INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Performance Analysis by Improving Energy Efficiency in IoT Based Wireless Sensor Network for Routing Algorithm

K C Shilpa[1]*, **S Chetan**[1], **H D Anand**[1]

1 Department of Electronics and Communication Engineering, Dr. Ambedkar Institute of Technology, Bengaluru, India

Check for updates

OPEN ACCESS

Received: 12-12-2022

Accepted: 11-02-2023

Published: 15-03-2023

Citation: Shilpa KC, Chetan S, Anand HD (2023) Performance Analysis by Improving Energy Efficiency in IoT Based Wireless Sensor Network for Routing Algorithm. Indian Journal of Science and Technology 16(11): 785-794. https://doi.org/10.17485/IJST/v16i11.2388

* **Corresponding author**.

shilpakc.ec@drait.edu.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To improve the energy efficiency in IoT-based wireless sensor networks. To increase the sensor node lifetime in any wireless sensor network (WSN) based on the Energy-efficient cluster and routing in WSN. The advancement in the electronic industry has to develop the low power-consuming and low-cost devices for multiple purposes. **Methods:** A new algorithm is proposed to improve the energy efficiency in IoT-based WSN for routing algorithms. The low power consuming devices are wisely chosen for the respected application and their power management. This study is intended to provide efficient routing algorithms with less energy consumption in wireless sensor networks. **Findings:** A wireless sensor network deployed with a number of non-static nodes in a communication network are beneficial for numerous fields such as the military, medical sector, structural health monitoring, transportation industries, etc. In this paper, the performance parameters like average throughput, average end-to-end delay, packet delivery ratio, average node energy, and normalized routing load are analyzed. **Novelty:** We designed and simulated the Distributed IoT-based wireless network system to analyze the information of nodes roaming in the vicinity of the zone area. In proposed technique energy efficiency is increased compared to the conventional algorithm. In node centric routing protocol, energy efficiency is increased from 55% to 68%. In data centric routing protocol, energy efficiency is increased from 65% to 75%. In source-initiated routing protocol, energy efficiency is increased from 68% to 80%. In destination-initiated routing protocol, energy efficiency is increased from 72% to 85%.

Keywords: Ad Hoc OnDemand stance Vector (AODV); DestinationSequenced DistanceVector Routing (DSDV); Dynamic source routing (DSR); MQ Telemetry Transport (MQTT); Quality of Services (QoS); Wireless Sensor Network (WSN)

1 Introduction

In the Wireless Sensor Network (WSN), the acting node says a significant part in data transmission, and keeping them alive for a longer period in WSN[1]. This study is focusing on increasing the lifespan of the node by increasing one's energy efficiency and smart routing in the WSN cluster. In this paper, considering of the information node has data intended for the destination node, the WSN routing for the transmission of data from the information node to the destination node is made possible with the help of the gateway, where the gateway has the information of all the nodes communicating with it frequently. Here, we are considering the information of the moving nodes in the area of the wireless network, with help of the message beacon technique. In the diversity of network topology, point-to-point, star, tree, linear, and mesh are the ways of connection and relationship of each node, each topology has its method to follow the rules of the methodology[(2,3)].

The existing IoT-based wireless sensor network is less energy efficient[(4)]. In particular, when the nodes are moving the proper information is not received[(5)]. We designed and simulated the Distributed IoT-based wireless network system to analyze the information of nodes roaming in the vicinity of the zone area. The proposed framework with moving nodes continuously gives information about their presence in the open area. In the proposed research work, we have improved the WSN parameters like average throughput, average end-to-end delay, packet delivery ratio, average node energy, and normalized routing load.

In this paper, we have considered data collection of sensors from the information area, which means the non-static nodes which are moving in the WSN, where a destination node needs the information from the source end. In a simple way of understanding, the data collection of node A intended for node K, where node K reacts to the data received from node A, and the happening of communication between the nodes creates the simplest path. Many algorithms like particle swarm optimization, intelligent opportunistic routing protocol (IOP)[(6)] also protocols AODV, DSDV, and DSR[(7,8)] routing protocol, etc.

In the proposed system, we are proposing an advanced technique for data transmission in a WSN network where the nodes are non-static and with limited energy supply in the vicinity. So, the consideration of data coming from the node end is with message information along with the node authentication which we broadly called as The Geographic-based Message Node Authentication Technique.

