Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Journal of Infection and Public Health 13 (2020) 1567–1575

Contents lists available at ScienceDirect

Journal of Infection and Public Health

journal homepage: http://www.elsevier.com/locate/jiph

Original Article

Secure and energy-efficient framework using Internet of Medical Things for e-healthcare

Tanzila Saba[a,*], Khalid Haseeb[b], Imran Ahmed[c], Amjad Rehman[a]

[a] Artificial Intelligence & Data Analytics Lab (AIDA) CCIS Prince Sultan University Riyadh, 11586, Saudi Arabia
[b] Islamia College Peshawar, Peshawar, Pakistan
[c] Institute of Management Sciences, Peshawar, Pakistan

ARTICLE INFO

Article history:
Received 21 April 2020
Received in revised form 20 June 2020
Accepted 25 June 2020

Keywords:
Internet of Medical Things (IoMT)
Biosensors
Data security
Energy efficiency
Health system
Healthcare

ABSTRACT

In various fields, the internet of things (IoT) gains a lot of popularity due to its autonomous sensors operations with the least cost. In medical and healthcare applications, the IoT devices develop an ecosystem to sense the medical conditions of the patients' such as blood pressure, oxygen level, heartbeat, temperature, etc. and take appropriate actions on an emergency basis. Using it, the healthcare-related data of patients is transmitted towards the remote users and medical centers for post-analysis. Different solutions have been proposed using Wireless Body Area Network (WBAN) to monitor the medical status of the patients based on low powered biosensor nodes, however, preventing increased energy consumption and communication costs are demanding and interesting problems. The issue of unbalanced energy consumption between biosensor nodes degrades the timely delivery of the patient's information to remote centers and gives a negative impact on the medical system. Moreover, the sensitive data of the patient is transmitting over the insecure Internet and prone to vulnerable security threats. Therefore, data privacy and integrity from malicious traffic are another challenging research issue for medical applications. This research article aims to a proposed secure and energy-efficient framework using Internet of Medical Things (IoMT) for e-healthcare (SEF-IoMT), which primary objective is to decrease the communication overhead and energy consumption between biosensors while transmitting the healthcare data on a convenient manner, and the other hand, it also secures the medical data of the patients against unauthentic and malicious nodes to improve the network privacy and integrity. The simulated results exhibit that the proposed framework improves the performance of medical systems for network throughput by 18%, packets loss rate by 44%, end-to-end delay by 26%, energy consumption by 29%, and link breaches by 48% than other states of the art solutions.

Introduction

Wireless Sensor Network (WSN) consists of various sensing stations also called sensor nodes that are dispersed into the observing area to sense the desired data [1–4]. All the nodes are self-governing and operated independently in an ad-hoc manner with nominal cost. The sensing data are further forwarded towards the sink node or Base Station (BS) via cluster head or local controller [5–7]. WSN is beneficial for many applications such as healthcare, military, agriculture, industries, smart vehicles, natural disaster, security, and surveillance, etc. However, the main problem of WSN is its restricted constraints on the part of sensor nodes in terms of memory, energy, transmission, and processing power [8,9]. The field of Wireless Body Area Network (WBAN) is a subset of WSN and can be exploited to determine the conditions of the human body. The medical experts obtained the required information from the BS using the Internet for continuing monitoring the status of patient's health. In healthcare applications, various biosensor nodes are attached to clothing or even implanted inside the human body to sense the activities of different parts.

The concept of the WBAN has been used firstly by ref. [10] and later many researchers have shown their interest. Like WSN and MANETs, WBAN has also some constraints in terms of energy, processing, computation, heterogeneity, and storage, etc. WBAN offers a remote facility to record the details of the patients' health based on biosensors. These biosensors are used to determine the

* Corresponding author.
E-mail addresses: drstanzila@gmail.com, rkamjad@gmail.com (T. Saba), khalid.haseeb@icp.edu.pk (K. Haseeb), imran.ahmed@imsciences.edu.pk (I. Ahmed), rkamjad@gmail.com (A. Rehman).

https://doi.org/10.1016/j.jiph.2020.06.027

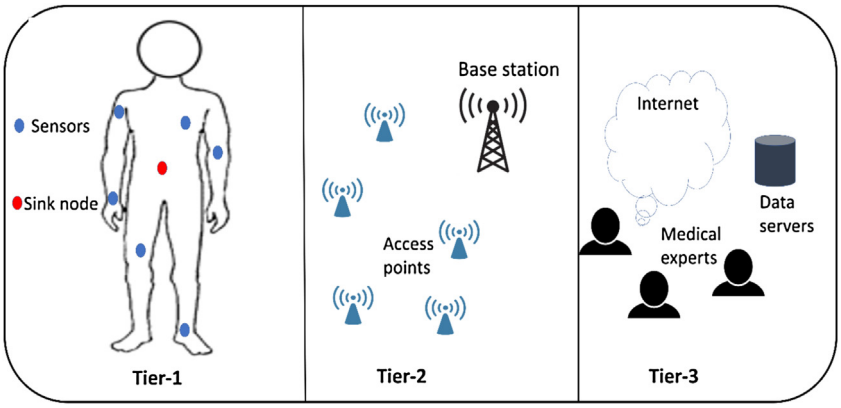

Fig. 1. The WBAN based medical system.

conditions of various parts of a patient's body such as temperature, ECG, blood pressure, heartbeat, motions, EEG, etc. The capture patient's data transmits to the central coordinator or sink node that is located inside the human body. The central coordinator further forwards the healthcare data towards BS through intermediate devices. Afterward, the medical experts obtained the required data from BS using the Internet for suitable tests and studies [11–13]. Accordingly, the doctor can suggest appropriate medicines to the patient or can take some immediate actions whenever sensors identify any problem. The architecture of WBAN can be divided into three tiers i.e. Intra WBAN, inter WBAN, and beyond WBAN. In Intra WBAN, biosensors are implanted inside the human body or deployed on the surface to detect different parts of the body and transmits the obtained reading towards the local coordinator. Usually, the local coordinator is a personal server and treated as a gateway, which interacts with another tier. In Inter WBANs, local coordinators or sink nodes processed and aggregate the received data and forwarded towards BS via various access points (AP). In the end, the beyond WBANs, the data are further transmitted from BS to medical centers for the storage patient history on various database servers. In the third tier, the doctor can be obtained the patient's data remotely and give the treatment on an emergency basis [14–16]. The infrastructure of a medical system based on WBAN technology is demonstrated in Fig. 1.

