International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I3P211

Volume 69 Issue 3, 58-63, March 2021
© 2021 Seventh Sense Research Group®

MPTR_QoS: Multi-Path Trust Routing for Improving QoS in Heterogeneous IoT Based WSN

D. I. George Amalarethinam[#1], P. Mercy*[2]

[#] *Associate Professor, *Research Scholar*
PG & Research Department of Computer Science
Jamal Mohamed College (Autonomous), Affiliated to Bharathidasan University,
Tiruchirappalli – 620020, Tamil Nadu, India.

[1]di_george@ymail.com, [2]mercyvijay23@gmail.com

Abstract *- The Internet of Things (IoT) provides an enhancement in real-time applications using smart sensors, internet technologies, embedded systems, and communication protocols. Sensor nodes are smart devices used to collect and forward the sensed data. These smart devices have limitations in terms of computation, processing, memory, and energy resources. One of the primary problems for IoT-based Wireless Sensor Network (WSN) applications is to achieve reliability with secure data transmission. It needs an effective routing protocol that not only enhancing the performance of the network but also improving the quality of service (QoS). This paper proposes Multi-Path Trust Routing (MPTR_ QoS) algorithm for improving QoS properties in heterogeneous IoT-based WSN. Three parameters are considered in the proposed routing algorithm to select multiple optimal paths, i.e., lifespan, distance from the node, and trust. The proposed multi-path trust routing algorithm improves throughput and reliability and minimizes the delay and packet loss. Extensive experiments are conducted in a simulated environment on various circumstances and show that the proposed MPTR _QoS algorithm improves the network properties compared to other techniques.*

Keywords: *Internet of Things, Wireless Sensor Network, Trust, Multi-path, Routing, Quality of Service.*

I. INTRODUCTION

In the field of wireless networking, the recent advancement of smart devices with wireless technology has created new perspectives and has enabled users to connect in a peer-to-peer manner from anywhere. As an emerging technology, the IoT is a revolutionary solution that enables billions of physical devices to be linked in the digital world through the use of diverse networks with heterogeneous objects in terms of energy resources, computing capacities, mobility, and communication technologies [1]. The general networking and IoT communities were fascinated by WSNs as an imperative module in the IoT environment. The base station in a WSN collects data from sensor nodes. Sensor nodes are primarily responsible for sensing the environment to collect the data as per the deployment of the nodes. The battery life associated with a sensor node plays a vital role in designing a sensor network during this process [2].

The routing has always been a significant factor in any form of the communication network. It has always been a challenging task to route packets to the destination effectively with minimal overhead. The transmission of a data packet from the Source node to the intermediate routing node and then to the destination node is called multi-hop routing. The Series of a hop is called a routing path or route [3]. The implementation of the routing algorithm is a challenge for researchers due to sensor resource constraints, such as limited resources, limited processing, and short communication range [4]. Many routing schemes are developed for message transmission. One of the routing schemes is trust-based routing [5]. In trust-based routing, malicious nodes have a lower trust value than normal nodes. The node with a higher trust value should be chosen for routing that will effectively increase the success rate of routing.

The trust-based routing also defends against the malicious node and protects the node from different attacks that reducing the energy consumption of the network. The paper is focusing on trust-based routing and not attack detection in the network. IoT-based WSN applications have many issues in terms of several sensor nodes, heterogeneous devices and standards, diverse communication protocols, battery power, and computational cost, etc.

The sensors used in the IoT paradigm are assigned with additional functionalities to face new challenges in terms of QoS. To improve the QoS, an efficient routing strategy is needed to minimize the loss of data and maximize the network lifetime. QoS based IoT network tries to promote more deterministic network behavior so that the knowledge carried by the network can be effectively delivered and network resources can be better used [6]. QoS highly depends on the most common parameters, including channel bandwidth, packet delivery, network lifetime, packet losses, reliability, throughput, energy, and coverage [7]. To increase the overall network efficiency and QoS in the network [8], there is an intense need to verify energy usage by the nodes. The selection of cluster head and cluster-based routing are considered efficient techniques to minimize the energy consumption of the nodes [9]. Many IoT based WSN applications need energy harvesting technique to increase the energy of each sensor nodes which in turn maximize the network lifetime. It also ensures that a path with reduced power usage is entrenched and improvised QoS metrics like improved throughput, packet delivery ratio and delay [10].

