



Multiple parameter decision for backoff counter optimization of medical body area network

Khushboo Dadhich¹ · Devika Kataria¹

Accepted: 31 March 2024

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2024

Abstract

Medical Body Area Networks are emerging as remote healthcare solutions where many sensors monitor the physiological parameters of the human body and communicate the data to a central hub. In this work, the goal has been to improve the reliability of data transmission using the Carrier Sense Multiple Access with Collision Avoidance protocol used in the medium access control layer. The authors propose an algorithm for optimizing backoff counter value using a multi-parameter decision-making algorithm called Criteria Importance through Intercriteria Correlation (CRITIC). We use CRITIC for deciding the user priority and backoff counter values, to reduce collisions and improve the reliability of medical body area networks. The work has evolved into three parts, the first part being the use of CRITIC to determine the sensor node's priority when multiple nodes with different packet sizes and data rates are ready for data transmission. The second part was to use CRITIC to compute the backoff counter value depending on node parameters. These new values have the advantage that they are dependent on the weights of various parameters associated with the sensor node and therefore minimize the waiting time. Thirdly, a Markov chain-based analytical model has been presented to obtain the expression for performance metrics such as reliability, probability of transmission, probability of channel access failure, and probability of packet drop due to maximum retransmission limit. Simulation have been done for 10 practical sensor nodes with various distinct parameters using MATLAB. The results validate that the CRITIC backoff counter value in IEEE 802.15.6 standard enhances the reliability as compared with the conventional IEEE 802.15.6 backoff counter value. The results in this work show that the probability of packet drop reduces from 0.93 to 0.49.

Keywords Medical body area network · CRITIC · IEEE 802.15.6 standard · Markov chain · Backoff counter · User priority

1 Introduction

In the ever-evolving landscape of healthcare technology, Medical Body Area Networks (MBANs) have emerged as promising solutions for monitoring and transmitting vital patient data [1–5]. MBANs consist of a network of body-worn sensors that collect real-time medical information and wirelessly transmit it to medical monitoring devices. To ensure seamless and accurate communication within these networks, the implementation of an efficient protocol is essential. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) has proven to be a reliable and effective protocol for MBANs, enabling improved channel

access, reduced interference, and enhanced overall network performance.

The CSMA/CA is a widely adopted protocol that governs access to the shared communication channel in wireless networks [6–10]. It allows devices to sense the carrier signals and determine if the channel is currently in use. If the channel is busy, the devices defer their transmission to avoid collisions, thereby reducing data corruption and ensuring reliable communication.

In MBANs, where multiple sensors are transmitting data simultaneously, CSMA/CA plays a critical role in preventing collisions and optimizing network efficiency. The protocol enables each sensor to sense the channel before transmitting data. If a sensor detects an ongoing transmission, it waits for the channel to become available. By avoiding collisions, CSMA/CA ensures that medical data is transmitted accurately and reliably, eliminating the need for retransmissions, and minimizing network congestion.

✉ Khushboo Dadhich
devikakataria@jkl.u.edu.in

¹ JK Lakshmipat University, Mahapura, India

CSMA/CA incorporates a collision avoidance mechanism to further enhance the reliability of data transmission in MBANs. After detecting a busy channel, a sensor will defer its transmission for a period, known as the backoff period [11]. This randomization process minimizes the chances of multiple sensors selecting the same backoff period simultaneously, reducing the likelihood of collisions when attempting retransmission. A lot of research is being conducted to enhance the performance of the CSMA/CA mechanism. Some of these methods that can be employed for backoff counter value selection in MBAN are as follows:

1. **Fixed Backoff:** In this method, a predetermined fixed backoff counter value is used for all devices. Each device waits for the specified duration before attempting retransmission after a collision. This approach is simple to implement but may not provide optimal performance in dynamic and varying network conditions.
2. **Random Backoff:** In this method, a contention window is defined, which represents the range of possible backoff counter values. After a collision, devices select a random value within the contention window and wait for that duration before retransmission. The contention window size can be adjusted dynamically based on network conditions to balance between collision avoidance and efficient channel utilization.
3. **Exponential Backoff:** The exponential backoff method adjusts the backoff counter value based on the number of consecutive collisions. After each collision, the device doubles the backoff duration, thereby increasing the waiting time before retransmission. This approach aims to avoid repeated collisions and allows network congestion to dissipate gradually [12].

However, these methods of back-off counter selection have the following drawbacks:

1. **Increased Delay:** Backoff counters introduce a waiting period before retransmission after a collision or contention. This waiting period can result in an increased delay in delivering data, especially in scenarios where multiple devices are contending for access to the wireless medium. The delay can affect the real-time nature of certain healthcare applications, potentially impacting the timely delivery of critical information.
2. **Fairness Issues:** Backoff counters aim to provide fairness by randomizing the retransmission attempts among contending devices. However, in some situations, certain devices may experience longer waiting times due to the random nature of backoff counter selection. This can result in unfairness, where some devices consistently have shorter access delays while others have longer delays, affecting overall network performance.

3. **Inefficiency in Sparse Networks:** In MBANs with a low density of devices or sporadic traffic patterns, backoff counters may lead to underutilization of the available bandwidth. Devices may need to wait for their assigned backoff counter durations even when the wireless medium is idle, resulting in decreased efficiency and potential wastage of opportunities for data transmission.
4. **Lack of Adaptability:** Traditional backoff counter mechanisms in MBANs often use fixed or static backoff values or simple randomization. These approaches may not be adaptive enough to handle dynamic network conditions, varying traffic loads, or changing channel conditions. As a result, the backoff counter values may not be optimally adjusted, leading to suboptimal network performance.
5. **Energy Consumption:** Backoff counter mechanisms require devices to stay active during the waiting period, consuming power even when they are not transmitting data. This continuous active state can contribute to increased energy consumption, leading to reduced battery life for battery-powered devices in MBANs. Energy efficiency is a critical consideration in healthcare applications where devices are often worn or implanted on the body.

It is important to carefully evaluate and balance the trade-offs associated with back-off counter mechanisms in MBANs. Researchers and engineers continue to explore advanced algorithms and adaptive approaches to mitigate the drawbacks and improve the efficiency and performance of backoff counter selection in MBANs.

We propose an Adaptive method for the selection of backoff counter value using Criteria Importance through Intercriteria Correlation (CRITIC). In the context of selecting the backoff counter value for CSMA/CA protocols, CRITIC can be applied to evaluate the importance of different parameters of the transmitting node and prioritize them accordingly.

To apply CIRITC, a set of criteria relevant to the backoff counter selection is identified. These criteria may include parameters such as packet size, data generation rate, or delay requirements. The interrelationships between these criteria are then analyzed to determine their correlation. By examining the correlations between the criteria, CRITIC assigns importance weights to each criterion [13–16]. Highly correlated criteria indicate a stronger influence on the decision-making process and are assigned higher weights. Conversely, criteria with weaker correlations are assigned lower weights. The weights reflect the relative importance of each criterion in the context of backoff counter-selection.

Once the important weights are determined through CIRITC, they can be used in a decision-making algorithm or model to guide the selection of the backoff counter value. The algorithm considers the weighted criteria collectively

and selects the backoff counter value that best satisfies the overall objectives and requirements of the system.

2 Literature review

Several works of literature examine the performance of the IEEE 802.15.6 standard and look at the impact of various factors, including backoff counters, user priorities, and the probability of sufficient time slots etc. Although this IEEE 802.15.6 standard is a guideline for MBAN, it is still evolving and there is scope for improvement of performance. Some of the noteworthy research conducted by various researchers to improve the performance of MBAN is highlighted in the state of art discussed in this section. Rashwand et al. proposed an analytical Markov chain-based IEEE CSMA/CA model for saturation and error-prone channels in MBAN by studying their access mechanisms. The study shows that the exclusive access phase (EAP) and random-access phase (RAP), which consist of many slots, should be flexible so that the bandwidth utilization is optimized. The researchers also recommend that EAP slots are not essential unless there are a variety of traffic types present in the network [17]. Sarkar et al. established an analytical model to present the impact of channel occupancy state, packet size, and data rate of the transmitting node on standard performance. The group compared their model which have five distinct user priorities with the standard where eight priority levels have been recommended and analyzed the performance variation with variable payload [18]. Bethaina et al. used UPPAL statistical model-checking (SMC) to assess the effectiveness of the IEEE 802.15.6 CSMA/CA access mechanism and found that short access phases could not handle the medium and high traffic and recommended a new architecture for superframe so as to reduce the idle waiting time for the nodes [19]. Another group has developed two models for heterogenous traffic nodes in a network, where the first model deploys M/G/1 queueing with non-preemptive priority for handling emergency data, while the second complementary model takes care of the service by using a renewal reward-based backoff process. The study revealed that using these complementary models helped to reduce the latency for emergency data traffic with the tradeoff of the performance of other nodes [20].

