Machine Learning-Enabled Communication Approach for the Internet of Medical Things

Rahim Khan[1,3], Abdullah Ghani[1], Samia Allaoua Chelloug[2,*], Mohammed Amin[4], Aamir Saeed[5] and Jason Teo[1]

[1]Faculty of Computing and Informatics, University Malaysia Sabah, Kota Kinabalu, Sabah, 88400, Malaysia
[2]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box, 84428, Riyadh, 11671, Saudi Arabia
[3]Department of Computer Science, Abdul Wali Khan University, Mardan, 23200, Pakistan
[4]College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, 31982, Saudi Arabia
[5]Department of Computer Science and IT, UET Peshawar, Jalozai Campus, Jalozai, 24240, Pakistan
*Corresponding Author: Samia Allaoua Chelloug. Email: Sachelloug@pnu.edu.sa

Abstract: The Internet of Medical Things (IoMT) is mainly concerned with the efficient utilisation of wearable devices in the healthcare domain to manage various processes automatically, whereas machine learning approaches enable these smart systems to make informed decisions. Generally, broadcasting is used for the transmission of frames, whereas congestion, energy efficiency, and excessive load are among the common issues associated with existing approaches. In this paper, a machine learning-enabled shortest path identification scheme is presented to ensure reliable transmission of frames, especially with the minimum possible communication overheads in the IoMT network. For this purpose, the proposed scheme utilises a well-known technique, i.e., Kruskal's algorithm, to find an optimal path from source to destination wearable devices. Additionally, other evaluation metrics are used to find a reliable and shortest possible communication path between the two interested parties. Apart from that, every device is bound to hold a supplementary path, preferably a second optimised path, for situations where the current communication path is no longer available, either due to device failure or heavy traffic. Furthermore, the machine learning approach helps enable these devices to update their routing tables simultaneously, and an optimal path could be replaced if a better one is available. The proposed mechanism has been tested using a smart environment developed for the healthcare domain using IoMT networks. Simulation results show that the proposed machine learning-oriented approach performs better than existing approaches where the proposed scheme has achieved the minimum possible ratios, i.e., 17% and 23%, in terms of end to end delay and packet losses, respectively. Moreover, the proposed scheme has achieved an approximately 21% improvement in the average throughput compared to the existing schemes.

1 Introduction

Due to the recent advancements in technology, preferably sensors and actuators, IoMT networks have become one of the dominant research domains both for scientists and industrial organisations, especially in the healthcare domain. The IoMT network is defined as a group of physical objects, "wearable things," that can interact with the environment and automatically control numerous activities in different sectors, such as the auto-control of machines in the manufacturing industry, especially those where human accessibility is either hard or dangerous for human health [1]. These networks are used in different application domains to assist human beings in monitoring and controlling various activities, preferably in industries, agriculture, smart cities, buildings, etc. IoMT has become more convenient and reliable if machine learning techniques are merged, i.e., if routing methodology within a device is based on machine learning, then it would be more feasible to find an optimal path, when a device is interested in triggering a communication process with the intended server or ordinary device in the IoMT networks. It is important to note that these devices Ci are bound to communicate directly with the intended server module if they are deployed in the coverage area of the concerned server module in the IoMT network. In scenarios where direct communication with the server module is not possible, a multi-hop communication strategy is adopted where it is highly likely that a packet may be sent through the longest route as the concerned device C_i considers only the routing table where different paths, preferably those available for communication, have been listed. However, finding an optimal path is not always possible with the existing methodologies, and these devices are needed to update based on the data values captured after every transmission of a packet [2]. Furthermore, In the proposed infrastructure, relaying devices are bound to transmit data from neighbouring devices in addition to their functionality, which is the capture and transmission of the collected data in the IoMT networks [3].

Generally, in IoMT networks, a multi-hop communication mechanism is adopted by devices in scenarios where the destination module is not located within the coverage area of the underlined device C_i. For this purpose, every device C_i needs to store additional information about devices C_i deployed in its coverage area and have strongly received signal strength indicators (RSSI) along with the hop count values that are used by the concerned device C_i for communication. However, these parameters are not sufficient to form an efficient and optimised routing strategy [4,5]. Furthermore, in the IoMT, an optimised feature extraction method was proposed for resolving this issue in a distributed environment. However, this model restricts the achievement of this goal without any compromise on latency or energy consumption [6]. Additionally, it is important to note that the majority of the routing schemes assume that every device C_i needs to have information about its first hop neighbour, which is somehow perfect in a certain situation, i.e., the locality of the device C_i, but it is not efficient globally. As a device, C_i may be more optimal locally, but it would not be efficient globally, i.e., as far as the whole path is concerned. Therefore, these devices should be smart enough to not only consider local information but also thoroughly examine the global effects of their decisions. Additionally, as numerous optimal path-enabled solutions are available in the literature, these approaches do not consider the overwhelming characteristics of machine learning approaches, especially for finding optimal neighbouring devices or paths in the IoMT networking infrastructure. For example, a possible solution could be the integration of machine learning or artificial intelligence-based methodologies with the available communication approaches, which may resolve this issue, but it should be ensured that other evaluation metrics of the networks are not affected, such as lifetime, end to end delay, and

overall throughput of the network. Moreover, the machine learning approach should be more efficient in terms of energy efficiency and, more specifically, its compatibility with the resource-limited nature of the IoMT networks.

