RESEARCH ARTICLE

Adaptive Switching Based Data-Communication Model for Internet of Healthcare Things Networks

MEHWASH WEQAR[1], SHABANA MEHFUZ[1], (Senior Member, IEEE), DHAWAL GUPTA[2], AND SHABANA UROOJ[3], (Senior Member, IEEE)

[1]Department of Electrical Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi 110025, India
[2]Chase India, Avian WE Group, New Delhi 110024, India
[3]Department of Electrical Engineering, College of Engineering, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

Corresponding author: Mehwash Weqar (mehwash.weqar@gmail.com)

ABSTRACT The Internet of Things (IoT) is a network of smart sensory objects. These objects collect environmental data and communicate to exchange this gathered data without human intervention. IoT has evolved as a revolutionary technology for over a decade. It is currently, widely applied in a variety of applications like Internet of Vehicles (IoV), Internet of Healthcare Things (IoHT), and the Internet of Everything (IoE). IoHT is one of the most beneficial and significant IoT applications. The quality of the connection in an IoT network is governed by the application layer communication protocol. Application type has a significant impact on the preference of protocol selection. In this paper, the performance of CoAP and MQTT-SN is compared. Based on the performance analysis it was concluded that in case of high traffic conditions network congestion occurs on the medical broker of MQTT-SN, which lowers the network efficiency. A framework is proposed to achieve reliability and time optimization in larger sensor-based healthcare networks. An adaptive switching-based data communication model has been designed. In the proposed model, we have enabled IoHT network to run two application protocols in parallel. The adaptive switching algorithm allows to switch between the two available protocols based on the status of the network condition. Network simulation has been performed using NODE-RED. This tool is used to test the proposed framework in different scenarios. In the end it was concluded that during network congestion conditions at medical broker of MQTT-SN, the adaptive switching algorithm allows the network to switch to CoAP connection for the time efficient and reliable transmission in the IoHT network.

INDEX TERMS IoT, Internet of Healthcare Things (IoHT), application layer protocols, MQTT, COAP, NODE-RED.

I. INTRODUCTION

The Internet of Things (IoT) is a network of actual physical things, gadgets, cars, buildings, and many other things with electronics, software, and sensors, embedded in them and have the capability to connect to a network, without the need for human intervention. These objects collect the environmental data and communicate to exchange this gathered data.

The associate editor coordinating the review of this manuscript and approving it for publication was Jose Saldana.

Furthermore, this gathered data is examined and then the specific action is performed as per the application required.

Technology has made it feasible for machines to connect with one another always at anytime, anywhere and as well as with people too. It has really been rapidly encroaching on people's homes and other locations [1].

The exponential growth in IoT technology has resulted in the interconnection of a vast number of devices or objects. These devices are of different make, supporting different technologies which give rise to a completely heterogeneous

environment [2]. To support seamless interconnection these heterogeneous devices should be able to support heterogeneous networking, allowing billions of devices to communicate with each other efficiently [3]. This paves the way for new heights of interconnectivity resulting in smarter, efficient and advanced applications like Internet of Vehicles (IoV), Internet of Healthcare Things (IoHT) and Internet of Everything (IoE).

Healthcare is an essential aspect of existence for humanity. Due to the huge demand for resources, maintaining an effective healthcare system for an ever-growing population has become increasingly challenging. Numerous studies have been conducted to raise the standard of healthcare and patient support [4].

The last ten years have seen the growth of various Internet of Things-based healthcare applications [5], [6]. IoT seems to be significant to the healing process for patients and the work of medical professionals. It comprises of a framework that interacts with network-connected devices, apps, and systems that can assist patients and physicians in monitoring, recording, and documenting patients' vital statistics and health data [7].

A variety of clinical gadgets, sensors, and imaging equipment can be regarded as intelligent devices in the context of healthcare, building the foundation of the IoT. Healthcare systems are anticipated to save costs, ease strain on the healthcare infrastructure, improve life quality, and enhance user satisfaction [8].

IoT perceives its potential for resolving current issues in healthcare monitoring systems with the assistance of various developed technologies, including wireless body area networks, wireless sensor networks, implants, and wearable sensors. It can contribute to improving service quality by performing remote monitoring and sending notifications while lowering healthcare expenses. By measuring and analysing a patient's vital signs, the Internet of Things (IoT) gives hospitals and clinicians a quick and easy approach [9] Thus, now one of the most significant IoT applications is in the field of healthcare [10]. A significant impact on the economic growth will come from IoT-based smart healthcare by (2025).

In order to enable all these smart applications, to work smoothly, these smart sensory objects should be able to communicate effortlessly without any hindrance [11]. There are various existing and developing communication protocols that enable these devices and servers to interact with one another in new, more integrated ways [12], [13], [14].

Application type has a significant impact on the preference of protocol selection. For various IoT applications like home automation, vehicle-to-vehicle communication in IoV, and wearable technology, many protocols, such as Advanced Message Queuing Protocol (AMQP), Extensible Messaging and Presence Protocol (XMPP), and Lightweight Machine-to-Machine (LwM2M) exist. For Machine-to-Machine (M2M) communication, two specialized protocols are Message Queue Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) [15]. In the modern IoT

applications, CoAP and MQTT are two of the most significant and popular protocols. Although certain other protocols have also been utilized, both have significance when it comes to machine communication. Concerning the application layer, there isn't a single protocol that supports all applications [16]. The choice of protocol is highly situation-dependent.

In this paper, the performance of two application layer protocols is compared, that are Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT)in an Internet of Things (IoT) scenario. Then based on the performance analysis an Adaptive switching-based data communication model has been designed. Detailed contribution of the proposed work has been provided in the following sub-section.

A. CONTRIBUTION OF THE PROPOSED FRAMEWORK

In the proposed framework, we have enabled IoHT network to run two application protocols in parallel. Here the network can adaptively switch between the two applications based on the network condition. The following is the contribution as well as utility of the framework proposed in this paper.

- Design and implementation of a novel framework for the IoHT network.
- Availability of two constrained application protocols namely CoAP and MQTT. This in turn increases the efficiency of the IoHT network.
- A Switching algorithm has been designed which allows to switch between the two available protocols based on the status of the network condition ie In case of large-size messages having payloads of more than 1024 byte, MQTT-SN will be used as the default transmission link of the proposed framework. And in case of network congestion occurring on the medical broker of MQTT-SN, the switching is carried out from the default protocol of the network i.e., MQTT-SN to CoAP.
- This provision of switching increases the IoHT network availability.
- This increases network efficiency in case of heavy network traffic.
- Time efficiency of the proposed framework has been studied and analysed.
- Various explanations and validations have been made for theoretical and experimental findings.

The remaining portions of this paper are arranged as follows: Section II discusses the working architecture of the IoT constrained network application protocols. Section III provides a performance comparison of CoAP and MQTT and Related work. Section IV discusses the contribution of the proposed work. Section V describes the working of IoHT-Net topology. Section VI gives the details of the working architecture of the proposed Framework. Section VII gives the simulation setup of the proposed network. Section VIII analyses the experimental results and finally Section IX concludes the paper giving the future scope of the proposed work.

II. IoT-CONSTRAINED NETWORK APPLICATION PROTOCOLS

The application layer is the internet protocol stack's top layer. It is the layer where the application protocols are found. Applications of various end systems use an application layer protocol to exchange data packet information with one another [17], [18].

For the IoT network, MQTT and CoAP are appropriate lightweight application layer protocols because they support the constrained network requirement of IoT networks. The first significant issue with the IoT network is related to an enormous number of connected nodes generating huge network traffic. So, to overcome this traffic problem these protocols make the network packet smaller in size thus in turn preventing the network bandwidth from being saturated.

It is not only sufficient to manage many devices. The performance level of the IoT network is also a significant quality. By limiting the data packet size, the resource constrained lightweight protocols decrease the volume of data the CPU processes, thus resulting in less battery consumption and decrease in the storage space requirement. Hence, the IoT's lifecycle enhances considerably.

A. ARCHITECTURE OF MQTT IN IOT APPLICATION

The Message Queuing Telemetry Transport (MQTT) protocol is a publish/subscribe-based messaging protocol. It is a lightweight protocol due to the minimal code size of all of its transmitting messages with a goal of monitoring physically dispersed sensors and actuators. Andy Stanford-Clark of IBM and Arlen Nipper of Arcom designed MQTT in 1999 [19]. The Organization for the Advancement of Structured Information Standards (OASIS), formalized MQTT in 2013 [20]. It was the goal of MQTT's designers to develop a small, high - throughput protocol that supported several levels of Quality of Service (QoS) and was data-interoperable.

The MQTT paradigm uses TCP as its transport layer protocol. Despite being intended to be lightweight, MQTT has two shortcomings for devices with resource limitations. Each MQTT client must support TCP, and they should maintain an active link to the broker. This is a concern in some contexts when packet loss is severe or where computational resources are limited. In order to function properly on wireless networks, MQTT-SN (MQTT for Sensor networks) was developed, which is a lighter version of previously designed MQTT. It specifies a UDP mapping of MQTT and adds broker support for indexing topic names and addresses both flaws [21]. The basic functioning of MQTT-SN is almost identical to MQTT.

The protocol's basic architecture as shown in Figure 1, consists of three main components called subscriber, publisher, and broker, is also known as publisher/subscribe or client/server model. A broker facilitates the message distribution between the publisher and subscriber not even directly revealing the other party's presence or capabilities [22]. It accomplishes this by separating the sender (publisher) from the receiver (subscriber).
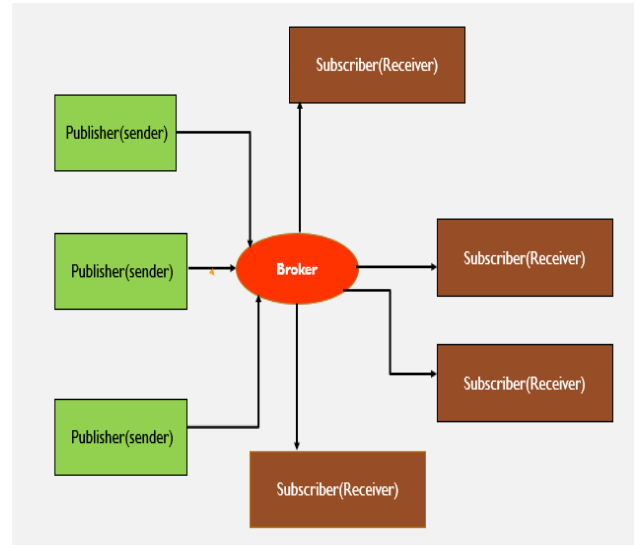

FIGURE 1. Basic architecture of MQTT.

MQTT is a message centered protocol. These protocols transmit data in separate groups or blocks, where one communication stops and another begins, can be determined by the data recipient. Each message is a unique piece of data that is unknown to the broker. Each data packet transmitted by the publisher is sent to a specific address called as a topic. Subscribers can sign up for several topics. All incoming messages are filtered, then distributed appropriately by the broker. Hence, each message sent to a topic is delivered to every client who has subscribed to it [23]. A message's components are a fixed header (2 bytes), an optional variable header, and a payload that can only be 256 megabytes (MB). This is a relatively high limit for the entirety of M2M and IoT applications, and most customers would likely never transmit such a large payload containing a message. It facilitates multi-cast transmission, which is also known as many-to-one or many-to-many communication. Hence this is suitable for most of the IoT application scenarios like the Internet of Healthcare Things (IoHT) Network.

Based on how data is received and delivered between the broker and publisher, there are three QoS profiles: QoS0, QoS1, and QoS2. These three models are based on how data is received and delivered between the broker and publisher [21]. In the IoHT framework, any of the three Quality of Service (QoS) profile models is utilized for the interchange of patient data.

