Mao et.al [7] proposed a scheme to select efficient forwarding list of node for forwarding the data. Author's objective of using the proposed scheme is to minimize the energy required for transmission and to increase the lifetime of the forwarding node along the selected path. The author identified the neighbour of a node through which data has to be transferred. Author determined the expected cost for forwarding packet through each and every neighbour. Determine an optimal forwarding list by arranging the node in increasing order based on the expected cost. The node with minimum cost gets selected. Author evaluated the performance of the proposed scheme by determining the throughput delay rate and packet delivery ratio. They observed that the proposed scheme achieved reliable and routing with low delay. The main drawback of this scheme is it does not include a mechanism to estimate the link quality level. This focuses only on the network lifetime and does not consider reliable data delivery.

A * algorithm is proposed [8] to find an optimal low cost path from the source to the BS. The next hop on the path is determined by an evaluation function. This process starts at the source node and navigates towards the destination node. After determining the evaluation function of all adjacent nodes the algorithm will find a solution if a node with relevant value exist. If not then assure that no such solution exist. This approach cannot be used to determine an optimal path at any circumstances and for all application such as rocky terrain. The memory required for storing the OPEN and CLOSE list is high and the process is time consuming.

S.Young, Moon et.al [10] proposed a false data filtering scheme which uses a deterministic approach to select efficient filtering node on the path of data transfer. This scheme addresses the issues faced by most of the filtering schemes which use a probabilistic approach for selecting en-route filtering node. Due to probabilistic approach it is difficult to predict exactly the deficiency such as false traffic ratio and residual energy of the selected filtering nodes. Fuzzy logic is used in selection of filtering nodes with the input parameters as residual energy of the nodes, false traffic ratio and size of message authentication code for verifying the authenticity. The mechanism used is not scalable and is not applicable in all circumstances. There are also many works related to hop-by-hop secure communication [21]

Xiaohan Lai et.al [22] introduces an energy efficient link-delay aware routing scheme known as Predicted Remaining Deliveries (PRD) for WSNs. This routing metric is used for application where environment changes drastically. Here the routing metric is designed in such a way that next hop is selected based on link quality, shortest end-to-end delay and highest residual energy. In metric calculation phase sensor nodes calculate routing metric for each neighbour. In score calculation phase each sensor node calculates route score for its neighbours and determines the best score. The computations performed to determine the route score is complex. This affects the performance of the scheme.

D.S. De Couto et.al [23] proposed a high throughput path metric which evaluates the link quality along the communication path. The proposed scheme known as ETX(Expected Transmission count) focus on the interference among the links along the path. This method does not consider the energy of the nodes along the communication path which affects the network lifetime as the routing nodes energy drain rapidly.

III. PROPOSED SCHEME

Reliability, security and performance are the important constraints to be considered for developing an efficient routing protocol for WSN. Their precedence level varies according to the environment where it is applied and the purpose for which it is used. For applications such as military and health it is essential to consider reliability as well as security. The proposed multi-hop routing protocol uses multiple routing metrics to be combined to determine an efficient forwarding node. The routing metrics include residual energy, link quality and authentication message. The specific metrics are selected with the aim of increasing the lifetime of the network and to achieve reliable communication within the network. The operation of the routing process consists of four phases. Set-up phase, metric calculation, Next hop selection and En-route authentication phase.

DESCRIPTION

A. Set-up phase

Sensor nodes are deployed in the application specific environment. During deployment they are assigned with the same energy level and with unique ID. Each node maintains a routing table which contains information about its neighboring nodes. Each sensor node periodically broadcast 'Hello' messages announcing its existence through identity and location information. This allows the neighbour nodes to be aware of the broadcasting sensor node. The one-hop neighboring nodes receiving the 'Hello' message send acknowledge message mentioning their existence. Periodically every node updates their neighbor information in their routing table.

When a source node has data packet to send to the sink, it needs to determine a suitable one hop neighbour for forwarding the data packet. Initially source node broadcast a route advertisement message.

