Research Article

Thermal-Aware Multiconstrained Intrabody QoS Routing for Wireless Body Area Networks

Muhammad Mostafa Monowar,1 Mohammad Mehedi Hassan,2 Fuad Bajaber,1 Md. Abdul Hamid,3 and Atif Alamri2

1 Department of Information Technology, Faculty of Computing and Information Technology, King AbdulAziz University, Jeddah 21589, Saudi Arabia
2 College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
3 Department of Computer Engineering, College of Computer Science and Engineering, Taibah University, Madinah 30001, Saudi Arabia

Correspondence should be addressed to Muhammad Mostafa Monowar; hemal.cu@gmail.com

Received 3 December 2013; Accepted 2 February 2014; Published 16 March 2014

1. Introduction

As of now, the extensive proliferation of Micro-Electro-Mechanical Systems (MEMS) [1] as well as the ever-increasing development of wireless networking technologies fostered the widespread utilization of e-healthcare applications in the medical sector. Wireless body area network (WBAN) is such a recent technology for promoting e-healthcare which exploits intelligent, low-power, miniaturized biomedical sensor nodes to monitor body functions and the surrounding environment.

An implanted biosensor is a special type of sensor that detects a physiological change in the biological environment and transmits the information to a controller device, known as Body Coordinator (BC) exploiting wireless communication. Since the propagation loss around the human body is very high [2], the direct communication between the sensors and the BC is not always possible, especially when low transmission power of the radio is required to save the precious energy available in the sensor nodes. It necessitates multihop communication where the biosensors cooperatively relay each other's sensed information towards the BC. However, the multihop communication poses significant challenges for a reliable and real time delivery of the sensitive information due to the unpredictable and dynamic behaviour of wireless channel inside the human body, which in turn entails...
the design of an effective intrabody communication protocol that could provide a reliable and timely data delivery to the BC through multihop data transmission.

An implanted biosensor, although it could provide accurate information due to its proximity to the body organ, it has thermal effect on human tissue [3]. The human tissue absorbs heat due to the radiation from wireless communication and power dissipation of an implanted sensor resulting in temperature rise. Some organs [4] could suffer from thermal damage due to the temperature rise even with modest heating. Hence, minimizing temperature rise is considered as one of the important design considerations while devising intrabody communication protocols for such a network with implanted biosensors.

Although WBAN was initially motivated with vital sign monitoring application, it has facilitated nowadays more wider range of applications [5] having distinct Quality of Service (QoS) requirements. Considering the different application requirements of WBAN, the most important QoS metrics are delay and reliability, together, which we denote as multi-constrained QoS. Devising communication protocols for WBAN satisfying the multi-constrained QoS is an extremely challenging problem. The situation could be even harder when a WBAN will be equipped with a number of simultaneous applications with diverse QoS requirements. For instance, a patient can be equipped with cardiac defibrillator/pacemakers, respiration monitoring sensors, and pH-level monitoring sensors. The pacemakers require real-time delivery of data with higher reliability. However, the applications such as respiration monitoring and pH-level monitoring have strict reliability requirements although those applications could tolerate delay to some extent. An effective communication protocol is thus required to meet such multi-constrained QoS demands of heterogeneous applications.

Some recent studies [6–9] proposed thermal-aware routing protocols with the aim of minimizing thermal effect on human tissue. These protocols mainly focused on selecting routes based on minimal temperature and also avoiding hotspot(s). The important concerns for ensuring the QoS are not considered on those thermal-aware protocols. On the other hand, very few routing protocols [10, 11] exist in the literature which considered QoS provisioning for WBAN. However, those protocols mainly considered inter-BAN routing and ignored the thermal effect of implanted biosensors.

In this paper, we propose TMQoS, a thermal-aware multi-constrained intrabody QoS routing for wireless body area networks, which ensures the multi-constrained QoS requirements for diverse applications and also maintains an acceptable temperature rise throughout the network. We classify the traffic based on their multi-constrained QoS demands. We develop a cross-layer proactive routing framework which maintains an ongoing routing table containing routes with minimum hop count to the BC through periodic beacon exchanges. This routing framework estimates hop-to-hop delay, link reliability, and node temperature and exchanges those metrics through beacon packet among neighboring nodes to have an end-to-end estimate of delay, reliability, and temperature of the routes from the nodes to the BC. We further devise a hotspot avoidance mechanism aiming to avoid routes containing hotspot(s) and keeping the temperature rise of the nodes to an acceptable level thus preventing thermal damage of the tissue. We develop a multi-constrained QoS-aware route selection algorithm which chooses the forwarder node(s) based on desired QoS demands of diverse traffic classes. Furthermore, we perform extensive simulations to evaluate the performance of TMQoS compared to the state-of-the-art protocols.

The rest of the paper is organized as follows. Section 2 summarizes the related works. Section 3 states some preliminaries behind our protocol design. Section 4 presents the detailed design of TMQoS protocol. Section 5 demonstrates the performance of TMQoS using simulations. Finally, Section 6 provides our concluding remarks.

2. Related Works

To date, a number of potential contributions to thermal-aware routing protocol design can be found in [6–9]. TARA [6] is one of the primitive protocols in this series. TARA forwards data packets based on localized temperature information and hop counts to the destination. A node listens to its neighbor activities and counts the number of packet transmission and reception. Based on this, a node evaluates the communication radiation and power dissipation of neighbors and estimates the temperature changes. A node defines the neighbor(s) as hotspot if the estimated temperature exceeds a certain threshold. TARA avoids the hotspot(s) by establishing another route toward the destination using a withdrawal strategy where a packet is sent back to its previous sender if all the neighbors are identified as hotspots. The sender then attempts to select alternate route to detour the hotspot(s). After cooling the temperature beneath some threshold, those hotspots can be considered for later routing. TARA suffers from high end-to-end delay, lower reliability, as well as high energy consumption since the packet needs to traverse many hops due to this withdrawal strategy.