The domain of WBAN is inherited from the WSN technologies, therefore like WSN, the implanted biosensor nodes are also needing long-run battery power for proper functioning and processing of the health care data. The low power consumption, low latency, secure data aggregation, and QoS-aware transmissions are some major requirements for WBAN [17,18]. The energy of the biosensors is depleted during sensing, processing, and transmission operation and it is not possible to change or recharge the battery source while functioning, therefore improving energy consumption among biosensors without affecting the delivery ratio of e-healthcare application is one of the open research issues [19–22]. Besides, the sensitive data of patients are transmitted over the insecure Internet, an unauthorized user can manipulate healthcare measurements, thus data security and integrity are another major research interest for WBAN [23–25].

Therefore, this paper aims to propose a secure and energy-efficient framework using IoMT for digital healthcare applications to decreases the excessive energy consumption of the biosensor nodes and promptly achieve data delivery. The proposed data gathering and routing strategy are based on artificial intelligence methods to incur the least communication overheads and transmission costs. The proposed framework is suitable for digital healthcare applications using IoMT to provide energy-aware and secure conversation algorithms to recognize the pre-primary maintenance information of patients. The proposed framework facilitates the digital healthcare-related applications to analyze the patients' data intelligently and accordingly, medical experts give possible treatment on time. The proposed framework integrates the techniques of artificial intelligence with biosensors to automate the analysis of patients' data and obtained the outcomes with the least computation and communication costs. Due to this, the digital healthcare-related applications massive ability to increase medical conclusions in terms of treatment analysis and recommendations. Moreover, the proposed framework also offers secure and authentic methods to prevent privacy breaches and information integrity for digital healthcare applications.

The contributions of the proposed framework using IoMT for e-healthcare are based on the 3-tiers that are highlighted below.

i Firstly, the IoMT are interconnected in the form of a complete graph, such that there should be a unique edge, and by using composite factors a numeric weight is assigned to each edge.
ii Secondly, by using Kruskal's algorithm, the subgraphs are extracted by evaluating the minimum cost value and optimizes the routing decision from IoMT sensors to medical centers with the least network overheads and energy consumption.
iii In the end, the critical and sensitive medical information of the patients is kept secure over the Internet from malicious and potential threats based on lightweight cryptographic methods. The proposed framework offers a secure and authentic mechanism to route the healthcare information of the patient and ensures their integrity by avoiding the dangerous harm to the patients' data.

The simulation results have been done and the experimental analysis demonstrated the improved outcomes for the e-healthcare and medical systems in the comparison of other work for various energy-efficient routing and data security parameters.

The rest of the paper is organized into the following subsections. The related studies and finding problems are addressed in section 2. Section 3 discusses the detail of the proposed framework along with its designed components. The setup for simulation is presented in Section 4. The experiments and their discussions are presented in Section 5. The research article concludes in Section 6 and endorses future work.

Related work

In recent decades, WBAN plays a very important role in medical and non-medical applications due to its efficient and low computation cost. Most of the WBAN-based proposed solutions are for medical purposes to monitor the patients' health, prescribe

medicines and emergency calls, etc. The non-medical applications using WBANs are sports, military, security, etc. that can be used to give-and-take information between machines and entities. WBAN performs a vital job for the patients that cannot be able to visit the hospitals regularly and needs mobility. Therefore, the biosensors are wearable or implanted inside the body of the patient in such a manner that the doctor can investigate the patient's body from a remote location over the Internet. During the investigation, if the doctor diagnoses any problem, then using a smart system alert message is sent to the patient cellular phone. Furthermore, the implant sensors do not create any dis-comfortability for the body and humans can continue their daily tasks very easily. The components are WBAN consist of modules, coordinator node, WBAN communication, and remote centers. The first part consists of different sensors that can be placed inside or outside the human body for continuous observing of functions of various body parts. Usually, these sensors are cost-effective with low powered battery and operate autonomously. All the biosensors offer their outcomes to the coordinator node, often called as Central Control Unit (CCU). Afterward, the coordinator nodes further transmit the biosensors data to the next station i.e. tier-2. There are several wireless communication approaches such as WIFI, 3 G, 4 G, GSM to forward the biosensors data from coordinator nodes to the next station. Afterward, the mobile cellular phone, personal computers, and router like devices can be treated as the gateway nodes to transfer the received biosignals towards the medical center via some wireless broadband services. In the end, the medical centers are composed of various database servers, mobile phones and PCs to send the text messages, observing the patient's conditions and store the information for future purposes [26,27].

The routing protocols in WBAN [28–30] can be divided into temperature-aware, QoS-aware, cluster-based and cross-layered categories. In the QoS-aware routing protocol, various network metrics are taken into account for data transmission. In cluster-based solutions, the network is divided into clusters with one cluster head inside each cluster, and the communication towards BS can be either a single-hop or multi-hop. Temperature-aware routing protocols aim to reduce the temperature rising of the sensor nodes while achieving balanced energy consumption and efficient routing decision. In cross-layer routing solutions, protocols are operated on different layers to share the network information and the optimal route is chosen based on the various network parameters. The authors [31], proposed a self-organization protocol (ANY-BODY) for WBAN, which aims to split the sensors into clusters, and data packets are transmitted from clusters towards the sink node. Instead of using multi-hop communication the proposed protocol makes use of single-hop and forwarded the data packets data directly from cluster heads to sink node. The proposed solution improved the network performance as compared to traditional LEACH protocol and decreases energy consumption among sensors. The authors in ref. [32], presents that network reliability and energy efficiency are the major research demands in WBAN for the accurate monitoring of the patients' health. They highlight the multi-hop problem during the collection of the data from the patient's body and due to traffic load, the uneven energy consumption incurs between WBAN sensors. They proposed the tree-based energy-efficient routing scheme (EERS) to achieve multi-hop routing with low overheads. Moreover, the proposed solution proposed an end-to-end routing path in an energy-efficient manner with an adaptive transmission power of WBAN sensors. In ref. [33], the authors proposed iM-SIMPLE, which aims to offer reliable and power-efficient routing protocol. The experimental results demonstrate the proposed solution increases network throughput and decreases energy consumption between sensor nodes. The cost function using residual energy and distance to sink and data forwarders are selected by using the minimum cost. Moreover, using an integer linear program the energy consumption and network throughput are formulated. Authors in ref. [34], proposed adaptive medium access control (A-MAC) protocol for WBAN based on linear programming, which aims to decreases energy consumption and increases data flow. In the proposed protocol, the sensors are continuously monitoring the various parts of the human body and provide updated information. If the current value is in the normal range, then the proposed solution offers that there is no need to access the channel. However, if the current value exceeds the permissible range, then sensors power on their transceiver and access the channels. The simulated results illustrate that the proposed protocol improves network lifetime and throughput in the comparison of existing work. An energy-efficient routing protocol (EERP) for WBAN is proposed by ref. [35], which aims to present an efficient and reliable solution for power consumption and stability of the network. In the proposed solution cost-based function is used using two different parameters and reduces the communication distance for data forwarding by using multi-hop data transmission. The simulation experiments reveal better results than other solutions. In ref. [36], the authors proposed an optimized cost-effective, and energy-efficient routing protocol for WBAN, which aims to increase energy efficiency and reliability. The proposed solution uses the Genetic algorithm and optimized cost function based on residual energy, link reliability, and path loss factors. Accordingly, the optimized route is used for data transmission from the body coordinators towards the sink node. Moreover, the proposed solution makes use of multi-hop routing and reduces the communication distance between sensor nodes. The simulation experiments reveal improved performance as compared to existing work. The authors in ref [37]. proposed a robust and efficient energy harvested-aware routing protocol with a clustering (EH-RCB) approach for WBAN. The proposed solution stabilized WBAN operations due to the selection of the best forwarder nodes. The forwarder node is chosen by using the cost function, which comprised of signal to noise ratio, transmission power, the distance between nodes and total available energy factors. The simulated results demonstrate improved network performance in terms of different performance metrics as compared to existing studies.

