International Journal of Informatics and Applied Mathematics
e-ISSN:2667-6990 Vol. 7, No. 2, 29-48

Routing with QoS and Fault Tolerance in WBAN: The HEALTH Protocol

Sakina Oussane[1], Haroun Benkaouha[1], and Amir Djouama[2]

[1] LSI Laboratory, USTHB University, Algiers, Algeria
[2] National School of Artificial Intelligence, Algiers, Algeria
soussane@usthb.dz haroun.benkaouha@usthb.edu.dz
amir.djouama@ensia.edu.dz

Abstract. The Internet of Things (IoT) is a technology for connecting physical objects through various digital systems, applied in many fields, including medical monitoring. In this context, Wireless Body Area Net works (WBANs) integrate seamlessly into the IoT infrastructure. The increasing adoption of WBANs in the medical sector is driven by their numerous advantages, such as continuous patient monitoring, early detection of health risks, and the provision of personalized medical care. However, several challenges remain, including managing energy consumption, ensuring consistent QoS, resilience to failures, and maintaining patient comfort. This study presents an innovative routing protocol, HEALTH, specifically designed for WBANs, aiming to ensure optimal service quality in terms of temperature, response time, energy consumption, and delivery rate. The protocol's performance was evaluated using the BNS and Castalia frameworks, based on the Omnet++ simulator. Simulation results confirm the protocol's effectiveness while maintaining sustained service quality.

Keywords: IoT · WBAN · Medical monitoring · Fault detection · QoS · Fault Tolerance · Routing · Protocol efficiency

Received: 16 December 2024 | Revised: 21 December 2024 | Accepted: 11 January 2025
DOI: 10.53508/ijiam.1602385

1 Introduction

The Internet of Things (IoT) refers to a vast interconnected network of smart devices and heterogeneous sensors. These objects, such as RFID tags, smartphones, and others, can autonomously detect, capture, process, and transmit data using wireless technologies. Their growing numbers form wireless sensor networks (WSNs) that communicate with each other [1][2]. IoT architecture refers to the organizational structure of these interconnected components, including sensors, communication devices, data processing platforms, cloud services, and software applications. Together, these elements enable physical objects to collect, communicate, and act on data through wireless networks [3]. With IoT, it becomes possible to randomly deploy energy-efficient devices in targeted areas for real-time data collection and analysis. This evolution extends the Internet beyond traditional computers by integrating connected objects, thus opening new avenues for process monitoring, automation, and optimization [4].

Wireless Body Area Networks are a special subcategory of WSNs designed to monitor individuals' health without disrupting their daily activities [5]. By using sensors embedded in the body or clothing, these networks collect essential physiological and medical data for health monitoring. The collected data is transmitted wirelessly to data collection devices called "sinks" or servers, enabling subsequent analysis or real-time monitoring. These data can then be routed to an external network, accessible remotely by healthcare professionals, facilitating the emergence of new applications in connected health and IoT [6][7]. However, WBANs face several challenges. These include managing energy consumption, the critical nature of the data processed, and the need to quickly and reliably transfer information to care centers while ensuring data availability in the event of system failures. Such failures may involve sensor node loss, communication link breakdown, or malfunctioning network components. Managing these errors is complex and requires fault-tolerance mechanisms to ensure proper system operation. Due to their critical impact, extensive research has been con ducted to develop effective fault-tolerance strategies [8]. Hence, it is essential to design an intra-WBAN routing protocol that is both efficient and resilient, ensuring optimal service quality.

To address these challenges, this article proposes a fault-tolerant routing protocol called HEALTH (High Energy Aware and Low Thermal Routing Protocol), which aims to reduce energy consumption while ensuring fault tolerance in WBANs, maintaining high service quality for efficient and resilient data management. HEALTH distinguishes between critical and non-critical nodes by applying a pathfinding strategy that considers the nodes' priority as well as their energy and temperature levels.

The article is organized as follows: Section 2 reviews previous work on routing in body sensor networks. Section 3 describes the working environment context. Section 4 presents the fault-tolerant routing protocol. Section 5 evaluates the performance of the HEALTH protocol using the Castalia and BNS frameworks based on Omnet++. Finally, Section 6 concludes the article by summarizing our contributions and presenting the prospects for future research.

2 Related works

The design of efficient routing protocols for wireless body area networks (WBANs) is essential due to the critical role data plays in human health. In this section, we review prior studies and existing routing protocols specifically developed for WBANs.

In 2020, Caballero et al. proposed the LATOR (Link-Quality Aware and Thermal Aware On-Demand Routing) [9].protocol for WBANs, designed to enhance packet delivery rates, minimize energy use, and extend node battery life. LATOR uses a Link Quality Indicator (LQI) approach for relay node selection and manages node temperature to prevent overheating during route disco very. Based on the AODV protocol [10], it includes route discovery and maintenance phases, where RREQ and RREPmessages are exchanged during discovery, and RERR and HELLO messages during maintenance. While LATOR improves packet delivery, it has a limitation on the maximum number of hops for routes, causing packet transmission failure if this limit is exceeded. Additionally, the sink node's responses to multiple RREQs may lead to network congestion, energy consumption, and collisions.

In 2013, Nadeem et al. introduced the SIMPLE (Stable and Intelligent Multi hop Protocol for Efficient Data Delivery in Wireless Body Area Networks) routing protocol [11], designed to be reliable, energy-efficient, and fast, making it ideal for continuous patient monitoring. In this protocol, sensors measuring critical data are placed near the central node for direct communication, while other nodes select retransmission nodes based on a cost function, which ensures high residual energy and short distance to the central node, thus guaranteeing reliable data delivery. The retransmission node uses TDMA to collect and forward data to the central node. Simulation results demonstrate that SIMPLE improves net work stability and extends node lifetime. However, using TDMA leads to longer transmission times for critical data, and selecting retransmission nodes close to the central node can deplete the battery life of nearby nodes more quickly.