Similar to TARA, Bag and Bassiouni [7] proposed LTR, where a node always chooses the “coolest” neighbor for data forwarding. To avoid the routing loop, each packet maintains a small list of nodes which it has most recently visited and ignores those nodes if they are the coolest ones. Because of the greedy approach, a packet in LTR is not always directed to the destination which significantly increases the hop count, thus resulting in higher delay and low reliability. In the same study, the authors of LTR presents a modified version of LTR, known as ALTR where packet is routed using shortest hop algorithm if it exceeds a certain threshold, MAX_HOPS_ADAPTIVE. Although, it optimizes the end-to-end delay a bit compared to LTR, it wastes network bandwidth through unnecessary transmissions until the hop count reaches the threshold value, and also a packet traverses through hotspot while utilizing shortest hop routing. The same authors again presented HPR [8], an opposite mechanism as explained in ALTR, where a node usually forwards the packets using shortest hop routing. But to prevent hotspot, it chooses the “coolest” neighbor if it encounters a hotspot in the shortest hop count path. Yet,
the coolest neighbor based forwarding causes considerable delay and poor reliability while the hotspot is encountered.

To address the problems of LTR and ALTR, the authors in [9] presented LTRT, which selects a least temperature route from all possible routes from a sender node to a destination exploiting the Dijkstra’s algorithm. Similar to the previous thermal-aware protocols LTRT also exploits temperature metric in choosing its forwarder and ignores the QoS metrics (i.e., delay, reliability) which prevents in ensuring the desired QoS demands of the traffic.

QoS provisioning for WBAN has received exiguous attention so far. Liang et al. [10] proposed a QoS-aware routing service framework for biomedical sensor networks. Exploiting the cross-layer design, the proposed work aims to provide prioritized routing service and user specific QoS support. In the proposed routing service framework, routes are determined by user specific QoS requirements, wireless channel status, packet priority level, and sensor node’s willingness to be a router. Furthermore, the routing service can send feedback on network conditions to the user application, so the application service level can be adjusted to adapt to the network conditions. This protocol, however, does not clearly define how the routing algorithm works. More importantly, the essence of temperature rising is totally overlooked in this work. Exploiting the geographic location, DMQoS [11] proposes a multiobjective QoS routing protocol for biomedical wireless sensor networks. This protocol considers the traffic diversity and provides differentiation in routing using QoS metrics. However, it mainly considers much less energy constrained inter-BAN routing and ignored the thermal effects that could cause in the context of intra-BAN routing. Moreover, the assumption of knowing the coordinates of a node using GPS or other location detection system is also not feasible for tiny body sensor nodes.

As discussed above, the existing thermal-aware routing protocols for WBAN considered only temperature as a routing metric and focused on minimizing the temperature rise of the nodes, avoiding the QoS issues. These protocols thus cannot meet the multi-constrained QoS requirements if diverse types of traffic exist in the network. In contrast, the state-of-the-art QoS-aware protocols for WBAN totally ignored the temperature metric in choosing the route which is an essential parameter for intra-BAN routing. The absence of an effective and complete solution considering both temperature rise and multi-constrained QoS for intra-BAN communication environment motivated us to devise TMQoS routing protocol.

3. Preliminaries

3.1. System Models and Assumptions. We consider a deployment scenario, in which diverse types of WBAN nodes are placed in (i.e., implanted) a human body, while there is a Body Coordinator denoted as BC attached to the body surface, serving as the central data sink for the WBAN as shown in Figure 1(a). A set of WBAN nodes are the Reduced Function Devices (RFD), which have only sensing and transmission capabilities while BC is considered as Full Function Device (FFD) having some enhanced functionalities (i.e., data processing, exchanging control and management packets etc.). The WBAN nodes are usually battery powered and hence energy constrained. The BC, in contrast, is assumed to have an external power supply with higher processing capabilities than WBAN nodes. The BC processes the received data from the nodes and then sends it to monitoring station (MS) or server through other networks (i.e., cellular, WLAN, or wired) and this communication paradigm is out of the scope of this paper.

![Figure 1: Network model.](image-url)
We model the above deployment scenario as a connectivity graph, \( G = (N, E) \), where \( N = \{n_0, n_1, n_2, \ldots, n_n\} \) is the set of vertices representing the nodes in the network, where \( n_0 = \text{BC} \), and \( E \) is the set of edges that represents all possible communication links as illustrated in Figure 1(b). We assume every node \( n_i \) uses fixed transmission power for the communication with neighboring nodes. We define the neighbor set of \( n_i \), denoted as \( \text{NB}(n_i) \) are the nodes with which \( n_i \) has communication link. We consider that all the communication links are symmetric; that is, if \( n_i \in \text{NB}(n_j) \), then \( n_j \in \text{NB}(n_i) \). To save battery power, all WBAN nodes are assumed to have very limited transmission range, meaning that they are connected to accessible BC through multiple hops. We assume that some nodes might act as source nodes (which generate data), some as forwarding nodes (forward other node’s data) or some might play both the roles.

3.2. QoS-Aware Traffic Classification. TMQoS is mainly designed for the QoS provisioning of traffic with diverse requirements while avoiding the hotspots. Considering delay and reliability as the primary QoS constraints in the context of WBAN, we classify the traffic as follows.

(i) C1: both delay and reliability constrained. This type of traffic has stringent delay and reliability requirements. A number of medical applications, for instance, electroencephalogram (EEG), electrocardiogram (ECG), electromyography (EMG), and so forth, generate real-time medical continuous data which need to be delivered within a certain deadline with higher reliability.

(ii) C2: reliability constrained, nondelay constrained. The traffic belonging to this type has strict reliability requirements but can tolerate delay. An example of this type includes respiration monitoring and pH-level monitoring. This type of traffic can be processed offline and hence nondelay constrained, but packet losses may cause disastrous consequences.

(iii) C3: delay constrained, nonreliability constrained. A certain deadline for this type of traffic must be satisfied; however, it can tolerate some packet losses. Examples of this type include telemedicine video streaming application. Although, the packet loss for this type of applications degrades the quality to some extent, however, the traffic validity is still preserved.

(iv) C4: nondelay, nonreliability constrained. This type of traffic does not have any strict delay or reliability constraints. The regular measurement of patient’s physiological parameters such as temperature and pressure corresponds to this class of traffic.