Node ID	TOM	TS	RE	LQ

Fig.1 Route advertisement message

The advertisement message includes the following fields as shown in Fig. 1.Node ID represents the unique ID of the node which initiates the communication by announcing route advertisement. Type of Message (TOM) specifies the category of the message that is being communicated. Time Stamp (TS) specifies the validity of the packet whether the message is outdated or not. The Residual Energy (RE) and Link Quality (LQ) fields specify the remaining energy of the receiving neighbour node and quality of the link maintained by the neighboring node with the parent source node. RE and LQ field values are updated by receiving node and initially it is specified as one. The nodes receiving the advertisement message send reply message. The format of the reply packet is same as that of the advertisement packet. All the fields have to be updated by the receiving node.

B. Metric Calculation:

Once a source node has data packet to be send to the sink, source node needs to decide to which neighboring node it should forward the data packet considering the trustworthiness of the node. When a one hop neighbour node receives an advertisement message, it needs to determine the routing metrics. The routing metrics includes the residual energy value and the link quality value. Residual energy is the remaining energy of a sensor node and link quality is determined by knowing the history about the packet delivery performed through the particular link as specified in the procedure.

Residual Energy:

Each sensor node consumes energy during data sensing, processing and communication. The sensing and processing parts consume low energy compared to the communication part. The initial energy assigned to a node is represented as E_{max} . The energy consumed by the nodes is represented as E_c. The rate of energy consumed can be calculated as

$$E = \frac{E_c}{E_{max}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Remaining Energy can be computed as

$$RE = \frac{E_{max} - E_c}{E_{max}} \quad \ldots\ldots\ldots\ldots. \quad (2)$$

If the Residual Energy value is less than 20% of E_{max} then the particular node is identified as weak node and it is unable function as forwarding node.

Link Quality:

In the proposed routing mechanism the routing metric, link quality of a node is determined based on the successful packet reception ratio for a specific period of time. Neighbour nodes determine their link quality using the historical data maintained about the recently received 'N' packets within time period 't_s" Success rate is derived from the packet sequence number of the received packets of the link with that source node. If there is no gap in the sequence number of the packets received, then it is represented that the packets have been successfully received. If there is gap in the sequence number of the packets received, then it is determined that some of the packets have been lost or dropped. The following describes the procedure executed at the receiver side for determining the LQ (link quality). The procedure executed for determining the LQ is given by

Procedure for finding link quality

```
1:  Set time: = $T_o$                // Initial time
2:  Source___> * : Hello        //Source broadcast
3:  RECV (HELLO)            // neighbor receiving packet
4:  If (Loss of packet =0)    // difference in sequence No.
5:  pos_count++;
6:  Else
7:   neg_count ++;
8:   Repeat steps 3 to 7
9:   If time reaches $T_s$ then compute LQ  //Specified time
     interval
10:    LQ = (pos_count) / (neg_count + pos_count)
11:    SEND(LQ)        // receiver send computed LQ value
```

The variable neg_count represents the count of unsuccessful transmitted packet. pos_count represent the count of successfully transmitted packet. The link quality (LQ) decides whether a link is currently reliable or unreliable for transmission and informs the requesting node.

C. Next hop selection:

After determining the Residual Energy (RE) and Link Quality (LQ) values, the one hop neighboring nodes update the fields in the reply packet including node ID, TOM, RE, LQ and TS. Reply packet is send to the requesting node. When the source node receives the reply message, it determines the efficiency of the node by computing the weight of the combined metrics. .... (1)

$$Weight = W_{RE}{*}\ RE + W_{LQ}{*}\ LQ_{(i,\,j)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

Where

Weight - weight for the next hop combining residual energy and link quality

W_{RE} – weight given for residual energy (40%)

W_{LQ} - weight given for link quality (60%)

$LQ_{(i,\,j)}$ – quality of the link connecting $node_i$ with $node_j$

Maximum value for RE and LQ is 1

It is determined that value for weight of a node lies between 0 and 1

$$0 < weight < 1$$

The source node calculates the weight for all its one hop neighbours which sends reply message. Selects the node with maximum weight value to function as the forwarding node. Table 2. specifies the possible range of values considered as weight for different categories of reliability.