In 2020, Ibrahim et al. introduced the R-SIMPLE (Reliable Stable Increased-throughput Multi-hop Protocol for Link Efficiency in Wireless Body Area Networks) routing protocol [12], an enhancement of the SIMPLE protocol. It incorporates an intelligent sleep mode where sensors are categorized as critical or non-critical. Non-critical sensors enter sleep mode based on a time schedule provided by the supervising physician. The protocol also includes data verification by non-critical sensors to ensure the data remains within defined critical values. Additionally, an acknowledgment request is added to confirm successful data transmission to the collection node. R-SIMPLE improves upon SIMPLE by optimizing the cost function for selecting data transmission paths, using a performance factor to choose the least costly path for efficient data transfer. While R-SIMPLE enhances energy efficiency, network reliability, stability, and lifetime, the data verification process may increase the processing load on sensors and potentially lead to higher energy consumption.

In 2020, Khan et al. proposed the EHCRP (Energy Harvested and Cooperative Enabled Efficient Routing Protocol) for wireless body sensor networks [13].

This protocol enhances data transmission efficiency and reliability by considering parameters like residual energy, the number of hops to the receiver, and congestion levels. It employs a path cost function to select the optimal relay node based on these factors. EHCRP improves multi-hop transmission efficiency, thereby extending network lifetime and optimizing data delivery. Additionally, it prioritizes data by classifying packets into ordinary and emergency types, ensuring timely transmission of critical information.

In 2024, Oussane et al. proposed the FTRBT (Fault-tolerance Routing Based Tree) [14] protocol for WBANs in the medical field. This protocol organizes nodes into a virtual tree structure to enhance the fault tolerance of health data while optimizing QoS. FTRBT operates in two phases: the recognition phase, where each collector creates its routing table, and the routing phase, where data is processed according to its nature (alert or best-effort) and connection status. Alert data is replicated in the event of a failure, while best-effort data is either sent to a connected node or replicated. An acknowledgment mechanism ensures data is stored in the cloud, and once nodes reconnect, the data is transmitted, and replica storage is freed.

Table 1 summarizes the strengths and weaknesses of the previously discussed routing protocols.

Table 1: Comparison of previous approaches.

Metrics	**LATOR [9]**	**SIMPLE [11]**	**R-SIMPLE [12]**	**EHCRP [13]**	**AODV [10]**	**FTRBT [14]**
Packet Delivery Ratio	✓	✓	✓	✓	✓	✓
Energy Efficiency	✓	✓	✓	✓	×	✓
Network Stability	✓	✓	✓	✓	×	✓
Latency Reduction	×	✓	✓	×	×	✓
Storage Overhead	×	×	✓	×	✓	×
Relay Selection Efficiency	✓	✓	✓	✓	×	✓

3 Environment and assumptions

The network under investigation is a WBAN, specifically designed for monitoring physiological vital signs. Its primary goal is to collect medical data and facilitate wireless communication between sensors and health monitoring systems, enabling real-time health monitoring for patients. The system prioritizes minimizing the impact of network failures by focusing on data preservation and ensuring continuous operation. It incorporates fault-tolerant routing to maintain a high quality of service.

Figure 1 illustrates the architecture of the proposed WBAN network, which includes sensor nodes (depicted in green), aggregation nodes (yellow), and a sink node (red). In addition, the following assumptions are necessary for the proper functioning of our system presented below:

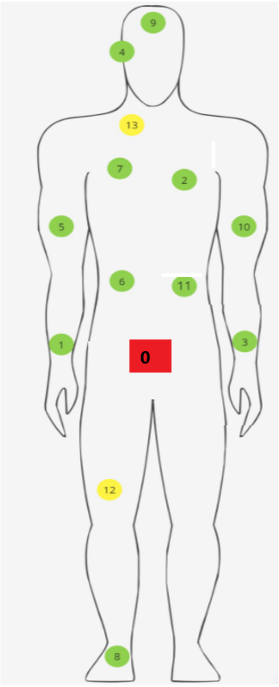


Fig. 1: Proposed Architecture.

- We consider a WBAN with a predefined number of nodes placed in the human body.
- Nodes can be sensors or relay nodes.
- Sensors can be critical sensors that detect a parameter threatening the patient's vital prognosis, or non-critical for non-threatening parameters.
- Messages can be system messages such as a node's temperature threshold exceeding or application messages concerning captured measurements such as temperature, EEG, etc.
- According to the architecture used, the master node is static and is placed in the human body.
- The computing capabilities of sensor and aggregation nodes are identical.
- The computing capabilities of the sink are higher than those of other nodes.

- The transmission capabilities of the nodes are identical.
- We assume that all nodes have the same transmission radius.
- The transmission radius can be increased according to the situation

We have opted for a configuration where the WBAN consists of the sensors described in Table 2.

Table 2: Location and Type of Sensors (DT = Data Type, Pos = Position, ST = Sensor Type, P = Periodic, EB = Event-based, WR = Wrist, RA = Right Arm, RC = Right Chest, LA = Left Arm, Abd = Abdomen, Impl = Implanted, W = Wearable).

Node	**Medical Sensor**	**Function**	**DT**	**Pos**	**ST**
0	Sink	Data collection	All sensors	Size	/
1	Heart Rate Sensor	Measures heart rate	P, EB	WR	W
2	ECG Sensor	Measures cardiac activity	P	Chest	Impl
3	Body Temperature Sensor	Measures body temperature	P, EB	WR	W
4	Pulse Oximeter Sensor	Measures oxygen saturation	P	Ear	W
5	Blood Pressure Sensor	Measures blood pressure	P, EB	RA	W
6	Glucose Sensor	Measures blood glucose levels	P, EB	Abd	Impl
7	Respiratory Sensor	Measures respiratory rate	P, EB	RC	W
8	Motion Sensor	Detects movements	P, EB	Foot	W
9	EEG Sensor	Measures brain activity	P	Scalp	W
10	EMG Sensor	Measures muscle signals	EB	LA	W
11	Lactate Sensor	Measures lactate concentration	EB	Abd	Impl

4 Proposed Approach

4.1 Basic ideas

The architectural design of our HEALTH protocol is based on a hierarchy of priorities for sensors and messages. Critical sensors are responsible for measuring sensitive data related to the patient's condition, such as the blood glucose sensor for diabetes. Non-critical sensors, such as the temperature sensor, have a lower priority.