To improve the QoS properties in heterogeneous IoT-based WSN, this paper proposes a multi-path trust routing algorithm (MPTR_ QoS). The optimal path is selected based on the lifetime of the node, the distance between nodes, and the trust value of the node. The proposed MPTR_QoS algorithm designs an efficient multipath trust routing algorithm to enhance the QoS in the IoT network by maximizing the network lifetime and minimizing the packet loss and packet delay.

Section 2 reviews the related work; the proposed methodology is described in Section 3, and Section 4 explains the simulation results of the proposed work, and Section 5 concludes the paper.

II. RELATED WORK

In WSNs, hundreds to thousands of sensor nodes are deployed in the area as per the requirement of IoT applications. Sensor nodes in WSN-assisted IoT are limited to resources such as storage, energy, and computation, etc. To sustain a long network lifetime and achieve higher energy usage, robust routing mechanisms are important. This section explains some routing methods used in IoT-enabled WSN.

Mohamed et al. [11] proposed a QoS- aware service selection algorithm based on the energy of the node that increases service availability and enhances energy utilization. Saima Abdullah et al. [12] suggested a message scheduling algorithm that focused on QoS parameters in the IoT environment to decrease latency and to avoid starvation of the node. J. S. Raj et al. [13] proposed a methodology to determine the shortest route by using a neural and simple fuzzy rule-based system to enhance routing capabilities for IoT with WSNs to improve QoS metrics.

Haseeb et al. [14] introduced a secret sharing scheme to enhance the effectiveness of energy efficiency with multi-hop data security against despicable behavior. This offers a lightweight solution for IoT-based constrained WSNs with secure data routing in a multi-hop approach. A distributed congestion management algorithm is suggested by Chanak et al. [15] for IoT-enabled WSNs to effectively overcome congestion for healthcare applications. This system alleviates congestion through a data routing technique based on priority. Besides greater flexibility, a priority queue-based scheduling scheme is presented.

Hatzivasilis et al. [16] developed SCOTRES, a trust-based framework for secure routing in ad-hoc networks that, by applying novel metrics, advances the intelligence of network entities. The energy metric takes into account the resource usage of each node, requires a comparable amount of coordination, and increases the network lifetime. The topology metric knows the locations of the nodes and increases load-balancing. Due to bad channel conditions, the channel-health metric offers tolerance for intermittent malfunctioning and protects the network against jamming attacks. The credibility metric assesses the coordination of each person for particular network activity, recognizing specialized attacks, while the confidence metric estimates the overall compliance, protecting against combinatorial attacks.

Xu et al. [17] proposed a new protocol for energy-efficient region source routing. A distributed energy area algorithm is used to select the source nodes dynamically based on the residual energy of the nodes. The source routing nodes then compute the optimal source routing path for each common node, allowing the participation of partial nodes in the routing process and balance the energy consumption of the sensor node. Shen et al. [18] suggested a centroid-based energy-efficient routing protocol to increase the efficiency of IoT networks. Three main components are included in this method: a new distributed cluster forming technique that allows local nodes to be self-organized. The cluster adaptation algorithm and cluster head rotation based on the centroid location balances the load of the sensor nodes that optimize the energy level of the nodes to decrease the energy consumption in long-distance communication.

T. M. Behera et al. [19] introduced the Enhancement of the existing Stable Election Protocol (SEP) that selects the cluster head based on a threshold value for a heterogeneous network. The threshold preserves the uniform distribution of energy between member nodes and CH nodes. The network load can be uniformly distributed based on the role of sensor nodes such as normal nodes, and intermediate nodes, and advanced nodes.

The WSN-IoT quality of service study puts difficulties and risks forward in particular due to cost and scalability constraints in physical testbeds and low credibility of simulation performance. The system architecture of a testbed with Adaptive Quality of Service (AQoS) is proposed by S. Ezdiani et al. [20]. The idea of the AQoS testbeds offers an opportunity for a versatile framework of experimentation that can respond to complex changes in network conditions.