Table 2. Node weight value in range

SL.No	Weight	Reliability
1	0.7 to 1	high
2	0.5 to 0.7	medium
3	0.2 to 0.5	low
4	< 0.2	Not reliable

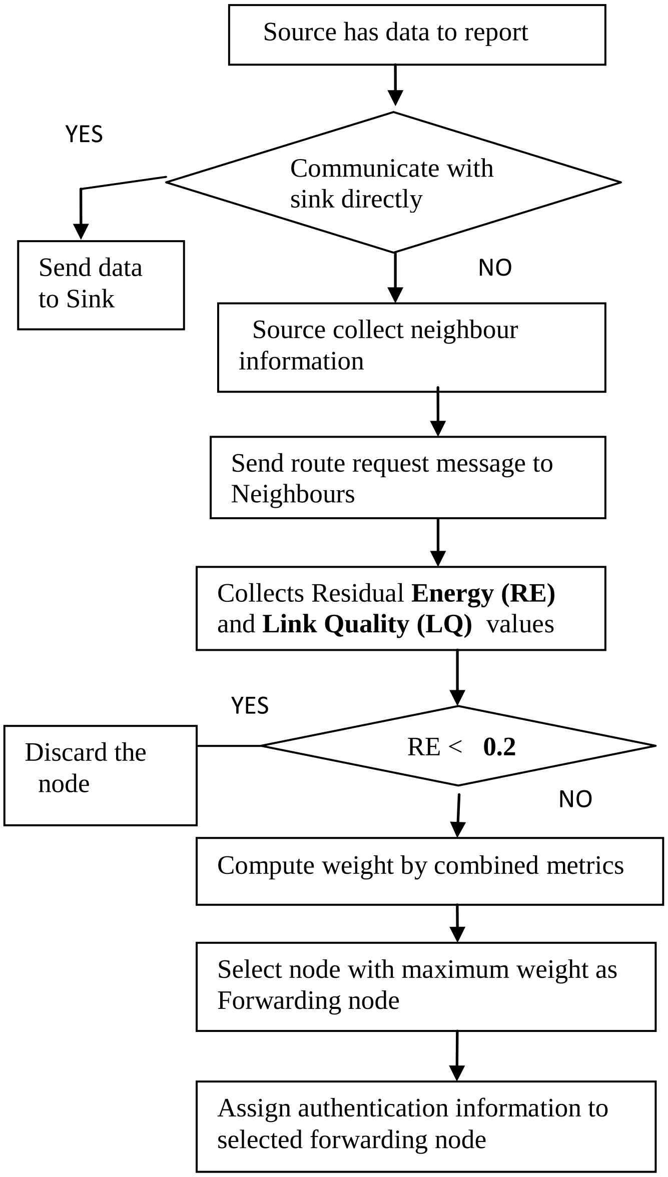
Source has data to report
YES
Communicate with sink directly
Send data to Sink
NO
Source collect neighbour information
Send route request message to Neighbours
Collects Residual Energy (RE) and Link Quality (LQ) values
YES
Discard the node
RE < 0.2
NO
Compute weight by combined metrics
Select node with maximum weight as Forwarding node
Assign authentication information to selected forwarding node

Fig. 2. Flowchart for the proposed scheme

D. En-route Authentication:

Once a source node determines its one hop forwarding node, it sends the route join request message. The selected neighbor node can collect the security related trust information from its parent node through this request message. The message includes the node identity, type of message, time stamp value and a token. Token specifies the link level authentication information to be shared between the nodes (neighbour node and parent node). This authentication message strengthens the security of the interaction between the nodes involved. Moreover, for every communication the authentication message is refreshed and different nodes (node pair) will be using different authentication message. This prevents the involvement of compromised or malicious nodes in the routing process. Each node is evaluated regarding its willingness and sincerity in the routing procedure. The format for this message is described in fig. 3:

ID	TOM	TS	TOKEN

Fig 3. Route join request message

ID- node identity
TOM- Type of message
TS- Time Stamp
TOKEN-H(ID||TS) - authentication message

The selected forwarding node verifies the validity of the message through the time stamp value and authenticity of the message through the TOKEN. If found valid then determine its next hop based on the steps followed in the next hop selection phase. The same process repeats until the next hop is the sink. Thus by the proposed routing mechanism reliable and trusted path is determined on demand. The security primitives included can improve the trust worthiness and reliability of the forwarding nodes. Thus the proposed routing scheme described through fig.2.can improves the success routing probability compared with that of related routing schemes.