In our system, there are two categories of messages: best effort messages and alert messages. Sensors regularly send measurements captured during each transmission period T, which may contain one or more measurement instants, as illustrated in Figure 2. The measured data are then aggregated and sent as best effort messages to the sink node. If a sensor detects sensitive data, an alert message is immediately sent to the main receiver.

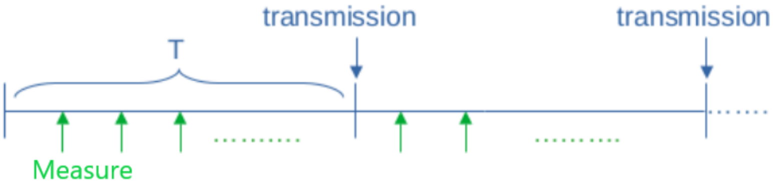


Fig. 2: Measurement and transmission time.

4.2 Description of the HEALTH protocol

In our protocol, we have used a priority order among messages. We distinguish priority rules as follows:

1. Alert messages take precedence over best effort messages.
2. Alert messages from a critical sensor take precedence over those from a non-critical sensor.
3. Application alert messages take precedence over system alert messages.

The message routing operates according to one of the following cases:

1. If the alert message comes from a critical sensor, the node increases its transmission radius.
2. If the alert message comes from a non-critical sensor, the node performs optimal route discovery in terms of hops.
3. In the case of best-effort messages, the node chooses the next hop based on a cost function C defined in Equation 1:

$$C(n_i) = \frac{E_i}{T_i} \tag{1}$$

Where n_i represents the node neighboring i, E_i is the energy level of node i and T_i is the temperature of node i.

If a sensor detects a low energy level (below the energy threshold α_E) or a high temperature (above the temperature threshold α_T), an alert message is sent to the sink. If the node's temperature returns to normal, a message is sent to its neighbors.

In this protocol, six categories of messages circulating in the network are used. Ping messages are exchanged during the recognition phase to calculate the cost function of the various neighbors and detect link breaks. DATA is a message containing the data measured by the sensor. RREQ, a route request message, is sent during route discovery to determine an optimal route in terms of the number of hops to the sink. RREP is a route response message, sent in response to RREQ by the sink or by a node with an active route to the sink in its routing table. RERR is a route error message sent by a node with a high temperature. ACK is an acknowledgement message sent by the sink or an intermediate node to confirm receipt of a critical alert message.

The flowchart in Figure 3 describes the general operation of the HEALTH protocol.

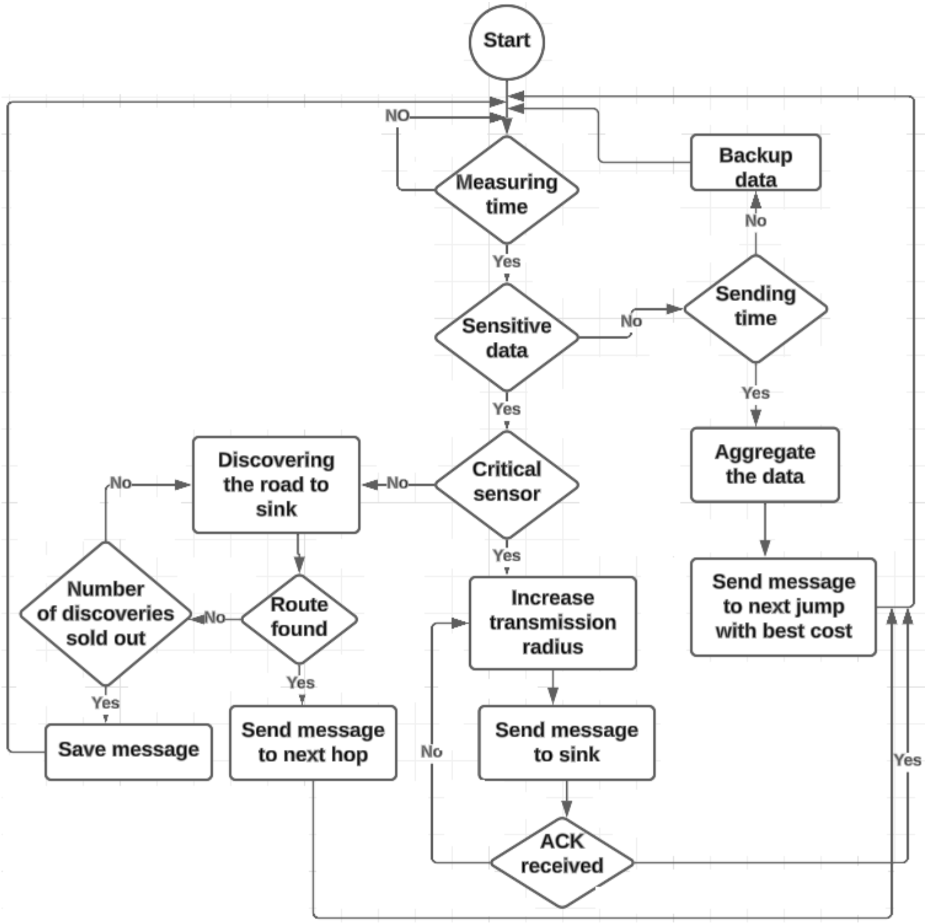


Fig. 3: HEALTH Protocol Flowchart.

Reconnaissance phase During initialization, the sink node sends a Ping message to all its neighbors. Each node that receives a Ping updates its timestamp and then propagates the message to its neighbors. This message exchange is then carried out periodically to update the routing table RT, which records paths to destinations as well as the node's neighbors. Additionally, each node deactivates the lines of neighbors from which it has not received a Ping for three periods.