For IoT-based Wireless Sensor Networks, Jaiswal and Anand [21] suggested an efficient QoS-aware multipath routing protocol. The optimum cost factor is determined by two variables, such as lifetime and congestion level of the node along the path from source to destination. Even though two kinds of packet control are adopted by the protocol, it provides less power consumption and better QoS.

III. PROPOSED METHODOLOGY

This section explains the proposed multi-path trust routing algorithm (MPTR_QoS) for improving the QoS properties of IoT networks. MPTR_QoS uses three factors to select the optimal path: The lifetime of the node, the distance between nodes, and the trust value of the nodes. The multipath trust routing is used to find the optimal path, which results in the excellent coverage and throughput that lead to the extended lifetime of the IoT network. Fig. 1. Shows the flow diagram of MPTR_QoS.

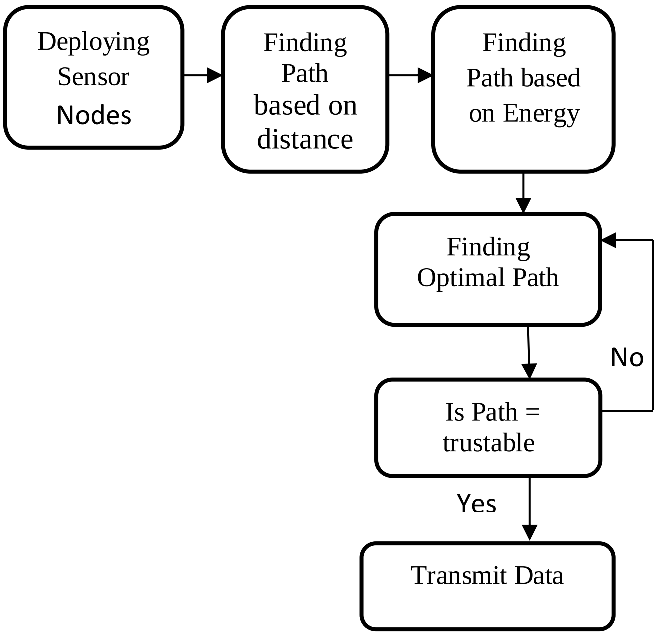

Fig 1: Proposed MPTR_ QoS Block Diagram

The following assumptions are assumed in the proposed work:

- Nodes are randomly deployed and periodically transmit their data
- The nodes are heterogeneous and have equal initial energy.
- Base Station/ Sink node is fixed in the middle of the network
- The nodes are grouped into the number of clusters, and the cluster head (CH) is selected based on their node distance.
- CH may interact with the base station either in a single hop or a multi-hop communication.

Trust management is applied in many fields of communication and information technology, such as wireless sensor networks, Mobile Ad-Hoc Networks (MANET), social networking, and recently the Internet of Things. The definition of trust is an intangible concept with various meanings, depending on both the parties involved and the circumstances, and it is influenced by factors that can or cannot be measured. There are various forms of confidence concepts that lead to difficulties in the development of standard and generic details that retain some unique provisions or exceptional circumstances. Trust is generally considered to be a numerical computational value expressed by the trustee-trustor interaction [22], described in a specific situation, computed by trust metrics, and evaluated by a method.

Trust management models can be used in wireless sensor networks as efficiently as possible to construct a stable and responsive routing technique. In the case of trust management models, the trust value of the member node and cluster head node of each cluster should be calculated, and then the resulting trust value can be used to identify a secure routing path in the network.

Communication trust is the trust values calculated between the nodes from the cluster head to the base station based on their cooperation in the transmission of network messages. The most significant consideration for checking the credibility of an individual node in trust assessment is communication trust. It decides whether the target node will act naturally in the future or not, and the process of trust calculation will be fast enough to save node energy. It can be calculated as [23],

$$\frac{XC_{ij}+1}{XC_{ij}+YC_{ij}+\varepsilon} \qquad (1)$$

where XC_{ij} = Total number of successful communication between node-i to node-j

YC_{ij} = Total number of unsuccessful communication between node - i to node-j

ε = random number between 0 to 1

The paths between source nodes to the base station are validated based on the communication trust value. Multiple paths are identified between the source node to the base station [BS] based on energy and distance. The optimal path is selected based on trust value. Figure 2 shows the proposed multipath trust routing algorithm.