In this paper, a machine learning-enabled transmission mechanism is reported to address the issues associated with the existing approaches in the IoMT networks. For this purpose, we have bound every device C_i to find optimal paths towards the destination module, i.e., the base station in this case, and prefer to communicate via the most optimal path. machine learning approach along with a graph-based approach, i.e., the Kruskal algorithm, which is a greedy algorithm, is used to find the most optimal path in the IoMT network. This algorithm considers every device C_i as a tree in the forest, whereas the whole IoMT network is assumed to be a forest. Additionally, it must store the second-best optimal in memory, which could be very useful in situations where the current communication path is either blocked or not available for communication. This may occur in the IoMT networks, as it is highly likely that two or more devices C_i will have the same optimal path. Thus, before the transmission, a device C_i must ensure the availability of the concerned path in the operational networks, and if it finds that the concerned shortest path is not available, it will opt for the second option. Thus, communication is guaranteed, as one path would be available for communication. Furthermore, if the battery level of a particular device falls below a certain threshold value, i.e., 75%, then it must broadcast a message to all neighbouring devices C_i to be informed about its status. In this case, devices C_i will communicate via another path if available and avoid transmission of packets via this path so that load on this device C_i is reduced to the minimum possible level, which will prolong its availability in the IoMT networks [7–9].

The remaining manuscript is organised as follows. In the subsequent section, we are going to describe and present an overview of the literature, especially the most relevant and closed approaches to the problem addressed. In Section 3, the proposed machine learning and graph theory-enabled communication mechanism is presented and explained in detail. Simulation results and observations of the proposed and existing schemes are presented in a separate section, i.e., Section 4. Finally, concluding remarks and future directives are given.

2 Literature Review

In the IOMT networks, load balancing or traffic distribution is assumed to be among the most important aspects of how to improve the operational life cycle of the underlined network. To address this issue, various optimisation and path identification schemes have been reported in the literature, where authors were eager to find a solution to the problem that is not applicable in terms of efficiency but is reliable across different platforms of the IoMT networks as well. Among those techniques, the majority focused on the development of a uniform distribution of traffic among the different available alternatives. However, this uniformity brought other problems as well, like massive delays in packet transmission from source to destination, as packets must follow the longest paths to ensure uniform load balancing in the networks. However, these solutions have resolved the core issue, which is uniform packet distribution. In this section, we are going to present a comprehensive overview of all those methods, especially those that are closely linked to the problem at hand. Apart from it, machine learning and IoMT have been used in various application areas such as smart buildings and cities, medicine, manufacturing, and industries, the healthcare sector, precision agriculture, etc. In the agriculture section, these approaches are used to identify various risk factors associated with different crops throughout the world [8]. Similarly, in healthcare, these approaches are used to find a solution

that assists doctors in their daily activities, while providing a solid platform for the 24/7 monitoring of patients, preferably without human intervention [7].

A cognitive radio-enabled Internet of Things (IoT) cross-layer routing mechanism is reported in the literature to enhance the efficiency of the routing and ensure the transmission of the optimised data. To ensure this, a proper controller (distributed in this case) has been designed that has multiple tasks like sensing neighbouring devices, distribution of traffic, and path learning through machine learning in configurable networking infrastructures [5].

A parametric-enabled path search approach, i.e., MetLearn, is proposed to ensure packet transmission via the most optimal paths in vehicular networks. This approach can train cluster heads (CHs) in such a way as to improve the forwarding mechanism for the route request through quality of service (QoS) metrics [9]. Likewise, a fuzzy logic-oriented framework has been designed and developed for mobile ad hoc networks, where the main theme is the optimisation of the routing paths through probabilistic QoS metrics. Furthermore, packets are synchronised to improve the QoS metric of the underlined MANETs [10]. A game-theoretic-enabled mechanism is presented to ensure a multi-cast transmission of packets where a game is designed that can construct a multi-cast tree (preferably least cost-based) as a candidate game. Their proposed scheme converges very quickly to the pure Nash equilibrium [11]. A multi-objective ant colony optimisation-based secure routing scheme is proposed to enable devices or servers to jump out easily from the local optima with the minimum possible energy consumption of nodes. Additionally, this algorithm has the built-in capacity to converge more rapidly than other approaches [12].

Li et al. [13] have developed an effective and efficient power consumption model for wireless sensor networks where limitations associated with the activated devices have been considered. This model has the built-in capacity to develop an efficient framework for resource management, especially energy, in the underlined resource constraint network. The light-path provision mechanism was developed by He et al. [14], which is based on a well-known technique in information theory. This approach has successfully achieved the expected level of load balancing through the scheduling of both routing and modulation levels in an active network. Liu et al. [15] have designed a balancing model for energy that is primarily based on the idea of heat points in the underlined sensing grid. In this model, the scheduling framework of the network is properly adjusted through power-aware resource strategies, whereas it has to compare the grid's sensing heat with the available heat points to ensure the allocation of resources, preferably in a dynamic way. Sun et al. [16] have discussed the efficacy of an analytical model to ensure traffic distribution in networks. In this approach, the energy consumption model of an authentic node is presented, and the results are convincing. Furthermore, they have focused on finding an optimised solution for the number of clusters in a particular network that can minimise the power consumption of the entire network. A quite different approach, i.e., one that is based primarily on the proper distribution of numerous tasks, is presented by Ang et al. [17] where a heuristic-enabled task scheduling mechanism is adopted and is successfully implemented in the realistic environment of wireless networks. Furthermore, this methodology is extremely useful in reducing the energy required by the devices to make certain valuable decisions. However, a common issue, that is tightly linked with this approach, is the required time to perform this activity, and due to the limited processing power of the node, this approach's performance is compromised if the time metric is used in the networks. Wang et al. [18] have focused on optimisation issues and presented a metric-oriented approach that is forced to consider numerous possible metrics such as the node's power consumption, reliability, and proper functioning. Although, this methodology was more optimised and has achieved exceptional results in terms of optimisation, the implementation complexity is an alarming issue with this scheme due to the limited power of the nodes. Shao et al. [19]