In ref. [38], the authors proposed an efficient next-hop selection algorithm for multi-hop body area networks (ENSA-BAN), which aims to improve the network performance in terms of existing routing solutions. The proposed algorithm aims to select the appropriate next-hop among the neighbors for multi-hop data transmission. The selection of the next-hop is based on the link cost function, which depends on residual energy, available buffer size, and link reliability. Using the cost function, the proposed algorithm balances the energy consumption and decreases the ratio for the end-to-end delay. The factor of link quality in the proposed algorithms affects the requirements of QoS and nodes' energy consumption. The authors in ref [39]. proposed energy-aware link efficient routing approach for WBAN (ELR-W), aims to improve the energy-oriented network metrics for healthcare-related application in the comparison of existing work. The proposed solution firstly makes use of beaconing information for the process of network initialization. Secondly, by using energy and link-aware efficiency, the path cost function selects the next-hop for data routing. The path cost function is based on residual energy, hop count, link efficiency, and distance to body node coordinator. The simulation-based evaluation demonstrates the improved performance for network throughput and energy consumption than other solutions. The authors in ref. [40] proposed the dual sink approach using clustering in the body area network, which aims to improve network stability and throughput. The proposed solution provided a cluster-based scheme with dual sinks to reduce the end-to-end delay and network congestion. Moreover, the forwarder node is selected based on the cost function that consists

of residual energy, distance to sink, and transmission power to achieve reliable routing. In ref. [41], the authors proposed energy-aware WBAN for health monitoring using critical data routing (CDR), which aims to increase the energy level and lifespan of the network. The proposed solution avoids the redundant data packets and only forwards the critical information towards the sink node. All the sensor nodes sensed the data and determine their threshold level, and accordingly, data packets are splits into critical or non-critical. The simulated experiments demonstrate that proposed solution improves the network performance for throughput, packet drop rate, ratio of collision and network stability as compared to other solutions. The authors proposed a simplified energy-balanced alternative-aware routing algorithm (SEAR) for WBANs [42], which aims to improve the procedure of route request and route response and according it modifies the routing cost. The proposed solution selects the alternative routing path along with main routing path to decrease the network delay in case of link failure. Moreover, based on the residual energy and data load factors, the intermediate node is selected for the role of next-hop. The experimental results illustrated the improved results for the end-to-end delay, energy consumption, and network throughput than existing solutions.

It is seen from the related studies that WBAN is the subgroup of WSN, and biosensors are restricted in terms of resource constraints. The significant limitations are energy, computing, processing, transmission, and storage resources. Different authors have proposed solutions to improve the network performance for WBAN, but still, energy-efficient and reliable data forwarding are most of the important research issues of WBAN healthcare applications. Some solutions are proposed based on the tree mechanism but such approaches increase the latency ratio and in case of bottleneck a lot of route rediscoveries are triggered. Although some solutions have been proposed and optimizing the network performance based on cost functions, such solutions incur too much exchange of control messages and do not consider the limited constraints on the part of biosensors, which results in the consumption of additional energy resources and network overheads. Moreover, some solutions are proposed based on clustering schemes, such approaches improved the network connectivity, however, they perform rapidly the phase of re-clustering without evaluating the status of the nodes. It is also observed that most of the WBAN based solutions incorporate link evaluation in computing the cost function, which results in routing stability with reliable data delivery performance. However, such solutions incur additional overheads to compute the cost function due to flooding of many control and beacon messages. Also, such solutions overlooked data security and nodes' integrity, which are also a significant parts of consistent and trustworthy healthcare-related applications. The sensitive data of patients is transmitted from the local body coordinators to remote medical centers via the Internet which is insecure and openly available for malicious and potential attacks, therefore, a secure data routing in terms of confidentiality, authentication and integrity should be considered to design routing solution for WBAN-based applications with nominal overheads on sensor nodes.

Proposed secure and energy-efficient framework using IoMT for e-healthcare

This section presents a detailed discussion of the proposed framework, which is designed and developed for medical applications. The proposed framework improving the energy consumption between biosensors and increases the security level of patients' data using WBAN from a sink node to medical centers. The framework offers efficient, reliable, and trusted techniques to monitor the physical health of patients from a remote location on an emergency basis. Before, discussing the details of the framework, we mention some network considerations for modeling and designing the framework. All sensor nodes have equipped with Global Positioning System(GPS) and known their adjacent nodes. All the sensor nodes have homogenous in terms of energy, memory, and transmission power. Sink node has no limitation of resources and has more computing power as compared to sensors. The sensor nodes capture the data from the patient's body and forwards towards the sink node, which is also located inside the patient's body. The healthcare data reach to medical experts via intermediate devices from the sink node. The malicious nodes can attack the network infrastructure to abolish data privacy, authenticity, and integrity. They solely drop the data packets and broadcast invalid packets for route requests and responses to show its realism.

Framework architecture

The design of the proposed framework is comprised of two main algorithms. In the first algorithm, biosensors interconnected to each other in the form of the complete graph $\boldsymbol{G}$ and there is a unique edge $\boldsymbol{E}$ between the set of nodes $\boldsymbol{N}$. Using a multi-parameters metric a weighted value is assigned to each edge which denotes its cost. The cost is comprised of weighted residual energy, hop counts to sink, distance to neighborhoods, and queuing delay factors. The cost function offers to generate spanning sub-graphs $\boldsymbol{S_i}$ in terms of minimum cost with some conditions as follows. Firstly, there is no cycle in the sub-graph, secondly, all the vertices must be connected and in the last, for $\boldsymbol{n}$ vertices, there should be $\boldsymbol{n}-1$ edges in the sub-graph. The sub-graph is constructed based on Kruskal's algorithm [43,44] such that each node contains the optimized list of neighbor nodes for forwarding healthcare information towards the sink node and from the sink node to medical centers. Unlike most of the other solutions, the proposed framework uses composite parameters to compute the cost function. Moreover, the subgraphs are restored based on the updated cost using optimum learning. Finally, in the end, the healthcare data is transmitted securely towards the medical experts based on the cipher block chaining algorithm [45,46]. The detail of the proposed algorithms is discussed in the following sub-sections. The research design of the secure and energy-efficient framework based on artificial intelligence for medical systems using IoMT is demonstrated in Fig. 2.