Routing phase The node takes measurements at regular intervals. If the measured data is sensitive, an alert message is immediately sent to the sink. The choice of the route depends on the type of emitter (critical or non-critical). If the measured data is not sensitive, the node stores them in a queue, then aggregates and sends them at regular intervals.

- **When it's an Alert message from a critical sensor:** The sensor increases its transmission radius to reach the sink node in a maximum of two hops. Once the packet is sent, the alert message is recorded in a dedicated queue for possible retransmission in case of failure. An acknowledgment timer is also initialized in the last line of the algorithm to check the reception of the message.
  When a node receives a critical alert message, it sends an acknowledgment to the sender if it is the sink or one of its neighbors. The sink's neighbors intercepting the alert message relay it to the sink. When the sender receives the acknowledgment, it removes the alert message from the queue. If the acknowledgment timer expires, the node retransmits alert messages from the queue if it is not empty.
- **In the case of an Alert message from a non-critical sensor:**The sensor explores the shortest path to the sink. If an active path to the sink exists, the sensor forwards the data packet to the next hop specified in the routing table. In the absence of an active path, the data packet is queued in a dedicated queue, while an RREQ message is dispatched to the node's neighbors, and an RREP timer is triggered.
  When a node receives a routing request *RREQ*, it checks if its temperature exceeds the *threshold* α_T . If the temperature is below the threshold and the node has not already received the *RREQ*, it adds the route to the source in its routing table. Then, it checks if there is already a route to the sink. If the node is the sink itself or if it already has an active route to the sink in its routing table, it responds with a routing reply *RREP* message. Otherwise, it forwards the RREQ to its neighbors. If the *RREQ* is received by another node, the sender is added to the list of nodes waiting for a route to the sink (predecessors field in the routing table). If the temperature exceeds the threshold, the node responds by sending a routing error *RERR* message to the *RREQ* sender. When a node receives an *RREP*, it adds the path to the sink to its routing table and indicates the reception of an *RREP*. If the node is the initiator of the *RREQ*, it forwards the data to the next hop. Otherwise, it forwards the *RREP* to all nodes waiting for a route to the sink. When the *RREP Timer* expires, the node checks if the *RREP reception indicator* is activated. If no *RREP* is received and the maximum number of attempts is not reached, the node resends an *RREQ*. When a node receives a *RERR*, all paths with the next hop being the initiator of the *RERR* are deactivated, and a *RERR* message is transmitted to their predecessors.
- **In the case of Best Effort messages :** The message follows a multi-hop path, where the next hop is selected from neighbors that meet energy and temperature constraints. A node is considered a candidate for routing

if its battery level is above a threshold α_E and its temperature is below a threshold $T_{\max}$, where $T_{\max} < \alpha_E$. The candidate chosen for routing is the one with the maximum value of the cost function C, defined in Equation 1. If two candidates have the same cost, we select the one with the highest energy level. If no candidate node is available, the message is routed to the neighbor with the highest energy level among nodes that meet the temperature constraint, if they exist. Otherwise, the message is sent back to the sender. The sender then chooses another route from the remaining candidate nodes. If the sender is the source of the message and no other alternative route is available, the message is queued until a system message indicates that the temperature of a neighbor node has returned to normal.

4.3 Discussion

The proposed protocol prioritizes energy efficiency and temperature control while maintaining a satisfactory packet delivery rate. It categorizes messages into three priority levels. Critical sensor alerts, these have the highest priority as they relate to urgent medical data. Sensors adjust their transmission range to ensure immediate delivery, and these messages are retransmitted until acknowledged. Non-critical alerts, these are time-sensitive but not life-threatening. The protocol avoids overheated nodes during route discovery for these messages. Best-effort messages, these are non-urgent and use multi-hop routing based on energy and temperature metrics. Their transmission can be delayed if necessary.

The protocol uses two temperature thresholds, $T_{\max}$ and α_T, to regulate node temperature and prevent overheating, balancing network efficiency and safety. However, the assumptions of identical sensor capabilities may not reflect real-world scenarios, as actual nodes may have varying performance due to hardware limitations. Accounting for these variabilities could improve the protocol's robustness in practical applications.

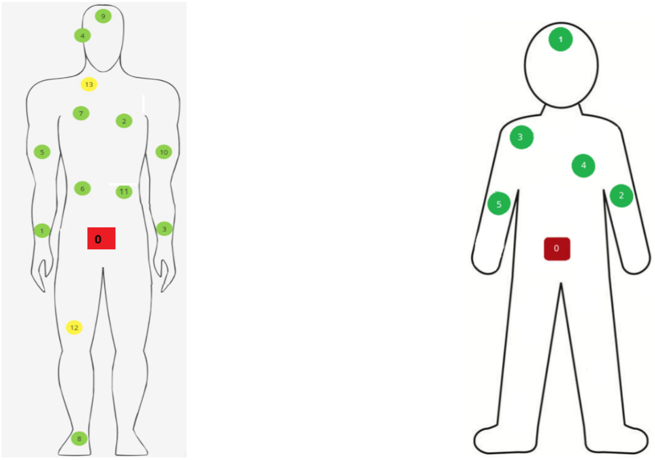
5 Performance Analysis

Simulations were conducted to evaluate the proposed solution using the Omnet++ and Castalia simulators. Omnet++ is a modular, object-oriented discrete event simulator [15], while Castalia is a framework specifically designed for WSN and WBAN networks based on the OMNeT++ platform [16]. To model body mobility, node temperatures, the IEEE 802.15.6 protocol, and a transmission channel compliant with WBANs, we also employed the Body Network Simulator (BNS) framework in the simulation [17].

5.1 Simulation parameters

To test the suggested routing protocol and evaluate its performance, we delimited a simulation area of dimensions 5 meters × 5 meters × 5 meters, representing an enclosed space where the patient moves. The simulation runs over a period of 1000 seconds. Each node starts the simulation with an initial energy of 18720 joules and an initial temperature of 37°C. Critical thresholds are set at 50% of the initial energy for the energy threshold (αE), and at a maximum temperature of 37.001°C for the lower temperature threshold (T_{max}) and the critical temperature threshold (αT). The MAC protocol used is 802.15.6 [18], with transmission power varying between -20dBm and -10dBm. Each node is allowed to send a maximum of 1000 data packets during the simulation.

