IQRA NATIONAL UNIVERSITY, PESHAWAR, PAKISTAN

NETWORKS MANAGEMENT

Program: MSCS/PhDCS	**FINAL-TERM EXAM**	**Semester: Spring 2020**
Maximum Marks: 50		**Time Allowed: 6 Hours**

Note : ***Write down the complete statements of Q1 otherwise just answers will lead to zero marks.***

The paper should be submitted in pdf form and plagiarism will be checked; ***2 students with the same plagiarism report and answers will lead to zero marks to both.***

Cc: ***to Vice Chancellor***

Controller of Examination

Head of Department

Q1. Select the correct answer of the given ones. (10)

1) Interactive transmission of data independent of a time sharing system may be best suited to
   (a) simplex lines (b) half-duplex lines (c) full-duplex lines (d) biflex lines

Answer: - (b) Half- Duplex Line

2) The loss in the signal power as of an Electromagnetic signal is called
   (a) attenuation (b) propagation (c) scattering (d) interruption

Answer: - (a) Attenuation

3) Early detection of packet losses improves ____________ acknowledgment performance.
   (a) odd (b) even (c) positive (d) negative

Answer: - (d) Negative

4) Additional signal introduced in the desired signal in producing hypes is called
   (a) fading (b) noise
   (c) scattering (d) dispersion

Answer: - (a) Fading

5) Token is a **logical Ring** that rotates around the ring.

6) Ring may have up to **800-bit-long frame** (802.5) or ____________ (IBM) nodes.

7) FDDI can support a maximum of **500** stations.

8) Error-correcting codes are **Not Advance** enough to handle all errors.

9) ACK is a small **control frame** confirming reception of an earlier frame

10) Electronics are **Slow** as compared to optics

Q2: Distinguish between error correction and error detection. Explain any two error detection techniques with mathematical examples other than given in slides, search from internet. (10)

Answer: -

1. Error correction

- ✓ Adding enough redundant bits to deduce what the correct bits are.
- ✓ Error Correction are too expensive and hard.

Error Correcting Codes

The codes which are used for both error detecting and error correction are called as "Error Correction Codes". The error correction techniques are of two types. They are,

- ✓ Single bit error correction
- ✓ Burst error correction.
- ✓

The process or method of correcting single bit errors is called "single bit error correction". The method of detecting and correcting burst errors in the data sequence is called "Burst error correction".

Hamming code or Hamming Distance Code is the best error correcting code we use in most of the communication network and digital systems.

Hamming Code

This error detecting and correcting code technique is developed by R.W.Hamming . This code not only identifies the error bit, in the whole data sequence and it also corrects it. This code uses a number of parity bits located at certain positions in the codeword. The number of parity bits depends upon the number of information bits. The hamming code uses the relation between redundancy bits and the data bits and this code can be applied to any number of data bits.

What is a Redundancy Bit?

Redundancy means "The difference between number of bits of the actual data sequence and the transmitted bits". These redundancy bits are used in communication system to detect and correct the errors, if any.

How the Hamming code actually corrects the errors?

In Hamming code, the redundancy bits are placed at certain calculated positions in order to eliminate errors. The distance between the two redundancy bits is called "Hamming distance".

To understand the working and the data error correction and detection mechanism of the hamming code, let's see to the following stages.

Number of parity bits

As we learned earlier, the number of parity bits to be added to a data string depends upon the number of information bits of the data string which is to be transmitted. Number of parity bits will be calculated by using the data bits. This relation is given below.

$$2^P >= n + P +1$$

Here, n represents the number of bits in the data string.

P represents number of parity bits.

For example, if we have 4 bit data string, i.e. n = 4, then the number of parity bits to be added can be found by using trial and error method. Let's take P = 2, then

$$2^P = 2^2 = 4 \text{ and } n + P + 1 = 4 + 2 + 1 = 7$$

This violates the actual expression.

So let's try P = 3, then

$$2^P = 2^3 = 8 \text{ and } n + P + 1 = 4 + 3 + 1 = 8$$

So we can say that 3 parity bits are required to transfer the 4 bit data with single bit error correction.

Example: -

Calculate the required number of parity bits.