The broker is a device that mediates communications between devices in MQTT [23]. All communications from publishing clients are acquired by the broker's software, which then forwards them to subscribers [24]. It maintains communication with stable customers. Thus, it manages all the multicast connections and so the brokers may sometimes behave as a bottleneck due to overloading of messages, which may result in message delay, low throughput and finally single point failure. This in the end may lead to lowering

network performance. Thus, the designers are required to determine the performance improvement alternatives for such network failure situations [25].

B. ARCHITECTURE OF COAP IN IOT APPLICATION

CoAP -Constrained Application Protocol is a client-server protocol that operates at the application layer. CoAP was initially developed by Constrained RESTful Environments (CoRE) working group of the Internet Engineering Task Force (IETF), which primarily supports applications that are Machine to Machine (M2M), Sensor to Machine (S2M), or Sensor to Sensor (S2S). The CoAP protocol was standardized in 2014.

This protocol is based on a request/response paradigm. It is built using the Representational State Transfer (REST)framework. REST is an architecture built on web standards that communicates data using HTTP. That is why CoAP is also called a RESTful web transfer protocol for networks and nodes with limited resources.

This protocol is suited for restricted networks, such as low-power wireless personal area networks, restricted terminals with minimal RAM or CPU ability, and other similar situations. [26]. A portion of HTTP features are used by CoAP. The resource limitations of many IoT devices have led to redesigning certain HTTP features. By altering HTTP methods, protocols can be created especially for IoT applications. [27]. The Transmission Control Protocol (TCP) is the core focus of HTTP. The resource limitations of many IoT devices have led to redesigning of certain HTTP features. By altering some of the HTTP methods, protocols supporting IoT systems are created. The ineffective traffic management issue and significant overhead are two of the many problems associated with TCP-based communications. Multicast roaming is also not facilitated by TCP., whereas CoAP uses User Datagram Protocol (UDP), which allows connectionless datagrams for communication between clients and servers thus resulting in much decreased overhead and enhanced multicast capability.

Many constrained IoT applications can support only lightweight and low energy-consuming communication techniques. Therefore, UDP is quite helpful in supporting these constrained network requirements. CoAP has two sub-levels: the communications sub-level and the request/response sub-level. The messaging sub-layer offers communication via the UDP transport layer while detecting duplications. However, REST communications are handled by the request/response sub-layer. Thus, CoAP was designed mainly to allow these IoT devices to use REST services over UDP in order to comply with the network resource limitations [28]. Figure 2 shows the basic architecture of the CoAP protocol.

CoAP supports 2 basic models of request–response, (i) Confirmable and (ii) non-confirmable. Confirmable is a reliable mode of one-to-one communication whereas non-confirmable is an unreliable mode of one-to-one communication. A combination of confirmable and non-confirmable
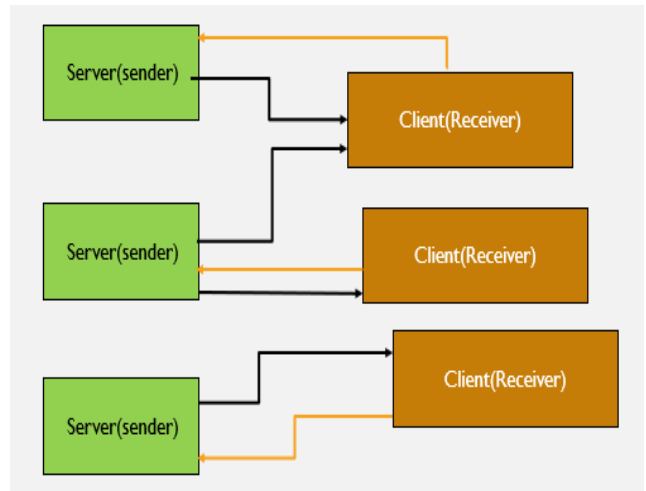

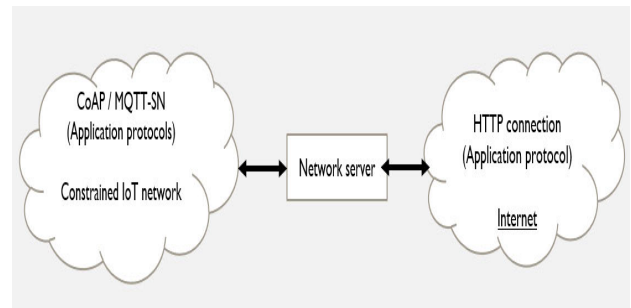**FIGURE 2.** Basic architecture of CoAP.

FIGURE 3. Basic IoHT network architecture.

messages ensures CoAP's reliability. The messages delivered between clients and servers primarily depict three aspects of reliability namely: network reliability, communication reliability, and message-sharing reliability.

UDP has a low overhead need for transmissions, enabling shorter start-up times and longer sleep phases thus, resulting in less power consumption and eventually longer battery life of IoT devices in the network. CoAP allows smaller size packets which have an upper bound of 1152 bytes for message and 1024 bytes for message payload in transmission. Hence it is more suitable for applications like IoHT, where generally smaller size messages of some few bytes are transmitted. Figure 3 shows a common IoHT network architecture. Typically, a CoAP version adds its own maximum packet length option. Because of the lower size of data packets, the transmission sessions are smaller and faster. An unfavorable condition of packet fragmentation occurs when messages to be transmitted are longer than an IP Data packet.

However, this means that it is not very suitable for applications where transmission messages are larger in size, like in case of vehicular networks.

III. PERFORMANCE COMPARISON OF COAP AND MQTT AND RELATED WORK

The IoT application layer protocols are necessary to enable the most potential IoT-based smart healthcare application

TABLE 1. Characteristic difference.

	MQTT-SN	COAP
Application Layer	Single Layer	Single Layer with two Conceptual layers (Message and Request /Response)
Reliability	Three Quality of Service levels	CON/NCON messages, ACK and Retransmission
Architecture	Publish/Subscribe	Request/Response, Resource/observe

TABLE 2. Comparative analysis of MQTT-SN and CoAP.

COAP	MQTT-SN
CoAP is more efficient in terms of message overhead	MQTT-SN is more efficient in terms of client complexity
Have one-to-one communication	Communication via broker
there is no single point of failure	single-point-of-failure problem exists
Preferred for security	Preferred for speed
More throughput and low latency in high-traffic conditions	Less throughput and high latency in high-traffic conditions

domains for patient monitoring, treatment, and diagnostics. CoAP and MQTT are the two primarily used protocols, in IoT networks to improve application like telemedicine, medical management, chronic illness identification, tracking of disease-causing micro parameters, real-time health monitoring, smart wearable devices, assisted senior healthcare, and chronic disease screening [29].

Both protocols are specifically appropriate for different implementational conditions. It is highly difficult to choose the most suitable protocol for each application. Table 1 shows the characteristic difference between the two protocols.

Many authors in [21], [23], and [30] have compared and analysed the working of these two protocols in IoT healthcare networks and came up with a conclusion that both protocols have their own advantages and disadvantages. Despite the many advantages and simplicity of MQTT-SN methodology in WSN, it creates a single point-of-failure issue. This means that communication in the entire network or the portion of the network handled by the broker suffers if there is congestion in this component of the network and thus results in message delay or complete loss of communication if the broker goes down in a severe case.

However, message-centric communication, which is provided by CoAP, heavily relies on communication between individual network nodes, that is one-to-one communication. As a result, there is no single point of failure, but in turn, it allows only smaller messages to be transmitted.

Additionally, CoAP is chosen when security requirements are strict while MQTT-SN is preferred for speed [31]. It was mentioned in [32] that when there is heavy traffic and a weak link, MQTT performance is affected badly as compared to CoAP in terms of throughput and latency.

The comparative analysis which has been carried out in this work for the two application protocols namely CoAP and MQTT-SN has been shown in Table 2.

The researchers [33] provide an investigation of the relationship between MQTT and CoAP in situations with diverse network conditions. The analysis demonstrates that the two

protocols differ in performance under several scenarios, such as during heavy network traffic CoAP performs well with some modifications. The chance of packet loss increases during network congestions. They concluded to implement MQTT when there is a single device and low throughput in network. Thus, the choice of a suitable application protocol emerges as one of the challenges for researchers over the time period. Hence to overcome this limitation the author in [34] studied and pointed out that varying protocols have varying performance characteristics within distinct categories, making them appropriate for various application types. They have proposed that the integration of these protocols is important.

Studies have found that in real-world IoT applications, there may be many fluctuating network circumstances as well as other difficulties including network load, energy demand, delay, etc. [35]. There isn't a particular protocol that could be fairly and appropriately put into operation and serve as a solution to all these problems.

Authors [36] have compared and analysed application layer protocols i.e. MQTT and MODBUS TCP which are running alongside simultaneously. They encourage the implementation of the proposed combination of protocols in industrial IoT applications. Another architecture of the IoT middleware was proposed in [37] which evaluates and compares the widely-used protocols in terms of the publish and subscribe timings, network traffic, and effectiveness. To overcome the previous shortcoming a framework for IoT communication has been described in [38], enabling smooth interactions between devices. The protocol translation is the main emphasis of this approach. However, the little rise in the consumption of energy is a minor drawback of this framework. The aforementioned proposals promote the integration of various IoT platforms. Working on a similar concept another author in [39] has examined some Internet of Things platforms that unify application layer protocols using open-source middleware frameworks into a single, functional system. This approach proposes a combination and integration of diverse application layer protocols using a middleware
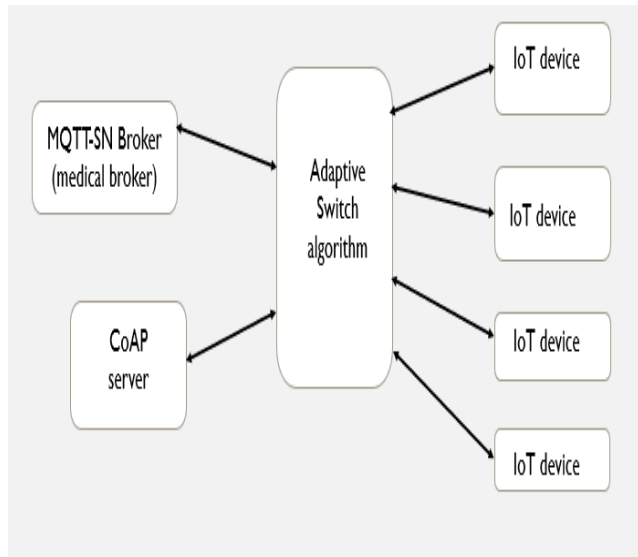
FIGURE 4. Block diagram of the proposed framework.

structure. But in case of heavy network traffic, extra delays in message delivery time along with additional complexities were recorded due to the involvement of a third-party server acting as a message broker.

Thus, to overcome the network limitations in the applications discussed earlier, we have proposed the **Adaptive Switching based data-communication model for IoHT networks.** In the proposed approach the system can run the two application layer protocols simultaneously based on conditional switching. The two constrained applications layer protocols i.e., CoAP and MQTT-SN will be available in the network to switch upon, based on the network requirement. As a result, there is no longer any compromise on the network performance that could arise from the availability of just one protocol.

IV. ARCHITECTURE OF THE PROPOSED FRAMEWORK

Considering the analysis given in Table 2, it has been concluded that MQTT-SN is best suitable for multicasting large data packets in low-traffic environments and CoAP is best suitable for transmitting small data packets in high-traffic conditions. Thus, to avail the advantages of both protocols we have proposed a framework that allows to use of both protocols in an application. Figure 6 shows the block diagram of the proposed framework. The proposed framework is based on the switching algorithm, which allows switching between the two protocols, CoAP and MQTT based on the application demand.