In Algorithm-1, the Source Cluster Head (CH_S) can directly send the messages to the base station when it is within the communication range. Otherwise, two possible paths are selected based on the shortest distance, and the highest energy level from the source cluster head to the base station is computed.

Algorithm-2 shows the steps to compute the shortest path based on the distance and highest energy of the node. The communication trust value is computed for both paths. The path with the highest trust value is selected to get optimal routing. When the trust value for P1 is greater than P2, the shortest distance is used for sending the messages to the BS.

Otherwise, Path with the highest energy node is selected from CH to BS for the transmission of messages. Sometimes the selection of Path P1 based on the distance might be deprived with the energy of the intermediate nodes between CH_s to BS, which results in the Packet Loss. It can be avoided using Path P2, which is based on the highest energy of nodes in Path P2. Thus proposed MPTR_QoS algorithm provides optimal routing with minimum packet loss and delay.

Algorithm-1 Multipath Trust Routing Algorithm

```
Input: Cluster Heads {$CH_1$,$CH_2$, …, $CH_k$}, Source Cluster Head (CHs)
Output: Optimal Path
If Base Station(BS) is within CHs communication range
    Message can be directly sent from CHs to BS
Else
    $P_1$ = Shortest Path (CHs, Distance)
    $P_2$ = Shortest Path (CHs, Energy)
    Calculate trust value for $P_1$ and $P_2$ using (1)
    If TV($P_1$) > TV($P_2$)
        Select $P_1$ for Routing (Shortest distance path)
    Else
        Select $P_2$ for Routing (Highest energy path)
    EndIf
EndIf
```

Fig 2: Multipath Trust Routing Algorithm

Algorithm-2 Proximate Cluster Head Selection Algorithm

```
Input: Source Cluster Head (CHs), Parameter (Param)
Output: Shortest Path (SP)

01. If Param == 'Distance'
02.     Find  the distance to the nearest CH
03.     Select CH with minimum distance
04.     SP = SP $\cup$ CH
05.     Repeat distance computation until Base Station is reached.
06. End If
07. If Param == 'Energy.'
08.     Select nearest CH, which has the highest energy
09.     SP = SP $\cup$ CH
10.     Repeat step 7 until Base Station is reached.
11. End If
```

Fig 3: Proximate Cluster Head Selection Algorithm

Fig. 4. Shows a sample network having 18 nodes, including Cluster Head Nodes with one Base Station.

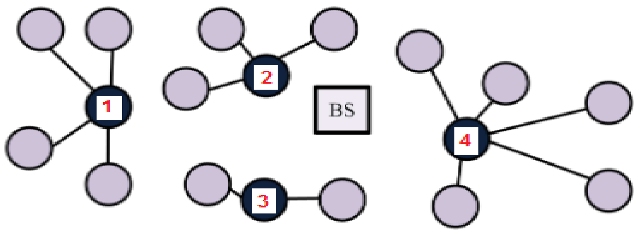

Fig 4: Sample Network

It is assumed that the energy of the cluster head and the distance between nodes are randomly given, which are given in is Table I.

TABLE I
CH ENERGY AND DISTANCE PROPERTIES

When the source CH1 sends the message to BS, the optimal path is to be selected based on the shortest distance and highest energy level. The optimal path based on the distance is $P_1 = 1 \rightarrow 3 \rightarrow BS$ and the path based on the energy is $P_2 = 1 \rightarrow 2 \rightarrow BS$. The trust value for both P_1 and P_2 are computed to select the path which has the higher trust value for the routing.

IV. SIMULATION RESULT

This section evaluates the efficiency of the proposed work. The experiment is conducted with MATLAB. 100 sensor nodes that are randomly deployed over a 100m × 100m area, and the base station is located at the center of the area. The parameters of simulations are shown in Table II.