Let P = 2, then

$2^P = 2^2 = 4$ and $n + P + 1 = 4 + 2 + 1 = 7$.

2 parity bits are not sufficient for 4 bit data.

So let's try P = 3, then

$2^P = 2^3 = 8$ and $n + P + 1 = 4 + 3 + 1 = 8$

Therefore 3 parity bits are sufficient for 4 bit data.

The total bits in the code word are 4 + 3 = 7

2. Error detection

- ✓ Error detection refers to a class of techniques for detecting garbled messages.
- ✓ Adding some Extra bits to detect Occurrence of error.
- ✓ Not enough to detect the position of errors.

Types of Error detection

1. Parity Checking.
2. Cyclic Redundancy Check (CRC).
3. Longitudinal Redundancy Check (LRC)
4. Check Sum

1. Parity Checking

Parity bit means nothing but an additional bit added to the data at the transmitter before transmitting the data. Before adding the parity bit, number of 1's or zeros is calculated in the data. Based on this calculation of data an extra bit is added to the actual information / data. The addition of parity bit to the data will result in the change of data string size.

This means if we have an 8-bit data, then after adding a parity bit to the data binary string it will become a 9-bit binary data string.

Parity check is also called as “Vertical Redundancy Check (VRC)”.

There is two types of parity bits in error detection, they are

- ✓ Even parity
- ✓ Odd parity

1. Even Parity

If the data has even number of 1’s, the parity bit is 0. Ex: data is 10000001 -> parity bit 0

Odd number of 1’s, the parity bit is 1. Ex: data is 10010001 -> parity bit 1.

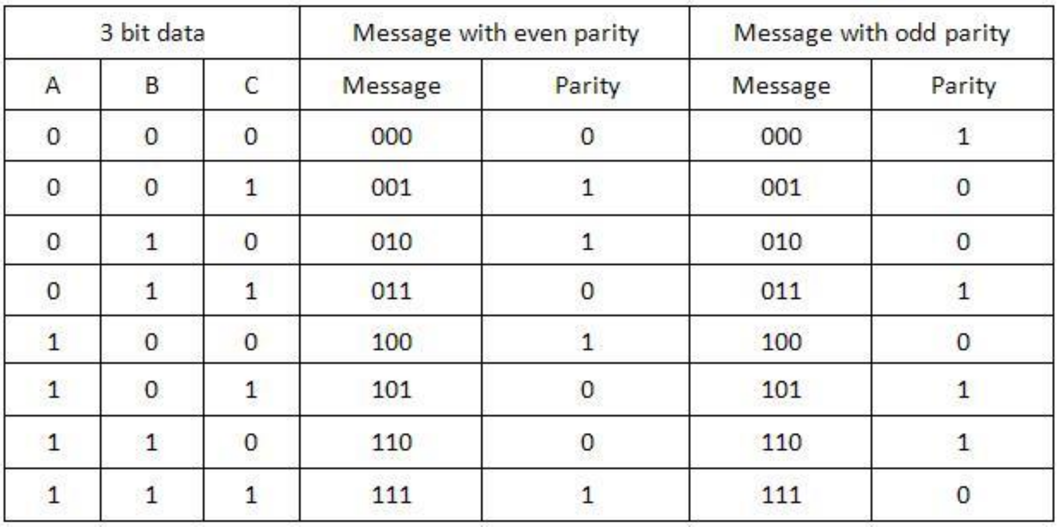
2. Odd Parity

If the data has odd number of 1’s, the parity bit is 0. Ex: data is 10011101 -> parity bit 0

Even number of 1’s, the parity bit is 1. Ex: data is 10010101 -> parity bit 1.

The circuit which adds a parity bit to the data at transmitter is called “Parity generator”. The parity bits are transmitted and they are checked at the receiver. If the parity bits sent at the transmitter and the parity bits received at receiver are not equal then an error is detected. The circuit which checks the parity at receiver is called “Parity checker”.