Figure 4 represents the block diagram of the proposed framework. In this scheme, all the IoT devices which are responsible for sensing and sending data are connected to the Adaptive switch which is in turn connected to the MQTT-SN broker and CoAP server. This is based on the network demand which is accordingly judged by the Adaptive Switching function.

A. WORKING OF THE ADAPTIVE SWITCHING ALGORITHM IN THE PROPOSED ARCHITECTURE

Figure 5 shows the flowchart of the Adaptive Switching function. This is a common adaptive switching algorithm that is suitable for commonly available IoT applications such as Smart Agriculture, and Internet of Vehicles (IoV). The working of the general adaptive algorithm function is such that the switch function decides which protocol to choose for transmission based on the IoT application demand. This function checks six conditions that are:

(1) **Type of communication**: - the protocol selection is based on the type of data transmission preferred in the application. If the application demands choice-based communication, then choose MQTT-SN, or else choose CoAP.

(2) **Type of document sharing: -** If the application requires M: N (many to many) sharing of data in the network then MQTT-SN is chosen, else CoAP is chosen for direct 1:1 sharing of data.

(3) **Reliability: -** If reliability is an essential requirement of the application network, then the preferred choice for protocol is CoAP, because, at times in case of high network traffic, a single point of failure is possible, in MQTT-SN at the broker.

(4) **Power consumption: -** CoAP protocol is chosen when the network is constrained over power consumption [35].

(5) **Data transfer size**: - protocol selection is based on the default size of the message transmitted in the network. CoAP protocol is chosen if the smaller size messages are transferred in the network, else MQTT-SN is selected for larger-size message propagation.

(6) **Implementation overhead: -** CoAP incurs less implementation overhead as compared to MQTT-SN [35]. Therefore, CoAP is chosen when the IoT application is checking for minimum overhead to implement the clients in a network.

V. THE IoHTNET TOPOLOGY

The organisation of various components in an IoT healthcare system is referred to as the IoHTNet topology, which shows illustrations of exemplary frictionless healthcare facilities. There exist many IoHT topologies based on the arrangement of IoHT network components. IoHT application requirement governs the organisation of components in the network. Many such IoHTNet topologies have been proposed over the decade [40], [41], [42], [43]. Thus, a commonly used IoHT Model comprises of remote sensing nodes, a network, and routing algorithms at various levels with accompanying infrastructure, memory, and a cloud infrastructure.

A scenario of the Internet of Healthcare Things network is depicted in Figure 6. It is an IoHTNet topology where a person's medical status and vitals are collected and recorded using wearable sensors and portable medical gadgets that are fastened to the patient's body. Data from numerous sensors
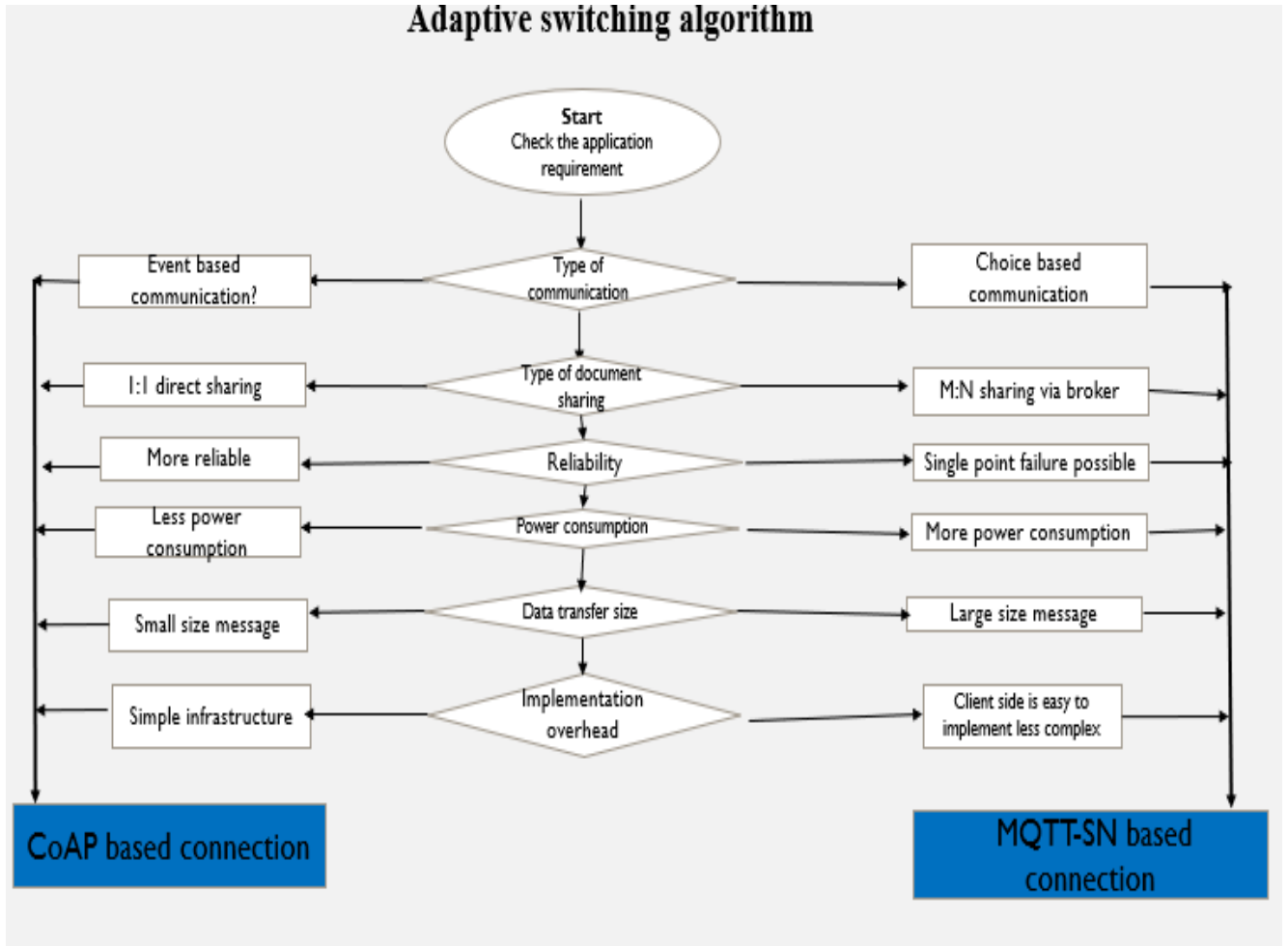
FIGURE 5. Flowchart of the general adaptive switching algorithm.

and machines is then transmitted over the network via a gateway to the desired medical service provider. These service providers can be a medical cloud or any medical analytics Centre, where this gathered data is then used for maintaining medical records after being evaluated and reviewed. Healthcare providers can monitor patients from any possible remote site and take appropriate action based on analysis and consolidated medical records.

Fig. 7 shows a diverse cluster of sensors creating a body sensor network [44]. When the human body is closely connected with lightweight sensors which are embedded in wearable devices, it is called as body sensor network. These sensors assemble massive volumes of data from vital indicators such as blood pressure (BP), body temperature, electrocardiograms (ECG), and oxygen saturation. etc.

Nowadays, as healthcare service providers are connected to the Internet, they have several systems to worry about and are facing an increased number of vulnerabilities that include security issues, heterogeneity issues, low network throughput, time delays, network congestions, and network

failure. These are some of the common problems faced in many healthcare network scenarios.

In this work, the main focus is to improve the throughput of a general IoHT Network. The throughput of a network depends on the amount of data transmitted and the time taken to deliver that data. Therefore, in order to gain high throughput, we have to choose an appropriate application protocol for network connection, which does not suffer from network delays.

The proposed adaptive switching algorithm is then further modified to be suitable for IoHT application. Figure 8 shows the flowchart of the Adaptive Switching Algorithm which is specific to the IoHT network. In this scenario, the algorithm first checks the size of the message payload, if it is greater than 1024 bytes then MQTT-SN protocol is chosen for message transfer, otherwise CoAP is chosen for message transfer. Generally, in IoHT networks the message payload size is larger than 1024 bytes, which is why in most of the cases MQTT-SN protocol is chosen for message transmission, we have compared the time taken and message payload size by simulating the IoHT network in NODE RED and
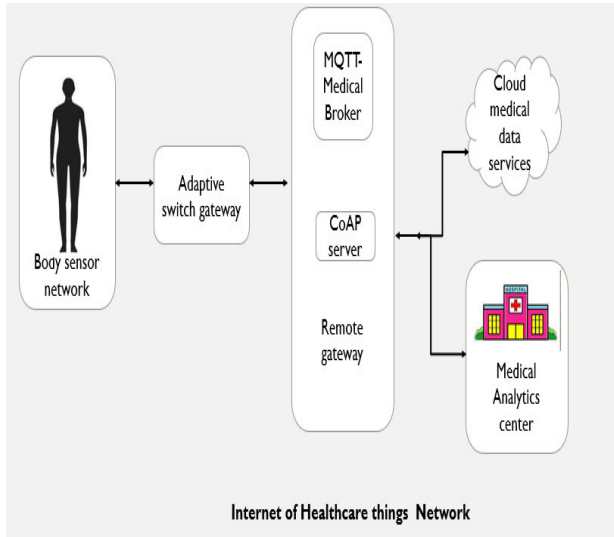
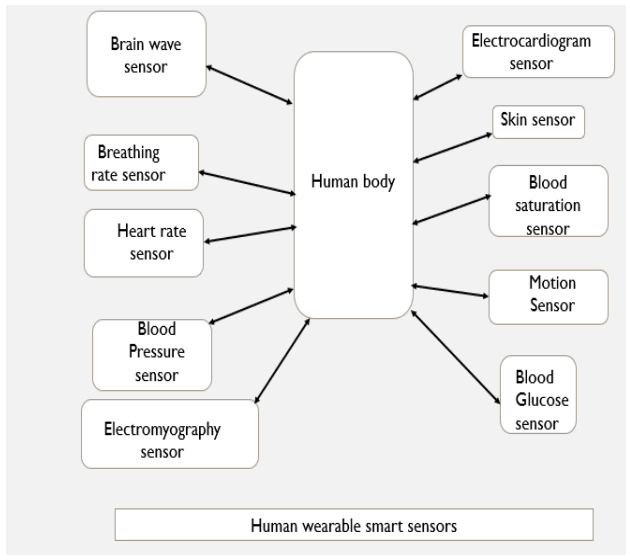**FIGURE 6.** Internet of healthcare things network.

FIGURE 7. Body sensor network.

then concluded that as the message payload size increases more than 1024 bytes, time taken in message transfer using COAP protocol shoots up., while this doesn't happen with the MQTT-SN protocol. That is why most of the time MQTT-SN is chosen.