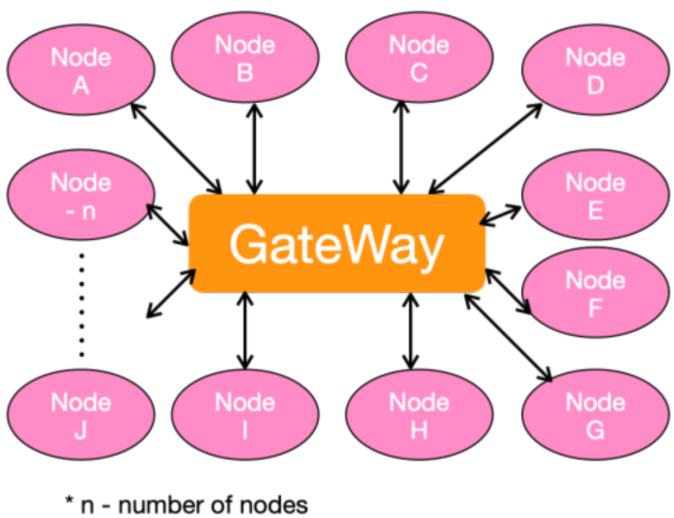

Fig 1. Distribution of nodes

Figure 1 broadly explains, each sensor node has to send a frequent message to the central gateway, the information contained in the message is having the Geo-location details with a time stamp[(9,10)]. While Gateway sends the message, a node will wake up and will send a reply message, after which it will be in sleep mode until its next wake call comes. This continuously happens for all the connected nodes in the application, the cross-checking of the recent message received at the gateway with respect to the particular node is continuously monitored for the liveliness of the respected node.

Figure 2 explains duplex communication in the wireless network with connectivity follows different protocols, which are of two kinds. The first one is the area limited and all the sensors are in ranges of Ble, Wi-Fi, LoRa, Z-Wave, ZigBee, for this type of communication, can make a choice of microcontroller enabled Linux-based system. Also, we can choose Gateway for WSN sensor nodes to monitor. The other way of possibility is when the sensor nodes are distributed in the vicinity of the network the Wi-Fi-enabled sensor nodes can be used to provide the internet. In both cases, the functionality of beacon messaging along with the area information of the non-static node id message will be inter-shared with the Gateway for processing and prediction of the shortest possible routing.

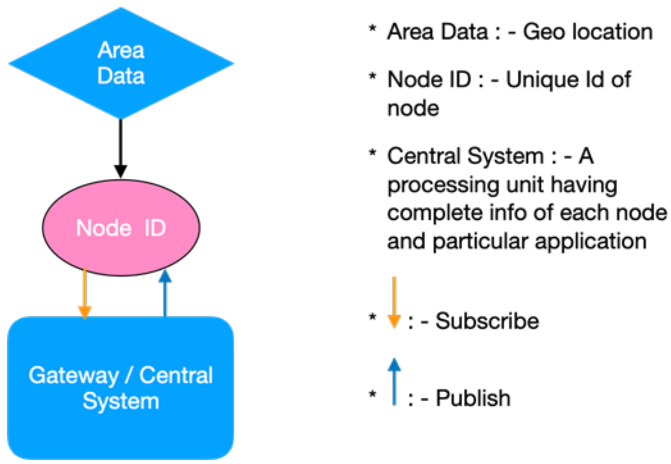

Fig 2. Node described

2 Quality of Service and Essentials

The timely based intercommunication of node and gateway has to happen for the authentication of the liveliness of the nodes. The check-in process in the real world takes place as below Quality of Services (QoS). The Quality of Service (QoS) level is a mutual concurrence of guarantee of delivery of a message between the sender and the receiving sensor nodes.

The below are classifications:

1. At most once (0)
2. At least once (1)
3. Exactly once (2)

There are two ways of message delivery in the proposed model of wireless communication:

1. Message delivery from the end node to the Gateway
2. Message delivery from the Gateway to the end node

We are defining the two ways of the message delivery system because there is a need for simple communication differences between the two[11,12]. The sensor node sends the information message communication to the Gateway end describes the quality-of-service degree. The Gateway transmits the message to subscribed nodes using the QoS level that each subscribed sensor node. If the subscribed sensor node defined a lower level QoS than the publishable sensor node, the Gateway sends a message with a low-level quality of service[13–15].

Let us understand the difference and the behavioral model of QoS levels implemented in the MQTT protocol:

Quality of Service level 0 is a type that is almost like ”fire and forget” and the guarantee of service is equivalent to TCP protocol as shown in Figure 3 a. The receiver will not acknowledge the message of receipt and the information will not be stored and re-transmitted by the sender. There will be no guarantee of delivery.

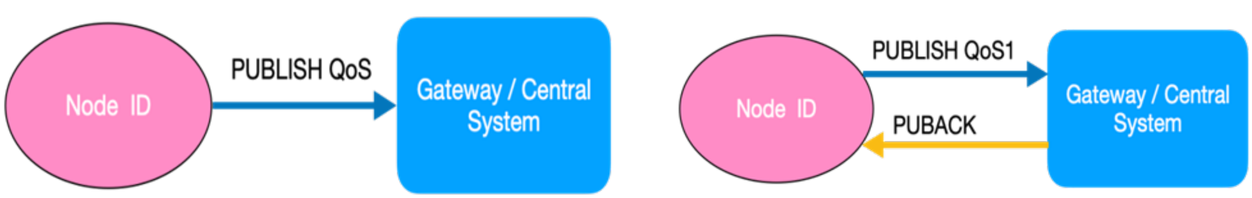

Fig 3. a - QoS0 - at most once , b - QoS1 - at least once

The sensor node requests the gateway by sending PUBLISH message, then waits for the publish acknowledgment message packet from the receiver end. This level 1 message will be delivered at least once to the receiver node end with a guarantee. It is possible for the information message to be sent or delivered numerous amounts of times as shown in Figure 3 b.