IV. DISCUSSION ABOUT PERFORMANCE OF PROPOSED SCHEME

In domain specific regions sensor nodes are randomly deployed and multiple paths exist between a source destination pair of a WSN. In order to achieve efficient communication, it is necessary to select an optimal path for data transmission. In the proposed scheme in order to achieve maximum throughput with increased network lifetime, forwarding nodes are selected based on their residual energy and link quality value. The nodes with maximum residual energy and high link quality are assigned highest priority. Further, the proposed scheme is able to handle the traffic efficiently since in the proposed scheme one of the metric considered for assigning priority for intermediate node is link quality which prevents radio interference that occurs in unreliable wireless link. In WSNs, the emerging significance of the network can be affected by their security problems. In order to solve the security problems it is essential to have security primitives which improve the robustness and reliability of the network. This can be achieved through the proposed scheme. Besides providing trust management service through routing metrics, residual energy and link quality the security services are included through authentication information shared during route determination process.

Link quality is measured as the percentage of packets that arrive undamaged on a link. Further, during data transmission in WSNs a packet can reach the destination through multiple paths. If the packet is sent through a randomly selected path the selfish nodes present in the path may attack the packet in different ways and deny the packet from reaching the BS. Also the unbalanced energy consumption in WSN can cause some nodes on the selected path to get exhausted quickly. This may reduce the lifetime of the network. These types of dangers are not allowed in the proposed method of routing since only authenticated nodes and nodes with maximum residual energy are allowed to forward the packet in transit. Moreover, the overhead occurred to establish a path using proposed scheme is low compared to related schemes. The proposed system is lightweight to provide good performance without affecting the functionality of the system.

V. SIMULATION RESULTS AND ANALYSIS

The performance of the proposed scheme is studied using NS2, a network simulator popularly used in the evaluation of network performance. For performance evaluation the proposed RLS is compared with PDR and ETX. The metrics used for performance evaluation are: Packet delivery ratio, End-to-End delay, probability of success routing, energy consumption, node lifetime.

- **Node lifetime:** Node Lifetime for a node at time‘t’ is defined as the ratio of residual energy of the node at time ‘t’ to the initial energy assigned to that node.
- **Packet Delivery Ratio:** Packet Delivery Ratio is defined as the ratio between the number of packets successfully delivered to a destination and the number of packets sent by source node.
- **End-to-End delay:** End-to-End delay is the total delay caused in packet delivery. This determines the time taken to deliver one packet to the destination. This delay includes processing delay, queuing delay, transmission delay and propagation delay.
- **Energy consumption:** The average energy consumed to forward one packet data successfully to the base station.
- **Probability of success routing :** The probability of success routing is defined as the probability of successfully delivering the packet to the destination in the presence of malicious nodes

Simulation Evaluation

The performance of the proposed routing metric is demonstrated by comparing with related routing schemes such as PDR [22] and with ETX [23].The performance of the proposed scheme is analyzed by several performance metrics. The performance metric includes i) Packet delivery Ratio ii) end-to-end delay iii) Energy consumed for a single transmission iv) Node lifetime v) Probability of success routing

In this section, a detailed simulation study that examined the performance of the proposed algorithm is reported. The evaluation is done based on several metrics such as routing energy, throughput and delay occurred during data transfer.

A. Simulation setting:

Table 3. Parameter setting for simulation

Parameter	Value
Number of nodes	500
Area of deployment	1000*1000m^2
Transmission range	50m
Simulation time	300seconds
Initial energy of node	1 joule
Energy consumption for sending a packet	16.5µJ
Energy consumption for receiving a packet	12.5 µJ

The work is implemented using NS2, the network simulator to evaluate the performance of the proposed scheme in large scale wireless sensor network. The experimental network topology was formed with 500 nodes randomly deployed into 1000xl000 m^2. All sensor nodes are assigned to have same hardware and transmission power. The initial energy assigned for each sensor node is 1Joule .The communication radius of each node is uniform throughout. A unique id is assigned to each node. The parameters used in simulation are summarized in table 3.