During the message transmission in the IoHT network, an enormous number of messages travel in a network. Sometimes MQTT-SN's medical broker may face congestion, which in turn may result in a delay in message transfer in the IoHT network. This will result in a decrease in the overall throughput of the network. During this time if a medical emergency occurs then due to large message delays in the network, the medical analytical center may not be able to receive the alert message on time which may lead to any unwanted condition. Hence to avoid any such circumstances
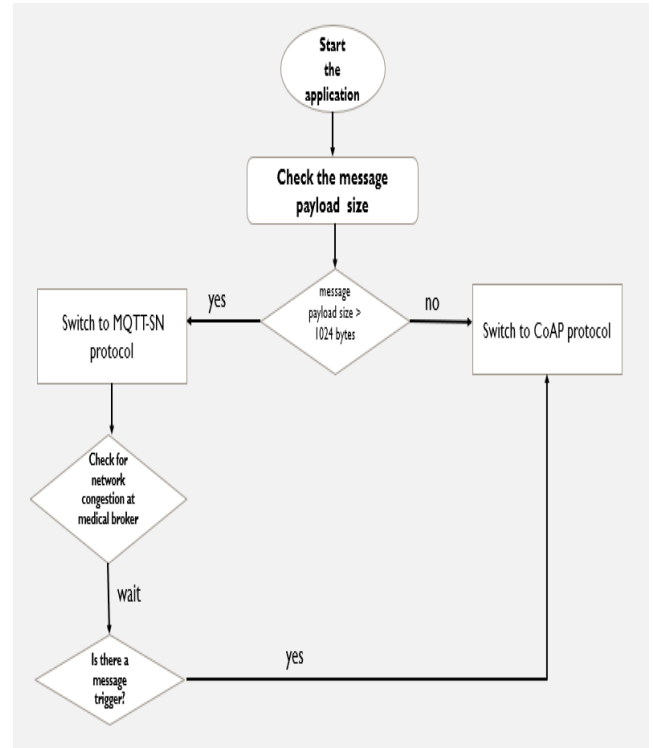

FIGURE 8. Flowchart of IoHT application-specific adaptive switching scenario.

from occurring, the conditional switch algorithm switches to CoAP to transfer trigger messages quickly and accurately to the receiver.

VI. SIMULATION SETUP

The investigation aims to assess the durations of end-to-end communication transmission. IoHT network simulation has been performed in NODE RED. It is a tool for Network-flow development. Here Node.js is used to build the runtime. JSON file format is used to store the flows that are created in Node-RED.

The proposed IoHT network with an adaptive switching function has been simulated on NODE RED. The timer function present in NODE-RED is used to record the time taken to transmit a message from sender to receiver. All the network simulation figures of the IoHT network have fixed color coding. Purple color represents the MQTT-SN nodes of the sender, receiver, and broker. The orange color represents the CoAP nodes of the sender and receiver. The light green color represents timer function nodes.

Figure 9 shows a small network of 1 sender and 1 receiver. As shown in Figure 9 a time function is attached at each link in the network to record the time of each transmission link. A switch function is used to switch between the two protocols i.e., CoAP and MQTT-SN. This switch function is based on the adaptive switching algorithm which examines for network congestion and allows switching.
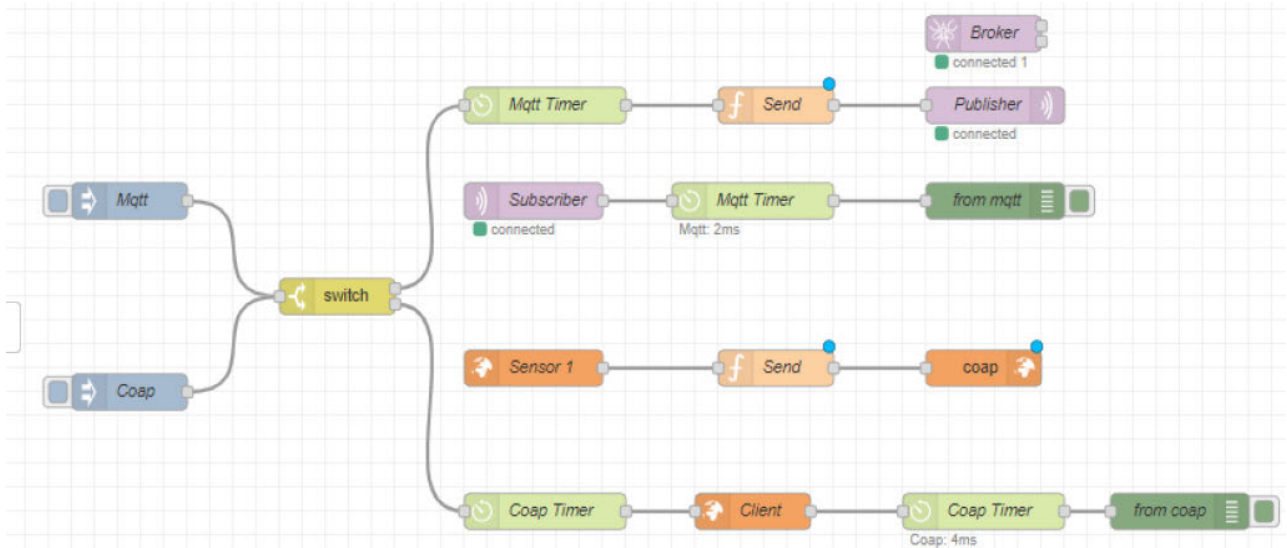
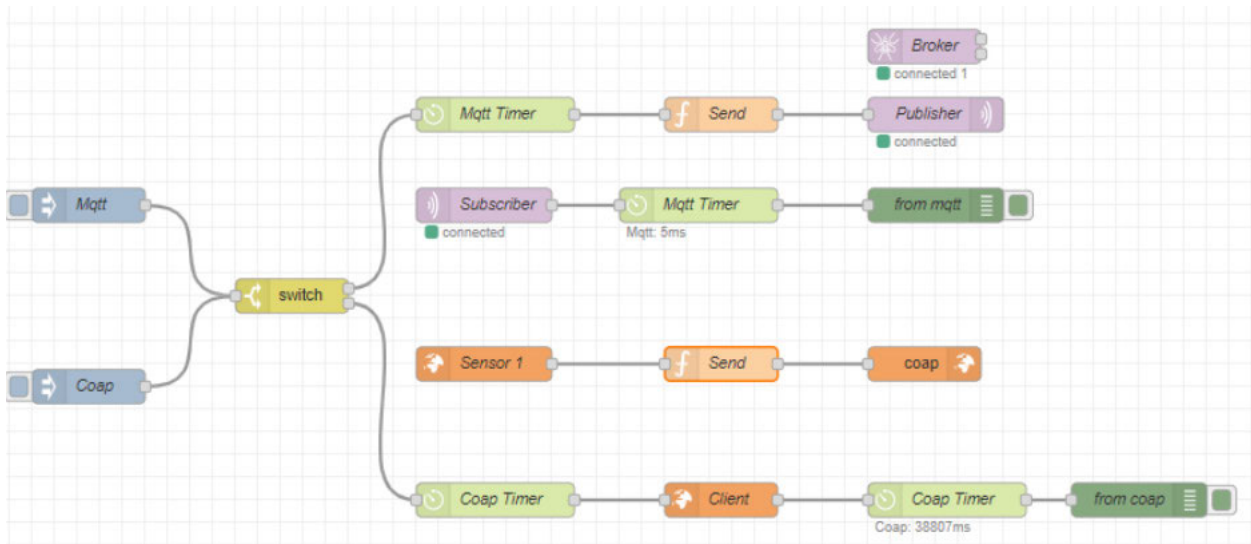**FIGURE 9.** Network of 1 sender and 1 receiver.

FIGURE 10. Network of 1 sender and 1 receiver showing payload exceeding max - threshold value for CoAP.

The simulation of the proposed framework shows that the time taken on each link is recorded. The condition of max–payload–support by each protocol link was also tested on the network. As discussed earlier it was studied that on increasing the payload size of the message from 1024 bytes a steep increase in transmission time on the CoAP link is recorded. As shown in Figure 10, for a message payload of more than 1024 bytes, the network link of MQTTN has recorded a transmission time of 5ms, whereas the transmission time on the CoAP link was recorded to be 3887ms, which was very high.

After this, the proposed network setup in the NODE- RED simulation window is tested for next scenario of increasing traffic on the network paths. It was analyzed that in the case of a smaller number of sender and receivers MQTT-SN con-nection path takes less amount of time but as the number of sender nodes and receiver nodes increases, the time taken by a message to reach a receiver increases. This has been shown in Figure 11.

Figure 11 shows the proposed framework with 3 senders and 3 receivers. In this case, while analysing the transmission time in the MQTT-SN connection path it was noted that the first receiver got the message in 8ms, the second receiver received the message in 11ms, and the third received it in 12ms, so a delay of 4ms recorded from first to third receiver was present. While recording the transmission times in the CoAP communication path it was found that the message delivery time had a delay of 2ms from the first to the third receiver. So, when the transmission time delays of both the
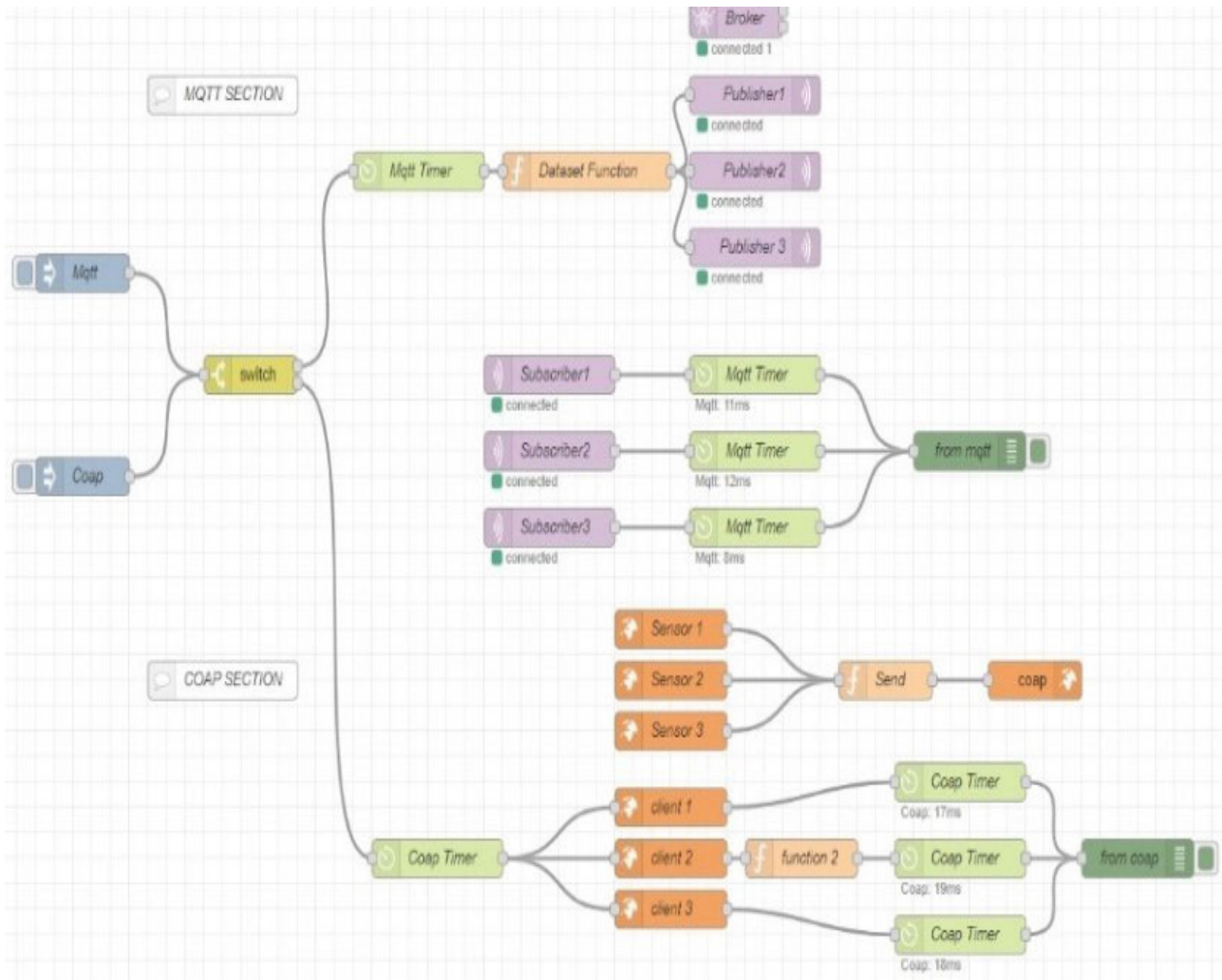
FIGURE 11. Proposed IoHT network of 3 senders and 3 receivers.

paths of the network were compared it was clearly recorded that the MQTT-SN communication path had a delay of 4ms as compared to 2ms in the CoAP communication path.