The traffic type for the sensors could be set a priori of attaching with the body or can be reset through special MAC command packets sent by the BC.

4. Proposed Protocol

4.1. Protocol Architecture. Figure 2 illustrates the different modules and their associated interactions for our proposed TMQoS routing protocol. The proposed routing protocol exploits the cross-layer interactions between layer 2 and layer 3.

TMQoS is a kind of proactive routing protocol that intends to maintain an ongoing routing table. Similar to the other proactive routing protocols, TMQoS constructs and maintains a routing table with information from neighboring nodes. TMQoS uses a beacon packet to exchange information among neighboring nodes with the aim of routing table creation and maintenance. Upon receiving a beacon packet from the neighboring WBAN nodes through MAC receiver module, the routing table constructor module constructs or updates the routing table by estimating the values of delay, reliability, temperature, and hop count. The delay estimator and the reliability estimator modules in layer 2 estimate the hop-to-hop delay and the link reliability for particular neighboring nodes and send the feedback to the routing table constructor module. Also, the temperature estimator module measures the node temperature and provides it to the routing table constructor module to update the temperature value. The routing table constructor module employs a hotspot avoidance mechanism if the node is identified as “hotspot” from the feedback sent by the temperature estimator module. The beacon packet constructor module constitutes a beacon packet from the current information of the routing table and sends it to the MAC transmitter module for further transmission to the neighboring WBAN nodes.

Upon receiving a data packet from the upper layers or other neighboring WBAN nodes, QoS-aware traffic classifier module categorizes the data packets according to their multiconstrained QoS requirements as described in Section 3 and directs it to the multiconstrained QoS-aware route selector module to identify the most suitable route based on its QoS demands. After choosing the appropriate route, the multiconstrained QoS-aware route selector module passes the data packet to the multiconstrained QoS-aware Queuing module that maintains two separate queues for storing delay constrained packets (DCP) (i.e., C1 and C3) and nondelay constrained packets (NDCP) (i.e., C2 and C4), where DCP queue is treated as higher priority queue. The data packet, upon appropriately scheduled, is further directed to the MAC transmitter module for its transmission to the intended WBAN node.

4.2. Beacon Packet and Routing Table. As a proactive routing protocol, every node \( n_i \in N \) exchanges a beacon packet periodically at an interval \( T_{bc} \) to construct and maintain a routing table. A beacon packet contains the values of the following parameters in addition to usual header information: (i) minimum hop count of the node \( n_i \) to the BC, denoted as \( H_{n_i} \), (ii) minimum delay for sending a packet from the node \( n_i \) to the BC, denoted as \( D_{n_i} \), (iii) the maximum reliability of path for sending a packet from the node \( n_i \) to the BC, denoted as \( R_{n_i} \), and (iv) least temperature of the route from node \( n_i \) to the BC, denoted as \( T_{n_i} \). At the BC, \( H_{n_{bc}} = 0, D_{n_{bc}} = 0, R_{n_{bc}} = 1 \), and \( T_{n_{bc}} = 0 \) (we neglect the temperature rise for the BC as it is attached to the body surface). Initially all \( H_{n_i} \) are set to a large number.
The change of the values in the beacon packet might occur when the state of the network changes dynamically. It may be due to the changes in the locally estimated values of the parameters or when a node receives a beacon packet from a neighbour node with updated values or when a new node is added to the routing table. Once a node obtains a path to the sink node, it broadcasts a periodic beacon packet to its neighbouring nodes. Since the parameter values for the BC are constant, the BC only sends a void beacon packet, which is a type of beacon packet containing nothing. A node, upon receiving a void beacon packet from a neighbour, responds to the node with its own beacon packet. Thus, a new node collects routing information by broadcasting void beacon packet to its neighbouring node, and creates its own routing table with beacon packet from its neighbouring nodes.

Figure 3 illustrates the routing table structure of a node, $n_i$. The routing table contains the following information: (i) node ID of a neighbour node of $n_i$, (ii) the hop count value of $n_i$ via a neighbour node $n_j \in \text{NB}_{n_i}$, denoted as $H_{n_i,n_j}$.
(iii) the delay cost of sending a packet from \( n_i \) to the BC via \( n_j \), denoted as \( D_{n_i,n_j} \), (iv) the reliability value for a path of sending a packet from \( n_i \) to the BC via \( n_j \), denoted as \( R_{n_i,n_j} \), and (v) the temperature value for a path from \( n_i \) to the BC via \( n_j \), denoted as \( T_{n_i,n_j} \).

Algorithm 1 presents the procedures for the construction and update of a routing table at every node \( n_i \). For convenience, we summarize the notations used in Algorithm 1 in Table 1. The procedure for routing table construction is called when a node \( n_i \) receives a beacon packet from \( n_j \) \( \in \text{NB}_n \) or when any change of values occurred in the delay estimator, reliability estimator, or temperature estimator module for local network status changes. When a node receives a beacon packet from a neighbouring node, it only adds the neighbouring node to the routing table (RT) if the neighbouring node is closer to the BC than it is, in terms of hop count value (lines 2–4 in Algorithm 1). Then, a node \( n_i \) adds the values for \( H_{n_i,n_j}, D_{n_i,n_j}, R_{n_i,n_j} \), and \( T_{n_i,n_j} \) for neighbour \( n_j \) using the equations as given in lines 5–8 and also updates the value of \( H_{n_i} \) (line 9). Here, \( D_{i,j} \) and \( R_{i,j} \) are the average delay and reliability for local link between \( n_i \) and \( n_j \), respectively. \( T_{i,j} \) denotes the average temperature estimated locally at node \( n_i \). The parameters, \( D_{i,j}, R_{i,j}, \) and \( T_{i,j} \) are estimated by the delay estimator, reliability estimator, and temperature estimator module, respectively, and the estimation methods will be discussed in Section 4.4. If some neighbour \( n_j \) of \( n_i \) already exists in the routing table, then \( n_i \) updates the parameter values (lines 11–13). Whenever a node receives a beacon packet from a neighbour node with higher hop count value than the node has, it immediately drops the beacon packet (lines 14–15). Lines 17–21 ensure that the routing table entries contain the information of only those neighbour nodes which are closer to the BC than node \( n_i \) by deleting the farther nodes.