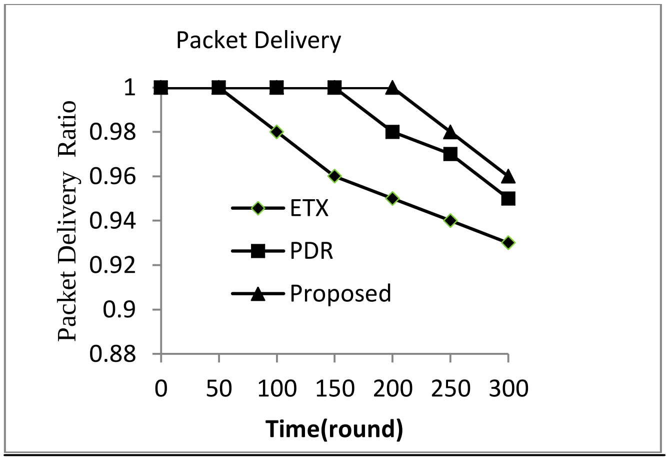

Fig. 4. Packet delivery ratio with varying time

Figure 4 illustrates the packet delivery ratio during the network lifetime. In all these schemes the packet delivery ratio is found to be high at the beginning of simulation. After time goes on, the packet delivery ratio decreases in ETX and PDR as represented in the figure. This decrease in packet delivery ratio is due to the poor link quality that occurs in the selected path. In these schemes when some of the forwarding nodes die, other existing nodes have poor link quality. Moreover, there is no link level authentication mechanisms. Presence of malicious or compromised node along the path causes packet dropping, route misdirection and other routing related attacks. Hence packet cannot be successfully delivered to the destination. But in proposed scheme, the mechanisms followed to achieve reliability and security increases the trust level of the forwarding node. So the packet delivery ratio decreases only at the end of the lifetime of a forwarding node.

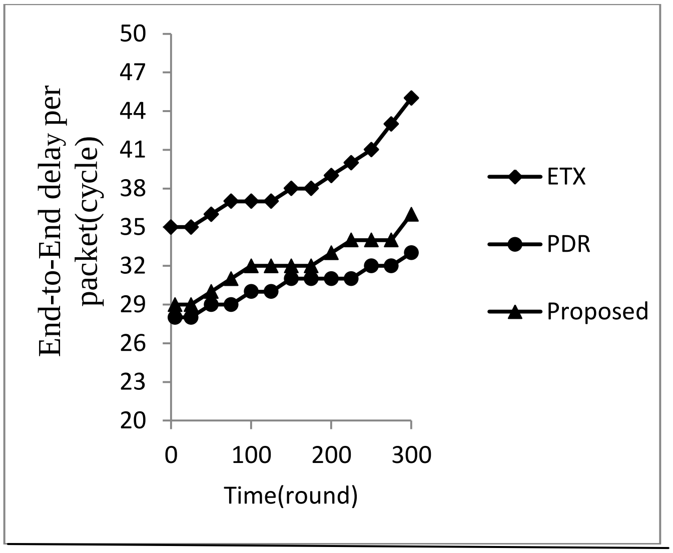

Fig. 5. End-to-End delay in packet transmission from source to destination

Delay is measured in terms of cycle. Cycle is defined as the time taken to transmit a packet from one hop to another hop. As displayed in the figure 5, End-to –End delay is stable at the beginning of simulation due to the stable link that exists between nodes during hop-by-hop routing. Existing scheme ETX does not focus on residual energy of the forwarding node. As time passes the energy gets drained resulting in the death of some of the forwarding node. This creates the necessity for alternate route determination and retransmitting the packet along the newly determined path. Frequent retransmission causes delay in delivering the packet to the destination. But the proposed scheme focuses on the remaining energy of the forwarding node which avoids frequent route determination and packet loss due to unstable link. Moreover, End-to-End delay for proposed scheme and ETX increases as the length of the path used for communication increases. Since these schemes do not consider hop count as a routing metric. But PDR uses hop count as one of its routing metric. Hence PDR achieve better performance of End-to-End delay.