Further, when the number of senders and receivers was increased in the same network set-up it was found that in a network where a large number of sensors exist resulting in high traffic, will always result in time delay at each receiver end. It has been also concluded that as the nodes increase in the network running the MQTT-SN protocol, huge traffic at the broker is gathered. This traffic at the broker results in broker congestion and eventually leads to higher message transmission time. Hence, the network throughput decreases. While this is not the case with a CoAP based connection, high traffic minutely affects the message transmission time.

VII. EXPERIMENTAL RESULT

In the experimental examination of the proposed network setup, the first scenario of the time taken by the IoT protocols to transmit various sizes of data packets has been analysed. It is concluded from the first experimental setup of the sim-

ulation performed in Figure 10. A time comparison has been shown in Figure 12, which is based on the message payload. It is noted that till the message payload remains less than 1024bytes, the time taken in both the protocols' communication paths is less but as soon as the payload increases to 1024bytes, the time taken in transmitting the data packet by CoAP protocol shoots up, this proves that CoAP is suitable in transmitting small data packets.

Further in the next experimental setup, we analyzed the different possible scenarios of the network setup in NODE RED. We tested the proposed network for various possible scenarios. In the first scenario, we studied the MQTT-SN-and CoAP-based network communication path. Here, a One-to-One scenario has been considered i.e., the case when the number of senders is equal to the number of receivers. It was observed that when the number of nodes is increased from 10 to 50, there is a sharp increase in transmission time. Table 3 shows the maximum time stamps of all the links. Figure 13 shows the time analysis of the discussed scenario. In this graph, the maximum time has been considered from
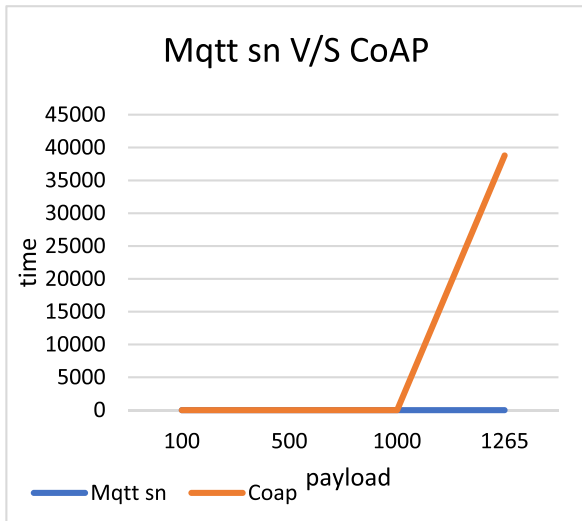
FIGURE 12. Time analysis of MQTT-SN and CoAP in the network.

TABLE 3. Transmission time in One -to-One scenario of the proposed IoHT network.

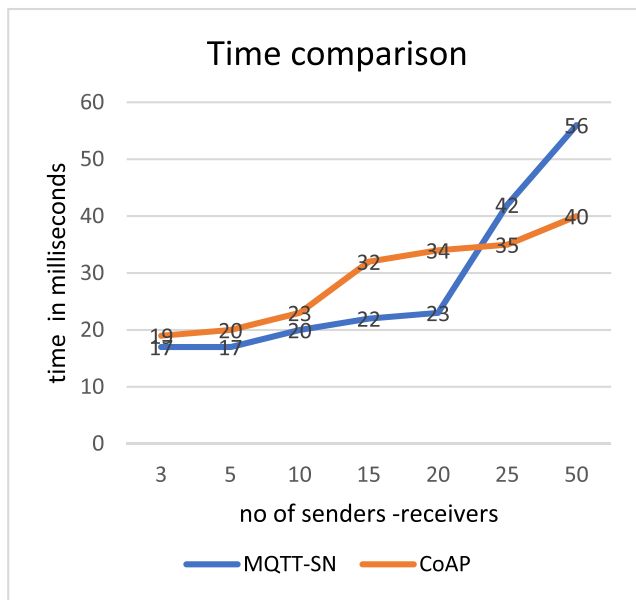| one-to-one scenario in the proposed IoHT network		
MQTT-SN	CoAP	No of senders(sensors)
17	19	3
17	20	5
20	23	10
22	32	15
23	34	20
42	35	25
56	40	50

FIGURE 13. Time comparison analysis of MQTT-SN and CoAP with the increasing number of sensors in a network.

all the links of the path due to the protocol in consideration. This means that considering the first case of 3 sensors, there were 3 transmission links in both the paths as per two protocols. For MQTT-SN protocol, the three-time stamps recorded were 15ms, 16ms, and 17ms out of which max-time-tamp of 17ms was considered. Similarly, for CoAP protocol three-time stamps recorded were 17ms, 18ms, and 19ms out of which a max-time-tamp of 19ms was considered. A rise in transmission times is clearly visible from the comparative analysis which has been carried out in Figure 13.

In another network setup, the time taken to transmit data packets in the IoT network was analysed. Time comparison

was performed in three scenarios (i) One -To -One, (ii) One -To- Many, and (iii) Many -To- One.

The first scenario of One-to-One transmission is tested. In this case, number of senders is equal to number of receivers. This scenario is tested for a varied number of nodes ranging from 10 to 50 nodes. The transmission time is recorded for each link. In the case of 10 nodes, there were 10 paths linking 10 senders to 10 receivers. Table 4 shows the transmission time in MQTT-SN path. The value present in each cell is the frequency of each time stamp. This means that:

- 2 linking paths recorded a 9ms transmission time.
- 3 linking paths recorded a 10ms transmission time.
- 4 linking paths recorded an 11ms transmission time.
- 1 linking path recorded a 12ms transmission time.

Likewise, the rest of the cases in the network are represented by the table. Figure 14 shows the time comparison of the MQTT-SN path for the increasing number of senders and receivers in the proposed IoHT network in the One-To-One scenario. This graph has been plotted based on data present in Table 4. The horizontal line (x-axis) of the graph represents the transmission time stamp and the vertical line (y-axis) represents the number of links in the network. From the graph, it can be noted that when the number of senders is 50, transmission time reaches to 66ms as compared to 12ms in the 10 senders' case. Hence, it is evident that as the number of sensors increases the transmission time also increases.

Similarly, Table 5 shows the transmission time in the CoAP path. Based on this table, Figure 15 shows a time analysis graph of the increasing number of senders and receivers on the CoAP transmission path in the proposed IoHT network.

It has been found from the comparison of these two graphs that when there were fewer senders both the protocol links had almost similar transmission times, but as the number of senders increased in the network, which resulted in high
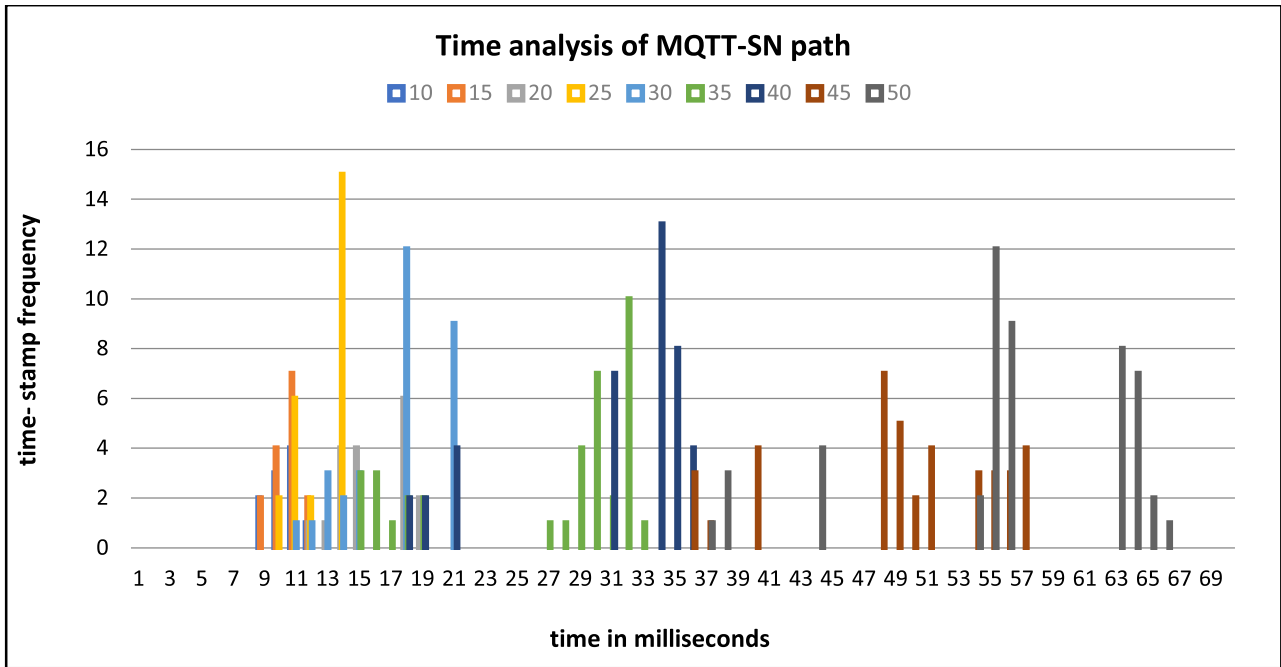
FIGURE 14. One- to- One scenario in MQTT-SN path.
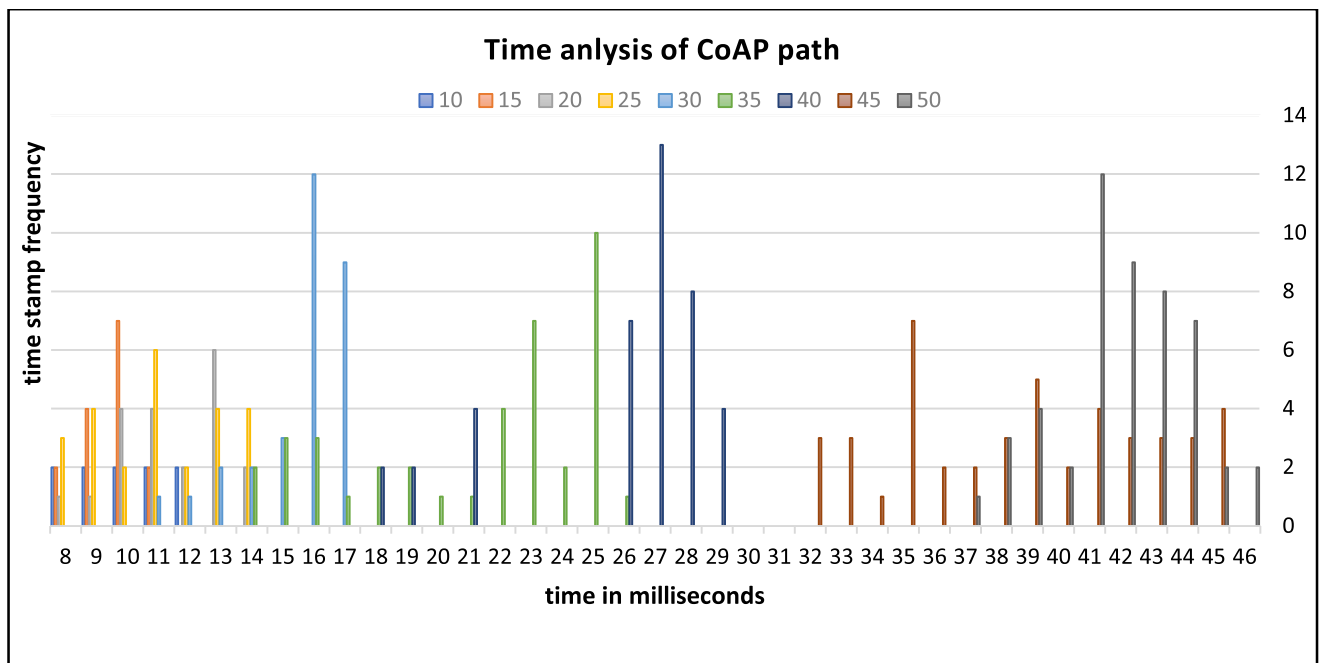
FIGURE 15. One to One scenario in CoAP path.

network traffic, transmission time recorded for the MQTT-SN path was high as compared to CoAP path. To get a better comparison of the two available protocol paths of the proposed IoHT network, the transmission time taken in both the paths has been shown in Figure 16. This comparison plot based on Table 6, considers the maximum time stamp of each case.