We perform simulations on two distinct scenarios. The first scenario, characterized by a high sensor density with relay nodes, is illustrated in Figure 4a. The second scenario, featuring a low sensor density without relay nodes, is shown in Figure 4b.



(a) Scenario 1:High density.

(b) Scenario 2: Low density.

Fig. 4: Architecture of the two scenarios.

The proposed scenarios are crucial for evaluating the protocol in various IoT contexts, as they test its ability to adapt to different sensor network configurations. This allows for an analysis of its performance in terms of energy, QoS, and latency management, and to verify if the protocol maintains its performance under varying network conditions, which is essential for real-time applications such as healthcare or automation.

The sending period is calculated on the basis of the rate (number of packets sent per second) of each node, as shown in Table 3.

We vary mobility in both architectures to obtain the different scenarios mentioned in Table 4. At the beginning of the simulation, each node periodically sends data packets, except for nodes 0 (sink), 10, and 12.

Table 3: Packet Rate of Nodes (packets/s).

Node	1	2	3	4	5	6	7	8	9	11
Packet Rate	86	0.40	0.96	192	1.20	0.024	0.048	1.00	0.048	35

Table 4: Simulation scenarios.

Scenario	Mobility	Architecture	Node Number Sending Alerts	Node Type	Alert Sending Rate
A	No	High density	3	Non-critical node	1/20
B	Yes		5	Critical node	1/3
			9	Critical node	1/2
C	No	Low density	3	Non-critical node	1/20
D	Yes		4	Critical node	1/2

5.2 Metrics

We evaluate the proposed protocol according to the following metrics:

- *Residual Energy or Remaining Energy:* Predicts the lifespan of a node and, consequently, the network.
- *Packet Delivery Ratio (PDR):* Represents the ratio of the number of received packets to the number of sent packets (see Equation 2).

$$\text{PDR} = \frac{\text{number of received packets}}{\text{number of sent packets}} \tag{2}$$

- *Node temperature:* An increase in the temperature of a node beyond a certain threshold is hazardous to humans.
- *End-to-End Delay:* Represents the duration of time required to deliver a packet to its destination.

5.3 Results interpretation

This section aims to evaluate the performance of the HEALTH protocol via simulations, examining various scenarios and comparing them with the LATOR protocol, given their similarity in operation. The results of simulations in different contexts will be analyzed with reference to the metric mentioned above.

Residual Energy: According to the graph in Figure 5, illustrating the variation of the average residual energy of nodes across scenarios, it can be observed that Scenarios C and D have lower energy consumption compared to Scenarios

A and B. In Scenarios C and D, both protocols exhibit similar energy consumption. However, in Scenarios A and B, the HEALTH protocol consumes slightly more energy than the LATOR protocol. Additionally, in Scenario 1, residual energy decreases slowly in the absence of mobility (Scenario A) compared to body mobility (Scenario B), while in Scenario 2, residual energy remains constant.

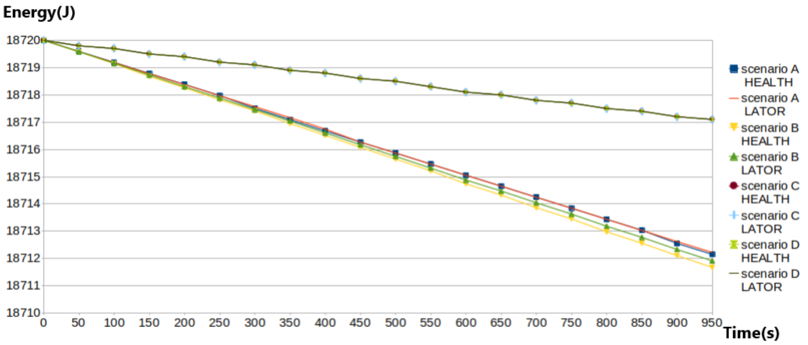


Fig. 5: Average energy

Regarding the plots in Figures 6 and 7 representing the evolution of the minimum residual energy of nodes, they show that this evolution is almost identical to that of the average residual energy for each scenario.

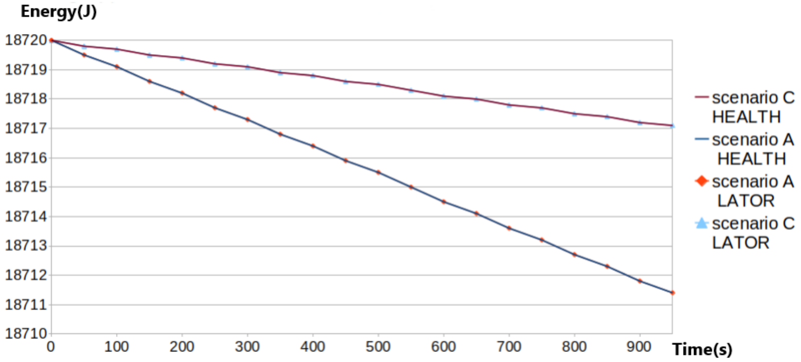


Fig. 6: Minimum Energy (without mobility).