have worked on the lifetime of the whole network along with possible optimal transmission latency, and to realise this methodology, the path distance metric is used. A hybrid mechanism is presented by Aissa et al. [20] to ensure optimum utilisation of the available power. This model is based on two different algorithms, i.e., the transmission of packets using multi-hop relay and the weighted revenue-enabled multi-path concept. Additionally, this approach can update collected data values, which are captured by sensor nodes deployed in close proximity of the underlined phenomenon, and paths simultaneously through dedicated mechanisms. A software definition-oriented mechanism is proposed in [21], which is primarily based on the idea that a normal sensor node could be upgraded to a smart sensor if and only if proper software-enabled configurations are used. Although, energy efficiency has been achieved up to a considerable level, this scheme is more complex to implement, thus, its realisation or implementation in the real environment of wireless sensor networks (WSNs) is difficult. One of the challenging issues associated with WSNs is the collection of data, especially in scenarios where numerous metrics are needed to be considered, such as delay, the energy needed for the processing of a single bit, and the performance of the underlined network, along with reliability metrics. Generally, due to the various constraints and restrictions on the devices belonging to a sensor network or IoT, these networks are more susceptible to path loss, malfunctioning of the device, and the highest ratio of average packet loss during communication [22]. Therefore, in these networks, a multi-hop communication concept is adopted to ensure a reliable communication infrastructure. Likewise, a time division multiple access (TDMA)-enabled load balancing scheme, which is designed specifically for devices, not paths, is presented to allow devices to use the time slot of another device if that device is not interested in transmitting in its dedicated time slot. It is important to note that empty slots are assigned to active devices on a need-based basis, so a device may have more slots at a particular time interval. However, a common problem with this approach is how it will handle the scenario when a dedicated slot is assigned, and the owner node captures data and is interested in sending it. Then, in this case, it will have to wait for the current frame and transmit data in the next frame. Moreover, the needy device will have to wait as the slot allocated to it is now used by the actual owner [23]. A fuzzy interference-enabled load distribution scheme is presented where the minimum possible inputs have been considered for the CH selection process. Additionally, the overall cost required to reach a particular CH is assumed as one parameter of the entire fuzzy system and has exceptionally reduced the overall energy consumption of nodes residing on paths [24]. Additionally, because IoT task distributions are spatially heterogeneous, certain edge clouds may be overburdened. We examine workload balancing issues to reduce transmission delay and calculation latency in task offloading processes while considering the constrained bandwidth resources of BSs and computing resources in edge clouds to tackle these issues. To examine the overall offloading choices, we structure the workload balancing problem as a population game. We utilise evolutionary game dynamics to evaluate the collective offloading choices made by mobile users, and we demonstrate that the game always reaches a Nash equilibrium (NE) [25].

3 Proposed Methodology for Healthcare Domain

Generally, the healthcare domain is one of the potential application domains of the IoMTs, as member devices in these networks could be anything ranging from wearable sensing devices to servers, which are all parts of the modern smart healthcare system. In these systems, the majority of the activities are controlled through autonomous devices that are either attached directly to the human body or could be deployed in close proximity. Keeping in view the potential of IoMT in the healthcare domain, in this section, we are going to describe in detail the various stages of the proposed scheme, which is specifically designed for the IoMT networking infrastructure, along with its design and

development plan. Furthermore, a detailed discussion will be provided on the capacity of the scheme to resolve the problem at hand, especially with the available resources. The proposed methodology, which is a machine learning-enabled transmission mechanism, has built-in capacity to address numerous issues related to the existing multi-hop communication approaches in the IoMT networks. For this purpose, we have bound every device C_i to find optimal paths towards the destination module, i.e., a graph-based station in this case, and prefer to communicate via the most optimal path, which is needed to be found through a hybrid methodology, i.e., machine learning and graph-based. A machine learning approach along with a graph-based approach, i.e., the Kruskal algorithm, which is a greedy algorithm, is used to find the most optimal path in the IoMT network. This algorithm considers every device C_i as a tree in the forest and tries to find the more optimal neighbouring trees in it. Furthermore, these trees are considered linked only if the weight of the connecting edge is below the threshold value, and surely it doesn't generate a loop or cycle. Additionally, it must store the second-best optimal in memory, which could be very useful in situations where the current communication path is either blocked or not available for communication. This may occur in the IoMT networks, as it is highly likely that two or more devices C_i will have the same optimal path. Thus, before the transmission, a device C_i must ensure the availability of the concerned path in the operational networks, and if it finds that the concerned shortest path is not available, then it will opt for the second option. Thus, communication is guaranteed, as one path would be available for communication. Furthermore, if the battery level of a particular device falls below a certain threshold value, i.e., 75%, then it must broadcast a message to all neighbouring devices C_i to be informed about its status. In this case, devices C_i will communicate via another path if available and avoid transmission of packets via this packet so that load on this device C_i is reduced to the minimum possible level, which will prolong its availability in the IoMT networks.

Initially, a refined form of the original Kruskal's algorithm is used which is used to generate a minimum spanning tree between the two devices, i.e., from source to destination a path is identified with minimum cost, i.e., distance in this case along with other metrics, and preferably without any cycle. Let us assume that C_i and S_j where i = 1,2,3,....n and j = 1,2,3...m represent active devices and server modules respectively in the IoMT networks. A device C_i can communicate directly with another device C_{i+1} if and only if the later device is deployed within the coverage area of its transceiver module. The probability of successful communication is presented as in the Eq. (1).

$$P_{TX}(C_i to C_{i+1}) = \begin{cases} Success\ if\ (C_i, C_{i+1}) & \leq Threshold \\ Fail & Otherwise \end{cases} \tag{1}$$

where d is the Euclidean distance between those devices C_i, which are deployed in the neighborhood, in the IoT networks. The threshold is an application or technology-dependent parameter, and its value is directly proportional to the coverage area of the respected XBeee module. The distance between any two active devices C_i is computed using the Euclidean distance as depicted in Eq. (2).

$$d(C_i, C_{i+1}) = \sqrt{(x_i, x_j)^3 + (y_i - y_j)^3 + (z_i - z_j)^3} \tag{2}$$

$$P_{TX}(C_i\ to\ C_{i+1}) = \begin{cases} 1, if\ d(C_i, C_{i+1}) < T_i \\ \delta, if\ d(C_i, C_{i+1}) == T_i \\ 0, if\ d(C_i, C_{i+1}) > T_i \end{cases} \tag{3}$$

where δ is a transceiver-oriented variable where it may communicate successfully, or a failure may occur.