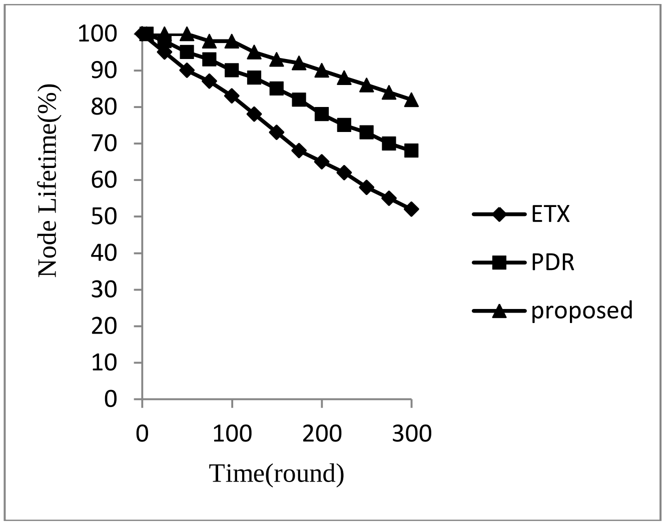

Fig. 6. Average Node lifetime with respect to time

Figure 6 displays the node lifetime of the proposed and related schemes. Proposed scheme balances the energy consumption among sensor nodes in WSN. This avoids early draining of energy of sensor nodes. Always during route determination one hop neighboring node with maximum residual energy is selected to act as forwarding node. Node whose residual energy is less than 20% of its initial energy is not considered for selection. This forces the node to maintain their energy without drain. The lifetime of a sensor node is purely based on their battery power. Also the proposed scheme considers traffic and route the packet through stable link. This avoids wastage of energy consumption due to packet loss. Hence lifetime of the node is increased. But in the related schemes the network functions continuously even if some of the sensor nodes die. In ETX the death occurs in the beginning due to uneven energy consumption and frequent retransmission in different rounds. ETX selects next hop with best link quality but does not consider the residual energy of sensor nodes. Also due to the small radius of the sensor network, death of the key sensor nodes in the surrounding area of the sink occurs earlier. The average node lifetime is less in those schemes.

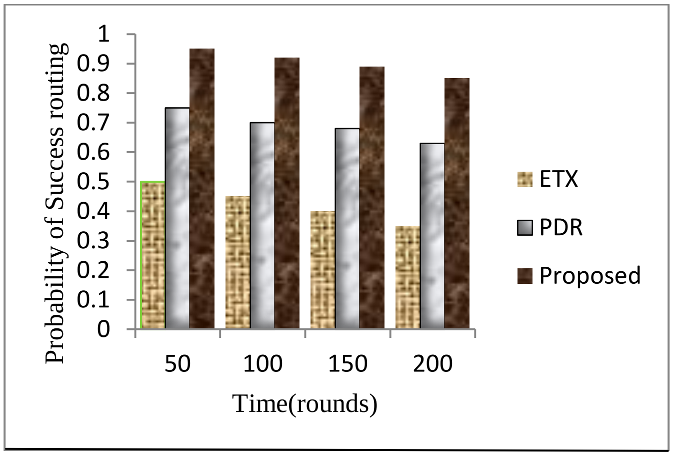

Fig.7. Probability of success in route determination for different schemes

As illustrated in figure 7 the probability of determining successful route is highly achieved through proposed scheme. The proposed scheme focuses on factors such as energy efficiency, stable link and security strength of the forwarding node. This results in determination of successful route that deliver data without any loss. But in related schemes even if stability is considered, they may not focus on security which results in packet loss due to compromised forwarding nodes. Hence the success probability of the determined route is high in proposed scheme when compared to existing schemes.