In summary, in dense environments (Scenarios A and B), residual energy depletes more rapidly due to the intensity of communications and increased energy

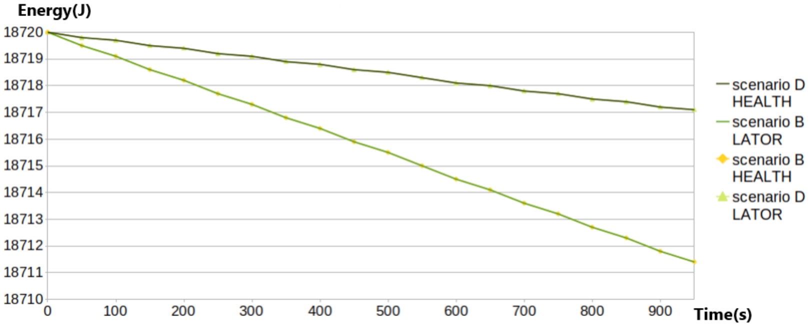


Fig. 7: Minimum Energy (with mobility).

demands. Node mobility has a limited impact on energy consumption, indicating that the protocol is not highly sensitive to sensor movement. The LATOR protocol stands out for its superior energy efficiency, primarily due to its ability to adjust the transmission radius of critical nodes during alert scenarios. This reduces retransmissions and improves communication reliability, a significant advantage in critical contexts. Conversely, the HEALTH protocol, while more energy-efficient in simple scenarios, is less effective in terms of packet delivery in demanding conditions. However, the difference in energy consumption between the two protocols becomes negligible when considering the higher packet delivery rate provided by LATOR. This trade-off is crucial for real-time applications, where transmission reliability is paramount.

Rate of packages delivered (PDR) The graphs in Figures 8 and 9 illustrate the Packet Delivery Ratio (PDR) of nodes across different scenarios.

In Scenario 1 (High density), the PDR of the LATOR protocol is zero due to strong interferences caused by node density. This leads to a focus on the PDR of the HEALTH protocol. In scenario A, nodes closest to the sink (8 and 9) achieve the highest PDR, followed by alert-sending nodes (3, 5, and 9). Nodes 2 and 6, located on the limbs, have better PDRs than those farther from the sink (1 and 11), despite the use of relay nodes. In scenario B, with mobility, the PDR of all nodes decreases. However, limb nodes (2, 5, and 11) show significant differences between Scenarios A and B. Node 6 loses fewer packets compared to others, but node 4 experiences heavy interference, nullifying its PDR and impacting node 3 as well.

In Scenario 2 (Low density), node 2 achieves the highest PDR, followed by nodes 1, 3, and 5, while node 4 has the lowest PDR despite being close to the central point. Nodes 1 and 4 show the worst PDRs in the LATOR protocol, with significant differences compared to the HEALTH protocol. Node 5 is the least impacted by mobility, showing minimal PDR variation between Scenarios

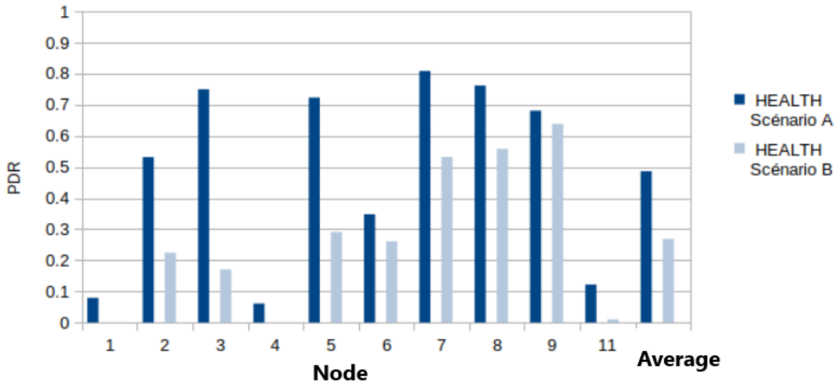


Fig. 8: Packet Delivery Rate (Scenario 1).

C and D. Overall, the HEALTH protocol demonstrates better average PDR performance compared to LATOR in both scenarios.

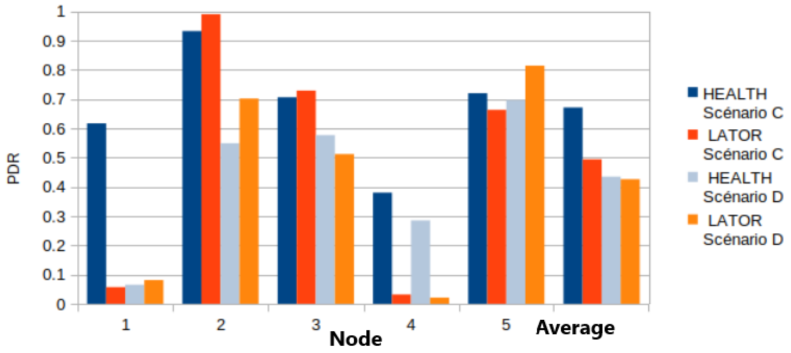


Fig. 9: Packet Delivery Rate (Scenario 2).

In dense environments (Scenarios A and B), residual energy depletes faster due to the intensity of communications and increased energy demands, while node mobility has a limited impact on energy consumption, indicating that the protocol is less sensitive to sensor movement. The LATOR protocol stands out for its better energy efficiency, particularly due to its ability to adjust the transmission radius of critical nodes during alert scenarios, which reduces retransmissions and improves communication reliability, a key advantage in critical contexts. On the other hand, while the HEALTH protocol is more energy-efficient in simpler scenarios, it performs less effectively in terms of packet delivery in more demanding environments. However, the energy consumption gap between the two protocols becomes negligible when considering the higher packet delivery rate provided by LATOR, a trade-off that is crucial for real-time applications where transmission reliability is paramount.

Node Temperature Figure 10 shows that the average temperature of nodes rises faster in Scenarios C and D due to fewer nodes, resulting in limited alternative routes and higher node workloads. However, the LATOR protocol demonstrates a slower temperature increase compared to the HEALTH protocol, despite both avoiding overheated nodes during routing.