Fourati et al. created a novel contention-based IEEE 802.15.6 MAC protocol through modifications to the retransmission and packet drop algorithms. The author introduced an enhanced channel access mechanism based on a new parameter called a starvation index and a new priority migration procedure. They developed the Markov model using four parameters which are the backoff counter, backoff stage, retransmission, and starvation index, where the last parameter was introduced to take care of the node being starved for

long durations while the channel was busy [21]. Samal et al. presented an energy-efficient, traffic-prioritized load-balanced scheduling algorithm where the probability of packets dropping is reduced by proper buffering of crucial packets [22]. Zia et al. proposed a Group based MAC (G-MAC) protocol, which adds a relay node to assist the main hub in handling emergency data. This relay node relieves the primary hub from nonemergency data and handles all the data transmission/collision of these nodes by acting as the cluster head. This approach reduces the latency of the emergency node relieving the primary hub from overheads of the entire traffic and reserving it for the highest priority node traffic [23].

Chen and Chiu introduced a cross-layered energy-aware resource allocation (CLEAR) protocol for Integrated Sensor Hubs. The findings of the study reveal that the CLEAR protocol delivers the quality of service (QoS) through interleaving the super frames and enhancing system energy efficiency [24]. Liang et al. developed an Energy-Efficient and Emergency-Aware Media Access Control (MAC) protocol (EEEA-MAC). This super frame is divided into three parts: the beacon component, the contention-free period (CFP), and the contention access period (CAP). In this case, each node has a distinct channel access strategy designed so that the source node uses the carrier sense multiple access collision avoidance (CSMA/CA) and the relay nodes adopt the hybrid CSMA/CA-TDMA. When the source node generates less data, this study helps in lowering collision, and the introduction of TDMA (time division multiple access) reduces conflicts and energy consumption at the relay node [25]. He et al. introduced a Joint Weight-Optimizing Timeslot allocation protocol to increase the sensor nodes' throughput. The weights for various sensors are determined using a hierarchical method and the weighted throughput is higher than the conventional throughput [26].

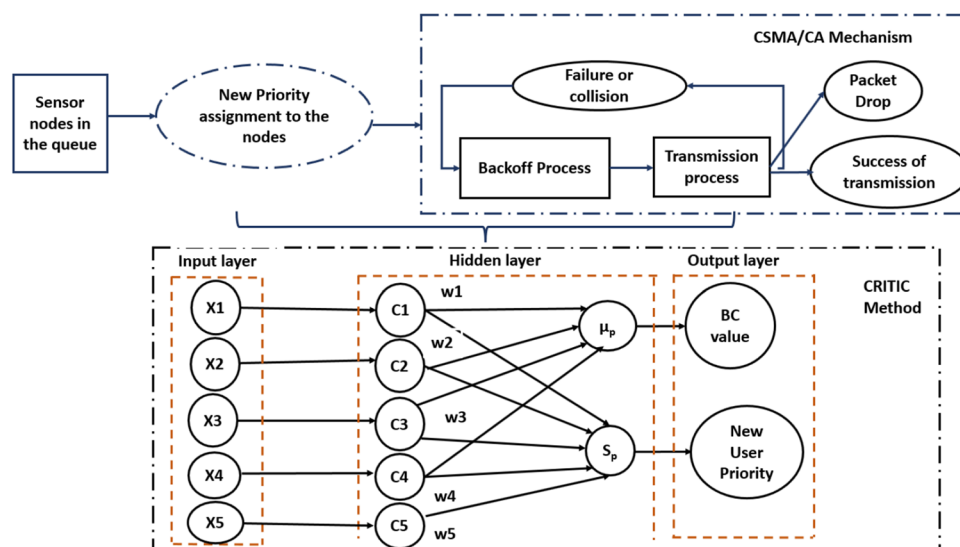
Saboor et al. described a technique for dynamic slot allocation based on non-overlapping contention windows. The Non-Overlapping Backoff Algorithm (NOBA) and the Dynamic Slot Allocation (DSA) scheme are two algorithms that are introduced by these authors. While the DSA distributes dynamic slots to reduce delay caused by the fixed slot in the super-frame structure, the NOBA eliminates back-off-induced inter-priority conflicts [27]. Enkoji et al. suggested a protocol in which the authors modify the duration of the exclusive access phase (EAP) and random-access phase (RAP) in accordance with the traffic detected by the hub during the beacon phases. The authors set aside specific EAP slots for emergency data. All non-emergency sensors in RAPs must compete for channel allocation. The outcome throughput is increased dynamically by changing the EAP and RAP slots according to the importance of the data to be transmitted [28]. In addition, Khan et al. recommended a Prioritized Fibonacci Backoff (PFB) approach

Table 1 Comparison with the state of art

Algorithms	Comparison parameters	
	Methodology	Observations
Binary exponential backoff (BEB) [27, 29]	The value of the backoff counter is chosen at random from the range $[1, CW_{min}]$ CW size is doubled up to CW_{max} for an even number of collisions	This algorithm exponentially increases the CW size which increases the idle listening time in between the process and affects the overall performance of the standard
Prioritized fibonacci backoff (PFB) [27, 30, 31]	Assign the backoff counter's value from the interval $[1, CW_{min}]$ Based on priorities, the CW value is updated	Since the node density anticipated by the IEEE 802.15.6 standard is lower than that of other IEEE standards, overlapped contention windows in the PFB algorithm result in collisions that underutilize the superframe
Non-overlapping backoff (NOBA) [19, 27]	Select the backoff counter's value from the range $[CW_{min}, CW_{max}]$ The sliding window was added to the modified CW values	Elevated lower bounds of contention windows result in extended listening times for lower user priority

Table 2 Contention window size with the user priorities

User priority	Traffic designation	Contention window minimum (CW_{min})	Contention window maximum (CW_{max})	Maximum back-off stage
UP0	Background	16	64	2
UP1	Best effort	16	32	1
UP2	Excellent effort	8	32	2
UP3	Video	8	16	1
UP4	Voice	4	16	2
UP5	Network control	4	8	1
UP6	High priority data	2	8	2
UP7	Emergency or medical implant data	1	4	2

Fig. 1 Proposed CRITIC method for redefining User Priorities and computation of optimized backoff counter value

for a constant and careful increase in contention window (CW) size before each retransmission. The suggested

approach helps in decreasing the delay, hence improving throughput and energy consumption [29].

Table 3 Sensor node parameters for CRITIC

Sensor	X_1 (UP)	X_2 (Packet size in bytes)	X_3 (Variable packet generation rate in packets/s)	X_4 (Data transmission rate in kbps)	X_5 (Buffer status)
Physical Activity	0	30	10	50	2
Temperature	1	50	15	57	3
Glucose	2	70	20	85	1
Respiration Rate	3	45	25	112	3
Ear Sensor	4	100	30	130	2
Oxygen Saturation	5	175	35	150	4
Blood Pressure	6	90	40	210	3
EEG	7	85	35	280	1
EMG	6	150	30	230	3
ECG	7	175	40	290	2

Fig. 2 Decision matrix for parameters

Sensor nodes / Parameters	X_1	X_2		X_N
0	a_{11}	a_{12}		a_{1N}
1	a_{21}	a_{22}		a_{2N}
:	:	:		
:	:	:		
M	a_{M1}	a_{M2}		a_{MN}

In another work by Saboor et al., the authors suggested a Unique Backoff Algorithm (UBA) for decreasing collisions and transmission delays. The technique uses a single contention window for all user-priority nodes; however, each node's backoff counter value varies depending on its user priority and preference assigned if there are many nodes within the same priority.

The UBA performed poorly in longer superframes due to the authors' assumption that a node could only transmit once per superframe [30]. Fourati et al. developed a unique backoff assignment function and achieved a higher Quality of Service [4]. A comparative study of the backoff algorithms is summarized in Table 1. Various Mathematical models have been studied and referenced in the methodology section of this work [31–34].

3 Mathematical model

Ten sensors have been simulated where they communicate with the hub using Beacon with superframe. The sensor nodes are assigned priorities within eight user priority designations as per the IEEE 802.15.6 standard. Each user priority is associated with the range of contention window (CW) whose minimum and maximum values are defined as shown in Table 2. Here, only the UP7 uses the EAP access phase; all other UPs send data using the RAP and CAP access phases [1–5]

This section describes an analytical model for improving the performance of the IEEE 802.15.6 standard's CSMA/CA mechanism. Three key components of the CSMA/CA process are the backoff stage, backoff counter, and contention window size. Nodes in MBAN set their backoff counter (BC) to a random value over the range [1, CW] in the conventional

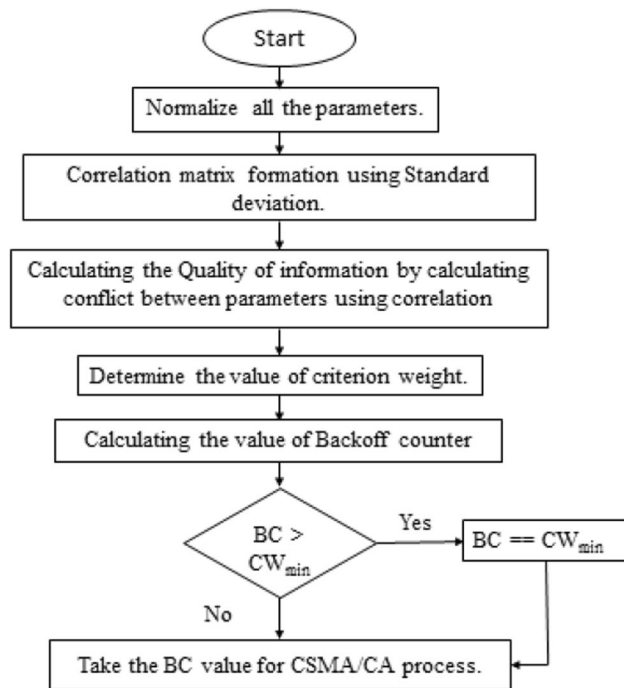


Fig. 3 Flowchart explaining the CRITIC computations for multiparameter decision

CSMA process. A node transmits a data packet when the backoff counter is zero. Applications that require a quick response time should not utilize the random BC value selection since high-value results in a long waiting time. If the value is lower, there is a higher chance of packet collision and packet drop on a network with high traffic.