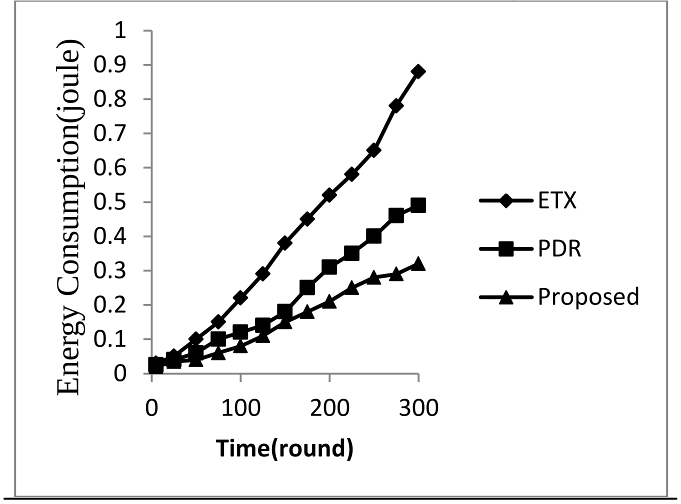

Fig.8. Average energy consumption for single packet transmission

Figure 8. displays the average energy consumed for delivering one packet data successfully to the base station. At the beginning of network lifetime energy consumption for packet transmission is minimum since the path is stable with maximum energy. In related scheme ETX as time passes some sensors drain their energy. This causes the necessity for alternate path determination and in some cases the length of the path also gets increased. Frequent retransmission and forwarding data through maximum number of hops results in increased energy consumption per packet transmission.

VI. CONCLUSION

This study proposes a novel routing mechanism based on the combined effort of the routing metrics link quality, residual energy and authentication. Forwarding node selection is based on weighted approach. This method increases packet delivery ratio, decreases energy consumption and end-to-end delay. The main purpose of this scheme is to balance the energy consumption among different sensor nodes and to increase the node lifetime there by increasing the network lifetime. The simulation results show that the proposed scheme out performs the related schemes in terms of node lifetime, packet delivery ratio, energy consumption, successful routing probability. The trust degree of the selected forwarding node is increased by means of the authentication concept followed in the proposed scheme. The lifetime of the nodes is increased thereby increasing the network lifetime. Hence it is concluded that the proposed routing mechanism can provide efficient reliable path for communication in WSN in harsh environment.

REFERENCES

[I] Nikolaos. A.Pantazis,"Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey", IEEE Communications Surveys and Tutorials. Vo.l5, No.2, 2013.

[2] Anfeng Liu, Zhongming Zheng, Chaozhang 'Secure and Energy efficient disjoint Multipath Routing For WSNs', IEEE Transations on Vehicular Technology ,Vol 61,No:7,pp. 3255-3265,2012.

[3] Junfeng XU,Keqiu Li ,Geyong Min,' Reliable and Energy-Efficient Multipath Communications in underwater Sensor Networks', IEEE Transactions on parallel and distributed systems, Vol. 23,No.7, pp. 1326-1335, 2012).

[4] Eliana Stavrou,Andreas pitsillides(201O), 'A Survey on Secure Multipath routing Protocol in WSNs" Computer Networks Vo1.54 ,pp. 2215-2238.

[5] l.F.Akyildiz, W.Su,Y. Sankarasubramanian, E. Cayirci, "A survey on sensor networks" , IEEE Communication magazine, VoI.40,No.8 ,pp.102-114,2002.

[6] Jiming Chen,Ruizhong Lin,LQER: "A Link Quality Estimation based Routing for Wireless Sensor Networks" ,journal of Sensors, VoI.8,pp.1025-1 038, 2008.

[7] Jae-Hwan Chang, L.Trassiulas,"Maximum Lifetime Routing in Wireless Sensor Networks", IEEE Transaction on Networking, vo1.l2, No.4, pp.609-619, 2004.

[8] Pi-cheng Hsiu,Tei-wei Kuo,"A maximum-residual multicast protocol for large-scale mobile ad hoc networks"IEEE transactions on mobile computing, VoI.8,No.11,pp.1441-1453, 2009.