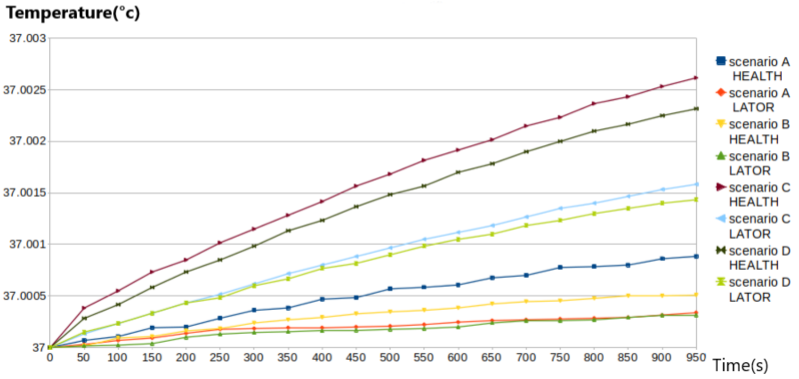


Fig. 10: Average Temperature.

Figure 11 reveals that in HEALTH Scenarios A, B, and C, the maximum temperature trend mirrors the average, indicating uniform heat distribution. Conversely, in all LATOR scenarios and HEALTH Scenario D, a significant gap between average and maximum temperatures suggests uneven heat distribution among nodes.

In summary, the HEALTH protocol provides better thermal balance than LATOR due to two main factors: the use of a cost function C for best-effort routing, which helps avoid thermal overload by directing packets to less stressed nodes, and the integration of lower and critical temperature thresholds to keep nodes at safe temperatures. These mechanisms ensure a uniform thermal management, whereas LATOR, although energy-efficient, does not specifically address thermal management, potentially leading to imbalances. Thus, even though LATOR slows down temperature rise, HEALTH proves more suitable in environments where precise thermal control is crucial.

End-to-End delay Since the packet delivery rate in Scenarios A and B is zero in LATOR, we only examine the distribution of packet reception delays in the

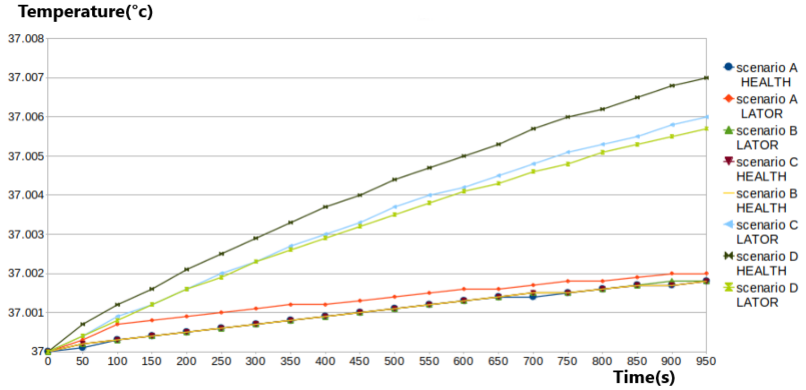


Fig. 11: Maximum Temperature.

HEALTH protocol, as shown in the graphs in Figures 12 and 13. All packets from the three priority levels have delays exceeding 500 ms. This is due to the density of the architecture, leading to increased congestion in the network and consequently longer transmission delays.

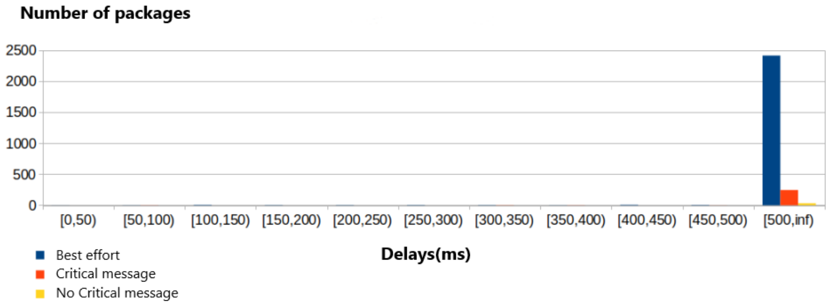


Fig. 12: Histogram of End-to-End Delays (HEALTH scenario A).

In Scenarios C and D, both protocols' end-to-end delays are compared based on packet priority. Most best effort packets reach the destination in under 100 ms, but in some cases (like in the HEALTH protocol in Scenario C and both LATOR and HEALTH protocols in Scenario D), delays exceed 1000 ms. Non-critical alert packets sent by the LATOR protocol consistently have delays above 1000 ms, whereas HEALTH protocol's alerts in Scenario C have delays under 600 ms, with fewer than 10 packets exceeding 1000 ms. In Scenario D, delays for most packets from the HEALTH protocol range from 500 ms to 1000 ms. Critical alert packets from both protocols have delays below 100 ms.

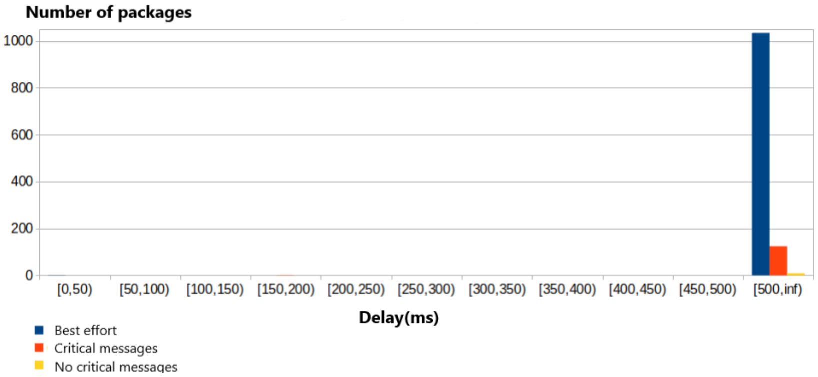


Fig. 13: Histogram of End-to-End Delays (HEALTH scenario B).