Intelligent routing based on the minimum and optimal cost computation

In this algorithm, biosensors are interconnected to each other in the form of the undirected graph using a cost function $f(c)$. The cost function is based on weighted residual energy *WRE*, the number of hops to sink $h(c)$, distance to neighborhoods N_{d} and queuing delay Q_{d} factors. All the factors are summed up in the collective form and each part has significant importance on the computation of cost function. All the biosensors generate a connected graph or spanning tree, such that each biosensor should be connected to its neighbors. There must be one unique edge between two consecutive nodes, which shows the calculated cost value by using multiple parameters.

In the beginning, the sink node advertised its position by flooding the location packet, and accordingly, sensors determine the current position of the sink. Each time when any sensor node receives the location packet of the sink node, it records the value of hop count in the routing table and increases the packet counter value by 1. The routing table of each node also comprised of the identification ID of its point-to-point neighbors. Moreover, sensor nodes compute the proportion of their weighted residual energy on periodic time interval Δt and flood the information to one-hop neighbors so they can update the routing tables. Let's consider that

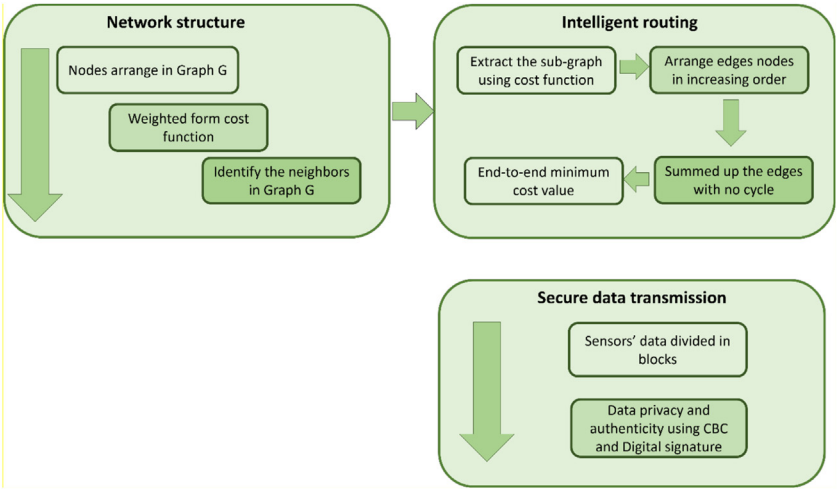

Fig. 2. The research design of the proposed secure and energy-efficient framework using IoMT for e-healthcare.

node i computes the ratio of consumed energy with a neighbor n by using Eq. 1.

$$C_e = (e_{init} - e_{tx}(k))/e_{net} \tag{1}$$

In Eq. 1, e_{max} is initial energy, $e_d(k)$ denotes the amount of transmission energy while forwarding k data bits on periodic time interval Δt, and e_{net} shows network energy. Accordingly, each node i determines the consumed energy $C_{e1}, C_{e2}, .., C_{en}$ with neighbors $n_1, n_2, \ldots, n_n$ during transmitting k data bits and determined the *WRE* as given in Eq. 2.

$$WRE = C_{e1} + C_{e2} + \ldots + C_{en} \tag{2}$$

Afterward, each node forwards the outcome of *WRE* to neighbors, and the obtained information is store in the routing table. The routing table is constructed only in the network initialization process and it updates the contents whenever there is any change arises among the neighbor attributes. The sensor nodes also compute the distance between their neighborhoods that originate in a certain region. Afterwads, the determined information is forwarded towards a one-to-one neighbor. Let's suppose, $d_{n1}, d_{n2}, .., d_{nn}$ are the communication distance of all the neighbors n, then the weighted distance to the source node N_{d} is determined as given in Eq. 3.

$$N_{\mathrm{d}} = (d_{n1} + d_{n2} + \ldots + d_{nn})/n \tag{3}$$

Moreover, along with the number of hops to sink, distance to neighborhoods and weighted residual energy, the cost function is also dependent on the queuing delay Q_{d}. The queuing delay depends on the arrival rate of the data packets to the sensor node and the transmission capacity of the outgoing link. Suppose that a_{r} is the arrival of the data packets D_{i} to sensor node i and t_{c} is transmission capacity of the link, then queuing delay Q_{d} can be computed as given in Eq. 4.

$$Q_d = (a_r + t_c)/D_i \tag{4}$$

Finally, each node makes use of the computed values of weighted residual energy, the number of hops, distance to neighborhoods, and queuing delay to determine the cost value by using Eq. 5.

$$f(c) = \mathrm{w1}^{*}WRE + \mathrm{w2}^{*}\left(\frac{1}{h_{\mathrm{c}}}\right) + \mathrm{w3}^{*}\left(\frac{1}{N_{\mathrm{i}}}\right) + \mathrm{w4}^{*}\left(\frac{1}{Q_{\mathrm{d}}}\right) \tag{5}$$

In Eq. 4, w_1, w_2, w_3, and w_4 are weighted coefficients and their summation must be equal to 1.

Afterward, the framework extracts the subgraph by using Kruskal's algorithm in such a manner that it gives the most optimal route entries based on minimum cost value. In this work, there are some rules to be followed to extract the sub-graph that is given below.

i If there are two parallel edges between nodes $\boldsymbol{n}_1$ and $\boldsymbol{n}_2$ then the least cost edge is selected.
ii If there are multiple edges between consecutive nodes with the same cost values than anyone can be chosen.
iii Arrange all the edges in the increasing order in terms of computed cost value.
iv Extract and summed up the edge that has the least cost value with no cycle. Repeat this process until the end-to-end routing path towards the sink node is extracted. Finally, the minimum cost $\boldsymbol{M_c}$ of the extracted sub-graph can be computed by summation as given in Eq. 6.

$$\boldsymbol{M_c} = \boldsymbol{f}(\boldsymbol{c_{n1}}) + \boldsymbol{f}(\boldsymbol{c_{n2}}) + \boldsymbol{f}(\boldsymbol{c_{n3}}) + \ldots + \boldsymbol{f}(\boldsymbol{c_{nn}}) \tag{6}$$

In Eq. 6, $\boldsymbol{n}1$, $\boldsymbol{n}2$, $\boldsymbol{n}3, \ldots,$ $\boldsymbol{nn}$ is set of nodes that give optimal routing decision towards sink node with minimum cost based on weighted energy, the number of hops to sink node, distance to neighborhoods, and queuing delay parameters.