In addition to the distance measure, other metrics are also considered when an optimal path is needed to identify the IoT networks. This may include latency, vulnerability, reliability, and cycles. Node or device-to-device Latency of a relay device in the network is represented by the Eq. (4).

$$\tau_0 = \sum_1^n [A(s,t) + S(s,t) + D(s,t)] \tag{4}$$

where

$$A(s,t) = \sum_{i=0}^{t-1} a_i \tag{5}$$

And

$$S(s,t) = \sum_{i=0}^{t-1} s_i \tag{6}$$

where a_i and S_i are the values, preferably instantaneous, which are captured during the ith interval of time.

Likewise, the vulnerability of a device, especially a relay device in the IoMT network, is defined as how important that device is from the perspective of the network connectivity. The vulnerability of a device C_i is computed using the equation given below.

$$C_i(Vul) = \frac{N_B}{N_A} * \frac{L_B + C}{L_A + C} \tag{7}$$

where A and B are used to represent values after and before removing the concerned device C_i from the IoT network, respectively. It is important to note that every server or CH module in the network has the responsibility to calculate the vulnerability of devices C_i reside in its coverage area. Additionally, packet travel time reliability is among the important metrics, especially when the communication path is shared among multiple devices C_i in the IoMT networks. The probability of a packet, especially in terms of travel time, is given in the Eq. (5).

$$R(t) = P(T < T_0) \tag{8}$$

where T and t are used to represent T is as the travel time and expected threshold time respectively. If we assume that the probability density function for a given path is represented as f(t) and distribution time as F(t$_0$), then the Eq. (9) can be represented as

$$R(t) = P(T < T_0) = \int_0^{t_0} f(t)\, dt = F(t_0) \tag{9}$$

The proposed scheme is bound to consider all these evaluation metrics, specifically those related to the link or path, while using Kruskal's algorithm to find a minimum spanning tree, preferably loop-free, of the most optimal path in the IoMT network.

In addition to these metrics, the cost factor associated with every neighboring device C_i is calculated and considered in the process of designing a reliable communication strategy. The cost factors of a device C_i in IoMT networks are given in the Eq. (10).

$$TXcost(C_i) = \sum_0^n \frac{TX(C_{i...n}) + RX(C_{i...n})}{n} \tag{10}$$

where TX represents the transmission cost of the packets from the source to the destination module. The device C_i prefers those neighbouring devices C_{i+1} in the network that have the minimum possible values as obtained in the Eq. (10). Additionally, it is important to note that it is not necessary that a neighbouring device with a minimum transmission cost factor be selected as a relaying device, rather,

this decision is based on other parameters as well, which are described earlier. Likewise, the weight of the concerned path is a vital metric, especially when a device C_i is interested in finding an optimal path, preferably the shortest possible with the minimum possible cost factor associated with it. For this purpose, weights are needed to be assigned to every edge in the connected graph, and then the shortest path is found based on the following equation.

$$w\,(Path) = \sum_0^k w(v_i, v_{i+1}) \tag{11}$$

To this end, the proposed scheme describes the whole IoT network as a connected graph, $G(v_i, e_j)$ where v_i & e_j are used to represent devices C_i and links or paths in the communication network, as shown in Fig. 1.
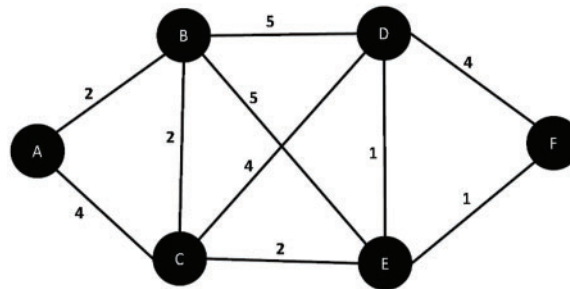
Figure 1: General IoT with weights

As the IoT network is represented in graphical form, the next step is to apply the refined form of Kruskal's algorithm to find the minimum spanning tree or shortest path between any two communication devices Ci, i.e., source and destination devices in this case. For example, if the optimal communication path between two devices, i.e., Ci & Sj, is needed to be found, then it starts from the source device, i.e., Ci in this case, and searches for the devices, i.e., Ci+1, to define the most optimal neighbours while considering the metrics. It is important to note that if two or more neighbours have similar weighted values, then all these are considered and refined further based on the second-hop neighbours.