Messages with even parity and odd parity



3 bit data			Message with even parity		Message with odd parity	
A	B	C	Message	Parity	Message	Parity
0	0	0	000	0	000	1
0	0	1	001	1	001	0
0	1	0	010	1	010	0
0	1	1	011	0	011	1
1	0	0	100	1	100	0
1	0	1	101	0	101	1
1	1	0	110	0	110	1
1	1	1	111	1	111	0

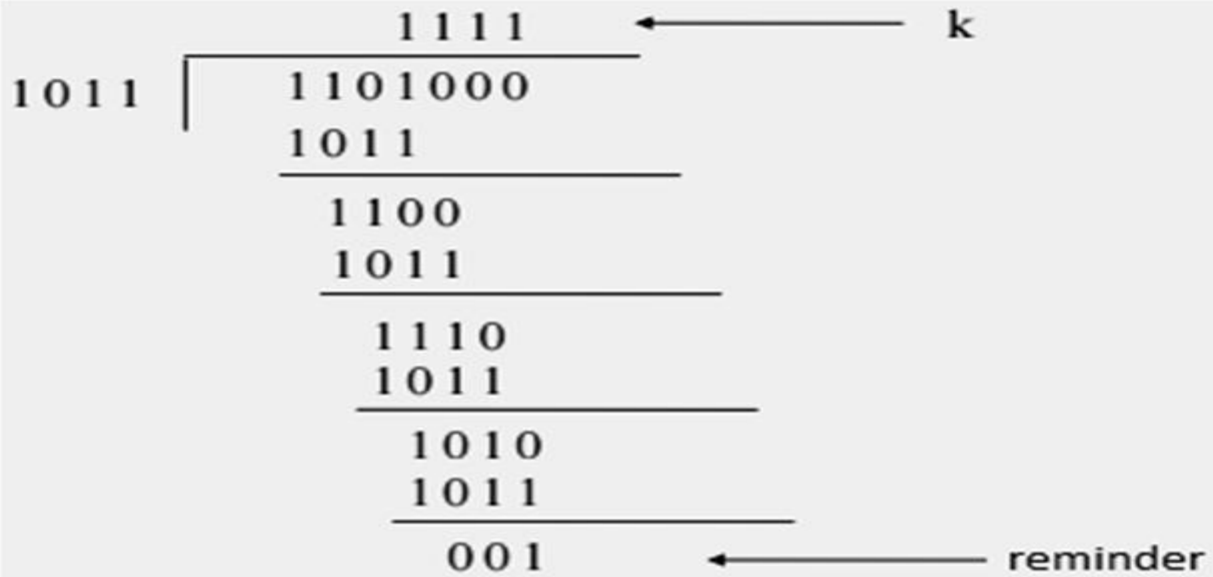
Cyclic Redundancy Check (CRC)

A cyclic code is a linear (n, k) block code with the property that every cyclic shift of a codeword results in another code word. Here k indicates the length of the message at transmitter (the number of information bits). n is the total length of the message after adding check bits. (actual data and the check bits). n, k is the number of check bits. The codes used for cyclic redundancy check there by error detection are known as CRC codes (Cyclic redundancy check codes).Cyclic redundancy-check codes are shortened cyclic codes. These types of codes are used for error detection and encoding. They are easily implemented using shift-registers with feedback connections. That is why they are widely used for error detection on digital communication. CRC codes will provide effective and high level of protection.

CRC Code Generation

Based on the desired number of bit checks, we will add some zeros (0) to the actual data. This new binary data sequence is divided by a new word of length n + 1, where n is the number of check bits to be added . The reminder obtained as a result of this modulo 2- division is added to the dividend bit sequence to form the cyclic code. The generated code word is completely divisible by the divisor that is used in generation of code. This is transmitted through the transmitter.

Example:-



At the receiver side, we divide the received code word with the same divisor to get the actual code word. For an error free reception of data, the reminder is 0. If the reminder is a non – zero, that means there is an error in the received code / data sequence. The probability of error detection depends upon the number of check bits (n) used to construct the cyclic code. For single bit and two bit errors, the probability is 100 % .

For a burst error of length n – 1,
the probability of error detecting is 100 %.