Cluster Head	**Energy (%)**	**Distance Measure in meters**	
		To Node	**Distance**
1	80	2	4
		3	2
2	92	3	5
		4	7
3	75	4	6

TABLE II
SIMULATION PARAMETER

Parameter	**Value**
Network Size	100 x 100 m
Base Station Location	(50,50)
Number of Nodes	100
Type of Node Distribution	Random
Node Initial Energy	1 Joule
Electronic energy	50nj/bit
Transmission amplification coefficient	10pj/bit/n^2
Packet size	1000 bits

The proposed MPTR_QoS is compared with HEED-FT [24] and FTCM [25] in terms of energy consumption, packet loss, and delay. Table III shows the comparison of energy consumption in FTCM, HEED-FT, and MPTR _QoS. The energy consumed by the nodes in the MPTR_QoS algorithm is 0.2j, which is lesser than 0.4j and 0.5j energy consumptions of FTCM and HEED-FT. When the number of rounds is increased to 1000, the MPTR_

QoS algorithm has the lowest energy consumption of the node 0.45j, which leads to maximization of the lifetime of the node.

TABLE III
COMPARISON OF ENERGY CONSUMPTIONS OF NODES (JOULE) IN FTCM, HEED-FT, AND MPTR_ QoS.

Number of Rounds	FTCM	HEED-FT	MPTR_QoS
1	0	0	0
100	0.14	0.19	0.05
200	0.18	0.3	0.13
300	0.22	0.4	0.17
400	0.29	0.55	0.2
500	0.4	0.6	0.22
600	0.43	0.72	0.27
700	0.5	0.81	0.3
800	0.58	0.85	0.31
900	0.62	1	0.39
1000	0.65	1	0.45

Fig. 5. shows that the proposed MPTR_QoS algorithm consumes a small amount of energy compared to other algorithms. The HEED-FT algorithm had no energy when it reached 900.

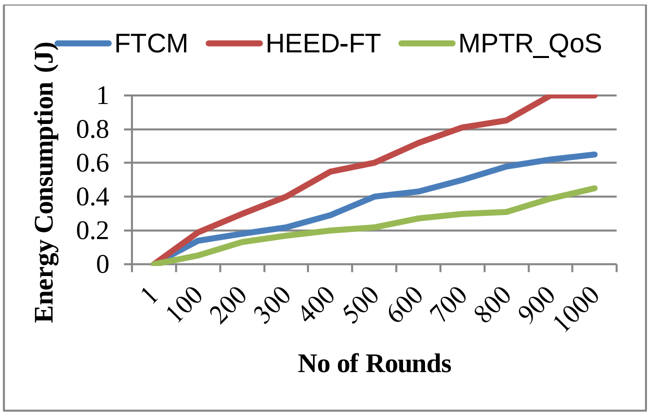

Fig 5: Energy Consumption of Nodes

The comparison of packet loss rate in FTCM, HEED-FT, and MPTR_QoS is shown in Table 4. The packet loss rate is 0.3% in MPTR_QoS and 0.4% and 0.5% in FTCM and HEED-FT, respectively when it reached around 500. When the number of rounds increased to 900, The Packet Loss rate of MPTR_QoS is 0.1%, and FTCM and HEED-FT is 0.24% and 0.4%. The proposed MPTR_QoS algorithm shows the lowest packet delay rate.

TABLE IV
COMPARISON OF PACKET LOSS RATE (%) IN FTCM, HEED-FT, AND MPTR_ QoS

Number of Rounds	FTCM	HEED-FT	MPTR_ QoS
1	0	0	0
100	0.7	1.5	0.5
200	1.5	2.4	1.2
300	2.9	4	2.3
400	3.6	5.2	3
500	4.3	6	3.9
600	5	7.1	4.2
700	6.1	7.5	5.9
800	7.3	8.2	6.1
900	8	9	6.8

The tabulated values given in Table 4 are graphically represented in Fig. 6. showing that MPTR_QoS has the minimum Packet loss rate when compared with FTCM and HEED-FT.

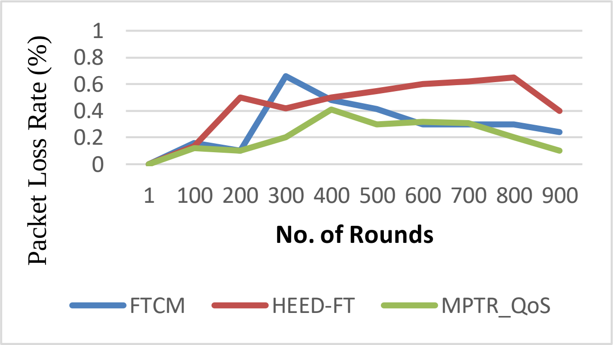

Fig 6: Packet Loss Rate

. Table V shows the end-to-end delay comparison of FTCM, HEED-FT, and MPTR_QoS.