The sender employs the packet identifier in every packet to match the PUBLISH message packet for the equivalent publish acknowledgment message packet[16,17]. If the node end does not receive a publish acknowledgment packet within a stipulated interval, the node will realize the non-delivery of the message and resends the PUBLISH packet.

The more advanced level of security will be achieved by QoS 2, as shown in Figure 4. The guarantee of this service level is for each recipient is only once the message receiving. The achievement of this type of security authentication is following the complex level where at the minimum two requests/response follows typically four-part handshake between the sender node end and the receiver sensor node end. The sensor node as well as the broker will continuously handshake with the use of the packet identifier of the original PUBLISH message.

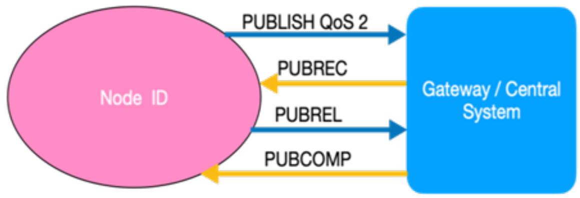

Fig 4. QoS2 - exactly once

The most advanced level of authentication is QoS 2. When a Gateway gets a quality of service 2 PUBLISH message packet from the sensor node, it proceeds with the published message respectively and responds to the sender node using publish receive (PUBREC) message packet that admits the PUBLISH message packet. If the sensor node would not receive a PUBREC packet from the Gateway, it dispatches the PUBLISH message packet yet again with a duplicate (DUP) flag until it receives an acceptance receipt[18–20].

Once the sensor node end picks up a PUBREC packet from the Gateway[21,22], the sensor node can easily reject the initial PUBLISH message packet[23]. The node preserves the PUBREC packet from the broker and responds with a Publish release (PUBREL) packet.

After the gateway receive the PUBREL packet[24,25], it can reject all stored states and respond with a Publish complete (PUBCOMP) packet (the same is true when the sender receives the PUBCOMP).

When the QoS 2 flow process is complete, both node and gateway are definite with the message remitted and the sender has delivery confirmation.

2.1 Proposed Model

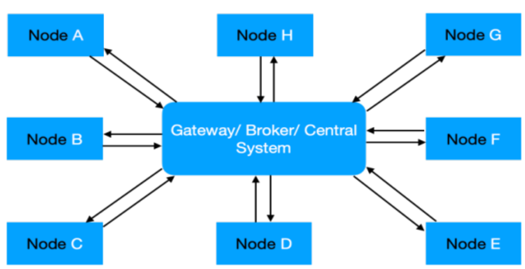

Fig 5. QoS 2 - exactly once

The advanced technique of communication between any nodes in the current technology trends follows the quality of service. In the concern of secured communication in the wireless sensor network, the sensor node energy can be conserved by the best practice of applying the quality-of-service methodologies. Here, in this proposed model as shown in Figure 5 , we are developing an algorithm called GANQ (Gateway Authentication of Nodes by Improving QoS) for non-static nodes distributed in WSN.

As we have proposed the types of QoS, the two modes of communication happen in a WSN. It depends on the Gateway ping to the distributed nodes, which are

1. Gateway ping 1 hop beacon messages
2. Ping for destination node finalize

2.1.1 Gateway Ping 1 Hop Beacon Messages

The gateway functionalities are defined as it beeps a message with the QoS pertaining to the Publish message containing the request message to the Nodes, asking for their area information along with the Publish Acknowledgment.

Here the nodes are movable nodes. Since they are non-static and have a unique ID for each node, Gateway can request nodes with their node Id and area information for processing.

Here the area considered is a zone, where the non-static nodes are switching between the zones; it is easy to identify the shortest path and node authenticity.

Here the area considered is a zone, where the non-static nodes are switching between the zones; it is easy to identify the shortest path and node authenticity. This yields the information of,

1. Node presence &
2. Area information of nodes

The process is followed like the below method

1. At a frequent time, the node will get a message from the Gateway, asking for its area information and node authentication.
2. The proposed mode of communication follows QoS1, since it is two ways of authentication (explained in QoS), as shown in Figure 6 a.