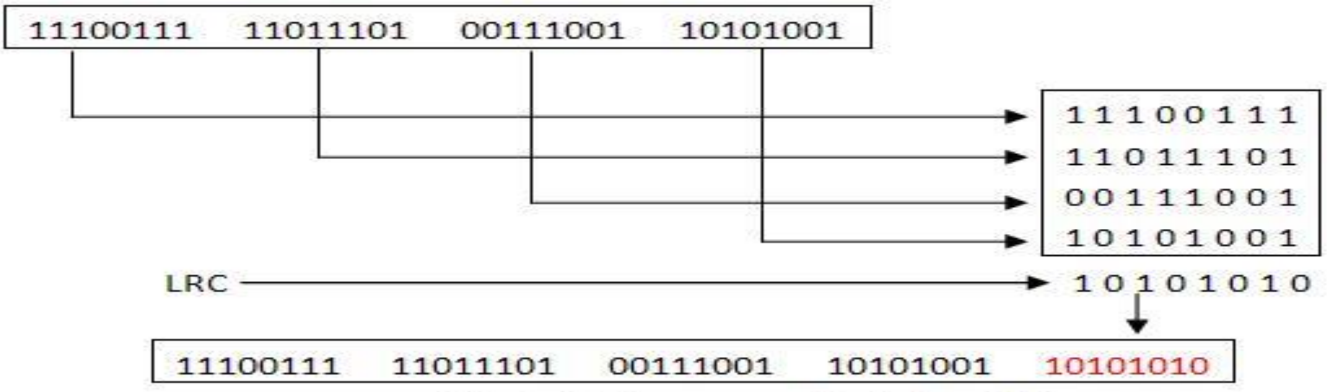
A burst error of length equal to n + 1,
the probability of error detecting reduces to 1 – $(1/2)^{n-1}$.

A burst error of length greater than n – 1, the probability of error detecting is 1 – $(1/2)^{n}$.

Longitudinal Redundancy Check

In longitudinal redundancy method, a BLOCK of bits are arranged in a table format (in rows and columns) and we will calculate the parity bit for each column separately. The set of these parity bits are also sent along with our original data bits.

Longitudinal redundancy check is a bit by bit parity computation, as we calculate the parity of each column individually. This method can easily detect burst errors and single bit errors and it fails to detect the 2 bit errors occurred in same vertical slice.



Original data message including LRC

****

Q3: What is encoding? Write down different types of encoding. Explain characteristics of AM, FM and PM with mathematical equations. (10)

Answer: -

Encoding: -

Encoding is the process of converting data into a format required for a number of information processing needs, including:

- ✓ Program compiling and execution
- ✓ Data transmission, storage and compression/decompression
- ✓ Application data processing, such as file conversion.
- ✓

Encoding can have two meanings:

- ✓ In computer technology, encoding is the process of applying a specific code, such as letters, symbols and numbers, to data for conversion into an equivalent cipher.
- ✓ In electronics, encoding refers to analog to digital conversion.

Types of Encoding

The four primary types of encoding are visual, acoustic, elaborative, and semantic.

✓ **Visual**

Visual encoding is the process of encoding images and visual sensory information. The creation of mental pictures is one way people use visual encoding. This type of information is temporarily stored in iconic memory, and then is moved to long-term memory for storage. The amygdala plays a large role in the visual encoding of memories.

✓ **Acoustic**

Acoustic encoding is the use of auditory stimuli or hearing to implant memories. This is aided by what is known as the phonological loop. The phonological loop is a process by which sounds are sub-vocally rehearsed (or “said in your mind over and over”) in order to be remembered.

- ✓ **Elaborative**

Elaborative encoding uses information that is already known and relates it to the new information being experienced. The nature of a new memory becomes dependent as much on previous information as it does on the new information. Studies have shown that the long-term retention of information is greatly improved through the use of elaborative encoding.

- ✓ **Semantic**

Semantic encoding involves the use of sensory input that has a specific meaning or can be applied to a context. Chunking and mnemonics (discussed below) aid in semantic encoding; sometimes, deep processing and optimal retrieval occurs. For example, you might remember a particular phone number based on a person's name or a particular food by its color.