The results show that the LATOR protocol has longer delays for non-critical packets, mainly due to the lack of a priority-based routing mechanism. Without this feature, LATOR treats packets equally, meaning even non-critical packets may follow the same paths or undergo the same processes as critical packets. This can lead to congestion or suboptimal paths, increasing delays for non-critical packets. On the other hand, HEALTH integrates a mechanism that prioritizes critical packets, meaning these packets are routed quickly with fewer hops, reducing delays, especially in scenarios where time-sensitive data, such as health alerts, needs to be transmitted quickly. This optimized routing for critical packets is particularly beneficial in networks where certain packets are more urgent than others, ensuring QoS for these essential packets. However, the situation is different for non-critical alert packets in HEALTH. These packets, although less urgent, undergo a route discovery process through flooding, which can lead to longer delays. Flooding, while effective for discovering new routes in dynamic networks, can add delays due to the time required to transmit information through all nodes in the network before a valid path is found. This mechanism, while effective in some cases, is not optimal for all types of data and may increase delays for less time-sensitive packets. In summary, HEALTH is more effective for transmitting critical packets by reducing hops, while LATOR suffers from longer delays for non-critical packets due to the lack of prioritization, but with a more homogeneous behavior for all types of packets.

6 Conclusion and Perspectives

This article proposes a fault-tolerant solution for WBANs in IoT networks, aiming to ensure data integrity and continuous system operation despite sensor failures or rapid battery discharge. The HEALTH protocol optimizes energy consumption by establishing a hierarchy of packet priorities and adapting routing based on the energy and thermal states of nodes. It also aims to reduce the number of exchanged packets and minimize latency. Simulations were conducted to evaluate its effectiveness across various scenarios, comparing it with the LATOR protocol. The results demonstrate HEALTH's superior performance within the BNS framework.

In the future, we plan to extend the implementation of our fault tolerance solution to a broader environment, with a particular focus on routing and integrating QoS across WBAN networks.

References

1. Keyur K Patel, Sunil M Patel, and P Scholar. Internet of things-iot: definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing*, 6(5), 2016.
2. Ochirkhand Erdene-Ochir, Marine Minier, Fabrice Valois, and Apostolos Kountouris. Resiliency of wireless sensor networks: Definitions and analyses. In *2010 17th International Conference on Telecommunications*, pages 828–835. IEEE, 2010.
3. Carlos Granell, Andreas Kamilaris, Alexander Kotsev, Frank O Ostermann, and Sergio Trilles. Internet of things. *Manual of digital earth*, pages 387–423, 2020.
4. Iqbal H Sarker, Asif Irshad Khan, Yoosef B Abushark, and Fawaz Alsolami. Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mobile Networks and Applications*, 28(1):296–312, 2023.
5. Israa Al-Barazanchi, Haider Rasheed Abdulshaheed, and Madya Safiah Binti Sidek. A survey: Issues and challenges of communication technologies in wban. *Sustainable Engineering and Innovation*, 1(2):84–97, 2019.
6. Merey Zhumayeva, Kassen Dautov, Mohammad Hashmi, and Galymzhan Nauryzbayev. Wireless energy and information transfer in wban: A comprehensive state-of-the-art review. *Alexandria Engineering Journal*, 85:261–285, 2023.
7. Umar Musa, Shaharil Mohd Shah, Huda A Majid, Ismail Ahmad Mahadi, Mohamad Kamal A Rahim, Muhammad Sani Yahya, and Zuhairiah Zainal Abidin. Design and analysis of a compact dual-band wearable antenna for wban applications. *IEEE Access*, 11:30996–31009, 2023.
8. Sakina Oussane, Haroun Benkaouha, and Amir Djouama. Fault tolerance in the iot: A taxonomy based on techniques. In *2023 Third International Conference on Theoretical and Applicative Aspects of Computer Science (ICTAACS)*, pages 1–8. IEEE, 2023.
9. Egberto Caballero, Vinicius C Ferreira, Robson A Lima, Célio Albuquerque, and Débora C Muchaluat-Saade. Lator: Link-quality aware and thermal aware on-demand routing protocol for wban. In *2020 International Conference on Systems, Signals and Image Processing (IWSSIP)*, pages 337–342. IEEE, 2020.
10. Charles Perkins, Elizabeth Belding-Royer, and Samir Das. Ad hoc on-demand distance vector (aodv) routing. Technical report, Internet Engineering Task Force (IETF), 2003.
11. Qaisar Nadeem, Nadeem Javaid, Saad Noor Mohammad, MY Khan, Sohab Sarfraz, and M Gull. Simple: Stable increased-throughput multi-hop protocol for link efficiency in wireless body area networks. In *2013 eighth international conference on broadband and wireless computing, communication and applications*, pages 221–226. IEEE, 2013.

12. Mohammed Abdulrahman Dawood Al-Obaidi and Abdullahi Abdu Ibarahim. R-simple: Reliable stable increased-throughput multi-hop protocol for link efficiency in wireless body area networks. In *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pages 1–5. IEEE, 2020.
13. Muhammad Dawood Khan, Zahid Ullah, Arshad Ahmad, Bashir Hayat, Ahmad Almogren, Kyong Hoon Kim, Muhammad Ilyas, and Muhammad Ali. Energy harvested and cooperative enabled efficient routing protocol (ehcrp) for iot-wban. *Sensors*, 20(21):6267, 2020.
14. S. Oussane, H. Benkaouha, and A. Djouama. Fault tolerant routing in iot based on wban. In *International IOT, Electronics and Mechatronics Conference 2024*, Imperial College London, United Kingdom, 2024. Springer.
15. András Varga and Rudolf Hornig. An overview of the omnet++ simulation environment. In *1st International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems*, 2010.
16. Tabassum Waheed, Faisal Karim Shaikh, Iqbal Uddin Khan, et al. Wban performance evaluation at phy/mac/network layer using castalia simulator. In *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, pages 1–6. IEEE, 2019.
17. Egberto Caballero, Vinicius Ferreira, Robson Araújo Lima, Julio César Huarachi Soto, Débora Muchaluat-Saade, and Célio Albuquerque. Bns: A framework for wireless body area network realistic simulations. *Sensors*, 21(16):5504, 2021.
18. Kyung Sup Kwak, Sana Ullah, and Niamat Ullah. An overview of ieee 802.15. 6 standard. In *2010 3rd international symposium on applied sciences in biomedical and communication technologies (ISABEL 2010)*, pages 1–6. IEEE, 2010.