To overcome this issue, parameters such as packet size and data rate are considered while determining the BC value. Each sensor node has a small memory or buffer to save the packets before they are transmitted. Despite this, when nodes starve for transmission slots over a long period, it causes buffer overflows and results in packet drops, which affects

the MBAN performance. Another circumstance that might lead to a collision is when two or more nodes that are ready to transmit data share the same user priority as defined by the standard. Figure 1 shows the process through which sensor nodes are assigned different priorities and backoff counter values are computed to avoid collision during data transmission. As shown in Fig. 1 the CRITIC method considers various sensor parameters as input and calculates weights to be assigned to these parameters so as to arrive at a decision for backoff counter value and priority.

3.1 CRITIC method

In this work, CRITIC method has been used to find efficient value for the backoff counter and determine their priority for data transmission. The main goal of this multiparameter decision-making algorithm is to enhance the reliability of MBAN [31, 32]. The sensor nodes in MBAN have diversity in terms of the importance of data (priority), packet size, data generation rate, etc. CRITIC associates weights to these parameters by computing the degree of contrast of each parameter as well as the correlation between the parameters.

At the beginning of the procedure, the hub initially gathers information about the sensor node's packet size, packet generation rate, and priority of data transmission. This information is used to create the sets of parameters that X_n that are used by CRITIC to determine the weights to be associated with these parameters. Here $n = 1, 2, 3, \dots$

$$X_n = \{X_1, X_2, X_3 \dots\} \quad (1)$$

Three parameters in this study are shown in Table 3 where it can be seen that user priority, packet size, packet generation rate, and data transmission rate, have been chosen as decision parameters. Some nodes have the same user priority, for example, two nodes in UP6 and two nodes in UP7. These priority conflicts in the network are resolved by

Table 4 Updated User Priorities calculated by CRITIC for new user priority

Sensor Node	User priority calculated by CRITIC	Previous Backoff counter value	CRITIC Backoff counter value	Retransmission attempts (r)
Physical activity	10 (LOWEST)	16	2	1
Temperature	9	16	2	2
Glucose	8	8	3	2
Respiration rate	7	8	2	4
Ear sensor	6	4	2	6
Oxygen saturation	5	4	2	8
Blood pressure	4	2	1	10
EMG	3	2	2	10
EEG	2	1	1	1
ECG	1 (HIGHEST)	1	1	1

reassigning the priorities using the CRITIC method. The method is extended to calculate back-off counter values.

Human bodies exhibit diverse characteristics and responses influenced by factors such as individual differences, environmental conditions, and dynamic physiological states. The values of parameters for each node shown in the above table were generated randomly so as to create a more realistic model for the human body. A decision matrix $M \times N$ is created using these sensor parameters as shown in Fig. 2, where indices M represents the sensor nodes and N represents the sensor parameter.

The methodology for the CRITIC has been shown as a flowchart in Fig. 3, where parameters are normalized in the first step.

The process of normalization involves converting the data into standard scales with a 0 to 1 range. The following mathematical equation is used for normalizing the parameter value.

$$a_{p,q} = \frac{a_{p,q}}{\sum_{p=1}^M a_{p,q}} \quad (2)$$

where p represents the sensor nodes, and q represents the parameter.

Next, calculate the standard deviation for each parameter. As an alternative, we may calculate the parameters'

Table 5 Probabilities definition for Markov model

Notation	Description
P_{idle}	Probability for start carrier sensing by nodes
P_{busy}	Probability of channel being busy after being sensed
P_L	Probability for insufficient time slot length
P_S	Probability of successfully packet deliver
P_f	Probability of collision
P_n	Probability of available slot

entropy and then determine how closely they are correlated. The correlation matrix is generated as a symmetric matrix with elements $X_{q,b} = \text{corr}(X_q, X_b)$ and $q, b = 1, \dots, n$. and shown as Eq. 3. This matrix is used for identifying the degree of conflict between the parameters using Eq. 4.

$$\begin{matrix} X_{11} & X_{12} & \dots & X_{1N} \\ X_{21} & X_{22} & \dots & X_{2N} \\ \vdots & \vdots & \dots & \vdots \\ X_{N1} & X_{N2} & \dots & X_{NN} \end{matrix} \quad (3)$$

$$\sum_{b=1}^N (1 - X_{q,b}) \quad (4)$$

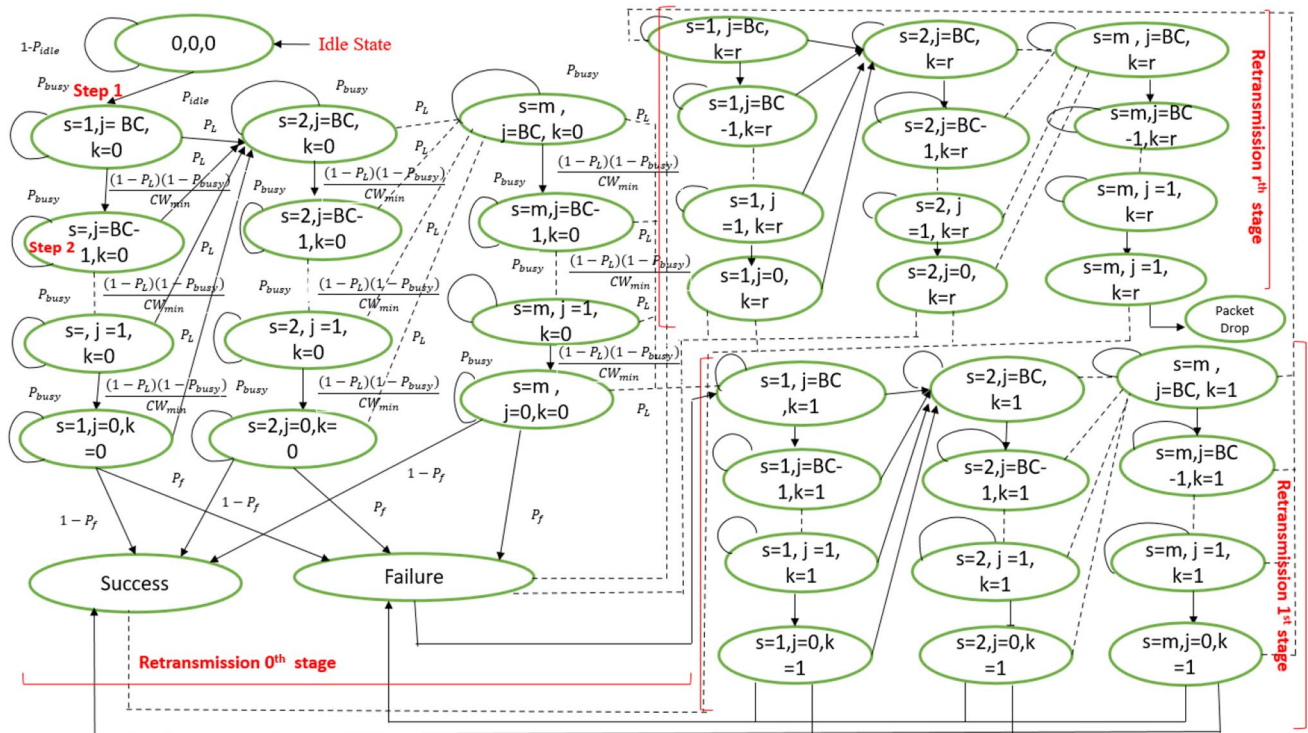


Fig. 4 Markov chain model for node showing the state transitions where backoff count, backoff and retransmission states for a node assigned any specific user priority between UP0 to UP7

where $q, b = 1, \dots, N$.

The quality of information is calculated using Eq. 5 where the standard deviation and degree of conflict are considered.

$$C_q = \sigma_q * \sum_{b=1}^N (1 - X_{q,b}) \quad (5)$$

Equation 6 is used for determining the weight of the parameters using the quality of information.

$$w_q = \frac{C_q}{\sum_{q=1}^N C_q} \quad (6)$$

As previously mentioned, in the situation of homogeneous data nodes, we utilize the CRITIC approach to give the priority to the nodes. Equations 2–6 were used for determining the decision matrix elements and the weights associated with each sensor parameter (X_1 to X_5). Sensor node priority was calculated by associating the decision matrix parameter with calculated weight of the parameter, using Eq. 7.

$$S_p = \sum_{q=1}^N a_{p,q} \times w_q \quad (7)$$

A normalization of the sensor device's priority value has been carried out using Eq. 8.

$$S_p = \frac{S_p - S_{\min}}{S_{\max} - S_{\min}} \quad (8)$$

Here, $S_{\max}$ and $S_{\min}$ represent the sensor nodes' highest and lowest priority values amongst the sensors. The updated priorities determined using this CRITIC method are used during channel access by the MBAN.