Secure data transmission

This section presents a developed secure algorithm of the proposed framework to forward sensitive information about the patient's body from a sink node to the medical centers by using a cipher block chaining algorithm. Also, the proposed algorithm validates the encrypted chain of sensors' data by computing the digital authentication using private-public cryptography. In this work, the data blocks $D_0, D_1, D_2, \ldots\ldots, D_n$ are encrypted in the form of chain and generates a set of cipher blocks $C_{b0}, C_{b1}, C_{b2}, \ldots\ldots C_{bn-2}, C_{bn-1}, C_{bn}$. Based on the cipher block chaining algorithm data block D_i for node i is XoR with the cipher block C_{bi-1} of the previous data block D_{i-1} and encrypted with the secret key K. Next, the encrypted block is digitally signed by the private key of node i PR_i as given in Eq. 7.

$$C_{bi} = E(PR_i(E_k(C_{bi-1} \oplus D_i))) \tag{7}$$

Afterward, the node $i+1$, firstly decrypts the entire data block using the public key of node i PU_i to verify the data and node authenticity as $E(PU_i(C_{bi})$. And accordingly, the data block D_{i+1} for

node $i+1$ is XoR with the cipher block Cb_{i-1} of the previous data block D_{i-1} for node i and encrypted with the same key K. Also, the encrypted block is digitally signed by the private key of node $i+1$ PR_{i+1} as given in Eq. 8. Accordingly, the cipher block of each data block depends on all the previous data blocks.

$$C_{bi+1} = E\,(PR_{i+1}\,(E_k\,(C_{bi-1} \oplus D_i))) \tag{8}$$

In this way, the data blocks are forwarded from the sink node towards medical centers via intermediate nodes in the form of a block of chains with data confidentiality, authentication and integrity. . Upon receiving the data blocks at medical centers, each data block is passed via the decryption algorithm using the same key K, and then the outcome is XoR with the previous cipher block to generate actual data block D_i as given in 9.

$$D_i = D\,(K\,(E_k\,(C_{bi-1} \oplus D_{i+1})) \oplus C_{bi-1}) \tag{9}$$

The pseudocode of the proposed SEF-IoMT framework is explained as follows.

Pseudocode: Secure and energy-efficient framework using IoMT for e-healthcare

1 procedure INTELLIGENT ROUTING (R)
2 arrange the sensor nodes in Graph G using cost function $f\,(c)$
3 for (i = 1; i<=neighbors ;i++)
4 do
5 Compute the cost function by using C_e, E, N_d, Q_d
6 $f(c)$ = w1 * $\frac{1}{WRE}$ + w2 * h_c + w3 * N_i + w4 * Q_d
7 end for
8 extract sub-graphs by applying Kruskal's algorithm with least cost edge
9 organize all the extracted edges in increasing order
10 minimum cost $M_c = f\,(c_{n1}) + f\,(c_{n2}) + f\,(c_{n3}) + \ldots + f(c_{nn})$
11 end procedure
12 procedure secure data transmission
13 for each $node_i \in [1 : R]$
14 do
15 node i also apply CBC mode with key K and digital signature using PR_i
16 C_{bi} = $E\,(PR_i\,(E_k\,(C_{bi-1} \oplus D_i)))$
17 node $i+1$ verifies the incoming cipher block using PU_i as $E\,(PU_i(C_{bi})$
18 performs CBC mode on the data block with key K and digital signature D_{i+1} as
19 C_{bi+1} = $E\,(PR_{i+1}\,((E_k\,(C_{bi-1} \oplus D_{i+1})))$
20 end for
21 data blocks $D_0, D_1, D_2, \ldots\ldots, D_n$ encrypted in chain of cipher blocks
22 $C_{b0}, C_{b1}, C_{b2}, \ldots\ldots C_{bn-2}, C_{bn-1}, C_{bn}$
23 medical centers apply decryption algorithm using the key K
24 $D_i = D(K\,(E_k\,(C_{bi-1} \oplus D_{i+1})) \oplus C_{bi-1}$
25 end procedure

Simulation setup

This section presents the simulation setup using the simulation tool NS3. The sensor nodes are deployed in the area of 15m2. The number of sensor nodes is set to 10 that are deployed on the body of the patient. The sink node is located in the center of the patient body and acts as a local coordinator. Sink node is considered as a more powerful node in terms of resources as compared to sensor nodes. The initial energy of the sensors is set to 1 j and their transmission range is fixed to 2 m. The simulation interval is set to 250 s. The data flow between sensors and the sink node is based on a constant bit rate (CBR). Table 1 illustrates the default simulation parameters. The malicious nodes are set to 5 between tier 2 and tier 3. The

Table 1
Simulation parameters.

Parameter	Value
Simulation area	15m × 15m
Sensor nodes	10
Malicious nodes	5
Packet size, k	32 bits
Energy level	1J
Transport layer protocol	UDP
Control message	25 bits
Simulation time	250 s
Transmission range	2 m
Traffic type	CBR

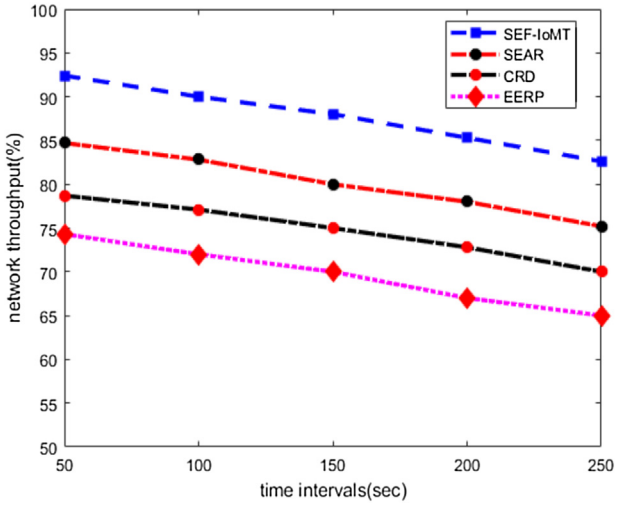

Fig. 3. Time intervals and network throughput.

packet size in terms of bits is set to 32. In this work, we assumed the energy model as adopted in ref. [47]. The energy consumption of sensor nodes varies based on the transmitted and received data bits as given in Eqs. 10 and 11.

$$E_{tx}\,(k, d) = E_{elect}{}^{*}k + k^{*}E_{fs}{}^{*}d^2 \tag{10}$$

$$E_{tx}\,(k) = E_{elect}{}^{*}k \tag{11}$$

Where E_{tx} and E_{rx} are the transmitting and receiving energy, k is data bits, d is the distance among sensor nodes, E_{elect} is the amount of consumed energy per data bit and energy of the transmit amplifier is denoted by E_{fs}.