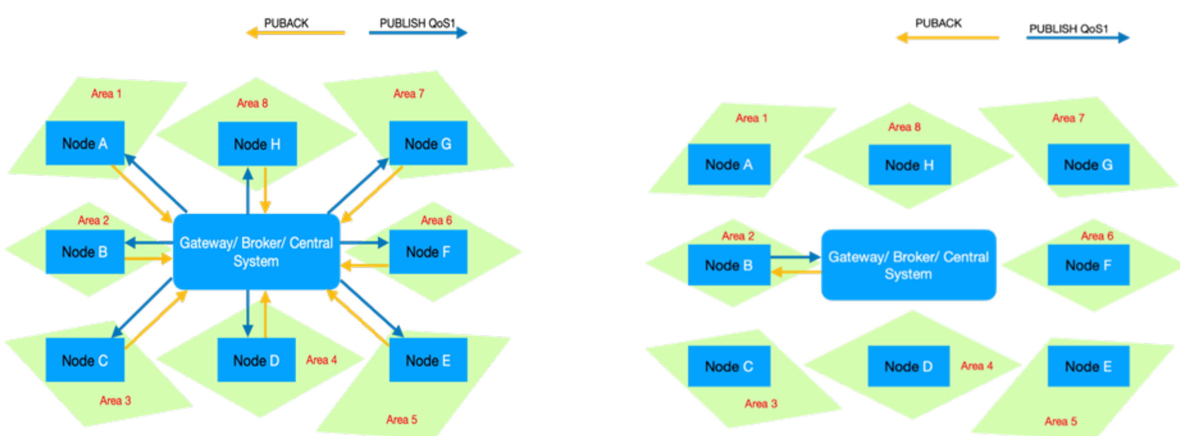

Fig 6. a- QoS2 - exactly once b- QoS 2 - exactly once

2.1.2 Ping for Destination Node Finalize

Considering a condition where the Node B requires information contained in the different zone and it needs to communicate with the node present in the intended area. The process of communication is,

1. Node B will publish the message with the request of information related to the intended zone area.
2. Gateway analyses the request and provides the zone area presence of which node
3. Node B – Gateway – zone is Node communication continues

The above process of A & B ping happens in the Wireless communication to save time and secure mode communication as shown in Figure 6 b.

Node B requests Gateway regarding the right selection of information node by passing the PUBLISH QoS1, in this case, gateway is having all information of the presence of nodes in the information areas.

3 Results and Discussion

Simulation results of our proposed Gateway response protocol in the Wireless Sensor Network using Hive swarm, MQTT-spy and other MQTT Simulator are presented. Along the comprehensive experiment, we demonstrate the properties and measure the network performance in regards to the throughput, Packet delivery ratio, Network Overhead and packet loss. The proposed Gateway response protocol extends the other technology standards like AODV and QOD protocol through inclusion of network density measures, data compression and data securing mechanism. In the Simulation, the set-up of the network is depicted in the following table set of nodes and central/gateway, as shown in Table 1.

Table 1. Simulation parameter to build protocol

Simulation Software	MQTT-spy and Hivemq swarm
Gateway/Central system/Broker	Local host
Ports used	8080 and 1883
Software development	Python
Node Activity	MQTT-spy or MQTT-fx and MQTTlens
Number of nodes	Restricted to 25
Estimation of n nodes	Gateway/Broker strength

The bit rate and size of data can be measured while the communication is established between Node and Gateway either, which is directly measured by the broker software upon calculation of start, stop and data bits.

$$\text{Total byte} = \text{Start byte} + \text{Stop byte} + \text{Data bytes} \tag{1}$$

$$= (2+2+2 \text{ byte to } 230\text{MB}) \tag{2}$$

In this simulation, we have observed the HiveMQ Swarm, which provides the successful distributed simulation environment to test millions of MQTT clients/nodes, millions of MQTT messages and hundreds of thousands MQTT topic addresses as shown in Figure 7 a. Finally, a tool to check the performance, scalability and reliability of your IoT solution before it is deployed into production.