Now consider the second scenario of One-to-Many. In this scenario, one sender is sending to many receivers. This scenario is tested for a varied number of receiver nodes ranging from 10 to 50. That means in the case of 10 senders (10 sensors) all senders are sending data to one receiver. The transmission time is recorded for each link. Table 7 shows the transmission time in the One-to-Many scenario in the

TABLE 4. Transmission time in One-to-One scenario in the MQTT-SN path of the proposed IoHT network.

One to One Scenario in Proposed IoHT Network — Number of Sensors — Transmission Time in Milliseconds

| Time	10	15	20	25	30	35	40	45	50
9	2	2							
10	3	4		2					
11	4	7		6	1				
12	1	2	1	2	1				
13			1		3				
14			4	15	2				
15			4		3	3			
16						3			
17						1			
18			6		12	2	2		
19			2			2	2		
20									
21				9			4		
22									
23									
24									
25									
26									
27						1			
28						1			
29						4			
30						7			
31						2	7		
32						10			
33						1			
34							13		
35							8		
36						4	3		
37							1	1	
38								3	
39									
40							4		
41									
42									
43									
44								4	
45									
46									
47									
48								7	
49								5	
50								2	
51								4	
52									
53									
54								3	2
55								3	12
56								3	9
57								4	
58									
59									
60									
61									
62									
63									8
64									7
65									2
66									1

TABLE 5. Transmission time in One-to-One scenario in the CoAP of the proposed IoHT network.

One to One Scenario in Proposed IoHT Network — Number of Sensors — Transmission Time in Milliseconds

Time	10	15	20	25	30	35	40	45	50
8	2	2	1	3					
9	2	4	1	4					
10	2	7	4	2					
11	2	2	4	6	1				
12	2		2	2	1				
13			6	4	2				
14			2	4	2	2			
15					3	3			
16					12	3			
17					9	1			
18						2	2		
19						2	2		
20						1			
21						1	4		
22						4			
23						7			
24						2			
25						10			
26						1	7		
27							13		
28							8		
29							4		
30									
31									
32								3	
33								3	
34								1	
35								7	
36								2	
37								2	1
38								3	3
39								5	4
40								2	2
41								4	12
42								3	9
43								3	8
44								3	7
45								4	2
46									2

TABLE 6. Transmission time in One-to-One scenario of the proposed IoHT network.

MQTT-SN	CoAP	No of senders
12ms	12ms	10
12ms	11ms	15
15ms	14ms	20
14ms	14ms	25
21ms	17ms	30
33ms	26ms	35
36ms	29ms	40
57ms	45ms	45
66ms	46ms	50
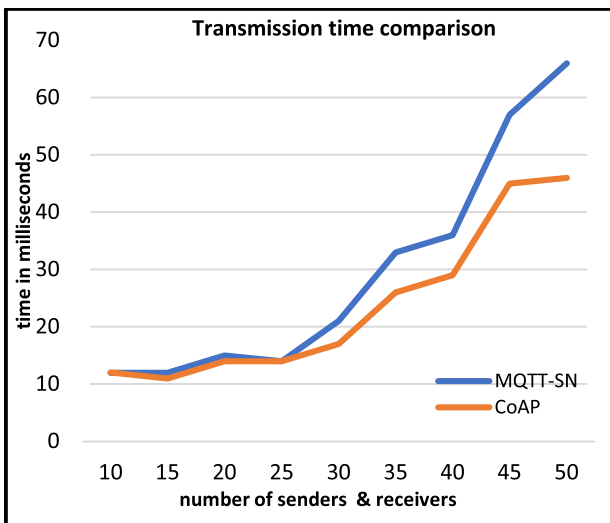
FIGURE 16. One to One scenario Time-comparison graph.

MQTT-SN path of the proposed IoHT network. The value of the cell depicts the frequency of each time stamp. Figure 17

shows the time comparison graph in the One-To-Many scenario of the MQTT-SN path. This graph has been plotted based on Table 7. The horizontal line (x-axis) of the graph represents the transmission time stamp and the vertical line (y-axis) represents the number of links in the network. It can be concluded from the graph that as the number of receivers increase from 10 to 50 transmission time increase from 2ms

TABLE 7. Transmission time in One -to- Many scenario of the proposed IoHT network in MQTT-SN path.

One to Many Scenario in Proposed IoHT Network										
	Number of Sensors									
		10	15	20	25	30	35	40	45	50
	1									
	2			1						
	3	5	1	4						
	4	5	3	6		1				
	5		4	6	1	3		3	3	2
	6		5	3	3	4		5	4	5
	7		2		3	4	1	5	4	7
	8				5	3	1	5	5	5
	9				6	4	3	4	4	1
	10				6	4	3		3	2
	11				1	5	4	2	3	2
	12					2	3	6	3	4
	13						4	5	4	2
	14						3	5	3	5
	15						3		4	5
	16						4			
	17						4			
	18						1			
	19						1			

(Left axis: Transmission Time in Milliseconds)

TABLE 8. Transmission time in One -to- Many scenario of the proposed IoHT network in CoAP path.

One to Many Scenario in Proposed IoHT Network										
	Number of Sensors									
		10	15	20	25	30	35	40	45	50
	2	5		1						
	3	5	2	4	1			3	3	
	4		4	6	3	1	1	5	4	7
	5		5	6	3	3	1	5	4	5
	6		4	3	5	4	3	5	5	1
	7				6	4	3	4	4	2
	8				6	3	4		3	4
	9				1	4	5	2	3	4
	10					4	6	6	3	2
	11					5	3	5	4	5
	12					2	4	5	3	5
	13						5		4	5

(Left axis: Transmission Time in Milliseconds)

TABLE 9. Transmission time in One -to- Many scenario of the proposed IoHT network in both the paths.

MQTT-SN	CoAP	No of senders
4	3	10
7	6	15
6	6	20
11	9	25
12	12	30
19	13	35
14	13	40
15	13	45
15	13	50

TABLE 10. Transmission time in One -to- Many scenario of the proposed IoHT network.

MQTT-SN	CoAP	No of senders
1	1	10
3	2	15
5	3	20
6	5	25
7	5	30
8	7	35
9	7	40
12	9	45
13	11	50

drawn. This graph shows a slight increase in the time taken to transmit a message from 10 receivers to 50 receivers in CoAP transmission link.

On analyzing the message transmission time in One-to-Many scenarios in different cases on both transmission paths, it was concluded that transmission time increases minutely, on increasing the receivers in the proposed IoHT network. To have a more clear understanding and to compare the message transmission time in the network, the time for both the paths' transmission twere plotted on the graph shown in Figure 19. This graph is based on Table 9 which has the max-time-stamp reading for each path in each case.

The third experimental setup involves testing the transmission time in the Many-to-One scenario of the proposed IoHT network. It is tested for both the transmission paths of the network. The time analysis of the MQTT-SN and CoAP transmission paths has been shown in Table 10. The value of the cell under the protocols depicts the time duration. Figure 20 shows the time comparison graph in the Many-To-One scenario. This graph is plotted based on Table 10.
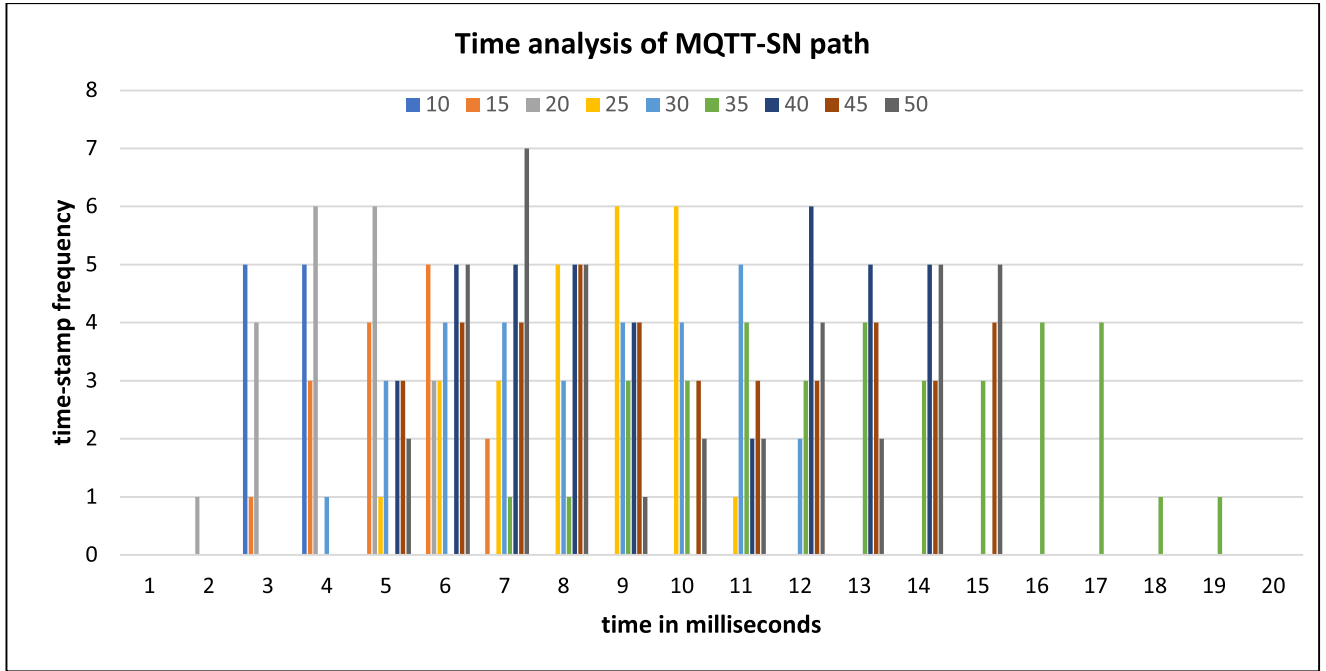
to 16ms which is quite less as compared to One-to-One scenario.