Statistical results and discussion

In this section, the statistical results of SEF-IoMT against existing solutions EERP [35], CRD [41], and SEAR [42] are discussed. This selection evaluates the performace for various network parameters. i.e network throughput, packet loss rate, end-to-end delay, energy consumption, and link breakages.

Network throughput

The Fig. 3 demonstrates the simulation experiment for network throughput between SEF-IoMT and exiting work. It is observed from the simulation results that SEF-IoMT remarkably increases the ratio of network throughput by 9%, 17%, and 29% under varying time intervals as compared to other solutions. This is due to that SEF-IoMT makes use of multi-hop data transmission between sensors and the sink node. Moreover, the existing solutions SEAR, CRD, and EERP do not consider the link measurement for data routing, and mostly weak transmission channels are adopted for

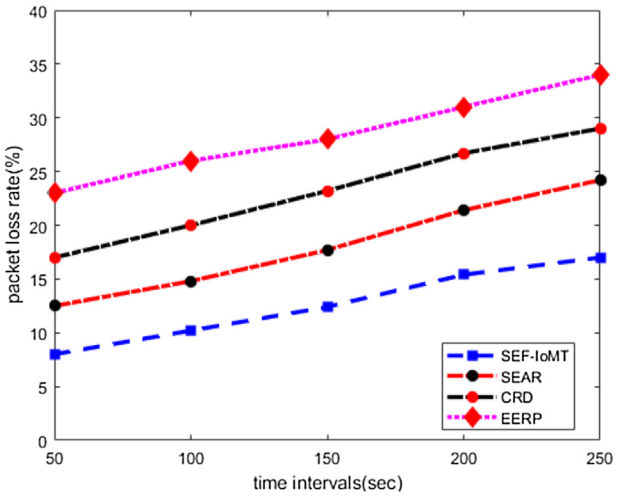

Fig. 4. Time intervals and packet loss rate.

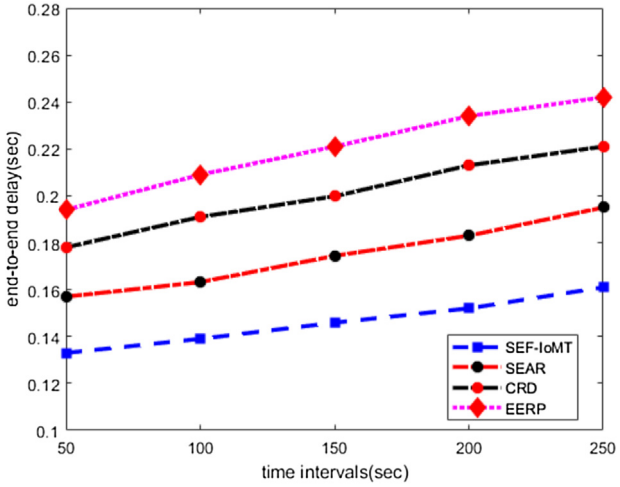

Fig. 5. Time intervals and end-to-end delay.

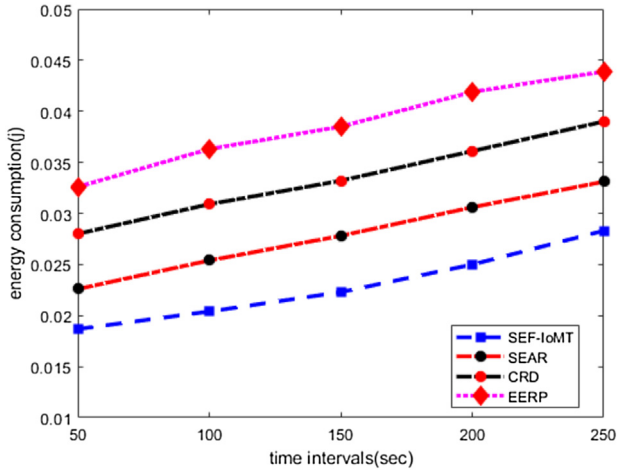

Fig. 6. Time intervals and energy consumption.

data forwarding. The proposed SEF-IoMT offers more reliable and energy-efficient links for routing using artificial intelligence-based techniques and leads to improved network throughput. Furthermore, the existing solutions overlooked data security in routing and false entities frequently generate route request packets, which results in heavy network congestion. Moreover, the existing solutions cannot avoid notifications by malicious nodes that brings down throughput to an unacceptable level.

Packets loss rate

Fig. 4 illustrates the behavior of SEF-IoMT in the comparison of existing solutions for the packet loss rate. It is seen from the simulation results that SEF-IoMT decreases the level of packet loss rate by 30%, 46%, and 56% as compared to other solutions at varying time intervals. The SEF-IoMT outperforms SEAR, CRD, and EERP because the designed cost function for SEF-IoMT based on multiple factors and leads to energy-efficient, shortest, and link-aware routing decisions. Moreover, the integration of data security using cipher block chaining also increases the security level on each data block and makes it very hard for malicious nodes to alter and drop the data packets. Due to the absence of link measurement and data security in existing solutions allow malicious nodes to generate the network traffic on the transmission medium thereby disturbing the flow of data packets. The SEF-IoMT achieves more stable routing paths from biosensors to sink node and from sink node to remote medical centers, which reduces the chances of packets dropping and increases the stability of data delivery performance.

End-to-end delay

Fig. 5 demonstrates the performance evaluation of SEF-IoMT against existing work in terms of end-to-end delay. The experimental results revealed that SEF-IoMT decreases the ratio of end-to-end delay by 17%, 28%, and 34% under varying time intervals as compared to other solutions. This is due to that SEF-IoMT chooses more energy-efficient, secure and stable routes for data transmission and minimizes the chances of data delay with fewer wireless retransmissions. Unlike the SEAR, CRD, and EERP solutions that select the next-hop without consideration of the conditions of the wireless channel and lead to rapid route re-discoveries, such approaches incur an additional end-to-end delay in data reception. The SEF-IoMT exploits artificial intelligence-based evaluation of next-hop and makes use of multi-parameters metric, such an approach increases the lifetime of the route and decreases the network latency. Moreover, the incorporation of security aspect in SEF-IoMT avoids the behavior of malicious nodes to route the data on longer routes and also decrease the prospects of network disconnection, which results in achieving improved end-to-end delay rate.