The routing table entries also need to be updated when any amendments are indicated for the parameters \( D_{i,j}, R_{i,j}, \) and \( T_{i,j} \) by the delay estimator, reliability estimator, and temperature estimator module, respectively. In this case, the current updated values of the delay and reliability parameters, denoted as \( D_{i,j}^d \) or \( R_{i,j}^r \) for any neighbour node \( n_j \), triggers the update of the parameters \( D_{n_i,n_j} \) and \( R_{n_i,n_j} \) for that neighbour only (lines 22–25) while the updated temperature value of node \( n_i \) denoted as \( T_{i,j}^t \) provokes for changes of the parameter \( T_{n_i,n_j} \) for all nodes in RT (lines 26–30).

The beacon constructor module at every node, \( n_i \), constitutes a beacon packet and broadcasts it at a period \( T_b \) to its neighbour nodes, once a path to the BC is established. The module consults the routing table constructor module to set the values for the beacon packet. Thus, after every \( T_b \) period, the parameter for the beacon packet is calculated as follows:

\[
H_{n_i} = H_{n_i,n_j}; \quad \forall n_j \text{ in RT}, \tag{1}
\]

\[
D_{n_i} = \min\left(D_{n_i,n_j}\right); \quad \forall n_j \text{ in RT}, \tag{2}
\]

\[
R_{n_i} = \max\left(R_{n_i,n_j}\right); \quad \forall n_j \text{ in RT}, \tag{3}
\]

\[
T_{n_i} = \min\left(T_{n_i,n_j}\right); \quad \forall n_j \text{ in RT}. \tag{4}
\]

The value of \( H_{n_i} \) in the beacon packet is set to any of the \( H_{n_i,n_j} \) values in RT, since the routing table contains the information of those neighbours which are closer to the BC than node \( n_i \) in terms of hop count value, which indicates that only those neighbour nodes will be stored in the routing table through which a node has minimum hop count value. As per (2) and (4), \( D_{n_i} \) and \( T_{n_i} \) are set to the minimum of all \( D_{n_i,n_j} \) and \( T_{n_i,n_j} \) values in RT, respectively, while \( R_{n_i} \) is set to the maximum of all \( R_{n_i,n_j} \) values in RT (3).

Figure 4 illustrates the example of a routing table and a beacon packet formation for TMQoS. For the topology as shown in Figure 4(a), only the routing table formation for node 3 has been shown in Figure 4(b). The black colour nodes
indicate all possible downstream nodes from node 3 to the node 0 (BC) according to Algorithm 1. As shown in the figure, node 3 has three neighbour nodes, 2, 4, and 6. Here, $H_2 = 3$, $H_4 = H_6 = 2$, and $H_3 = 3$. Hence, $H_{3,2} = 4$ and $H_{3,4} = H_{3,6} = 3$. Thus, node 3 adds only node 4 and 6 in its routing table since these nodes are closer to the BC than node 3 in terms of hop count. Similarly, node 4 adds nodes 10 and 5, and node 6 adds nodes 5 and 7 in their corresponding routing table. Now, as shown in Figure 4(b), while forming the beacon packet from the routing table information, node 3 selects $H_2 = 3$, $D_3 = 0.05$ (minimum value), $R_3 = 0.89$ (maximum value), and $T_3 = 0.06$ (minimum value) as per (1)–(4).

4.3. Hotspot Avoidance. TMQoS aims to avoid hotspot(s) while building up a route to the BC. We refer the hotspot as the node when its estimated average temperature exceeds a certain threshold. If the temperature of the hotspot is not cooled down by preventing it from further communication activities, it could cause serious damage to the body tissue. When the temperature estimator module of a node identifies it as a hotspot, then immediately it sets all the $T_{n_{i,j}}, D_{n_{i,j}},$ and $R_{n_{i,j}}$ values of its routing table as INFINITY (a very large number). Consequently, the beacon packet also contains the value of INFINITY for $D_{n_{i}}, R_{n_{i}},$ and $T_{n_{i}}$ and the beacon packet is sent immediately without waiting for the next beacon period. The rationale behind it is to prevent a hotspot node to be chosen as a forwarder node even if it has the lowest delay, and/or maximum reliability, and/or minimum temperature on its path to the BC. A node again resumes its regular operation in setting the value of the routing table when the temperature falls below the threshold.

**Table 1: Notation in Algorithm 1.**

| Notation | Meaning |
|----------|---------|
| $n_j$    | A neighbor of node $n_i$ |
| RT       | Routing table |
| $H_n$    | Minimum hop count of the node $n_i$ to the BC |
| ID$_{n_j}$ | ID of $n_j$ |
| $H_{n_{i,j}}$ | The hop count value of $n_i$ via a neighbour $n_j$ |
| $D_{n_{i,j}}$ | The delay cost of sending a packet from $n_i$ to the BC via $n_j$ |
| $R_{n_{i,j}}$ | The reliability value for a path of sending a packet from $n_i$ to the BC via $n_j$ |
| $T_{n_{i,j}}$ | The temperature value for a path from $n_i$ to the BC via $n_j$ |
| $D_{t_{i,j}}$ | The average delay for local link between $n_i$ and $n_j$ |
| $R_{t_{i,j}}$ | The average reliability for local link between $n_i$ and $n_j$ |
| $T_{t_{i,j}}$ | The average temperature estimated locally at node $n_j$ |
| $D_{t_{i,j}}^c$ | Current updated average delay value for local link between $n_i$ and $n_j$ |
| $R_{t_{i,j}}^c$ | Current updated average reliability value for local link between $n_i$ and $n_j$ |
| $T_{t_{i,j}}^c$ | Current updated temperature value of node $n_j$ |

**Figure 4:** Example of the routing table and the beacon packet formation.

Figure 5 presents a graphical example of hotspot avoidance considering the topology as shown in Figure 4(a). Here, upon identifying node 4 as a hotspot by its temperature estimator module, all the $D_{n_{i,j}}, R_{n_{i,j}},$ and $T_{n_{i,j}}$ values of its routing table are set to 999 (infinity). The beacon packet is also formed immediately with the values [3, 999, 999, 999] and is broadcasted. After receiving the beacon packet, node 3 updates its routing table and its own beacon packet with the values [3, 0.07, 0.89, 0.06]. Thus, being a hotspot, although node 3 had the lowest delay path through node 4 previously (Figure 4(b)), currently it is changed to node 6, and no information of node 4 will be further broadcasted by node 3 through its beacon packet and it will not be selected as a forwarder until node 4 becomes a regular node after cooling down.