In a similar fashion, the One-to-Many scenario in the CoAP communication path of the proposed IoHT network setup is considered. Table 8 shows the transmission times of different links. Based on Table 8, a time analysis graph has been

FIGURE 17. Time analysis of One- to- many scenario in MQTT-SN path.
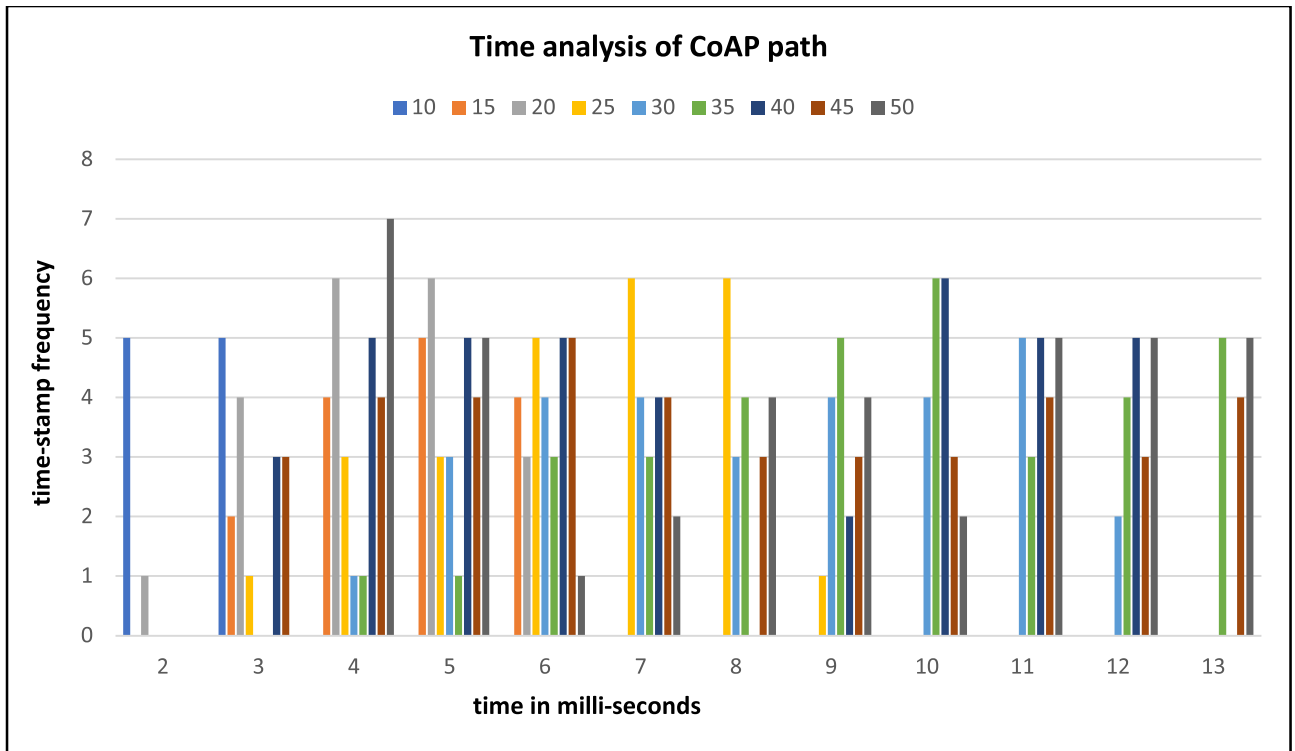

FIGURE 18. Time analysis of One to many scenario in CoAP path.

In this scenario, many senders are sending to one receiver. This is the most common scenario available in real-world IoT healthcare applications, where many wearable medical sensors are sending huge amounts of data to the medical analytics center. This scenario is tested for a varied number of sender nodes ranging from 10 to 50 and a single receiver node. The transmission time is recorded for each link. It can be seen from the graph that generally as the number of

TABLE 11. Conclusion of experimental analysis of three different scenarios.

Scenario tested	Time change	Time comparison analysis
One -to-One	Steep increase in time with the increase in the number of nodes	
One -to-Many	Steady increase in time with the increase in the number of nodes	
Many -to- One	Steep increase in time with the increase in the number of nodes	

senders increases in the network, transmission time increases. However, during high traffic conditions, the time taken on the MQTT-SN path records a steep increase as compared to the time taken on the CoAP path.

From the experimental analysis of three different scenarios, it was deduced that there is a steady increase in transmission time in the network in One- to- Many scenario. whereas there is a steep increase in transmission time recorded in the One-to- One and Many -to- One scenario. It is because of the greater number of sensors generate more traffic at the broker resulting in traffic congestion and more time delays.

It was also concluded that in all three scenarios as soon as high traffic condition occurs, the MQTT-SN connection path starts to show more steep delays in transmission times as compared to CoAP connection paths.

A. REAL-TIME IOHT NETWORK SCENARIO

Thus, taking into account a real-time scenario of the IoHT network, the senders are the numerous sensors attached to the human body and the receiver is a medical analytical center, where continuous monitoring of medical data is performed. This time analysis shows that in network congestion condi-
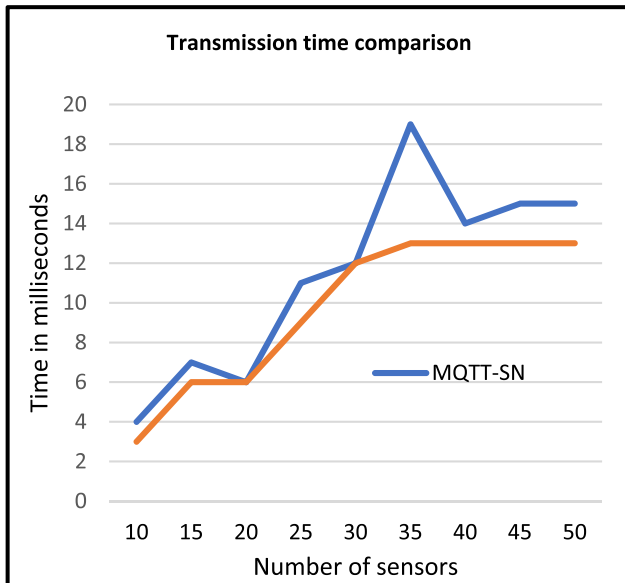
FIGURE 19. Time comparison of One to many scenario of both the paths.
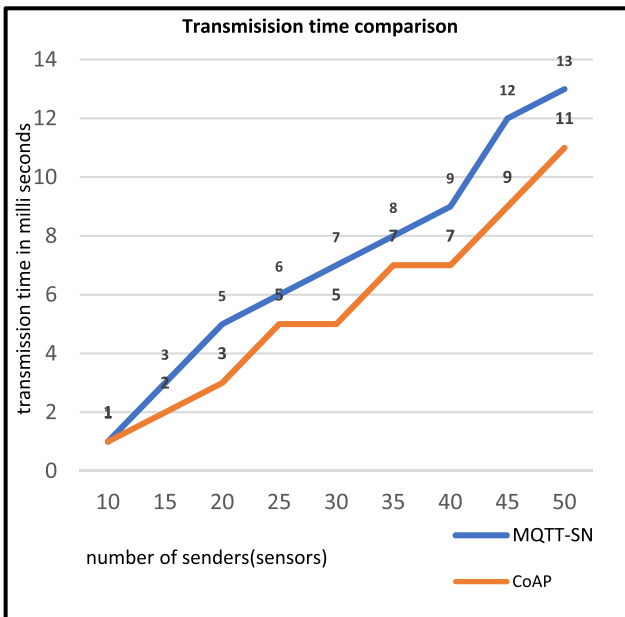

FIGURE 20. Many to one scenario.

tions MQTT-SN transmission link of the proposed network suffers from time delays, resulting in less throughput of the connection path. So, in that case, if a trigger message arrives which is a high-priority message, signaling any medical emergency condition, the proposed adaptive switching model switches from the current active default path of MQTT-SN to CoAP to quickly transmit the trigger message to the receiver.

Table 11 shows the experimental analysis of different tested scenarios.

VIII. CONCLUSION AND FUTURE WORK

The two application layer protocols namely CoAP and MQTT-SN that can be utilized particularly with IoHT net-

works are studied, evaluated, and compared in this paper. Performance analysis concluded that while selecting one of them, consider the quality of service, availability, and reliability the application requires. Both protocols are specifically appropriate for different implementational conditions. An Adaptive switching-based data communication model has been designed to gain reliability and time optimization in complex IoHT networks. NODE RED tool is used to test the proposed framework in different scenarios. For future work, this framework can be made secure by applying various security techniques. This framework will be deployed and analysed in real-time physical IoHT applications. The stability and robustness of the proposed framework will then be tested in real-time scenario.

REFERENCES

[1] V. A. Orfanos, S. D. Kaminaris, P. Papageorgas, D. Piromalis, and D. Kandris, "A comprehensive review of IoT networking technologies for smart home automation applications," *J. Sensor Actuator Netw.*, vol. 12, no. 2, p. 30, Apr. 2023, doi: 10.3390/jsan12020030.

[2] B. A. Begum and S. V. Nandury, "Data aggregation protocols for WSN and IoT applications—A comprehensive survey," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 2, pp. 651–681, Feb. 2023, doi: 10.1016/j.jksuci.2023.01.008.

[3] M. A. Abid, N. Afaqui, M. A. Khan, M. W. Akhtar, A. W. Malik, A. Munir, J. Ahmad, and B. Shabir, "Evolution towards smart and software-defined Internet of Things," *AI*, vol. 3, no. 1, pp. 100–123, 2022, doi: 10.3390/ai3010007.

[4] E. Perrier, *Positive Disruption: Healthcare, Ageing and Participation in the Age of Technology*. Sydney, NSW, Australia: The McKell Institute, 2015.

[5] A. Rejeb, K. Rejeb, H. Treiblmaier, A. Appolloni, S. Alghamdi, Y. Alhasawi, and M. Iranmanesh, "The Internet of Things (IoT) in healthcare: Taking stock and moving forward," *Internet Things*, vol. 22, Feb. 2023, Art. no. 100721, doi: 10.1016/iot.2023.100721.

[6] S. Krishnamoorthy, A. Dua, and S. Gupta, "Role of emerging technologies in future IoT-driven healthcare 4.0 technologies: A survey, current challenges and future directions," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 1, pp. 361–407, Jan. 2023, doi: 10.1007/s12652-021-03302-w.

[7] P. Gupta, D. Agrawal, J. Chhabra, and P. K. Dhir, "IoT based smart healthcare kit," in *Proc. Int. Conf. Comput. Techn. Inf. Commun. Technol. (ICCTICT)*, Mar. 2016, pp. 237–242.

[8] S. M. R. Islam, D. Kwak, MD. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[9] P. Salunke and R. Nerkar, "IoT driven healthcare system for remote monitoring of patients," *Int. J. Mod. Trends Sci. Technol.*, vol. 3, no. 6, pp. 100–103, Jun. 2017.

[10] D. Furtado, A. F. Gygax, C. A. Chan, and A. I. Bush, "Time to forge ahead: The Internet of Things for healthcare," *Digit. Commun. Netw.*, vol. 9, no. 1, pp. 223–235, Feb. 2023, doi: 10.1016/j.dcan.2022.06.007.

[11] M. Kumar, A. Kumar, S. Verma, P. Bhattacharya, D. Ghimire, S.-H. Kim, and A. S. M. S. Hosen, "Healthcare Internet of Things (H-IoT): Current trends, future prospects, applications, challenges, and security issues," *Electronics*, vol. 12, no. 9, p. 2050, Apr. 2023, doi: 10.3390/electronics12092050.

[12] M. L. Umashankar, S. Mallikarjunaswamy, N. Sharmila, D. M. Kumar, and K. R. Nataraj, "A survey on IoT protocol in real-time applications and its architectures," in *ICDSMLA* (Lecture Notes in Electrical Engineering), vol. 947, A. Kumar, S. Senatore, and V. K. Gunjan, Eds. Singapore: Springer, 2023, pp. 119–130, doi: 10.1007/978-981-19-5936-3_12.