Energy consumption

In Fig. 6, the performance results of SEF-IoMT is compared with existing work in terms of energy consumption. The numerical analysis demonstrates that SEF-IoMT improves energy consumption by 17%, 31%, and 40% in varying time intervals as compared to other work. The SEAR, CRD, and EERP solutions consumed additional communication costs and energy consumption in the construction of reliable routing paths. As such solutions do not judge the condition and status and transmission medium while sending the data packets, which results in deplete high proportion of energy resources in the re-construction of routes. The design of SEF-IoMT focuses on energy-efficient, shortest, consistent, and secure routing paths, which balances the energy consumption between the sensor nodes. The multi-parameters metric reduces the extra overheads on node levels due to the selection of most trusted links for data forwarding and decreases the ratio of energy consumption of the nodes in generating unnecessary route request packets. Moreover, the robust and intelligent based nodes extraction in subgraphs

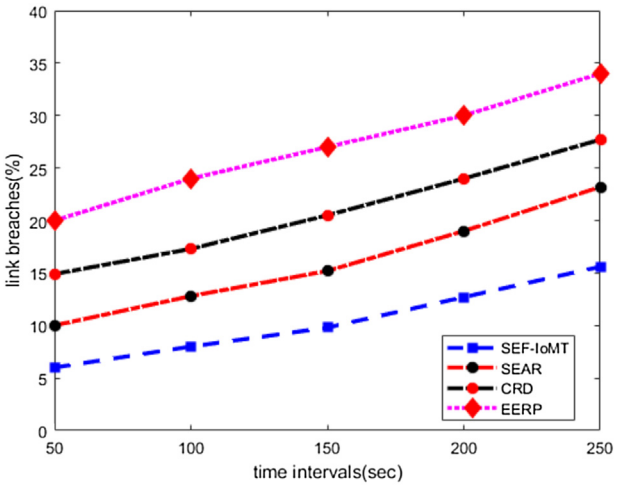

Fig. 7. Time intervals and link breaches.

leads to choose the minimal weighted cost route in terms of energy efficiency, distance, and link performance.

Link breaches

In Fig. 7, the experimental results have been shown between SEF-IoMT and other solutions in terms of link breaches. The numerical analysis demonstrates that SEF-IOMT outperforms the reducing rate of link breaches by 35%, 49%, and 61% as compared to existing solutions. The SEAR, CRD, and EERP solutions suffer from choosing trusted routing links because they overlooked both the evaluation of wireless channels and security level between next-hops. Due to this, the routing paths in SEAR, CRD, and EERP are more prone to failure and need a lot of route requests and route re-discoveries packets, which caused additional overheads of sensor nodes. In SEF-IoMT, the proposed security mechanism based on a cipher block chaining and digital signature guarantee to achieve reliable and secure routing while maintaining the energy efficiency. Moreover, extracting sub-graphs based on the artificial intelligence approach increases the strength of chosen routes based on the composite cost function. As a result, the SEF-IoMT requires minimal calls for route maintenance and leads to stable network performance.

Conclusion

WBAN performs a vital role in medical systems by observing the health of patients and forward the information towards remote medical centers for appropriate actions. However, due to the limited constraints of sensors, it needed an energy-efficient and reliable data transmission solution. Moreover, patients' sensitive data are more prone to potential threats and leads to compromised data security. In this work, we proposed a secure and energy-efficient framework using IoMT for e-healthcare, which aims to decrease energy consumption and increase data delivery on time towards medical experts. The next-hop is selected based on multi-parameters which achieves an optimal and minimal cost routing path by using the Kruskal algorithm. Based on the Kruskal algorithm, the proposed framework extracts the subgraph intelligently from the complete graph and decreases the overall communication overhead. Moreover, since patients' data is transmitted over the insecure Internet via various access points, such data forwarding is harmful to data privacy and negotiated with data integrity. In this work, SEF-IoMT makes use of cipher block chaining to forward the data in the form of chains and increase the security level of e-healthcare data against malicious traffic. Moreover, along with the cipher block chaining algorithm, the private-public key based digital authentications are also incorporated in data transmission to ensure its validation and integrity. The simulation-based experiments are done and their statistical analysis demonstrated the SEF-IOMT is energy-efficient and more secure with lower network delay as compared to other work. In future work, we aim to improve the SEF-IoMT in mobility-based medical scenarios where sensors position are mostly transformed due to the movement of the human body. Also, the proposed SEF-IoMT framework needs to improve the level of energy consumption and network security for Inter-WBAN data transformation.

Funding

This work was supported by the research Project [Diagnosis of COVID-19 through Imaging Modalities using Deep Learning]; Prince Sultan University; Saudi Arabia [COVID19-CCIS-2020{54}].

Competing interests

None declared.

Ethical approval

Not required.

Acknowledgement

This work was supported by the research Project [Diagnosis of COVID-19 through Imaging Modalities using Deep Learning]; Prince Sultan University; Saudi Arabia [COVID19-CCIS-2020{54}].

References

[1] Ali A, Ming Y, Chakraborty S, Iram S. A comprehensive survey on real-time applications of WSN. Future Internet 2017;9(4):77.
[2] Banđur Đ, Jakšić B, Banđur M, Jović S. An analysis of energy efficiency in Wireless Sensor Networks (WSNs) applied in smart agriculture. Comput Electron Agric 2019;156:500–7.
[3] Hezaveh M, Shirmohammdi Z, Rohbani N, Miremadi SG. A fault-tolerant and energy-aware mechanism for cluster-based routing algorithm of WSNs. In: Integrated network management (IM), 2015 IFIP/IEEE international symposium. Ottawa: IEEE; 2015.
[4] Mahajan S, Malhotra J, Sharma S. An energy balanced QoS based cluster head selection strategy for WSN. Egypt Inform J 2014;15(3):189–99.
[5] Ahmed G, Zou J, Zhao X, Sadiq Fareed MM. Markov chain model-based optimal cluster heads selection for wireless sensor networks. Sensors 2017;17(3):440.
[6] Thakkar A, Kotecha K. Cluster head election for energy and delay constraint applications of wireless sensor network. IEEE Sens J 2014;14(8):2658–64.
[7] Wang A, Yang D, Sun D. A clustering algorithm based on energy information and cluster heads expectation for wireless sensor networks. Comput Electr Eng 2012;38(3):662–71.
[8] Dishongh TJ, McGrath M, Kuris B. Wireless sensor networks for healthcare applications. 1 ed. Artech House; 2014.
[9] Suciu G, Suciu V, Martian A, Craciunescu R, Vulpe A, Marcu I, et al. Big data, internet of things and cloud convergence – an architecture for secure E-Health applications. J Med Syst 2015;39(11):141.
[10] Van Dam K, Pitchers S, Barnard M. Body area networks: towards a wearable future. Proc. WWRF Kick off Meeting, Munich, Germany 2001.
[11] Darwish A, Hassanien AE, Elhoseny M, Sangaiah AK, Muhammad K. The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. J Ambient Intell Humaniz Comput 2017:1–16.
[12] Thota C, Sundarasekar R, Manogaran G, Varatharajan R, Priyan M. Centralized fog computing security platform for IoT and cloud in healthcare system. In: Fog computing: breakthroughs in research and practice. IGI Global; 2018. p. 365–78.
[13] Xiong N, Vasilakos AV, Yang LT, Song L, Pan Y, Kannan R, et al. Comparative analysis of quality of service and memory usage for adaptive failure detectors in healthcare systems. Selected Areas in Communications, IEEE Journal on 2009;27(4):495–509.
[14] Peng Y, Wang X, Guo L, Wang Y, Deng Q. An efficient network coding-based fault-tolerant mechanism in WBAN for smart healthcare monitoring systems. Appl Sci 2017;7(8):817.