**4.4. Estimation of the Parameters**

4.4.1. Delay Estimation. The Delay estimator module of a node $n_i$ estimates the parameter $D_{t_{i,j}}^c$ as follows:

$$D_{t_{i,j}}^c = D_{t_{i,j}}^{DCPQ} + D_{t_{i,j}}^{DPP} + D_{t_{i,j}}^{prop}. \quad (5)$$
transmission delay, a node \( n_j \) records the time when a packet becomes the head of the queue and the time when the same packet is transmitted or dropped after a maximum number of retransmission, denoted as \( \text{MAX}_S \). It includes all MAC layer delays due to contention such as channel sensing, backoff time slots, and retransmission. Let \( S \) be the sample size of the packets, in particular, the number of last transmitted \( S \) packets and \( w(i) \) be the time weighted function. We estimate the average of \( D_{i,j}^\text{tr} \) using Time Weighted Moving Average formula (TWMA) [13] as follows:

\[
D_{i,j}^\text{tr} = \frac{\sum_{i=1}^{S} D_{i,j}^\text{tr} \times w(i)}{\sum_{i=1}^{S} w(i)}, \tag{7}
\]

where

\[
w(i) = \begin{cases} 
1, & 1 \leq i \leq \frac{S}{2}, \\
1 - \frac{i - \frac{S}{2}}{\frac{S}{2} + 1}, & \frac{S}{2} < i \leq S. 
\end{cases}
\tag{8}
\]

The TWMA places heavier weight on more recent samples so the estimation can be more adaptive to temporal changes of the link quality.

### 4.4.2. Reliability Estimation

The reliability estimator module at node \( n_i \) estimates average link reliability, \( R_{i,j} \) for its neighbours \( n_j \) in RT using Window Mean with EWMA (WMEWMA) [13]. WMEWMA computes an average success rate over a time window which is proven as one of the best methods for estimating link reliability [13]. Let \( r \) be the number of successfully received messages over a time window, \( \delta t \) on a particular link \((i-j)\), and \( f \) be the sum of all losses on that link. Hence, the mean \( \bar{r} = r/(r + f) \) represents the success probability of the link for that time window. The \( R_{i,j} \) is thus estimated as follows:

\[
R_{i,j}^l = R_{i,j}^l \times \alpha + (1 - \alpha) \times \bar{r}. \tag{9}
\]

Here, \( \alpha \) is a smoothing factor which controls the history of the estimator and \( 0 < \alpha < 1 \). The value of \( \alpha \) is also empirically chosen and we use the value 0.4 in our simulation.

### 4.4.3. Temperature Estimation

The temperature estimator module estimates the temperature of a node \( n_i \) using the procedure as described in [3, 6]. In particular, the temperature rise of the tissue surrounding the WBAN nodes is measured. One of the main sources for temperature increase is the radiation from the node antenna. Specific absorption rate (SAR) is used to determine the level of radiation being absorbed by body tissue. The space near the antenna is known as near field, the extent of which is \( \lambda /2\pi \), where \( \lambda \) is the radio frequency (RF) wavelength for the wireless communication.
According to [14, 15] the SAR in the near field (≤λ/2𝜋) and far field (>λ/2𝜋) can be estimated as follows:

\[
\text{SAR}_{\text{NF}} = \frac{\sigma \mu \omega}{\rho \sqrt{\sigma^2 + \varepsilon^2 \omega^2}} \left( \frac{1}{R^2} \right)^2 \left( \frac{1}{R^2} + \frac{V}{R} \right)^2,
\]

\[
\text{SAR}_{\text{FF}} = \frac{\sigma}{\rho} \left( \frac{\alpha^2 + \beta^2}{\sqrt{\alpha^2 + \omega^2 \varepsilon^2}} \right) \frac{1}{4\pi} \frac{\sin^2 \theta e^{-\alpha R}}{R^2},
\]

where \( R \) is the distance from the source to the observation point, \( \nu \) is the propagation constant, \( dl \) is the length of short conducting wire for a short dipole antenna, \( \sigma \) is the medium conductivity, \( I \) is the amount of current, \( \varepsilon \) is the relative permittivity, \( \mu \) is the permeability, \( \rho \) is the mass density, and \( \sin \theta = 1 \).

Another reason for temperature increase [3] is the power dissipation of the sensor node circuitry, which can be quantified as power dissipation density, \( P_e \) (the power consumed by the sensor circuitry divided by the volume of the sensor). Considering both the sources for temperature rise, the temperature of a node at a grid point \((x, y)\) at time \( t \), denoted as \( T^t(x, y) \) can be estimated as follows [3]:

\[
T^t(x, y) = \left( 1 - \frac{\Delta^t b}{\rho C_p} - \frac{4\Delta^t K}{\rho C_p \Delta^2} \right) T^{t-1}(x, y) + \frac{\Delta^t \text{SAR}}{C_p} + \frac{\Delta_t b}{\rho C_p} T^b + \frac{\Delta_t K}{\rho C_p \Delta^2} \times \left( T^{t-1}(x + 1, y) + T^{t-1}(x, y + 1) + T^{t-1}(x - 1, y) + T^{t-1}(x, y - 1) \right).
\]

(11)

Equation (11) exploits Finite-Difference Time-Domain (FDTD) modeling technique [16] that discretizes the differential form of time and space and the problem space is discretized into small grids. In (11), \( \Delta_t \) is the discretized time step, \( \Delta \) is the discretized space step, \( b \) is the blood pressure perfusion constant, \( C_p \) is the specific heat of the tissue, \( T_b \) is the fixed blood temperature, \( K \) is the thermal conductivity of the tissue. From (11), the temperature of a node at grid point \((x, y)\) at time \( t \) can be determined through a function of the temperature at \((x, y)\) at time \( t - 1 \) and the function of the temperature of neighbouring nodes at grid points \((x + 1, y), (x, y + 1), (x - 1, y), \) and \((x, y - 1)\). Since the sensor nodes are surgically implanted, the positions of the nodes are fixed and can be easily known. Once the properties of the tissue, the properties of blood flow, and the heat absorbed by the tissue will be obtained, the temperature at a given time can be estimated. The details of this temperature estimation modeling can be found in [3].