This calculated weight of parameters (X_1 to X_4) decided the backoff counter value BC of sensor node as shown in Eqs. 9 and 10:

$$\mu_p = \frac{\sum_{q=1}^N w_q \times a_{p,q}}{\sum_{q=1}^N w_q} \quad (9)$$

$$BC = \text{Ceil}(\mu_p \times CW_{\max}) \quad (10)$$

where μ_p is mean value of all the parameters and N is the number of parameters and w_q is the weight of q^{th} parameter. With the help of CRITIC, we can calculate the BC counter value depending upon the sensor node parameters instead of random value from the range of 1 to $CW_{\min}$.

The sensor node priorities and backoff counter values calculated using CRITIC are shown in Table 4. The rightmost column has been added to show the maximum retransmissions for reduced probability of packet drop and improved

reliability for the node and is uncorrelated to other parameters of the sensor node.

As seen in Table 4, whenever two or more nodes have the same user priority, the CRITIC method helps us to identify which of these nodes should be given higher preference. The sensors are placed in ascending order of priority after CRITIC priority redesignation. Table 4 shows that backoff count values have become smaller with CRITIC and although few nodes have same backoff counter values, their new priorities as assigned by CRITIC are distinct, so the nodes do not content for channel at same time.

Having the sensor node priorities and backoff counter values computed using the CRITIC, a stochastic model has been proposed where the reliability of data transmission and probability of packet drop due to maximum retransmission limit of the nodes are studied for variable traffic and has been discussed in the next section.

4 Markov chain model

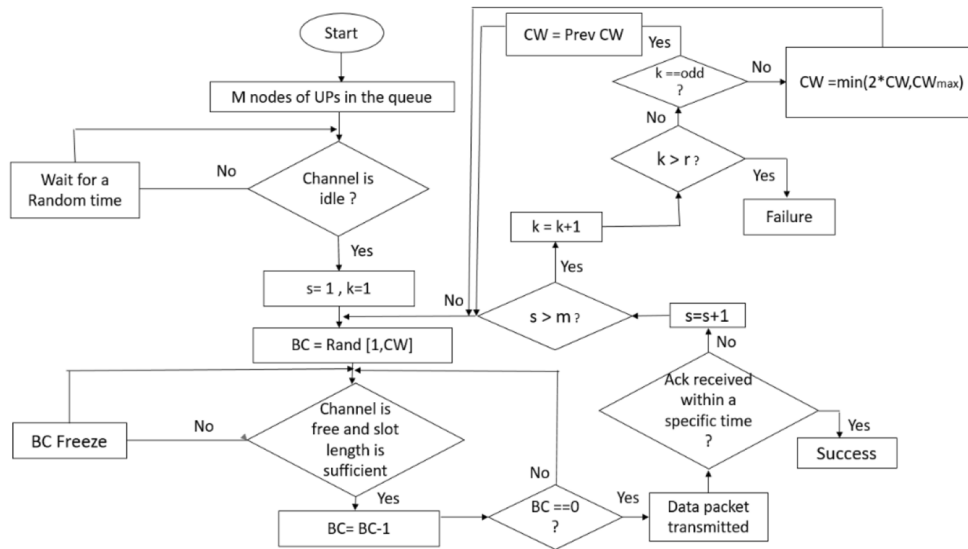
To compute the performance of MBAN, we have used the Markov chain model in this section. The backoff stage, backoff counter, and retransmission counter are the three parameters we use in the Markov chain model. The formula computes the value of the backoff stage as shown in Eq. 11.

$$CW_{\max} = 2^m \times CW_{\min}, \quad (11)$$

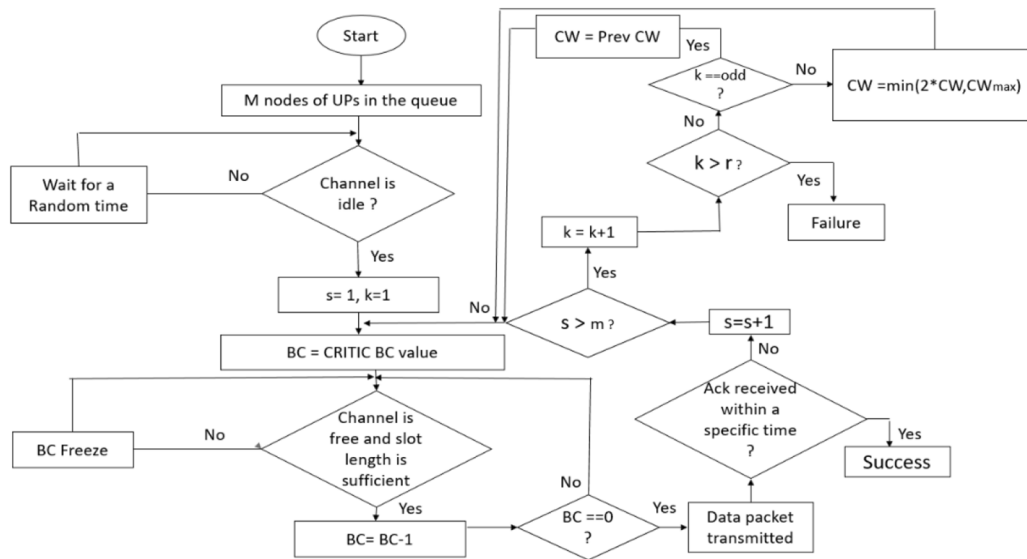
where m is the number of backoff stages

The backoff stages computed using this equation for different user priorities as shown in Table 2 and are used as indexes in the Markov chain model.

The Markov model for a user node is shown in Fig. 4, where the sensor node is initially in a state where the indexes s, j, k for backoff counter, backoff stage, and retransmission counter are initialized as 0, 0, 0. The probabilities associated with the states and transitions are shown in Table 5. In step 1: The sensor node starts carrier sensing the channel for availability in a random time slot and with probability P_{idle} . In step 2: the probability of the channel being free is $1 - P_{\text{busy}}$, so the node initializes its backoff counter after it is able to access the channel. The node now checks for sufficient duration time slot where it can send its data. The probability of the availability of sufficient duration time slot availability is $1 - P_L$, where P_L is the probability of time slots being of insufficient duration. As next steps the node initializes its backoff counter j which begins to decrease at every time slot until it reaches zero when the node attempts to transmit the data and depending on whether the packet meets collision or not, the node reaches Success or Failure states. This is shown as block marked Retransmission 0th stage marked in the Fig. 4.



(a) Flow chart showing the channel access and data transmission for M nodes where user priorities are assigned as per the IEEE 802.15.6 standard and the back count value is chosen randomly within the contention window.



(b) Flow chart showing the channel access and data transmission for M nodes where the user priority as well as the backoff count values are computed using CRITIC method using two separate decision matrices.

Fig. 5 **a** Flow chart showing the channel access and data transmission for M nodes where user priorities are assigned as per the IEEE 802.15.6 standard and the back count value is chosen randomly within the contention window. **b** Flow chart showing the channel

access and data transmission for M nodes where the user priority as well as the backoff count values are computed using CRITIC method using two separate decision matrices

There also exist possibility that the node may not find time slot of sufficient duration with probability P_L , even if it is able to find the channel free, and in this case the back off counter is frozen and the node moves to the next backoff stage by incrementing the index s , where it again senses the channel for availability and starts decrementing backoff counter when it finds slot of suitable duration. The process is repeated and, until successful transmission is achieved or if all back-off

stages and retransmission attempts are completed for the node and after that packet has been dropped out. The retransmission process starts when the node is unable to transmit data successfully even after all backoff stages for that attempt have expired and these are shown by blocks marked Retransmission 1st stage /Retransmission r^{th} stage.

The Markov chain model of Fig. 4 has been explained in pseudo code shown below and has been used for further calculations.

Pseudo code of Markov chain model.

Input: Node with User Priority, Backoff counter value, Backoff stage value, Retransmission no.

Output: Failure and Success

Idle State: All nodes are waiting in the queue and one node get the slot for the transmission:

Step 1: Markov Chain state for the selected node.