Furthermore, to attain the maximum level of reliability, every device Ci is bound to have at least two different optimal paths for communication. As an optimal path may be shared by multiple devices Ci in the IoT network. Therefore, every device should store an alternative path, preferably the second optimal path, as a reserved path, which is very useful in situations when the current optimal path is no longer available or has a huge traffic flow. An optimal path is based on the following equation:

$$OPT\,(C_i) = \min\left[\sum_0^n \left(\frac{Vul\,(C_{i+1}) + d\,(C_{i+1}, S_j)}{C_i}\right)\right] \tag{12}$$

where l represents the total neighbours of the concerned device Ci in the IoT networks. This process is repeatedly applied by every source module or device Ci to find the optimal path, and then those paths are enforced for communication as long as they are available. However, as it is highly likely that multiple devices Ci, specifically those in the coverage area, will have a similar set of neighbouring devices Ci, the proposed scheme forces every device to spit the available traffic between the two paths by maintaining the defined ratio, i.e., 70:30, which means that out of 100, 70 packets will be sent via the most optimal path, whereas 30% of the packets are sent via the second optimal path in the IoT network. This approach reduces the expected probability of the underlined path, and equally ensures

the prolonged connectivity of every device Ci in the networks. A generalised sketch of the shortest possible paths in the underlined IoT network is presented in Figs. 2 and 3.
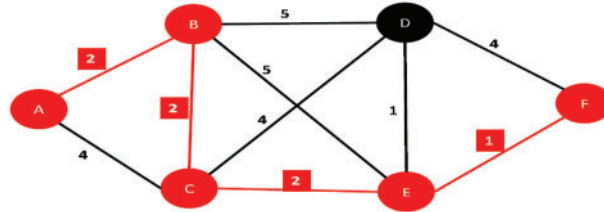

Figure 2: Shortest path in the underlined IoT network through refined Kruskal's algorithm
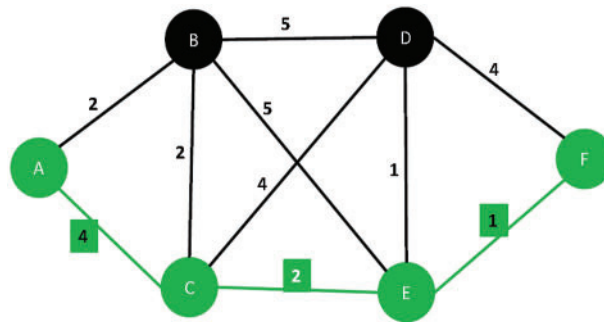

Figure 3: Alternative shortest path in the IoMT network through refined Kruskal's algorithm

Additionally, if we force every device Ci to use a single shortest path for communication every time, then it is highly likely that this path will become obsolete after a certain time interval. Furthermore, this situation will become tenser if two or more devices Ci share this same path and are continuously transmitting data packets over it. Thus, to improve the stability of the link, we have distributed the entire communication among two participants, i.e., paths in this case, to share the load. The step-by-step process of the proposed methodology is presented in the algorithm given below.

Algorithm-1: Finding the Shortest Possible Path in the IoMT

Output: Shortest Path

    E_j Represents all Edges of the IoMT network.

    V_i Represents all vertices of the IoMT network.

    w_k Represents the weights associated with every edge.

    For (i=0; i <= n; i++)

            Sort E_i accordingly as given below

            If $(E_i > E_{i+1})$**then**

                    $E_i \leftarrow$ Val (E_{i+1})

                    $E_{i+1} \leftarrow$ Val (E_i)

            Else

                    Advance the pointer.

            end if

(Continued)

Algorithm-1 (continued)

        for all E_i select $Opt(E_i)$ where E_i are ordered

$$Opt(E_i) = \min \left[\sum_0^n \left(\frac{Vul\,(C_{i+1}) + d\,(C_{i+1}, S_j)}{C_i} \right) \right]$$

        end for

        RETURN Optimal Path from $\{C_i\}$ to S_j

In this algorithm, initially, the IoMT network is represented as a planner graph G(v, e), such that there is no cycle in it. The next step is the organisation of all edges, preferably from every source device Ci to the destination module Sj, either in ascending or descending order. In the next step, optimal edges are identified in every step based on various weighted metrics that are assigned to every edge in the IoMT network. Thus, every device Ci identifies and finds the most optimal path in the network, along with an alternative path. Additionally, it is important to note that if a path failure is encountered, every device Ci has an alternate way or path to communicate.

4 Simulation Results and Analysis

In this section, we are going to present how the proposed scheme is implemented, along with environmental details. To be consistent with the real-time deployment of IoT networks, we have considered random deployment, not engineered, as it is not always possible to deploy these devices at preferred locations in the actual environment. For this purpose, we have implemented the proposed scheme in OMNET++, i.e., an open-source simulation environment specially designed for resource-limited networks, where devices were deployed through a random query. In these simulations, we have considered benchmark models for the transmission and reception of packets, i.e., the power required by the Arduino pro-boards. Likewise, the battery power of these devices Ci is assumed to be like that of actual devices available on the market. Moreover, we have carried out extensive simulations of the proposed schemes along with the field-proven algorithms, which are benchmark schemes available in the literature, using similar environmental and networking statistics, i.e., the same devices, networks, weights, etc. in the IoMT. Numerous parameters, preferably those that are important from the implementation perspective, are provided in Table 1. In this table, the residual energy Er of a device Ci represents the operational capacity of the concerned device Ci. Furthermore, the proposed methodology is extensively compared with field-proven approaches using numerous well-known performance evaluation metrics such as the average delay in transmission of packets, the ratio of the successfully delivered packets to the lost ones, etc.

4.1 Power Consumption

In resource-limited networks such as IoMT, available power, i.e., onboard battery power, is assumed to be one of the most vital resources, and it should be utilised as effectively as possible, preferably without compromising on other evaluation metrics. As per our understanding from the literature, efficient utilisation of the available power is more important for the relaying devices, i.e., those devices Ci that are responsible for the transmission of neighbouring device packets in addition to their own; therefore, these are considered the most critical, especially in the networking infrastructure where deployment is random and every device Ci cannot communicate directly with its intended destination devices. Hence, these devices Ci must be treated on a priority basis, and their energy consumption model should be efficient and monitored throughout the network to keep them active for a longer period of time. The proposed methodology, which is not only energy efficient but could

also utilise machine learning approaches to refine the transmission paths in the IoT networks, Apart from that, the proposed scheme is energy efficient in the sense that it forces devices Ci to utilise the most optimal path whenever possible, however, an alternative path, preferably less optimal, is used in scenarios where either the optimal path is shared by multiple source devices Ci or is not available for communication. We have observed that the proposed scheme's performance is much better than the existing approaches in the IoT networks, as shown in Fig. 4. Furthermore, we have compared the energy consumption of the individual devices Ci, i.e., both source and relaying devices, using the proposed methodology with the available scheme, and the results were convincing.