TABLE V
COMPARISON OF PACKET DELAY(S) IN FTCM, HEED-FT, AND MPTR_QoS.

Number of Rounds	FTCM	HEED-FT	MPTR_ QoS
1	0	0	0
100	0.16	0.133	0.12
200	0.1	0.5	0.1
300	0.66	0.42	0.2
400	0.48	0.5	0.41
500	0.416	0.55	0.3
600	0.3	0.6	0.32
700	0.3	0.62	0.31
800	0.3	0.65	0.2
900	0.24	0.4	0.1

The proposed MPTR_QoS algorithm shows a packet delay of 3.9s when compared to the FTCM and HEED-FT algorithm that has 4.3s and 6s delay when the number of the round is 500. When it reached round 900, the packet delay of the MPTR_QoS algorithm is 6.8s, and FTCM and

HEED-FT are 8s and 9s. The result shows that MPTR_QoS has the minimum packet delay when compared to other algorithms.

Fig. 7. shows that the HEED-FT method has a high time delay compared to other methods. The proposed MPTR_QoS has taken less time to reach the destination.

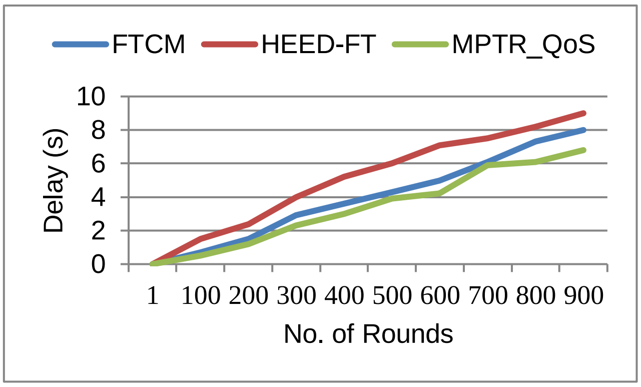

Fig 7: Packet Delay

V. CONCLUSION

IoT facilitates the idea of linking millions of small devices to collect and exchange data on various domains, including health care, the weather, and industry. The IoT confronts several problems, mainly increase network lifespan, improves throughput, increases the number of alive nodes, decreases packet latency and packet loss, and reduces energy consumption. The multipath trust routing is proposed to enhance the quality of service in IoT based WSN network. The multipath trust-based routing finds the optimal path based on the shortest distance and highest energy of the nodes, which enhances QoS Parameter by reducing the energy consumption and minimizing the packet loss and delay. Thus the Proposed MPTR_QoS algorithm provides maximum energy efficiency that increases the network lifetime. The increased network lifetime with enhanced QoS provides optimal routing mechanism in many real-time IoT applications.

REFERENCES

[1] W. A. Jabbar, W. K. Saad, and M. Ismail, MEQSA-OLSRv2: A Multicriteria-Based Hybrid Multipath Protocol for Energy-Efficient and QoS-Aware Data Routing in MANET-WSN Convergence Scenarios of IoT, in IEEE Access, 6(2018) 76546-76572.

[2] K. Jaiswal and V. Anand, An Optimal QoS-aware multipath routing protocol for IoT based Wireless Sensor Networks, 2019 3rd International Conference on Electronics, Communication, and Aerospace Technology (ICECA), (2019) 857-860.

[3] Amol Dhumane, Routing Challenges in Internet of Things, CSI communications, March (2016).

[4] M. Ilyas, Z. Ullah, F.A Khan, M.H. Chaudary, M.S.A Malik, Z. Zaheer, H.U.R. Durrani, Trust-based energy-efficient routing protocol for Internet of things–based sensor networks, Int. J. Distrib. Sens. Netw., 16(10)(2020).

[5] Z. A. Khan, J. Ullrich, A. G. Voyiatzis and P. Herrmann, A trust-based resilient routing mechanism for the internet of things, Proceedings of the 12th International Conference on Availability Reliability and Security, (2017).

[6] J. Tang, A. Liu, J. Zhang, Z. Zeng, N. Xiong, and T. Wang, A security routing scheme using traceback approach for energy harvesting sensor networks, Sensor s, 18(3)(2018).