[15] Manirabona A, Fourati LC. A 4-tiers architecture for mobile WBAN based health remote monitoring system. Wirel Netw 2018;24(6):2179–90.
[16] Saif S, Gupta R, Biswas S. Implementation of cloud-assisted secure data transmission in WBAN for healthcare monitoring. In: Advanced computational and communication paradigms. Springer; 2018. p. 665–74.
[17] Bradai N, Fourati LC, Kamoun L. WBAN data scheduling and aggregation under WBAN/WLAN healthcare network. Ad Hoc Netw 2015;25:251–62.
[18] Bradai N, Fourati LC, Kamoun L. Investigation and performance analysis of MAC protocols for WBAN networks. J Netw Comput Appl 2014;46:362–73.
[19] Mosavat-Jahromi H, Maham B, Tsiftsis TA. Maximizing spectral efficiency for energy harvesting-aware WBAN. IEEE J Biomed Health Inform 2016;21(3):732–42.
[20] Hu F, Liu X, Shao M, Sui D, Wang L. Wireless energy and information transfer in WBAN: an overview. IEEE Netw 2017;31(3):90–6.
[21] Demir SM, Al-Turjman F, Muhtaroğlu A. Energy scavenging methods for WBAN applications: a review. IEEE Sens J 2018;18(16):6477–88.
[22] Akhtar F, Rehmani MH. Energy harvesting for self-sustainable wireless body area networks. IT Prof 2017;19(2):32–40.
[23] Dodangeh P, Jahangir AH. A biometric security scheme for wireless body area networks. J Inf Secur Appl 2018;41:62–74.
[24] Usman M, Asghar MR, Ansari IS, Qaraqe M. Security in wireless body area networks: from in-body to off-body communications. IEEE Access 2018;6:58064–74.
[25] Bharathi KS, Venkateswari R. Security challenges and solutions for wireless body area networks. In: Computing, communication and signal processing. Springer; 2019. p. 275–83.
[26] Pramanik PKD, Nayyar A, Pareek G. WBAN: driving e-healthcare beyond telemedicine to remote health monitoring: architecture and protocols. In: Telemedicine technologies. Elsevier; 2019. p. 89–119.
[27] Aktas F, Ceken C, Erdemli YE. IoT-based healthcare framework for biomedical applications. J Med Biol Eng 2018;38(6):966–79.
[28] Zuhra FT, Bakar KA, Ahmed A, Tunio MA. Routing protocols in wireless body sensor networks: a comprehensive survey. J Netw Comput Appl 2017;99:73–97.
[29] Yessad N, Omar M, Tari A, Bouabdallah A. QoS-based routing in Wireless Body Area Networks: a survey and taxonomy. Computing 2018;100(3):245–75.
[30] Ahmed G, Mahmood D, Islam S. Thermal and energy aware routing in wireless body area networks. Int J Distrib Sens Netw 2019;15(6):1550147719854974.
[31] Watteyne T, Augé-Blum I, Dohler M, Barthel D. Anybody: a self-organization protocol for body area networks. Proceedings of the ICST 2nd International Conference on Body Area Networks 2007.
[32] Liang L, Ge Y, Feng G, Ni W, Wai AAP. A low overhead tree-based energy-efficient routing scheme for multi-hop wireless body area networks. Comput Netw 2014;70:45–58.
[33] Javaid N, Ahmad A, Nadeem Q, Imran M, Haider N. iM-SIMPLE: iMproved stable increased-throughput multi-hop link efficient routing protocol for Wireless Body Area Networks. Comput Human Behav 2015;51:1003–11.
[34] Javaid N, Ahmad A, Rahim A, Khan ZA, Ishfaq M, Qasim U. Adaptive medium access control protocol for wireless body area networks. Int J Distrib Sens Netw 2014;10(3):254397.
[35] Khan RA, Mohammadani KH, Soomro AA, Hussain J, Khan S, Arain TH, et al. An energy efficient routing protocol for wireless body area sensor networks. Wirel Pers Commun 2018;99(4):1443–54.
[36] Kaur N, Singh S. Optimized cost effective and energy efficient routing protocol for wireless body area networks. Ad Hoc Netw 2017;61:65–84.
[37] Ullah Z, Ahmed I, Ali T, Ahmad N, Niaz F, Cao Y. Robust and efficient energy harvested-aware routing protocol with clustering approach in body area networks. IEEE Access 2019;7:33906–21.
[38] Ayatollahitafti V, Ngadi MA, bin Mohamad Sharif J, Abdullahi M. An efficient next hop selection algorithm for multi-hop body area networks. PLoS One 2016;11(1), e0146464.
[39] Anwar M, Abdullah AH, Altameem A, Qureshi KN, Masud F, Faheem M, et al. Green communication for wireless body area networks: energy aware link efficient routing approach. Sensors 2018;18(10):3237.
[40] Ullah Z, Ahmed I, Razzaq K, Naseer MK, Ahmed N. DSCB: dual sink approach using clustering in body area network. Peer-to-peer Netw Appl 2019;12(2):357–70.
[41] Sagar AK, Singh S, Kumar A. Energy-aware WBAN for health monitoring using critical data routing (CDR). Wirel Pers Commun 2020:1–30.
[42] Mu J, Liu X, Yi X. Simplified energy-balanced alternative-aware routing algorithm for wireless body area networks. IEEE Access 2019;7:108295–303.
[43] Kruskal JB. On the shortest spanning subtree of a graph and the traveling salesman problem. Proc Am Math Soc 1956;7(1):48–50.
[44] Kershenbaum A, Van Slyke R. Computing minimum spanning trees efficiently. Proceedings of the ACM Annual Conference-Volume 1 1972.
[45] Ehrsam WF, Meyer CH, Smith JL, Tuchman WL. Message verification and transmission error detection by block chaining. Google Patents; 1978.
[46] Bellare M, Kilian J, Rogaway P. The security of cipher block chaining. In: Annual international cryptology conference. Springer; 1994.
[47] Heinzelman WR, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks. In: System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference. 2000.