[13] IoT. (2020). *Standards and Protocols*. [Online]. Available: www.postscapes.com

[14] V. J. Aski, V. S. Dhaka, A. Parashar, S. Kumar, and I. Rida, "Internet of Things in healthcare: A survey on protocol standards, enabling technologies, WBAN architectures and open issues," *Phys. Commun.*, vol. 60, Oct. 2023, Art. no. 102103, doi: 10.1016/j.phycom.2023.102103.

[15] D. Bilal, A.-U. Rehman, and R. Ali, "Internet of Things (IoT) protocols: A brief exploration of MQTT and CoAP," *Int. J. Comput. Appl.*, vol. 179, no. 27, pp. 9–14, Mar. 2018, doi: 10.5120/ijca2018916438.

[16] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015, doi: 10.1109/COMST.2015.2444095.

[17] S. Saritha and V. Sarasvathi, "A study on application layer protocols used in IoT," in *Proc. Int. Conf. Circuits, Controls, Commun. (CCUBE)*, Dec. 2017, pp. 155–159.

[18] R. Bhowmik and M. H. Riaz, "An extended review of the application layer messaging protocol of the Internet of Things," *Bull. Electr. Eng. Informat.*, vol. 12, no. 5, pp. 3134–3141, Oct. 2023, doi: 10.11591/eei.v12i5.5236.

[19] A. Stanford-Clark and H. L. Truong, "MQTT for sensor networks (MQTT-SN) protocol specification," *Int. Bus. Mach. (IBM) Corp. Version*, vol. 1, no. 2, pp. 1–28, 2013.

[20] A. Banks and R. Gupta, "MQTT version 3.1.1," OASIS Standard, Oct. 2014. [Online]. Available: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html

[21] S. Mijovic, E. Shehu, and C. Buratti, "Comparing application layer protocols for the Internet of Things via experimentation," in *Proc. IEEE 2nd Int. Forum Res. Technol. Soc. Ind. Leveraging Better Tomorrow (RTSI)*, Sep. 2016, pp. 1–5, doi: 10.1109/RTSI.2016.7740559.

[22] F. Iqbal, S. M. Akhtar, and R. Anwar, "A survey of application layer protocols of Internet of Things," *Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 11, pp. 301–311, 2021, doi: 10.22937/IJCSNS.2021.21.11.41.

[23] S. Imane, M. Tomader, and H. Nabil, "Comparison between CoAP and MQTT in smart healthcare and some threats," in *Proc. Int. Symp. Adv. Electr. Commun. Technol. (ISAECT)*, Nov. 2018, pp. 1–4, doi: 10.1109/ISAECT.2018.8618698.

[24] M. K. Tom, "MQTT-SN protocol—A review," *India Int. J. Res. Eng., Sci. Manag.*, vol. 1, no. 10, Oct. 2018. [Online]. Available: www.ijresm.com

[25] C. Bayilmis, M. A. Ebleme, Ü. Çavusoglu, K. Küçük, and A. Sevin, "A survey on communication protocols and performance evaluations for Internet of Things," *Digit. Commun. Netw.*, vol. 8, no. 6, pp. 1094–1104, Dec. 2022, doi: 10.1016/j.dcan.2022.03.013.

[26] M. A. Tariq, M. Khan, M. T. Raza Khan, and D. Kim, "Enhancements and challenges in CoAP—A survey," *Sensors*, vol. 20, no. 21, p. 6391, Nov. 2020, doi: 10.3390/s20216391.

[27] L. Coetzee, D. Oosthuizen, and B. Mkhize, "An analysis of CoAP as transport in an Internet of Things environment," in *Proc. IST-Africa Week Conf. (IST-Africa)*, Botswana, May 2018, pp. Page 1 of 7–Page 7 of 7.

[28] T. Salman and R. Jain. (2016). *Networking Protocols and Standards for Internet of Things*. [Online]. Available: https://www.cse.wustl.edu/jain/cse570-15/ftp/iotprot/index.html

[29] M. Milon Islam, S. Nooruddin, F. Karray, and G. Muhammad, "Internet of Things device capabilities, architectures, protocols, and smart applications in healthcare domain: A review," 2022, *arXiv:2204.05921*.

[30] H. M. Hasan and S. A. Jawed, "IoT protocols for health care systems: A comparative study," *Int. J. Comput. Sci. Mobile Comput.*, vol. 7, no. 11, pp. 38–45, 2018.

[31] M. Martí, C. Garcia-Rubio, and C. Campo, "Performance evaluation of CoAP and MQTT_SN in an IoT environment," *Multidisciplinary Digit. Publishing Inst. Proc.*, vol. 31, no. 1, p. 49, 2019.

[32] F. Ouakasse and S. Rakrak, "A comparative study of MQTT and COAP application layer protocols via. Performances evaluation," *J. Eng. Appl. Sci.*, vol. 13, no. 15, pp. 6053–6061, 2018.

[33] M. Collina, M. Bartolucci, A. Vanelli-Coralli, and G. E. Corazza, "Internet of Things application layer protocol analysis over error and delay prone links," in *Proc. 7th Adv. Satell. Multimedia Syst. Conf. 13th Signal Process. Space Commun. Workshop (ASMS/SPSC)*, Livorno, Italy, Sep. 2014, pp. 398–404.

[34] J. Dizdarevic, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for Internet of Things and related challenges of fog and cloud computing integration," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–29, 2019.

[35] V. Seoane, C. Garcia-Rubio, F. Almenares, and C. Campo, "Performance evaluation of CoAP and MQTT with security support for IoT environments," *Comput. Netw.*, 197, Oct. 2021, Art. no. 108338, doi: 10.1016/j.comnet.2021.108338.

[36] S. Jaloudi, "Communication protocols of an industrial Internet of Things environment: A comparative study," *Future Internet*, vol. 11, no. 3, p. 66, 2019.

[37] L. Zilhão, R. Morla, and A. Aguiar, "A modular tool for benchmarking IoT publish-subscribe middleware," in *Proc. IEEE 19th Int. Symp. 'World Wireless, Mobile Multimedia Networks' (WoWMoM)*, Chania, Greece, Jun. 2018, pp. 14–19.

[38] A. E. Khaled and S. Helal, "Interoperable communication framework for bridging RESTful and topic-based communication in IoT," *Future Gener. Comput. Syst.*, vol. 92, pp. 628–643, Mar. 2019.

[39] C. Akasiadis, V. Pitsilis, and C. D. Spyropoulos, "A multi-protocol IoT platform based on open-source frameworks," *Sensors*, vol. 19, no. 19, p. 4217, Sep. 2019, doi: 10.3390/s19194217.

[40] G. Yang, L. Xie, M. Mäntysalo, X. Zhou, Z. Pang, L. D. Xu, S. Kao-Walter, Q. Chen, and L.-R. Zheng, "A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2180–2191, Nov. 2014.

[41] A. J. Jara, M. A. Zamora, and A. F. Skarmeta, "Knowledge acquisition and management architecture for mobile and personal health environments based on the Internet of Things," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 1811–1818.

[42] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous data accessing method in IoT-based information system for emergency medical services," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1578–1586, May 2014.

[43] C. Doukas and I. Maglogiannis, "Bringing IoT and cloud computing towards pervasive healthcare," in *Proc. 6th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, Jul. 2012, pp. 922–926.

[44] V. Loseu, J. Wu, and R. Jafari, "Chapter 5.2—Mining techniques for body sensor network data repository," in *Wearable Sensors*, E. Sazonov and R. M. Neuman, Cambridge, MA, USA: Academic Press, 2014, pp. 383–407.

MEHWASH WEQAR was born in India, in 1986. She received the B.Tech. degree in computer engineering from the Faculty of Engineering and Technology, Jamia Millia Islamia, India, and the M.Tech. degree in computer science and technology from the Al-Falah School of Engineering and Technology, MDU University, in 2011. She is currently pursuing the Ph.D. degree in electrical engineering with Jamia Millia Islamia. She has coauthored four papers in conferences and book chapters.

SHABANA MEHFUZ (Senior Member, IEEE) received the B.Tech. degree in electrical engineering from Jamia Millia Islamia, New Delhi, India, in 1996, the M.Tech. degree in computer technology from IIT Delhi, in 2003, and the Ph.D. degree in computer engineering from Jamia Millia Islamia, in 2008.

She has been with the Department of Electrical Engineering, Jamia Millia Islamia, for the past 22 years. She has guided seven Ph.D. candidates and is supervising six other candidates. She has published more than 70 papers in international journals and conferences. Her research interests include computer networks and computational intelligence. She is a Life Member of ISTE, a member of the Institution of Engineers, and a Life Member of the Computer Society of India. She has received grants for research projects from agencies like AICTE and UGC. She has been awarded the International Inspirational Women Award 2020 for Best Performer in Government Award by the GISR Foundation. She has acted as the track chair of two flagship International IEEE conferences.

DHAWAL GUPTA received the B.Tech. degree in electronics and communication engineering from Chatrapati Sahu Ji Maharaj University, Kanpur, India, in 2001, and the Ph.D. degree in earthquake-signatures from the Indian Institute of Technology, Delhi, in 2012. Then worked four months as a Trainee with Rohits Measurons (India) Private Ltd., Roorkee, Uttarakhand, India. Appointed as a Design Engineer with AG Measurematics Private Ltd., from October 2001 to January 2004 (two years four months). He was a Design Engineer with Elcome Systems, from February 2004 to April 2004 (three months), Gurugram, Haryana, India, and then he was a Project Scientist with the Indian Institute of Technology, Delhi, from May 2004 to April 2008 (four years). Then, he was appointed as a Scientist C of Standardization, Testing and Quality Certification Directorate, from May 2008 to April 2014 (six years). Then, he was appointed as a Scientist D of the Ministry of Electronics and Information Technology, from May 2014 to January 2019 (four years nine months), New Delhi, Government of India. He was promoted to a Scientist E and the Head of Cyber Policy, Cyber Law, from January 2019 to April 2023 (four years four months). He has been the Group Business Director of Chase India, since April 2023 (six months). He is currently an information technology and techno-management professional, with more than 21 years of diversified experience in the areas of policy formulation and implementation, cyber policy research, develop policy strategy and engagement plan to build trust, and address existing and emerging technology policy issues in the cyber space in Indian and global context. Involved in complex policy analysis and development of appropriate implementation strategies.

SHABANA UROOJ (Senior Member, IEEE) received the B.E. degree in electrical engineering and the M. Tech. degree in electrical engineering (instrumentation and control) from Aligarh Muslim University, Aligarh, Uttar Pradesh, India, in 1998 and 2003, respectively, and the Ph.D. degree in electrical engineering from the Department of Electrical Engineering, Jamia Millia Islamia (A Central University), Delhi, India. She served the industry for three years and teaching organizations for more than 20 years. She is currently working with the Department of Electrical Engineering, College of Engineering, Princess Nourah bint Abdulrahman University, Saudi Arabia. She has authored and co-authored more than 200 research articles, which are published in high-class international journals, reputed conference proceedings, quality books, and patents. She has completed several editorial responsibilities for reputed journals and several quality books and proceedings. She was a recipient of several renowned international awards; namely Leadership Excellence Women's Award, the Springer's Excellence in Teaching and Research Award, the American Ceramic Society's Young Professional Award, the IEEE's Region 10 Award for Outstanding Contribution in Educational Activities, the Research Excellence Award for Quality Publishing/Authorship, and several other best paper presentation awards. She is serving as an Active Volunteer of the Institute of Electrical and Electronics Engineering (IEEE) in various capacities and committed to the technological and professional development of society.

● ● ●