[7] H. Mostafaei, Energy-efficient algorithm for reliable routing of wireless sensor networks, IEEE Transactions on Industrial Electronics, 66(7)(2019) 5567-5575.

[8] M. Manisha Singh and G. Baranwal, Quality of Service (QoS) in the Internet of Things, 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE, (2018) 1-6.

[9] K. Thangaramya, K. Kulothungan, R. Logambigai, M. Selvi, S. Ganapathy, A. Kannan, Energy-aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT, Computer Networks, 151(2019) 211-23.

[10] S.K.S.L Preeth, R. Dhanalakshmi, R. Kumar, P.M. Shakeel, "An adaptive fuzzy rule-based energy-efficient clustering and immune-inspired routing protocol for WSN-assisted IoT system, Journal of Ambient Intelligence and Humanized Computing, (2018) 1-3.

[11] Mohamed EssaidKhanouche, YacinAmirat, AbdelghaniChibani, MoussaKerkar, and Ali Yachir, Energy-Centered and QoS-Aware Services Selection for Internet of Things, IEEE Transactions On Automation Science And Engineering, (2016).

[12] Saima Abdullah, Kun Yang, A QoS aware message scheduling algorithm in Internet of Things environment, IEEE, (2017).

[13] J.S. Raj, QoS optimization of energy efficient routing in IoT wireless sensor networks, Journal of ISMAC, 1(1)(2019) 12-23.

[14] K. Haseeb, N. Islam, A. Almogren, I. Ud Din, H. N. Almajed and N. Guizani,Secret SharingBased Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs, in IEEE Access, 7(2019) 79980-79988.

[15] P. Chanak and I. Banerjee, Congestion Free Routing Mechanism for IoT-Enabled Wireless Sensor Networks for Smart Healthcare Applications, in IEEE Transactions on Consumer Electronics, 66(3)(2020) 223-232.

[16] G. Hatzivasilis, I. Papaefstathiou, and C. Manifavas, SCOTRES: Secure Routing for IoT and CPS, in IEEE Internet of Things Journal, 4(6)(2017) 2129-2141.

[17] C. Xu, Z. Xiong, G. Zhao, and S. Yu, An Energy-Efficient Region Source Routing Protocol for Lifetime Maximization in WSN, in IEEE Access, 7(2019) 135277-135289.

[18] J. Shen, A. Wang, C. Wang, P. C. K. Hung, and C. Lai, An Efficient Centroid-Based Routing Protocol for Energy Management in WSN-Assisted IoT, in IEEE Access, 5(2017) 18469-18479.

[19] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand and A. H. Gandomi, I-SEP: An Improved Routing Protocol for Heterogeneous WSN for IoT-Based Environmental Monitoring, in IEEE Internet of Things Journal, 7(1)(2020) 710-717.

[20] S. Ezdiani, I. S. Acharyya, S. Sivakumar and A. Al-Anbuky, An IoT Environment for WSN Adaptive QoS, 2015 IEEE International Conference on Data Science and Data Intensive Systems, (2015) 586-593.

[21] K. Jaiswal and V. Anand, An Optimal QoS-aware multipath routing protocol for IoT based Wireless Sensor Networks, 2019 3rd International Conference on Electronics, Communication, and Aerospace Technology (ICECA), (2019) 857-860.

[22] N.B. Truong, U. Jayasinghe, T.W. Um, G.M. Lee, A Survey on Trust Computation in the Internet of Things, The Journal of Korean Institute of Communications and Information Sciences (J-KICS), 33(2)(2016) 10-27.

[23] M. Sitha Ram, K. Nageswara Rao, S. Krishna Rao, Trust-based cluster head selection with secure routing algorithm for wireless sensor network, International Journal of Advanced Science and Technology, 28(20)(2019) 19-30.

[24] Y. Zhou, et al., Fault-tolerant multi-path routing protocol for WSN based on HEED, International Journal of Sensor Networks, 20(1)(2016) 37–45.

[25] E. Moridi, M. Haghparast, M. Hosseinzadeh, & S.J. Jassbi, Novel fault-tolerant clustering-based multipath algorithm (FTCM) for wireless sensor networks, Telecommunication Systems, (2020).