State = {Value of all counters are assigned : Backoff counter = BC value , Backoff stage = 1, and Retransmission counter = 0}

Step 2: Check if the channel is free

if channel_is_free & sufficient_time_slot_is_available ():
decrement the Backoff counter by 1

else:

Backoff counter frozen

Check if Backoff counter is zero

Transmit data

if transmission_successful ():

Reset all the counters and update the success state

else if:

Increment the Backoff stage =< Max Backoff stage value

Reset the Backoff counter and run the whole process again

else

Increment the Retransmission counter =< Max Retransmission counter value

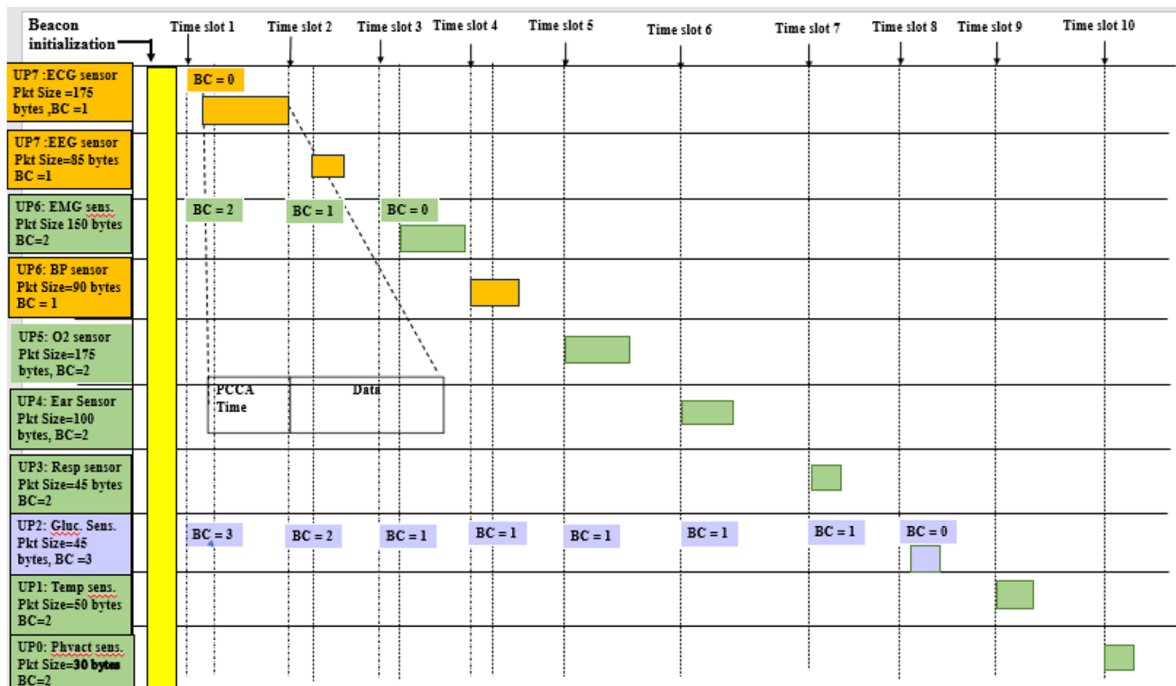
Reset Backoff counter, Backoff stage and run the whole process again

Check the limit of Retransmission is exceeded

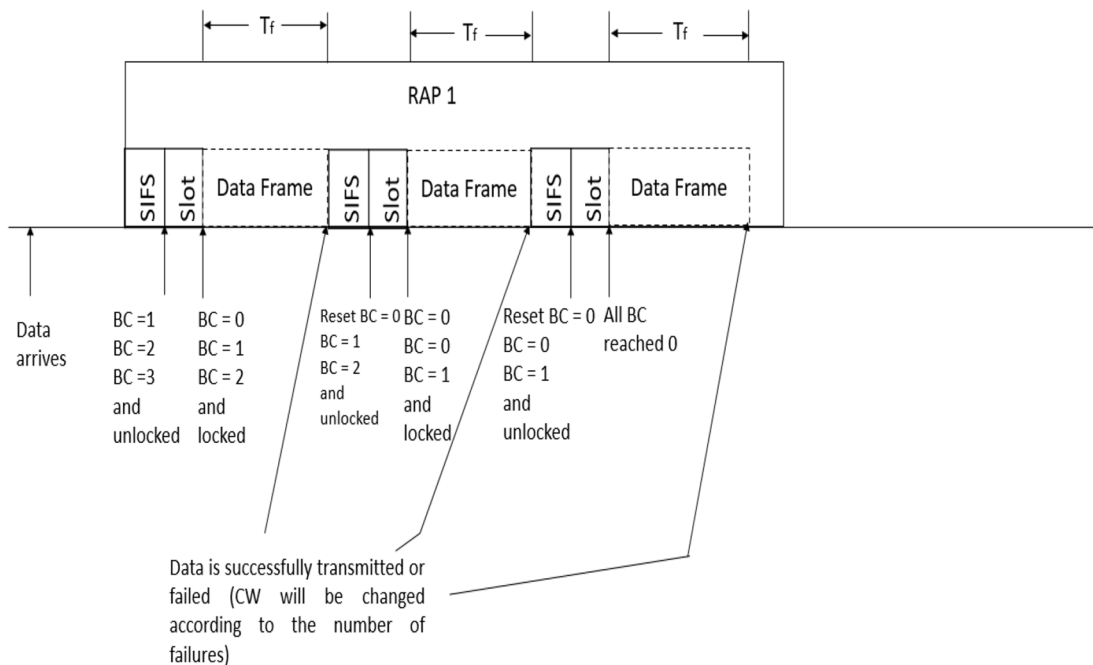
Retransmission counter value == Max Retransmission counter value + 1

Stop the process and update the failure state

Return to the Idle State



(a) Slot distribution where many sensors have same backoff counter value but different priorities.



(b) channel access mechanism in a superframe, where SIFS is the short interframe space after which node decrement the backoff counter and finally transmits packet in the Data Frame time (T_p).

Fig. 6 **a** Slot distribution where many sensors have same backoff counter value but different priorities. **b** channel access mechanism in a superframe, where SIFS is the short interframe space after which

node decrement the backoff counter and finally transmits packet in the Data Frame time (T_p)

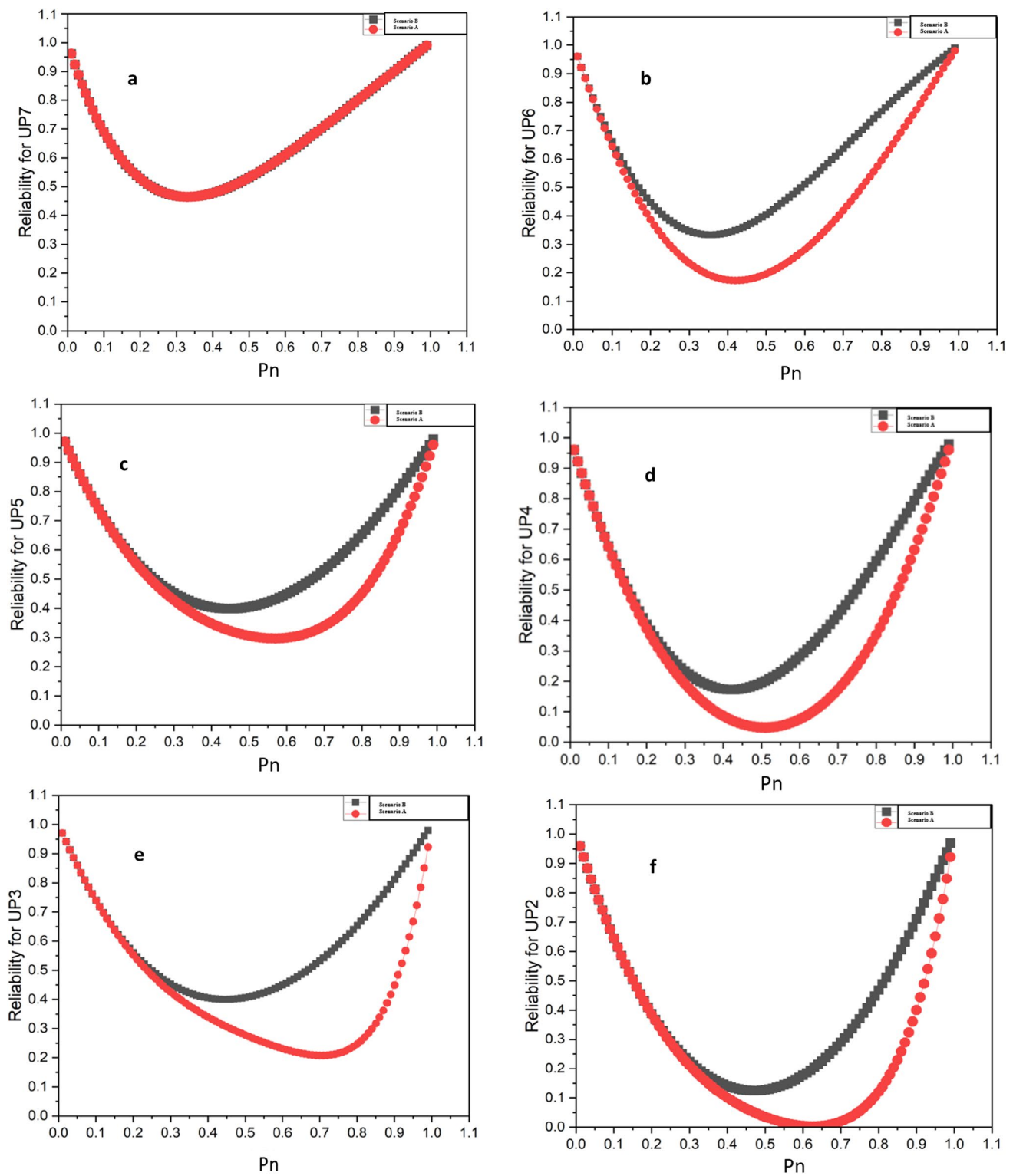


Fig. 7 Reliability comparison graphs for all user priorities, the reliability is improved for scenario B as compared to scenario A for all user priorities (b to h) and remains unchanged in case of highest priority node (a)