4.5. Multiconstrained QoS-Aware Route Selection. Upon obtaining a path to the BC, a WBAN node starts sending data packets received from the other nodes, or its own sensed data packets. TMQoS selects the appropriate route for a data packet based on its multiconstrained QoS demand.

The multiconstrained QoS-aware route selector module consults the routing table to choose the next hop after receiving a data packet of particular type. A node \( n_i \), selects the next hop according to Algorithm 2.

As presented in Algorithm 2, if a data packet belongs to the class C4 (non-delay, non-reliability constrained), the minimum temperature path will be selected so that it does not increase the temperature of the minimum delay or maximum reliable path. In case of C3 (delay constrained, non-reliability constrained) and C2 (reliability constrained, non-delay constrained) classes of packet, the algorithm selects minimum delay path and maximum reliable path, respectively, to ensure the appropriate QoS for the corresponding classes. However, the packet belongs to C1 class which is both delay and reliability constrained, the algorithm first selects the next hop which ensures minimum delay, and then it selects another next hop node that guarantees the maximum reliability. The minimum delay path ensures that at least one packet reaches the BC with shortest possible time while the maximum reliable path ensures that the desired path reliability for the packet has been attained. Moreover, sending the multiple copies of the packet on two paths also increases the data reliability [17].

Notably, since the hotspot avoidance is performed while building up the routing table, TMQoS guarantees that no packet will be routed to a HOTSPOT even though, in reality, the HOTSPOT is on the minimum delay, maximum reliable, or minimum temperature path.

4.6. Multiconstrained QoS-Aware Queuing. Upon selecting the next hop(s), the data packets are passed to the multi-constrained QoS-aware queuing module, which maintains two separate queues, namely, DCPQ and NDCPQ for storing delay constrained packets (C1 and C3) and non-delay constrained packets (C2 and C4), respectively. The DCPQ has the higher priority than that of NDCPQ. It signifies that the packets from NDCPQ will not be sent until the DCPQ becomes empty. The rationale behind is the delay intolerance.
properties of the DCP packets. However, it might cause starvation problem where the packets from NDCP queue could be indefinitely blocked by DCP. To avoid the problem we adopt the similar mechanism as described in [11], in which a time-out based policy has been employed. In this policy, a packet will be moved to a higher priority queue (irrespective of its type) if it waits in a lower priority queue until a time-out occurs.

5. Performance Evaluation

This section presents the simulation-based performance evaluation of TMQoS protocol. The results show that TMQoS successfully achieves its design objectives.

5.1. Simulation Environment. We consider a 4 × 4 mesh topology as shown in Figure 6, where the pairs of neighbour nodes are connected by links. In this topology, every node is connected to each other. All the white-coloured nodes are the regular WBAN nodes while the black one is the BC. In the simulation, the nodes sense data and route the packets to the BC through multihopping. The simulation program has been developed in C++.

Table 2 presents the different parameters and their values used in the simulation. The values for tissue properties and dielectric characteristics are obtained from [18, 19]. Initially, the temperature of all the sensors is set to 37°C. In this topology, among 15 WBAN nodes (BC is excluded), C1, C2, and C3 traffic classes are equally distributed to the 12 nodes while traffic class C4 is assigned to the remaining 3 nodes. To distribute the traffic class, nodes are chosen randomly. In this study, we compare TMQoS with LTRT and TARA. The performance of the algorithms is compared for different data generation rates. In this study, each sensor of a particular traffic class sources traffic at a given rate. We randomize the initial data generation of the sensors to avoid the synchronized periodic reports. We implemented the basic functionalities of nonbeacon enabled mode of IEEE 802.15.4 MAC protocol with the default values defined the standard [20]. The links are randomly assigned Bit Error Rate (BER) values ranging from $10^{-5}$ to $10^{-2}$. The payload size for all traffic classes is set to 256 bits. When the average temperature rise exceeds 0.1°C, we set it as a threshold for detecting the hotspot. Each simulation has been performed for 1000 seconds and we averaged the value obtained over 10 random runs.

As a proactive protocol, exchanging beacon packets increases the network traffic and has significant impact on the protocol performance. Too frequent exchange of beacon packets degrades the performance of TMQoS. In contrast, if the beacon packets are exchanged too infrequently, the actual network status is not updated in time. Therefore, to select a suitable beacon interval, we simulated TMQoS with varying beacon intervals. Here, we fix the data generation interval as 1 packet/sec with the same topology as shown in Figure 6. Figure 7 illustrates the result. We choose beacon interval as 5 s based on the result.

Table 2: Parameters and their values used in the simulation.

| Parameter | Meaning | Value       |
|-----------|---------|-------------|
| $\beta$   | EWMA weighting factor in (6) | 0.2         |
| $\alpha$  | Smoothing factor in (9) | 0.4         |
| $\epsilon$ | Relative permittivity at 2 MHz | 826         |
| $P_c$     | Power dissipation density | 0.002       |
| $b$       | Blood perfusion constant | 2700 [J/m³°C] |
| $T_b$     | Fixed blood temperature | 37°C        |
| $\rho$    | Mass density | 1040 kg/m³ |
| $\Delta$  | Discretized space step | 0.005 m     |
| $S$       | Sample size in (7) | 8           |
| $T_{bc}$  | Beacon interval | 5 s         |
| $\sigma$  | Conductivity at 2 MHz | 0.5476 [S/m] |
| $C_p$     | Specific heat | 3600 [J/kg°C] |
| $\Delta_t$| Discretized time step | 5 s         |
| $I$       | Current provided to sensor antenna | 0.1 A       |
| $K$       | Thermal conductivity | 0.498 [J/ms°C] |
| MAX$_R$   | Maximum retransmission limit | 5           |
5.2. Performance Metrics. To evaluate TMQoS, the following metrics are used.