Table 1: Numerous parameters used in the IoMT

| Parameter name	Approximate or exact value
Deployment area for the IoMT networks	$1000 * 1000$
Devices C_i	100, 300, 500, 800, 1000
Sink or base station modules	1
Transmission interval of EGWN	20 S
O-board battery power of device C_i, i.e., E_i	50,000 mAh
Channel or link bandwidth	8 Mbps
Energy cost of the transmission T_x	75.6 mW
Energy cost of a device C_i during normal state	1.2 mW
Energy cost of a device C_i during sleep mode	0.7 \$/mu \$W
Coverage area of the transceiver module	400 M
Packet size	128 Kbps
Type of the network traffic	UDP and CBR
Transmission interval of device C_i	As per requirement
Topology T_x	Random deployment
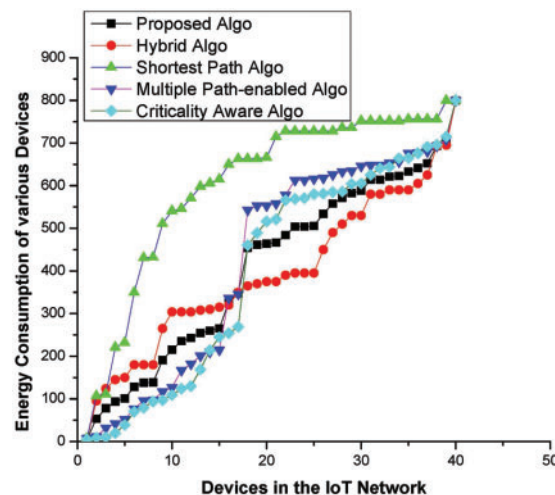
Figure 4: Energy consumption metric *vs.* the number of devices

4.2 Lifespan of the IoT Networks and Individual Devices

In addition to the efficient utilisation of the onboard batteries, the lifespan of the network is equally important, and eventually, those techniques will be preferred that ensure the maximum lifespan of the entire IoT network. Additionally, we have assumed that a network becomes disconnected if the very first device Ci consumes its onboard battery power. In the proposed methodology, devices Ci are smart such that a path or neighbouring device Ci is skipped if its available power is below the defined threshold value, i.e., 70% of the onboard battery. From the network's lifetime perspective, the proposed scheme performs exceptionally well compared to the existing state-of-the art approaches because every device Ci is bound to communicate through the most optimal path(s) available in its coverage area or domain. Additionally, devices Ci may use alternative paths, but the ratio of packets transmitted via those paths is minimal as compared to the optimal path in the IoT networks. Performance comparisons of the proposed and existing mechanisms are presented graphically in Fig. 5, where it is evident that the proposed methodology is one of the possible solutions for homogeneous IoMT networks.
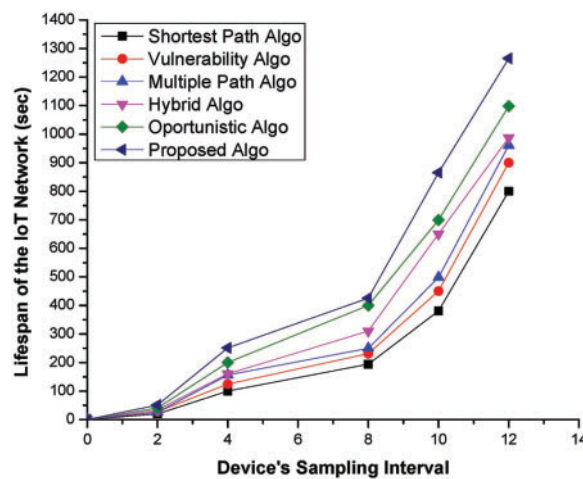

Figure 5: Statistical lifespan metric *vs.* the sampling interval

4.3 Networks Throughput Analysis

The throughput is defined as how many packets were generated, transmitted, and successfully received by the intended destination device in the IoMT networks. This metric is very important as far as load balancing schemes are considered, where maximum throughput is always appreciated and is a requirement of every organisation. We have observed that the proposed methodology, i.e., machine learning-enabled scheme, has attained the maximum possible ratio in almost all formats, which is evident from Fig. 6. These results are convincing, as the proposed approach not only ensures transmission of packets via the most optimal path, but also enhances the operational capabilities of these devices, especially in terms of making an informed decision. Thus, if decisions are informed, i.e., machine learning based, then it is highly likely that the maximum possible throughput is attained, as is evident from the graphical results. Moreover, since it is possible that multiple devices share a common path, this may lead to rapid disconnection if maximum traffic is forwarded via this path. To resolve this scenario, the proposed approach has bound every device C_i to send packets on two different paths. Additionally, a device C_i should inform its neighbours if its battery falls below a certain threshold value.
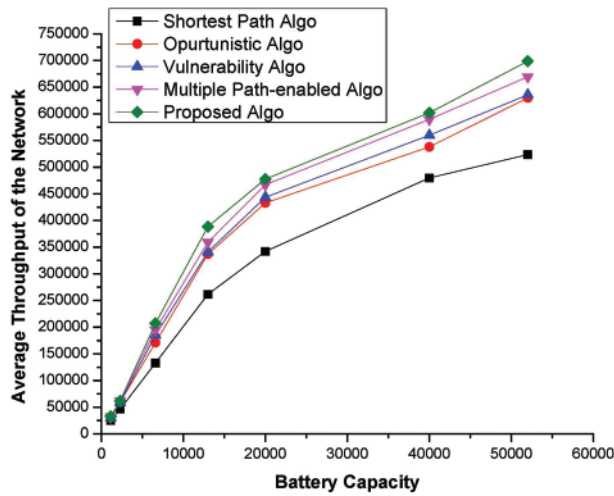
Figure 6: Throughput metric *vs.* the battery capacity