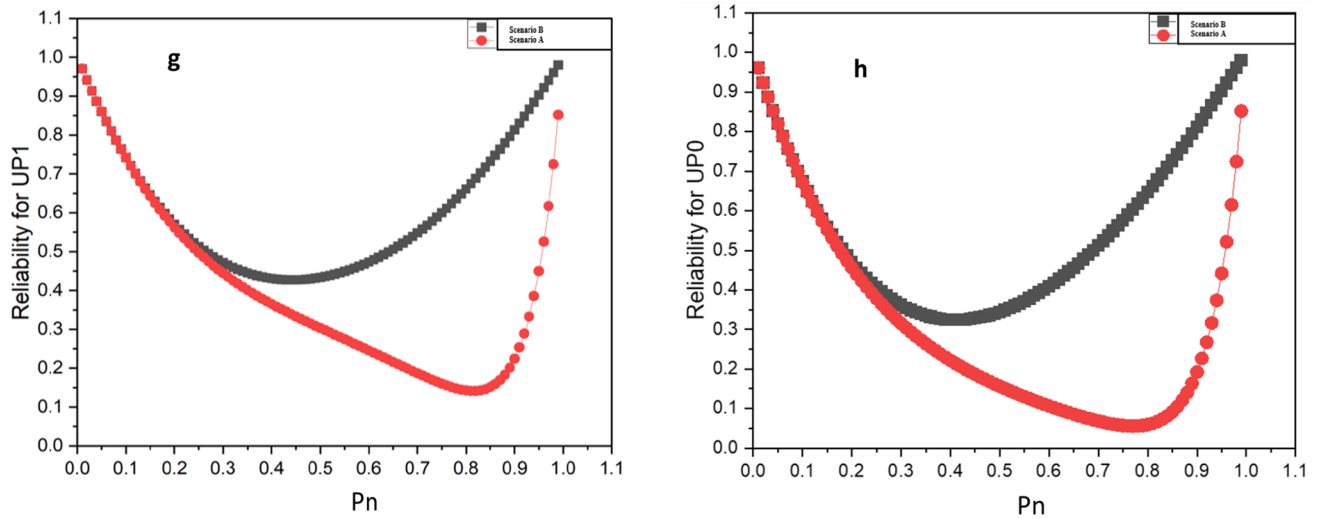
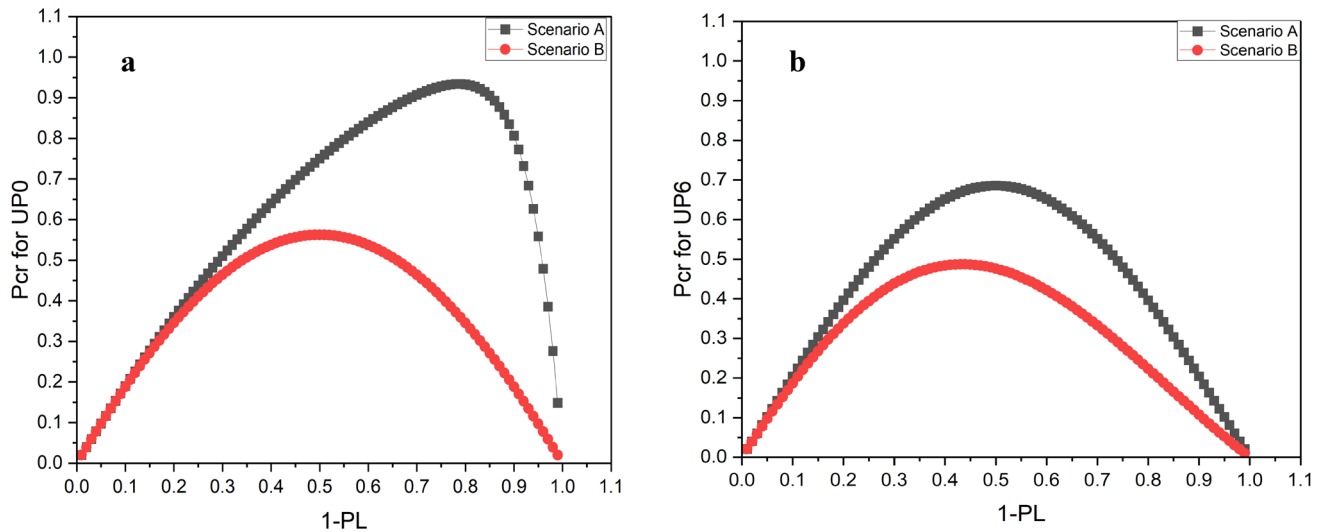


Fig. 7 (continued)

Fig. 8 a and b) Graph of probability of packet drop due to the maximum retransmission limit (P_{cr}) for UP0 and UP6

Performance equations for calculating the reliability of user priorities are derived using Markov chain model [33, 34].

The stationary states of the Markov chain are represented by Eq. 12.

$$S_{s,j,k} = \lim_{t \rightarrow \infty} (a(t) = s, b(t) = j, c(t) = k) \quad (12)$$

where backoff stage $s \in [1, m]$, backoff counter $j \in [1, BC]$ and retransmission counter $k \in [1, r]$.

From Fig. 4, the following transition probabilities between the various stationary states of the Markov chain are written in generalized Eqs. 13–23 form for all user priorities.

$$P(0, 0, 0|0, 0, 0) = 1 - P_{idle} \quad (13)$$

$$P(m, BC, 0|0, 0, 0) = P_{idle} \quad (14)$$

$$P(m, BC, 0|m, BC, 0) = P_{busy} \quad (15)$$

$$P(m, BC - 1, 0|m, j, 0) = (1 - P_{busy})/CW_{min} \text{ for } j \in [1, BC] \quad (16)$$

$$P(s + 1, j, k|s, j, k) = P_L \text{ for } s \in [1, m], k \in [1, r] \quad (17)$$

$$P(s, BC - 1, k|s, j, k) = 1 - P_L \text{ for } j \in [1, BC], s \in [1, m] \quad (18)$$

$$P(\text{Success}|s, 0, k) = 1 - P_f \quad (19)$$

$$P(\text{Failure}|s, 0, k) = P_f \quad \text{for } k \in [1, r-1] \quad (20)$$

$$P(\text{PacketDrop}|s, 0, r) = P_f \quad (21)$$

$$P(\text{PacketDrop}|s, j, k) = P_L \quad \text{for } k \in [1, r] \quad (22)$$

$$P(0, 0, 0|\text{PacketDrop}) = 1 \quad (23)$$

Equations 24–27 show how performance equations have been computed using these stationary equations.

$$P_t = \sum_{k=1}^r \sum_{s=1}^m \sum_{j=1}^{BC} \left(\frac{(1 - P_{\text{busy}})}{CW_{\min}} P_L^{s-1} (1 - P_L)^j \right)^k \quad (24)$$

The transmission probability P_t may be used to indicate the probability of failure packet transfer P_f .

$$P_f = 1 - P_t^{M-1} \quad (25)$$

Using the probabilities of failed packet transmission, probabilities of channel access failure P_{cf} , and probability of packet drop due to maximum retransmission limit P_{cr} .

$$P_{cf} = \sum_{k=1}^r \sum_{s=1}^m \sum_{j=1}^{BC} \left(P_L^{s-1} (1 - P_L)^j P_f \right)^k P_L^m (1 - P_L)^{j-1} \quad (26)$$

$$P_{cr} = \sum_{k=1}^r \sum_{s=1}^m \sum_{j=1}^{BC} \left(P_L^{s-1} (1 - P_L)^j P_f \right)^k \quad (27)$$

Equations 26 and 27 are used to compute reliability (R) in Eq. 28.

$$R = 1 - P_{cf} - P_{cr} \quad (28)$$

The above Markov model has been run for two scenarios as follows:

Scenario A: User Priorities and random backoff value, process shown in Flow chart 1, Fig. 5a.

Scenario B: User Priorities and back off count value determined using CRITIC, process shown in Flow Chart 2, Fig. 5b.

A comparison of these flowchart shows that the process of channel access is similar in both the scenarios, however, the backoff count values for a specific user priority are different and therefore this contributes to different performance of the network. Also, user priorities are reassigned by CRITIC method in Scenario B and problem of more than one node being assigned same user priority is resolved for homogeneous traffic. The performance results have been compared and discussed in the next section.