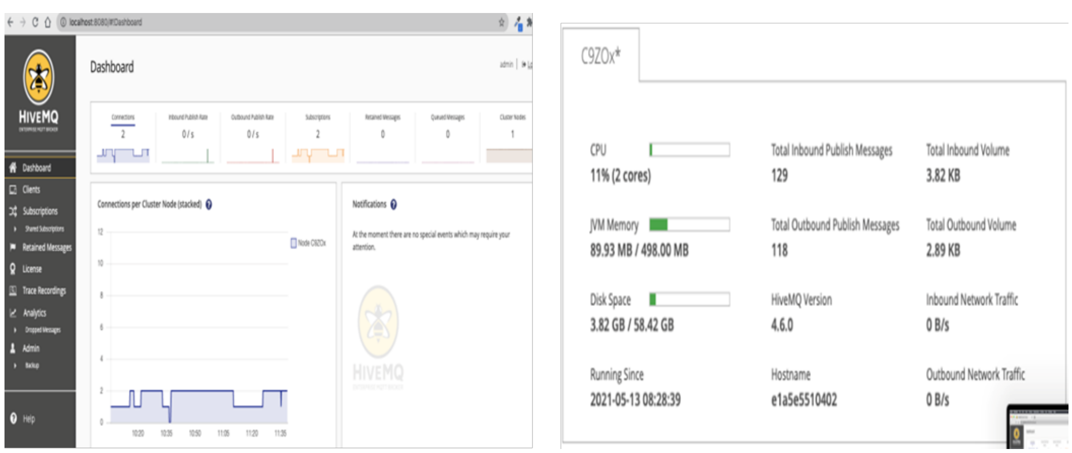

Fig 7. a- HiveMQ simulation software local host, b- Data transmission statistics

Data transmission rate statistics in Figure 7 b is continuously displayed in local host

The Source node is selected in stochastic manner for the transmitting the data of size as cited in the above statistic per cluster Node. The Gateway and one of the node connections is as in the below Figure 8 a.

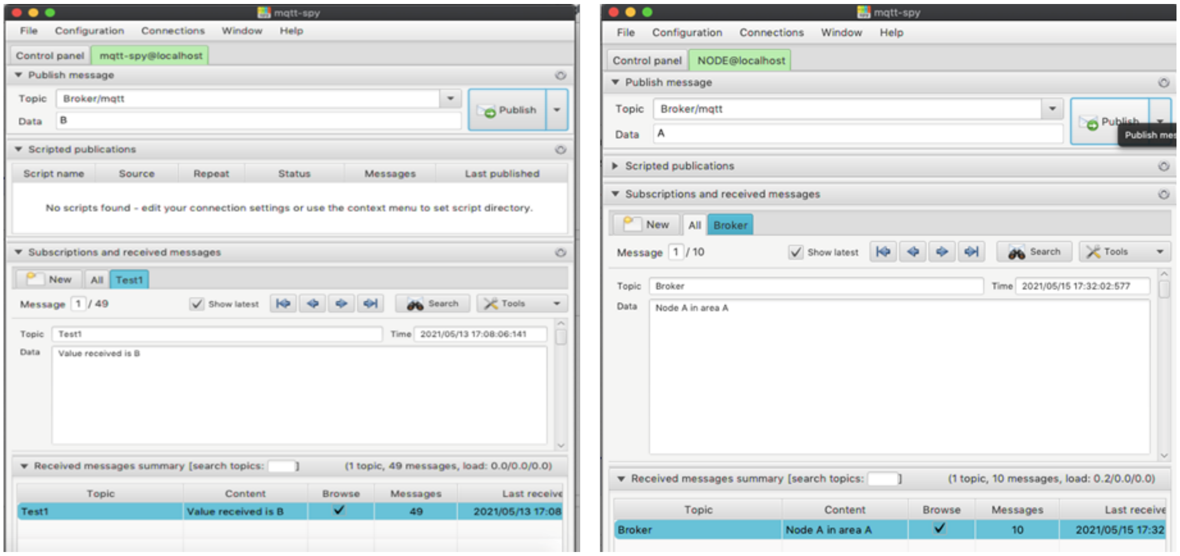

Fig 8. a- Node side: Publish and response with respect to test case respect to test case, b- Node asking Gateway by publishing a message A and response from the Broker script

MQTT-spy is initialized to forward area request packet to base station or intermediate past every 10seconds at the topic address Broker/MQTT and the response comes at the subscribed topic Test1 and path of network has to be chosen with assigned to the intermediate node against the node density and energy levels of the nodes. Node traffic is considered with constant bit rate (CBR). The information packet length is calculated by moss calculation of data transmission, as per the test result cases

$$\text{Size of Outbound data} = \text{Outbound Volume / Total outbound publish messages} \tag{3}$$

= 2.89KB/ 118

= 24 Bytes

$$\text{Size of Inbound data} = \text{Inbound volume / Total inbound publish messages} \tag{4}$$

= 3.82KB / 129

= 29 Bytes

One can question, why the difference between inbound and outbound message difference, this is because of wrong enquiry to the broker or node in battery dead mode.

Approximating the data size will come around 26 bytes, in the vicinity of WSN, the size of data traffic is very negligible, shown in Figure 8 b.

A manual simulation of transfer of data is achieved by using the MQTT-spy, when the operation is performing, one can see the broker receive and transmit of the information by simple deployment of python script. The python script is running continually at the server/ broker machine for the analysis purpose, which can be seen in below Figure 9 a & b.

In Figure 10 a, by default, the MQTT-spy provides the operation of data transfer to the broker is estimated with respect to the time stamp of 10 seconds, 30 seconds and 5 minutes. The graph which determines the messages are popping in particular broker topics.