4.4 Latency Analysis

An important evaluation metric is latency, and every load balancing scheme must ensure the attainment of the minimum possible value for this metric. Latency is affected by various metrics, such as the number of devices in a potential optimal path. Latency is the delay, that is encountered due to transmission, processing, and waiting in a queue, along with other metrics. If device C_i is increased, then it is highly likely that average latency will increase dramatically. Therefore, in the proposed methodology, we have tried to attain the minimum possible latency by bounding potential source devices C_i to transmit the majority of their packets on a preferably optimal path, where latency is one metric in the search process for the underlined optimal path. From Fig. 7, it is evident that the proposed scheme has achieved the minimum possible latency ratio in different networking infrastructures as compared to the existing state-of-the-art approaches.
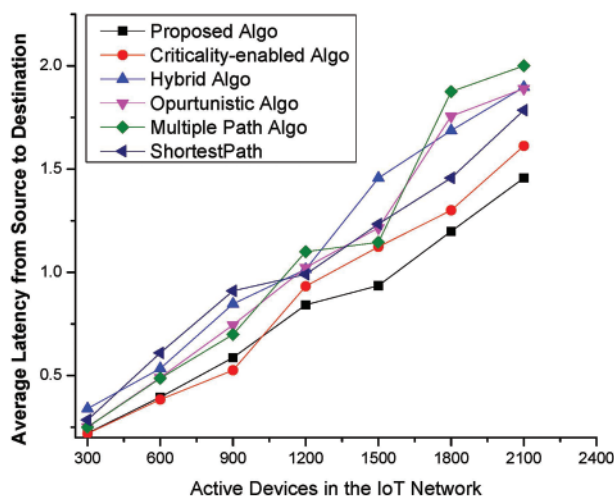

Figure 7: Latency metric *vs.* the number of active devices

4.5 Analysis of the Packet Delivery Ratio

Packet delivery ratio (PDR) is defined as the total number of packets received during the entire transmission, which is affected due to several reasons such as collision, congestion, path loss, etc. Additionally, the reliability of the scheme, preferably routing or load balancing, is measured through the PDR ratio, and a scheme with a minimum ratio is assumed to be the best. A comparative analysis of the proposed machine learning-enabled load balancing approach with its counter-approches is presented graphically in Fig. 8, where it is clear that the proposed scheme's performance is better than other available approaches. To achieve this minimum possible PDR ratio, various checks have been imposed, and packets are forwarded via the most optimal but reliable paths in the networks. Additionally, devices C_i a minimum residual energy of E_r are skipped from the list of potential candidate devices to forward packets where it is likely that packets will be lost if the device consumes its power. Additionally, if a device observes that the current optimal path is congested, it will update its record and start forwarding packets on an alternative route, preferably the second optimal path.
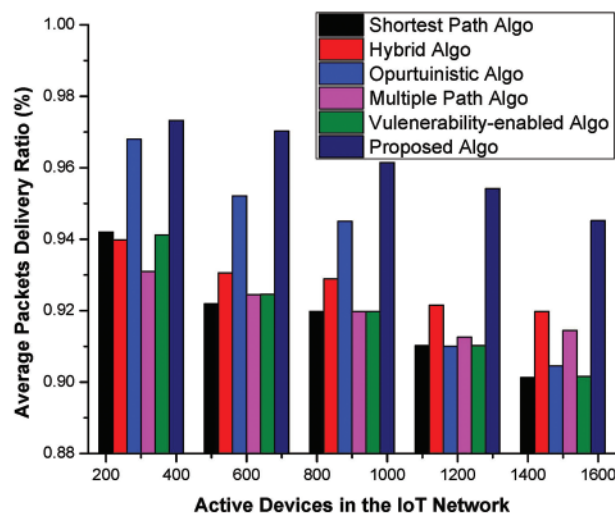

Figure 8: Packets delivery ratio metric *vs.* the number of active devices

5 Conclusion

Generally, the broadcasting mechanism is used for the transmission of packets in the IoMT networks, however, these approaches have some problems, such as congestion, energy efficiency, and excessive load on a particular device. In this paper, a novel approach based on machine learning is presented to find optimal paths among the interested communicating devices in the IoMT networks. For this purpose, it has extensively evaluated multiple neighbouring devices to find a reliable and shortest possible communication path between the two interested parties and then transmit frames via that path simultaneously. Additionally, every device is bound to hold a supplementary path, preferably a second optimised path, for situations where the current communication path is no longer available for communication. Furthermore, the machine learning approach will enable these devices to update their routing tables simultaneously, and the optimal path could be replaced if a better one is identified. The proposed mechanism has been tested using a smart environment developed for the Internet of Medical Things, especially smart healthcare. Simulation results show that the proposed machine learning-oriented approach performs better than existing approaches.

The proposed work could be extended by considering IoMT networks with mobile devices or multiple servers in place. Additionally, a direct or two-tier communication infrastructure could be a possible extension.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. M. Kamrul, S. Islam, I. Memon, A. F. Ismail, S. Abdullah *et al.,* "A novel resource oriented DMA framework for internet of medical things devices in 5G network," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 8895–8904, 2022.

[2] P. k. Sadhu, V. P. Yanambaka, A. Abdelgawad and K. Yelamarthi, "Prospect of internet of medical things: A review on security requirements and solutions," *Sensors*, vol. 22, no. 15, pp. 5517, 2022.