5 Results and discussions

5.1 Channel access by nodes with new user priority and backoff counter values

The CRITIC method reassigns user priorities and calculates backoff counter values based upon the node parameters. This information about the nodes is sent to the central hub during connection establishment [35]. The nodes access the superframe, where it starts with beacon initialization. If the channel is free after the beacon initialization, all nodes should decrease the backoff counter; once the counter reaches zero, the data will be sent after the clear channel assessment time. As shown in Fig. 6a and b when two or more nodes of same user priority want to transmit in the same superframe and the backoff counter value have simultaneously reached zero, the node with the higher UP according to the CRITIC method initiates transmission.

This can be seen for UP7 and UP6, where the back-off counters of ECG, EEG and Blood Pressure (BP) sensor node are set to 1. These three nodes have their backoff counter decrement to zero after one time slot and all other nodes back off counters are locked. As per CRITIC priority, the ECG sensor transmits the packets first and after it successfully completes data transmission, all nodes unlock their backoff counter and start decrementing it with every time slot. The EEG sensor and Blood Pressure have already reached zero state of Backoff counter, however since user priority of EEG sensor is high, it will start data transmission. At this stage the EMG sensor also decreases its back-off count value and both EMG and BP sensors are ready to transmit their data. Again, since the EMG sensor has higher priority as compared to BP sensor, it transmits its packets and then the whole process is repeated. This procedure of backoff counter decrement, locking and unlocking, and data transmission after the counter reaches zero is shown in Fig. 6a and b.

In Fig. 6b the timing diagram shows where the data transmission is defined in the Random-Access Phase (RAP), with SIFS as short interframe space and T_f as the data-frame time. After SIFS time, the node begins decrementing its backoff counter for transmission, and the entire process is completed as discussed in Sect. 3.2 Markov Chain model.

5.2 Reliability of data transmission

Reference is made to Table 3 where we find that for UP7 there are two nodes, with different packet sizes, EEG sensor of 85 bytes and ECG sensor 175 bytes and data generation rates of 35 and 40 packet per sec. respectively. When CRITIC is applied to choose the backoff counter, we get the same backoff counter value for both these nodes, however,

their user priority changes as shown in Table 4 where ECG sensor with high packet size of 175 bytes gets higher priority than EEG sensor of lower packet size of 85 bytes and their priorities become 1 and 2 amongst the 10 node priorities. Reliability of nodes is compared in the three cases, namely CRITIC with modified user priority 2 and 1 (Highest) and conventional user priority 7, we get same reliability behavior. This can be explained by the justification that reliability depends on both the backoff count value and the probability of available slots. The reliability reduces initially even when the probability of available slots is increasing, because the back off count value is non-zero and the node is unable to start the transmission. However, as the number of slots increases beyond 0.33 for ECG and EEG sensors for both scenarios A and B, the reliability starts increasing because the backoff count value has become zero and the node is able to find slots. It can be seen from Fig. 7a, the reliability for the highest user priority nodes starts increasing once the probability of available slots is 0.33 or more.

In scenario A, for user priorities UP0 to UP6, the reliability decreases as the probability of available slots increases from 0 to some fixed value (between 0.4 and 0.8). As seen in Table 4, the backoff counter values for lower user priorities is high in conventional method. As an example, UP0 in conventional method has backoff counter value of 16. Such large backoff counter value causes the nodes to wait for longer durations of time before sensing the channel and therefore many available slots are not utilized for data transmission. For Scenario B it is observed that this window of minimum reliability becomes less wide so that this window becomes 0.4 to 0.5. Table 4 shows that the backoff counter values have reduced significantly and nodes start transmission at lower probability of available slots as seen in all the graphs. As seen in Fig. 7 the reliability for scenario is higher as compared to scenario A, for any fixed probability of available slots. This has been analyzed in terms of probability of packet drop in the next subsection.

5.3 Probability of packet drop

The probability of packet drop due to maximum retransmission limit (P_{cr}) has been analyzed and shown in Fig. 8 for UP0 and UP6. This probability depends on the probability of collision as well as on the probability of available slots and retransmission attempts. As can be seen in Fig. 8a, the P_{cr} is high for scenario A, even for high probability of available slots, the highest value being 0.93. In the case of scenario B for UP0, P_{cr} peak value reduces to 0.49 as the backoff counter value has been optimized, leading to reduced waiting time. This improvement in P_{cr} dropping for scenario B

is also observed for other user priorities as shown for UP6 in Fig. 8b, where we see that the CRITIC method helps to reduce the P_{cr} values over the entire range of probabilities of slot.

6 Conclusion

A variety of methods for optimizing back-off counter values have been developed in various works. In the Binary Exponential Backoff (BEB) algorithm for IEEE 802.15.6, backoff counter values are chosen within a contention window range such that the nodes with lower user priority have higher waiting times as compared to higher priority nodes. With every even number collision, the backoff counter value increases exponentially, thereby reducing the chances of the next collision, however increasing the node's waiting time [27, 29]. This is overcome in Prioritized Fibonacci Backoff [PFB] algorithm, where the backoff counter values increase using a Fibonacci series weights for even numbered collisions, this resulting in lesser waiting times for nodes as compared to BEB [27, 30, 31]. The IEEE 802.15.6 standard does not anticipate having node density as high as other IEEE standards; hence, overlapped contention windows in the PFB algorithm lead to collisions that underutilize the super frame. This problem is overcome in Nonoverlapping Backoff algorithm [NOBA] where the contention window incorporates a sliding window, so that there is no overlap in contention windows for various user priorities [19, 27]. However elevated lower boundaries of contention windows lead to extended listening times for lower user priorities. The above algorithms recommend ways to minimize collisions and listening times of nodes by modifying the backoff counter values using optimized contention windows and have been summarized in Table 1.

However, these algorithms do not take into consideration the sensor node parameters while making channel access decisions. Our study addresses the challenges posed by existing algorithms through the introduction of the Criteria Importance through Intercriteria Correlation (CRITIC) algorithm. In CRITIC, the calculation of the backoff counter value is based on the node's specific parameters, including user priority, packet size, packet generation rate, and data transmission rate. Unlike algorithms relying on random selection from contention window ranges, CRITIC leverages node-specific information, considering the quality of information and the degree of conflicts among parameters. CRITIC assigns a unique backoff counter value to each user priority, ensuring a tailored approach based on the specific characteristics of each node. Even when nodes share the

same user priority due to traffic designation, CRITIC mitigates conflicts arising from identical backoff counter values by introducing new local user priorities. The CRITIC algorithm thus offers a more intelligent and customized solution, considering various node parameters to optimize contention and enhance overall system performance.

Using CRITIC our simulation results show improved reliability at lower probabilities of available slots. It may be concluded through the analysis, that instead of random value selection within the contention window, a fixed value obtained by CRITIC provides better results in terms of reliability and probability of packet drop. The packet drop probability reduces from 0.93 to 0.49, which is a significant improvement. While calculating reliability we have assumed that performance is measured for nodes that are able to get available slots for data transmission. We plan on further investigating the dynamic slot time allocation in our future work, paying particular attention to the properties of the node in our sensor network framework. We will also be assessing the latency or waiting time for data transfer from the sensor nodes to the hub.

Acknowledgements The authors acknowledge using ChatGPT for the Introduction section of this paper. We also acknowledge the JK Lakshmipat University for support on the MATLAB license and other resources related to this work.