**End-to-End Latency.** End-to-end latency of a packet is measured as the time difference between the packet generation time and the time when it is received by the BC. Delays experienced by distinct data packets are averaged over the total number of distinct packets received by the BC.

**Reliability.** It is the ratio of the total number of unique packets received by the BC to the total number of packets generated by the WBAN nodes.

**Maximum Temperature Rise.** Maximum temperature rise denotes the highest temperature rise of any node inside the whole WBAN. The metric signifies the performance of the protocols regarding the hotspot formation and the associated tissue damage.

**Average Temperature Rise.** The average temperature rise of the nodes presents the average change in temperature of the nodes from that at the initial simulation period.

**Energy Efficiency.** In this study, we define the energy efficiency as \( \frac{N_t}{N_r} \), where \( N_t \) denotes the number of bytes transmitted to the BC for a period of time, \( N_r \) denotes the number of bytes received to the BC for the same amount of time, and \( N_h \) denotes the average number of hops a delivered packet travels. A smaller value indicates better energy efficiency.

5.3. Simulation Results. This section presents the simulation results obtained through evaluating TMQoS using the metrics as stated above.

5.3.1. Delay Performance. Figure 8 illustrates the average end-to-end latency of the protocols for different data generation rates. TMQoS exhibits the lowest end-to-end delay for the delay constrained traffic (C1 and C3) for all traffic loads as it chooses the least delay path for the delay constrained traffic. Interestingly, the nondelay constrained traffic (C2 and C4) also shows better delay performance than those of LTRT and TARA. The reason is TMQoS chooses the path with minimum hop count value to the BC even for the nondelay constrained traffic. However, both TARA and LTRT have the poor average delay performance irrespective of the traffic class since both the protocols exploit the temperature metric only in choosing the next hop. Comparatively, TARA exhibits the highest delay as the packet traverses a large number of hops due to its withdrawal strategy.

Figures 9 and 10 exhibit the percentage of packets meeting the deadline for different delay deadline of delay constrained traffic at low traffic (0.25 packet/sec) and high traffic (3 packet/sec) load, respectively. As Figure 9 shows, at low traffic load, for a very strict delay deadline of 100 ms, more than 90% of C1 and C3 traffic meet the deadline while for the same traffic class the percentage is slightly more than 50% for LTRT and 40% for TARA. However, for the more relaxed deadlines, the percentage increases rapidly for all the protocols. While the deadline is set to 200 ms, all the packets reached the deadline for TMQoS, which is 350 ms for LTRT and 450 ms for TARA. In contrast, at higher traffic load as shown in Figure 10, all the protocols show poor performance while the deadline is set strictly to 100 ms. Yet, TMQoS shows better performance (more than 55%) than LTRT and TARA which are 30% and 2%, respectively. Similar to the low traffic load, the increase in the deadline also increases the percentage dramatically for all the protocols. In this traffic load, 100% of packets reached the deadline at 300 ms for TMQoS and 450 ms for LTRT; however, even at the most relaxed deadline (500 ms), the maximum percentage of packets meeting the deadline for TARA is 75%.
Figure 10: Percentage of packets meeting deadline for different delay deadline at high traffic load.

Figure 11: Reliability for reliability constrained traffic varying data generation rate.

5.3.2. Reliability Performance. Figure 11 portrays the reliability of reliability constrained traffic (C1 and C2) for different traffic load. Here, the BER for the links varies randomly ranging from $10^{-5}$ to $10^{-2}$. As the figure shows, with the increase in traffic load, reliability decreases for all the protocols. TMQoS achieves the highest reliability for C1 traffic in all traffic loads as it employs both the path reliability and data reliability for forwarding this class of packets. TMQoS also exhibits significant reliability performance for C2 traffic in all traffic loads due to choosing the best reliable path. However, due to the absence of reliability metric for the forwarder selection, both LTRT and TARA shows poor reliability performance with the increasing traffic load.

Comparatively, TARA has the lowest reliability as it experiences large number of hops by detouring the packet away from the heated zone.

5.3.3. Temperature Rise. The maximum temperature rise of any node in the network for the protocols till the simulation period is illustrated in Figure 12. As the figure shows, the maximum temperature increases with the increasing traffic load for all the protocols. However, the presence of hotspot detection and avoidance mechanism in all the protocols prevents the maximum temperature rise exceeding the threshold value (0.1°C). LTRT shows the best performance in this case as it always chooses the least temperature route. TARA also shows considerable performance as it chooses the next hop based on the minimal temperature. However, the maximum temperature rise for TMQoS is higher than the other protocols. The reason behind is that, although TMQoS avoids the route containing hotspot, to ensure the QoS of the corresponding traffic classes, it prioritizes the desired QoS metric while choosing the next hop than the temperature metric, which eventually increases the temperature of the nodes, still beneath the threshold.

Figure 12: Maximum temperature rise varying data generation rate.

Figure 13 shows the average temperature rise of the nodes for different traffic load. LTRT still exhibits the best performance for average temperature rise. Interestingly, TMQoS shows comparatively better performance than TARA in this regard. The result is characterized by the fact that TARA employs withdrawal mechanism whenever it encounters a hotspot and reroute the packet through alternate paths. It involves many nodes in the network in routing packets which in turn increases the average temperature of the nodes. TMQoS, in contrast, always chooses the path having minimum hop count to the BC along with the desired QoS metrics. Hence, although the maximum temperature rise of
TMQoS is higher than TARA, it shows better performance in average temperature rise.

5.3.4. Energy Efficiency. Figure 14 illustrates the energy efficiency of the protocols for different traffic load. All the protocols exhibit poor energy efficiency as the traffic load increases. TARA shows the worst performance as the packets need to traverse too many hops along with the poor reliability. Due to the lesser hop count per arrived packet, LTRT also shows better performance than TARA. TMQoS exhibits the highest energy efficiency in all traffic loads as the packet traverses least number of hops to reach the destination, and also TMQoS has the least retransmitted packets due to its higher reliability performance.