[3] M. A. Santos, M. Roberto, O. Rodrigo, P. R. Pedro, F. Rebouças *et al.,* "Online heart monitoring systems on the internet of health things environments: A survey, a reference model and an outlook," *Information Fusion*, vol. 53, pp. 222–239, 2020.

[4] R. A. Haraty, S. Kaddoura and A. S. Zekri, "Recovery of business intelligence systems: Towards guaranteed continuity of patient centric healthcare systems through a matrix-based recovery approach," *Telematics and Informatics*, vol. 35, no. 4, pp. 801–814, 2018.

[5] U. Zaman, M. Faisal, I. Naeem, K. Jungsuk and I. Muhammad, "Towards secure and intelligent internet of health things: A survey of enabling technologies and applications," *Electronics*, vol. 11, no. 12, pp. 1893, 2022.

[6] O. Hashash, S. Sharafeddine and Z. Dawy, "MEC-based energy-aware distributed feature extraction for mHealth applications with strict latency requirements," in *2021 IEEE Int. Conf. on Communications Workshops (ICC Workshops)*, Montreal, Quebec, Canada, pp. 1–6, 2021.

[7] M. Sharma and G. Singh, "Need and design of smart and secure energy-efficient IoT-based healthcare framework," in *Energy Conservation for IoT Devices: Concepts, Paradigms and Solutions*, vol. 206. Singapore: Springer, pp. 259–281, 2019.

[8] R. Akhter and S. A. Sofi, "Precision agriculture using IoT data analytics and machine learning," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 5602–5618, 2022.

[9] Y. Natarajan, K. Srihari, G. Dhiman, S. Chandragandhi, M. Gheisari *et al.,* "An iot and machine learning-based routing protocol for reconfigurable engineering application," *IET Communications*, vol. 16, no. 5, pp. 464–475, 2022.

[10] A. Nahar and D. Debasis, "MetaLearn: Optimizing routing heuristics with a hybrid meta-learning approach in vehicular ad-hoc networks," *Ad Hoc Networks*, vol. 138, pp. 102996, 2023.

[11] M. Vargheese, S. Vanithamani, D. Stalin and G. K. Rao, "Design of fuzzy logic control framework for QoS routing in MANET," *Intelligent Automation & Soft Computing*, vol. 35, no. 3, pp. 3479–3499, 2023.

[12] S. Kumar, G. Antriksh, G. Ruchir, P. S. Satya and A. Lay-Ekuakille, "A game-theoretic approach for cost-effective multicast routing in the internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 18041–18053, 2022.

[13] C. Li, L. Yang, X. Jing and Z. Jie, "MCEAACO-QSRP: A novel QoS-secure routing protocol for industrial internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18760–18777, 2022.

[14] S. He, D. Mianxiong, O. Kaoru, W. Jun, J. Jianhua *et al.,* "Software-defined efficient service reconstruction in fog using content awareness and weighted graph," in *GLOBECOM 2017-2017 IEEE Global Communications Conf.*, Singapore, pp. 1–6, 2017.

[15] Z. Liu, Z. Jiawei, L. Yanan, B. Lin and J. Yuefeng, "Joint jobs scheduling and lightpath provisioning in fog computing micro datacenter networks," *Journal of Optical Communications and Networking*, vol. 10, no. 7, pp. B152–B163, 2018.

[16] Z. Sun, L. Longxing, X. Xiaofei, L. Zhiguo and N. N. Xiong, "A novel nodes deployment assignment scheme with data association attributed in wireless sensor networks," *Journal of Internet Technology*, vol. 20, no. 2, pp. 509–520, 2019.

[17] K. L. M. Ang, J. K. P. Seng and A. M. Zungeru, "Optimizing energy consumption for big data collection in large-scale wireless sensor networks with mobile collectors," *IEEE Systems Journal*, vol. 12, no. 1, pp. 616–626, 2017.

[18] T. Wang, H. Luo, W. Jia, A. Liu and M. Xie, "MTES: An intelligent trust evaluation scheme in sensor-cloud-enabled industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2054–2062, 2019.

[19] Y. Shao, C. Li, Z. Fu, L. Jia and Y. Luo, "Cost-effective replication management and scheduling in edge computing," *Journal of Network and Computer Applications*, vol. 129, pp. 46–61, 2019.

[20] Y. B. Aissa, A. Bachir, M. Khalgui, A. Koubaa, Z. Li *et al.,* "On feasibility of multichannel reconfigurable wireless sensor networks under real-time and energy constraints," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 3, pp. 1446–1461, 2019.

[21] Y. Miao, Z. Sun, N. Wang, Y. Cao and H. Cruickshank, "Time efficient data collection with mobile sink and vMIMO technique in wireless sensor networks," *IEEE Systems Journal*, vol. 12, no. 1, pp. 639–647, 2016.

[22] P. D. Singh, G. Dhiman and R. Sharma, "Internet of things for sustaining a smart and secure healthcare system," *Sustainable Computing: Informatics and Systems*, vol. 33, pp. 100622, 2022.

[23] J. Tan, W. Liu, T. Wang, N. N. Xiong, H. Song *et al.,* "An adaptive collection scheme-based matrix completion for data gathering in energy-harvesting wireless sensor networks," *IEEE Access*, vol. 7, pp. 6703–6723, 2019.

[24] D. K. Sah, T. N. Nguyen, K. Cengiz, B. Dumba and V. Kumar, "Load-balance scheduling for intelligent sensors deployment in industrial internet of things," *Cluster Computing*, vol. 25, no. 3, pp. 1715–1727, 2022.

[25] P. S. Mehra, "Lbecr: Load balanced, efficient clustering and routing protocol for sustainable internet of things in smart cities," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, pp. 1–23, 2022.