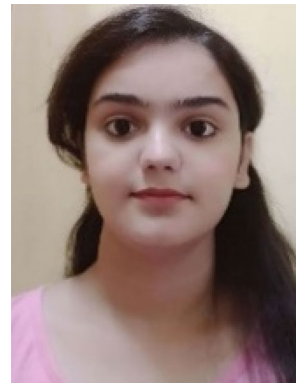
References

- Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., & Jamalipour, A. (2014). Wireless body area networks: A survey. *IEEE Communications surveys & Tutorials*, 16(3), 1658–1686. <https://doi.org/10.1109/SURV.2013.121313.00064>
- Bradai, N., Belhaj, S., Chaari, L., & Kamoun, L. (2011). Study of medium access mechanisms under IEEE 802.15.6 standard. In *2011 4th joint IFIP wireless and mobile networking conference (WMNC 2011)*, Toulouse, France, pp. 1–6. <https://doi.org/10.1109/WMNC.2011.6097231>
- Ullah, S., Mohaisen, M., & Alnuem, M. A. (2013). A review of IEEE 802.15.6 MAC, PHY, and security specifications. *International Journal of Distributed Sensor Networks*, 9(4), 950704. <https://doi.org/10.1155/2013/950704>
- Fourati, H., Idoudi, H., & Saidane, L. A. (2016) A novel IEEE 802.15.6 CSMA/CA service differentiation. In *2016 IEEE/ACS 13th international conference of computer systems and applications (AICCSA)* (pp. 1–7). IEEE, 2016. <https://doi.org/10.1109/AICCSA.2016.7945686>
- Dadhich, K., & Kataria, D. (2023) Wearable IoT using MBANs. In *Applied intelligence in human–computer interaction* (pp. 113–127). CRC Press.
- Liu, Q., Mkongwa, K. G., & Zhang, C. (2021). Performance issues in wireless body area networks for the healthcare application: A survey and future prospects. In *SN Applied Sciences*, 3(2), 2021.
- Kwak, K. S., Ullah, S., & Ullah, N. (2010). An overview of IEEE 802.15.6 standard. In *2010 3rd international symposium on applied sciences in biomedical and communication technologies (ISABEL 2010)* (pp. 1–6). IEEE.
- Kaitalidou, D. S., Boulogeorgos, A. A. A., & Pavlidou, F. N. (2016). Comparison of CSMA/CA protocols applied in wireless body area network standards. In *2016 18th mediterranean electrotechnical conference (MELECON)* (pp. 1–6). IEEE.
- Kurunathan, J. H. (2015). Study and overview on WBAN under IEEE 802.15.6. *U. Porto Journal of Engineering*, 1(1), 11–21.
- Kaur, T., & Kumar, D. (2019). QoS mechanisms for MAC protocols in wireless sensor networks: a survey. *IET Communications*, 13(14), 2045–2062. <https://doi.org/10.1049/iet-com.2018.5110>
- Kim, B. S., Shah, B., He, T., & Kim, K. I. (2022). A survey on analytical models for dynamic resource management in wireless body area networks. *Ad Hoc Networks*, 135, 102936. <https://doi.org/10.1016/j.adhoc.2022.102936>
- Huang, W., & Quek, T. Q. S. (2015). Adaptive CSMA/CA MAC protocol to reduce inter-WBAN interference for wireless body area networks. In *Proceedings of the IEEE International Conference on Wearable & Implantable BSN*. Cambridge, MA, pp. 1–6.
- Diakoulaki, D., Mavrotas, G., & Papayannakis, L. (1994). Determining objective weights in multiple criteria problems: The critic method. *Computers & Operations Research*, 22(7), 763–770.
- Zizovic, M., Miljkovic, B., & Marinkovic, D. (2020). Objective methods for determining criteria weight coefficients: A modification of the CRITIC method. *Decision Making: Applications in Management and Engineering*, 3(2), 149–161. <https://doi.org/10.31181/dmame.2003149z>
- Odu, G. O. (2019). Weighting methods for multi-criteria decision making technique. *Journal of Applied Sciences and Environmental Management*, 23(8), 1449–1457. <https://doi.org/10.4314/jasem.v23i8.7>
- Akpahou, R., & Odoi-Yorke, F. (2023). A multicriteria decision-making approach for prioritizing renewable energy resources for sustainable electricity generation in Benin. *Cogent Engineering*, 10(1), 2204553. <https://doi.org/10.1080/23311916.2023.2204553>
- Rashwand, S., & Mišić, J. (2012). Effects of access phases lengths on performance of IEEE 802.15.6 CSMA/CA. *Computer Networks*, 56(12), 2832–2846. <https://doi.org/10.1016/j.comnet.2012.04.023>
- Sarkar, S., Misra, S., Bandyopadhyay, B., Chakraborty, C., & Obaidat, M. S. (2015). Performance analysis of IEEE 802.15.6 MAC protocol under non-ideal channel conditions and saturated traffic regime. *IEEE Transactions on computers*, 64(10), 2912–2925. <https://doi.org/10.1109/TC.2015.2389806>
- Touijer, B., Maissa, Y. B., & Mouline, S. (2021). IEEE 802.15.6 CSMA/CA access method for WBANs: “Performance evaluation and new backoff counter selection procedure. *Computer Networks*, 188, 107759. <https://doi.org/10.1016/j.comnet.2020.107759>
- Benmansour, T., Ahmed, T., Moussaoui, S., & Doukha, Z. (2020). Performance analyses of the IEEE 802.15.6 wireless body area network with heterogeneous traffic. *Journal of Network and Computer Applications*, 163, 02651. <https://doi.org/10.1016/j.jnca.2020.102651>
- Fourati, H., Idoudi, H., & Saidane, L. A. (2018). Intelligent slots allocation for dynamic differentiation in IEEE 802.15.6 CSMA/CA. *Ad Hoc Networks*, 72, 27–43. <https://doi.org/10.1016/j.adhoc.2018.01.007>
- Samal, T., & Kabat, M. R. (2021). A prioritized traffic scheduling with load balancing in wireless body area networks. *Journal of King Saud University-Computer and Information Sciences*, 34(8), 5448–5455. <https://doi.org/10.1016/j.jksuci.2020.12.023>
- Zia, Y., Bashir, F., & Qureshi, K. N. (2020). Dynamic super-frame adaptation using group-based media access control for handling traffic heterogeneity in wireless body area networks. *International Journal of Distributed Sensor Networks*, 16(8), 155014772094914. <https://doi.org/10.1177/1550147720949140>

24. Chen, D.-R., & Chiu, W.-M. (2018). Collaborative link-aware protocols for energy-efficient and QoS wireless body area networks using integrated sensors. *IEEE Internet of Things Journal*, 5(1), 132–149. <https://doi.org/10.1109/JIOT.2017.2775048>
25. Liang, B., Liu, X., Zhou, H., Leung, V. C. M., Liu, A., & Chi, K. (2021). Channel resource scheduling for stringent demand of emergency data transmission in WBANs. *IEEE Transactions on Wireless Communications*, 20(4), 2341–2352. <https://doi.org/10.1109/TWC.2020.3041471>
26. He, M., Hu, F., Ling, Z., Mao, Z., & Huang, Z. (2021). A dynamic weights algorithm on information and energy transmission protocol based on WBAN. *IEEE Transactions on Vehicular Technology*, 70(2), 1528–1537. <https://doi.org/10.1109/TVT.2021.3053964>
27. Saboor, A., Ahmad, R., Ahmed, W., Kiani, A. K., Alam, M. M., Kuusik, A., & Moullec, Y. L. (2020). Dynamic slot allocation using non overlapping backoff algorithm in IEEE 802.15.6 WBAN. *IEEE Sensors Journal*, 20(18), 10862–10875. <https://doi.org/10.1109/JSEN.2020.2993795>
28. Enkoji, A., Li, M., Brisky, J. D., & Melvin, R. (2019). Dynamic EAP based MAC protocol for wireless body area networks. In *2019 international conference on computing, networking and communications (ICNC)* (pp. 531–536). Honolulu, HI, USA. <https://doi.org/10.1109/ICCNC.2019.8685495>
29. Khan, P., Ullah, N., Ali, F., Ullah, S., Hong, Y.-S., Lee, K.-Y., & Kim, H. (2017). Performance analysis of different backoff algorithms for WBAN-based emerging sensor networks. *Sensors*, 17(3), 492. <https://doi.org/10.3390/s17030492>
30. Saboor, A., Ahmad, R., Ahmed, W., & Alam, M. M. (2019). A unique backoff algorithm in IEEE 802.15.6 WBAN. In *2018 IEEE 88th vehicular technology conference (VTC-Fall)*, IEEE, (pp. 1–5). <https://doi.org/10.1109/VTCTFall.2018.8690812>
31. Das, K., & Moulik, S. (2021). PBCR: Parameter-based backoff counter regulation in IEEE 802.15.6 CSMA/CA. In *2021 international conference on communication systems & Networks (COM-SNETS)*, IEEE, (pp. 565–571). <https://doi.org/10.1109/COMSNETS51098.2021.9352747>
32. Das, K., Moulik, S., & Chang, C. Y. (2021). Priority-based dedicated slot allocation with dynamic superframe structure in IEEE 802.15.6-based Wireless Body Area Networks. *IEEE Internet of Things Journal*, 9(6), 4497–4506. <https://doi.org/10.1109/JIOT.2021.3104800>
33. Mukherjee, A., Bandyopadhyay, B., Das, D., Chatterjee, A., Ahmed, Sk. J., & Naskar, M. (2014). Markov chain based analysis of IEEE 802.15.6 MAC protocol in real life scenario. In *Proceedings of the 9th international conference on body area networks, London, Great Britain*. <https://doi.org/10.4108/icst.bodynets.2014.257202>
34. Dadhich, K., & Kataria, D. (2022). Effect of channel slot time on performance of IEEE 802.15.6-based medical body area network. In *Advanced network technologies and intelligent computing. ANTIC 2022. Communications in computer and information science*, Vol. 1797. Springer, Cham. https://doi.org/10.1007/978-3-031-28180-8_25
35. Kim, B.-S., Shah, B., & Kim, K.-I. (2022). Resource allocation in wireless body area networks: a smart city perspective. In *Emerging Trends in Wireless Sensor Networks*. IntechOpen. <https://doi.org/10.5772/intechopen.102325>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.



Khushboo Dadhich received her B.Tech degree in Electronics and Communication Engineering from Rajasthan Technical University in India. She is pursuing her PhD at JK Lakshmipat University, and her area of interest includes medical body area networks and wireless sensor networks. She has work experience as a network engineer at a networking company and has held academic positions as a lecturer of electronics and communication engineering in earlier years.



Devika Kataria is a Professor at JK Lakshmipat University and has over two decades of experience including 10 years in academics and the rest as an engineering professional. She teaches courses in IoT, Internet of Medical Things, Industrial IoT, Cyber Security, and Digital Systems Design. Her research involves Cyber Physical Systems and Flexible Sensors. She also mentors' teams for Circular Economy Innovation Challenges.

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH (“Springer Nature”).

Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users (“Users”), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use (“Terms”). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.

These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.

We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.

While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval, sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.

These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.

To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.

Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.

If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com