[9] S.V.Annlin Jeba, B. Paramasivan, "Energy efficient multipath data transfer scheme to mitigate false data injection attack in wireless sensor networks", Computers and Electrical Engineering, Elsevier, vo1.39 issue 6,pp.1867-1879,2013

[10] H.C.Leligou, P.Trakadas, S.Maniatis,"Combining trust with location information for routing in wireless sensor networks",

wireless communications and mobile computing,Vo1.l2, No.12, pp.1091-1103,2012

[11] Ninal Nasser: Yun feng Chen."SEEM: Secure and energy efficient multipath routing protocol for WSNS" Computer Comunications ,Elesivier 3 0(2007) 2401- 2412.

[12] Wenjing Lou, Kwan's," SP READ: A Hybrid Multipath Scheme for Secure and Reliable data collections in WSNs" IEEE Transations on Vehicular Technology, vol 55,no.4, pp. 1320-13 3 0,2006.

[13] G. Zhan, Wei song Shi, " Design and Implementation of TARF:A Trust-Aware Routing Frameworks for WSNS",IEEE Transactions on Dependable and secure computing, Vo:9,issue:2,pp.184-197,20l2

[14] Imad S.Alshawi, Lianshan Van, Wei pan" Life time enhancement in wireless sensor networks using fuzzy approach and A-star algorithm", IEEE sensors journal, Vol.12,No.1 0,pp.30 I 0-3018,20 12.

[15] Xufei Mao, Shaojie Tang, Xiahua Xu. "Energy efficient opportunistic routing in wireless sensor networks". IEEE transaction on parallel and distributed systems, Vol. 22, No.ll, pp. 1934-1942, 2011.

[16] S.Young Moon, Tae Ho Cho, " Fuzzy Based Assignment Method of Filtering Nodes in Wireless Sensor Networks". Wireless Sensor Networks. Vol.4,No.2,pp.40-44, 2012.

[17] Prasenjit Bhavathankar, Subarna Chatterjee, Sudip Misra, "IEEE Link-Quality Aware Path Selection in the Presence of Proactive Jamming in Fallible Wireless Sensor Networks", IEEE transactions on communications, VOL. 66, NO. 4, pp.1689-1704, 2018.

[18] Sheng-Shih Wang and Ze-Ping Chen," LCM: A Link-Aware Clustering Mechanism for Energy-Efficient Routing in Wireless Sensor Networks", IEEE sensors journal, VOL. 13, NO. 2, pp.728-738, 2013.

[19] Korhan Cengiz and Tamer Dag," Energy Aware Multi-Hop Routing Protocol for WSNs", IEEE Access, V0L. 6, PP. 2622-2633.

[20] Hossein Shafieirad , Raviraj S. Adve and Shahram Shahbazpanahi, "Max-SNR Opportunistic Routing for Large-Scale Energy Harvesting Sensor Networks", IEEE transactions on green communications and networking, VOL. 2, NO. 2, pp.506-516, 2018.

[21] Danyang qin, Songxiang yang, Shuang jia, Yan zhang, Jingya ma, and Qun ding," Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network", IEEE Access, volume 5, pp.9599-9606, 2017

[22] Xiaohan Lai, Xiaoyu Ji "Energy efficient link-delay aware routing in wireless sensor networks", IEEE sensors journal, vo1.18, issue 2, pp.837-848,2018.

[23] D.S. De Couto, D.Aguayo,"A high-throughput path metric for multi-hop wireless routing ", Wireless Networks, vol.11. PP. 419-434,2005.

Authors Profile

Mrs.S.V.Annlin Jeba pursed Bachelor of Engineering from Manonmaniam sundaranar university in 2000. She received her master's degree and Ph.D degree from Anna University. She is currently working as a Associate Professor in Computer Science and Engineering department of Sree Buddha College of Engineering. She has published more than 10 research papers in reputed international journal s. Her main areas of research focus on Network Security, Privacy in communication, wireless sensor networks. She has more than 15 years of teaching experience and 4 years of research experience.

Mr.D.R. Gnana King received his BE degree from Anna University in 2007. Also received his master's degree and PH.D degree from Anna University. He is working as an Associate Professor in department of Electronics and Communication Engineering of sahrdaya college of Engineering and Technology. He has published number of papers in National and International Journals and presented more than 10 papers in international conferences. He has more than 10 years of teaching experience and 2 years of research experience. Her main areas of research focus on Networking, Compression techniques.