Figure 10 b shows the energy efficiency comparison in conventional and proposed technique. There are four different techniques of wireless sensor network are considered. In this paper, we have considered node centric, data centric, source initiated and destination initiated techniques are considered. From Figure 10 b, it is cleared that in proposed technique energy efficiency is improved compared to conventional technique. The conventional technique is based on centralised network system. In centralised IoT based wireless sensor network, energy efficiency is degraded[11]. In proposed distributed IoT based wireless sensor network energy efficiency is improved. The conventional centralised system is failed when there is a fault in the central CPU unit, while in proposed distributed system network load is divided among the number of subsection. The energy consumption in centralised system is also increased which leads to the decreased in the energy efficiency[2] [5]. In proposed distributed system, energy consumption is decreased due to the load of the network is divided among different subsection which leads to the increase in the energy efficiency of the proposed technique.

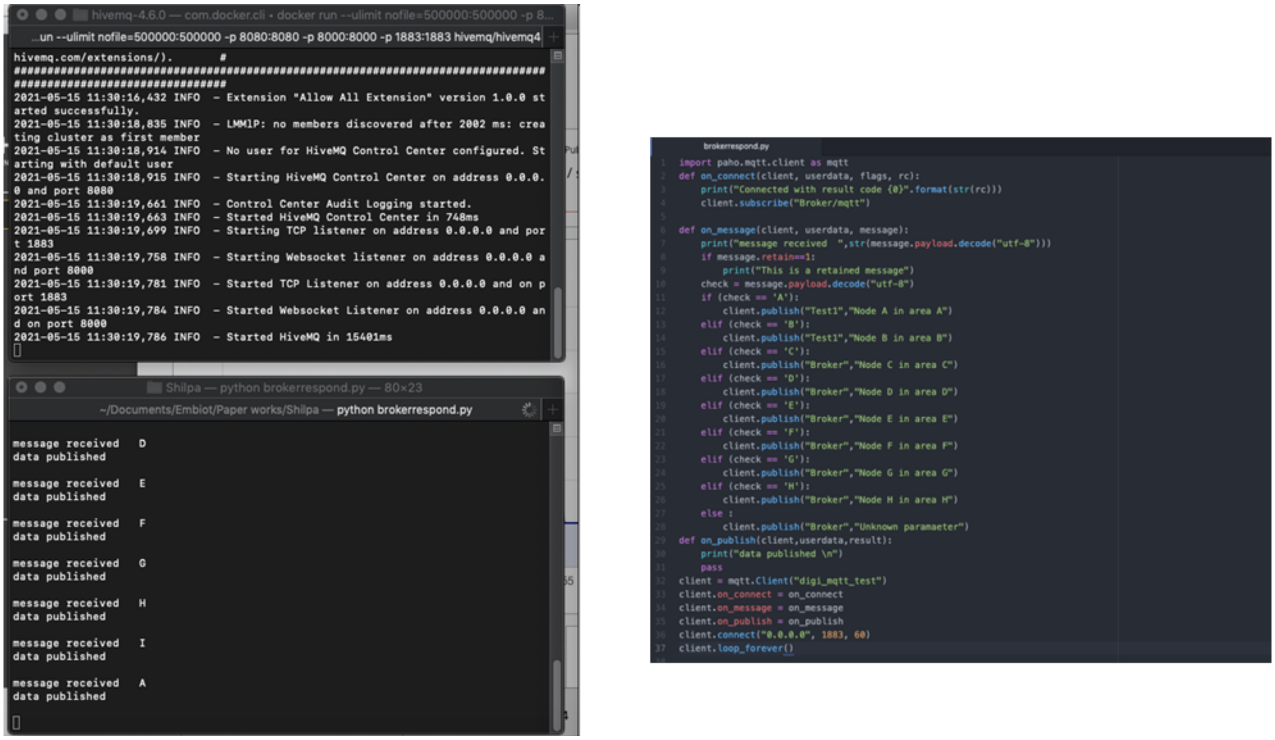

Fig 9. 9a- Server running and response to the node request of A, 9b- Script running in a local host server machine

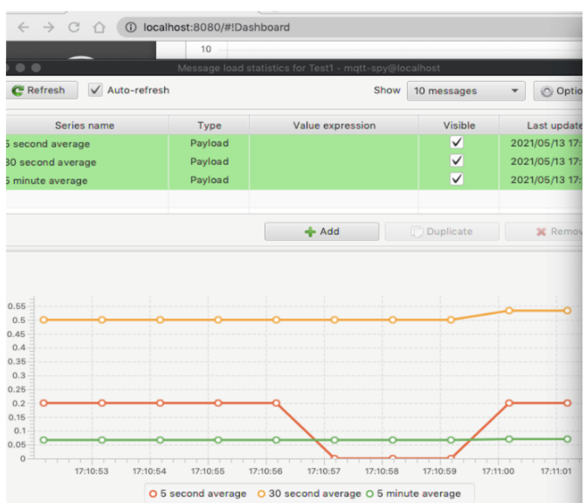

Fig 10. Each topic traffic analyses with respect to 5 seconds, 30 seconds, and 5 minutes