6. Conclusion

This paper presents TMQoS—a thermal-aware multiconstrained intrabody QoS routing for wireless body area networks that mainly concerns about both achieving multiconstrained QoS requirements of different application types and maintaining acceptable temperature rise throughout the network. TMQoS is a proactive routing protocol that maintains an ongoing routing table through periodic beacon exchanges among neighbour nodes. It exploits cross-layer functionality through estimating hop-to-hop delay, link reliability, and node temperature at the MAC layer to construct the routing table that includes multiple shortest path routes for diverse QoS demands of traffic classes. TMQoS employs a hotspot avoidance mechanism to prevent traffic traversing through hotspot(s) to maintain low temperature rise.

To evaluate the efficiency of TMQoS, we performed extensive simulations comparing TMQoS with TARA and LTRT. The results reveal that TMQoS achieves significant lower delay and higher reliability performance for delay constrained and reliability constrained traffic, respectively, as compared to both TARA and LTRT. TMQoS also maintains a moderate average temperature rise throughout the network. Furthermore, TMQoS exhibits the highest energy efficiency than the other thermal-aware routing protocols. In summary, TMQoS successfully ensures the desired QoS demands of diverse application types, maintains moderate temperature in the entire network, and shows higher energy efficiency.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors would like to extend their sincere appreciation to the Deanship of Scientific Research at King Saud University for its funding of this research through the Research Group Project no. RGP-VPP-281.

References

[1] B. A. Warneke and K. S. J. Pister, “MEMS for distributed wireless sensor networks,” in Proceedings of the 9th IEEE International Conference on Electronics, Circuits and Systems (ICECS’02), vol. 1, pp. 291–294, September 2002.
[2] L. Roelens, S. Van Den Bulcke, W. Joseph, G. Vermeeren, and L. Martens, “Path loss model for wireless narrowband communication above flat phantom,” Electronics Letters, vol. 42, no. 1, pp. 10–11, 2006.
[3] Q. Tang, N. Tummala, S. K. S. Gupta, and L. Schiebert, “Communication scheduling to minimize thermal effects of implanted biosensor networks in homogeneous tissue,” IEEE Transactions on Biomedical Engineering, vol. 52, no. 7, pp. 1285–1294, 2005.
[4] A. Hirata, G. Ushiq, and T. Shiozawa, “Calculation of temperature rises in the human eye exposed to em waves in the ism frequency bands,” IEICE Transactions on Communications, vol. E83-B, no. 3, pp. 541–547, 2000.
[5] R. Bashirullah, "Wireless implants," *IEEE Microwave Magazine*, vol. 11, no. 7, pp. S14–S23, 2010.

[6] Q. Tang, N. Tummala, S. K. S. Gupta, and L. Schwiebert, "TARA: Thermal-Aware Routing Algorithm for implanted sensor networks," in *Proceedings of the 1st IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS '05)*, vol. 3560 of *Lecture Notes in Computer Science*, pp. 206–217, Springer, Berlin, Germany, July 2005.

[7] A. Bag and M. A. Bassiouni, "Energy efficient thermal aware routing algorithms for embedded biomedical sensor networks," in *Proceedings of the IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS '06)*, pp. 604–609, October 2006.

[8] A. Bag and M. Bassiouni, "Hotspot preventing routing algorithm for delay-sensitive biomedical sensor networks," in *Proceedings of the IEEE International Conference on Portable Information Devices (PORTABLE '07)*, pp. 604–609, 2007.

[9] D. Takahashi, Y. Xiao, F. Hu, J. Chen, and Y. Sun, "Temperature-aware routing for telemedicine applications in embedded biomedical sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2008, Article ID 572636, 26 pages, 2008.

[10] X. Liang and I. Balasingham, "A QoS-aware routing service framework for biomedical sensor networks," in *Proceedings of the 4th IEEE International Symposium on Wireless Communication Systems (ISWCS '07)*, pp. 342–345, October 2007.

[11] A. Razzaque, C. S. Hong, and S. Lee, "Data-centric multiobjective QoS-aware routing protocol for body sensor networks," *Sensors*, vol. 11, no. 1, pp. 917–937, 2011.

[12] J. M. Lucas and M. S. Saccucci, "Exponentially weighted moving average control schemes. Properties and enhancements," *Technometrics*, vol. 32, no. 1, pp. 1–12, 1990.

[13] A. Woo and D. Culler, "Evaluation of efficient link reliability estimators for low-power wireless networks," Tech. Rep. UCB/CSD-03-1270, EECS Department, University of California, Berkeley, 2003, http://www.eecs.berkeley.edu/Pubs/TechRpts/2003/6239.html.

[14] S. K. S. Gupta, S. Lahwani, Y. Prakash, E. Elsharawy, and L. Schwiebert, "Towards a propagation model for wireless biomedical applications," in *Proceedings of the International Conference on Communications (ICC '03)*, vol. 3, pp. 1993–1997, May 2003.

[15] M. Bethesda, *A Practical Guide to the Determination of Human Exposure to Radio Frequency Fields*, National Council on Radiation and Protection and Measurements (NCRP), 1993.

[16] D. M. Sullivan, *Electromagnetic Simulation Using the FDTD Method*, IEEE Press, Piscataway, NJ, USA, 2000.

[17] J. Sen and A. Ukil, "An adaptable and QoS-aware routing protocol for wireless sensor networks," in *Proceedings of the 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless (VITAE '09)*, pp. 767–771, May 2009.

[18] "Tissue dielectric properties," http://transition.fcc.gov/oet/rfsafety/dielectric.html.

[19] S. C. DeMarco, G. Lazzi, W. Liu, J. D. Weiland, and M. S. Humayun, "Computed sar and thermal elevation in a 0.25-mm 2-d model of the human eye and head in response to an implanted retinal stimulator—part I: models and methods," *IEEE Transactions on Antennas and Propagation*, vol. 51, no. 9, pp. 2274–2285, 2003.
Submit your manuscripts at http://www.hindawi.com