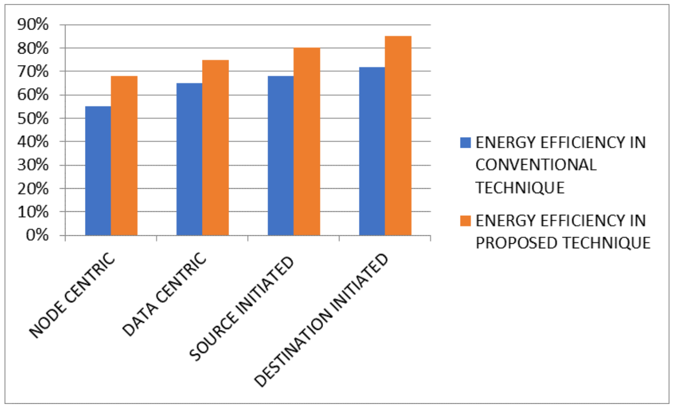

Fig 11. Energy Efficiency Comparison in conventional and proposed technique

4 Conclusion

We designed and simulated the Distributed IoT based wireless network system to analyses the information of nodes roaming in a vicinity of zone area. The framework using moving nodes which will continuously give the information of their presence in open area. We analyse the traffic with respect to 5 seconds, 30 seconds and 5 minutes. We have compared the different protocols of wireless sensor network with respect to the energy efficiency. In proposed technique energy efficiency is increased compared to the conventional algorithm. In node centric routing protocol, energy efficiency is increased from 55% to 68%. In data centric routing protocol, energy efficiency is increased from 65% to 75%. In source initiated routing protocol, energy efficiency is increased from 68% to 80%. In destination initiated routing protocol, energy efficiency is increased from 72% to 85%. The performance parameters like average throughput, average end-to-end delay and packet delivery ratio is also improved in proposed algorithm compared to conventional algorithm. The data transmission and capacity of the complete system purely depends on the central system CPU and its performance.

Acknowledgement

The authors thank the management of PVP Welfare trust, Bengaluru, India, and the support from Department of Electronics and Communication Engineering, Dr. Ambedkar Institute of Technology.

References

1) El-Fouly FH, Khedr AY, Sharif MH, Alreshidi EJ, Yadav K, Kusetogullari H, et al. ERCP: Energy-Efficient and Reliable-Aware Clustering Protocol for Wireless Sensor Networks. *Sensors*. 2022;22(22):8950. Available from: https://doi.org/10.3390/s22228950.
2) Adumbabu I, Selvakumar K. Energy Efficient Routing and Dynamic Cluster Head Selection Using Enhanced Optimization Algorithms for Wireless Sensor Networks. *Energies*. 2022;15(21):8016. Available from: https://doi.org/10.3390/en15218016.
3) Yousefiankalareh A, Najari A, Hosseynzadeh M. Tree-based Routing Protocol in Wireless Sensor Networks using Optimization Algorithm Batch Particles with a Mobile Sink. In: 2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET). IEEE. 2020;p. 1–5. Available from: https://doi.org/10.1109/HONET50430.2020.9322844.
4) Jain S, Agrawal N. Development of Energy Efficient Modified LEACH Protocol for IoT Applications. In: 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN). IEEE. 2020;p. 160–164. Available from: https://doi.org/10.1109/CICN49253.2020.9242619.
5) Sonthalia M, Jha A, Gupta U, Thyagarajan J. A Real Time Implementation of Hierarchical Routing Protocol for IoT based Wireless Sensor Network. In: 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET). IEEE. 2019;p. 512–516. Available from: https://doi.org/10.1109/WiSPNET45539.2019.9032753.
6) Amutha J, Sharma S, Sharma SK. An energy efficient cluster based hybrid optimization algorithm with static sink and mobile sink node for Wireless Sensor Networks. *Expert Systems with Applications*. 2022;203:117334. Available from: https://doi.org/10.1016/j.eswa.2022.117334.
7) Dogra R, Rani S, Kavita, Shafi J, Kim S, Ijaz MF. ESEERP: Enhanced Smart Energy Efficient Routing Protocol for Internet of Things in Wireless Sensor Nodes. *Sensors*. 2022;22(16):6109. Available from: https://doi.org/10.3390/s22166109.
8) Behera TM, Samal UC, Mohapatra SK, Khan MS, Appasani B, Bizon N, et al. Energy-Efficient Routing Protocols for Wireless Sensor Networks: Architectures, Strategies, and Performance. *Electronics*. 2022;11(15):2282. Available from: https://doi.org/10.3390/electronics11152282.
9) Bensaid R, Said MB, Boujemaa H. Fuzzy C-Means based Clustering Algorithm in WSNs for IoT Applications. In: 2020 International Wireless Communications and Mobile Computing (IWCMC). IEEE. 2020;p. 126–130. Available from: https://doi.org/10.1109/IWCMC48107.2020.9148077.
10) Ding Z, Shen L, Chen H, Yan F, Ansari N. Energy-Efficient Relay-Selection-Based Dynamic Routing Algorithm for IoT-Oriented Software-Defined WSNs. *IEEE Internet of Things Journal*. 2020;7(9):9050–9065. Available from: https://doi.org/10.1109/JIOT.2020.3002233.

11) Sharmin A, Anwar F, Motakabber SMA, Hashim AHAA. Secure ACO-Based Wireless Sensor Network Routing Algorithm for IoT. In: 2021 8th International Conference on Computer and Communication Engineering (ICCCE). IEEE. 2021;p. 190–195. Available from: https://doi.org/10.1109/ICCCE50029.2021.9467223.
12) Zhang DG, Qiu JN, Zhang T, Wu H. New Energy-Efficient Hierarchical Clustering Approach Based on Neighbor Rotation for Edge Computing of IoT. In: 2019 28th International Conference on Computer Communication and Networks (ICCCN). IEEE. 2019;p. 1–2. Available from: https://doi.org/10.1109/ICCCN.2019.8847073.
13) Yarde P, Srivastava S, Garg K. A Delay Abridged Judicious Cross-Layer Routing Protocol for Wireless Sensor Network. In: 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS). IEEE. 2019;p. 634–638. Available from: https://doi.org/10.1109/CCOMS.2019.8821743.
14) J CRK, D VK, B MA, Majid MA. Energy-Efficient Adaptive Clustering and Routing Protocol for Expanding the Life Cycle of the IoT-based Wireless Sensor Network. *2022 6th International Conference on Computing Methodologies and Communication (ICCMC)*. 2022;p. 328–336. Available from: https://doi.org/10.1109/ICCMC53470.2022.9753809.
15) A HN, H AA, A A, Kuchansky. Emerging Technology Trends on the Smart Industry and the Internet of Things assisted. In: A Novel Minimized Energy Routing Technique for IoT. 2022. Available from: https://ceur-ws.org/Vol-3149/short3.pdf.
16) Mohamed A, Saber W, Elnahry I, Hassanien AE. Coyote Optimization Based on a Fuzzy Logic Algorithm for Energy-Efficiency in Wireless Sensor Networks. *IEEE Access*. 2020;8:185816–185829. Available from: https://doi.org/10.1109/ACCESS.2020.3029683.
17) Pang L, Xie J, Xu Q. Neural Network-Based Routing Energy-Saving Algorithm for Wireless Sensor Networks. 2022. Available from: https://doi.org/10.1155/2022/3342031.
18) Xu C, Xiong Z, Zhao G, Yu S. An Energy-Efficient Region Source Routing Protocol for Lifetime Maximization in WSN. *IEEE Access*. 2019;7:135277–135289. Available from: https://doi.org/10.1109/ACCESS.2019.2942321.
19) Dogra R, Babbar H, Krah D. Energy-Efficient Routing Protocol for Next-Generation Application in the Internet of Things and Wireless Sensor Networks Roopali Dogra, Shalli Rani, Himanshi Babbar, and Daniel Krah. *Wireless Communications and Mobile Computing*;2022. Available from: https://doi.org/10.1155/2022/8006751.
20) Arya G, Bagwari A, Chauhan DS. Performance Analysis of Deep Learning-Based Routing Protocol for an Efficient Data Transmission in 5G WSN Communication. *IEEE Access*. 2022;10:9340–9356. Available from: https://doi.org/10.1109/ACCESS.2022.3142082.
21) Samarji N, Salamah M. ESRA: Energy soaring-based routing algorithm for IoT applications in software-defined wireless sensor networks. *Egyptian Informatics Journal*. 2022;23(2):215–224. Available from: https://doi.org/10.1016/j.eij.2021.12.004.
22) Sheth SD, Verma Y, Kaur G, Chanak P. An energy optimized routing algorithm for IoT-enabled WSN. *2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT)*. 2021;p. 308–312. Available from: https://doi.org/10.1109/CCICT53244.2021.00064.
23) Shaha S, Jadejaa A, Doshi N. An Analytical Survey of Energy Efficiency in IoT Paradigm. *Procedia Computer Science*. 2022;210:283–288. Available from: https://doi.org/10.1016/j.procs.2022.10.151.
24) Gupta SK, Singh S. Survey on energy efficient dynamic sink optimum routing for wireless sensor network and communication technologies. *International Journal of Communication Systems*. 2022;35(11):5194–5194. Available from: https://doi.org/10.1002/dac.5194.
25) Karabekir B, Aydin MA, Zaim AH. Energy-Efficient Clustering-Based Mobile Routing Algorithm For Wireless Sensor Networks. *Electrica*. 2021;21(1):41–49. Available from: https://doi.org/10.5152/electrica.2021.20035.