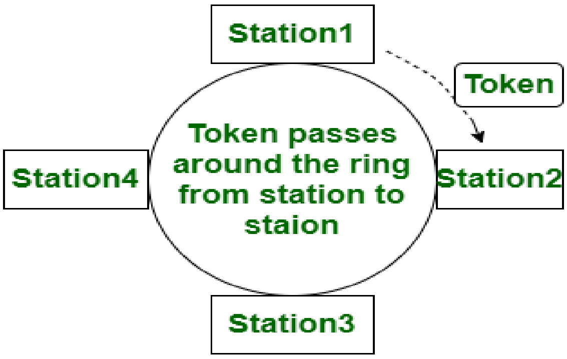
****

Q4: Compare Ethernet and Token Ring concept of data networking with diagrams. Which one is better in your opinion and why? (10)

Answer: -

TOKEN RING:

In the token ring a token ring passes over a physical ring. Token ring is defined by IEEE 802.5 standard. In token ring, there is a station and a special frame called token. A station in token ring can transmit data frame if it contains a token. After the successful transmission of data frame token are pointed(issued). Token ring is a Star shaped topology and handles priority in which some nodes may give priority to the token.



Ethernet :

IEEE 802.3 defines the Ethernet. It uses CSMA/CD mechanism. It means that if many stations exist at the same time to talk, all stations will be closed. To resume them, wait for a random time. Unlike token ring it doesn't employ any priorities. And it is less costly than token ring network.

Difference between the token ring and Ethernet: -

S#	TOKEN RING	ETHERNET
1.	In the token ring, the token passing mechanism is used.	While Ethernet uses CSMA/CD(Carrier-sense multiple access/collision detection) mechanism.
2.	Token ring is defined by IEEE 802.5 standard.	Whereas Ethernet is defined by IEEE 802.3 standard.

3.	Token ring is deterministic.	While it is non-deterministic.
4.	Token ring is a Star shaped topology.	While Ethernet is a Bus shaped topology.
5.	The token ring handles priority in which some nodes may give priority to the token.	While Ethernet does not employ priority.
6.	Token ring costs more than Ethernet.	While Ethernet cost seventy percent less than token ring.
7.	In the token ring telephone wire is used.	While in Ethernet coaxial cable(wire) is used.
8.	The token ring contains routing information.	While Ethernet does not contain routing information.

In my Opinion Ethernet is better than token ring. Ethernet 100M bit/sec Ethernet will be several times faster than the 16M bit/sec token ring as a general rule. The cost of Ethernet hardware is far cheaper than token ring

****

Q5. Explain the concept and review of Reliable Transmission with diagram (from a research paper of 2019 or 2020) and its functionality. The name and reference of paper should be given. (10)

Answer: -

Paper Tittle: - "Reliable Transmission of Critical Packets in IEEE 802.15.4-based Body Area Networks"

Reference:- https://sci-hub.tw/10.1109/ANTS47819.2019.9118022.

Abstract: - In this article, we propose a mechanism to ensure the reliable transmission of critical data packets in the body wireless network (WBAN). Because WBAN is responsible for real-time health monitoring, it must have a high success rate in data packet transmission. Most importantly, packaging that contains basic health information should be given priority. To ensure this, in this work, we express the probability of successfully transmitting a packet as a function of the maximum number of interruption steps (an important MAC parameter) so that we can adjust its value wisely to achieve transmission reliability. The maximum value of the key node. IEEE 802.15.4 is used as the basic communication standard. We use a simple two-dimensional Markov chain to model the channel access mechanism of CSMA-CA based on the IEEE802.15.4 standard, which forms the basis of the entire work. We compared the proposed method with the maximum number of disconnection steps randomly assigned to human sensor nodes. The results show that, compared with this method, wise adjustment of this value can make reliable packet transmission efficiency increase by 25%.

INTRODUCTION

Since the beginning of this century, we have witnessed the trend of people around the world wearing one or more devices to improve their overall quality of life. These portable devices are responsible for detecting, collecting and downloading enduser physiological data 24 hours a day. At the same time, we find that more and more physical objects are connected to the Internet at an unprecedented speed, and the concept of the Internet of Things (IoT) becomes a reality. Together, these two phenomena focus on a broader research topic called Wireless Human Body Network (WBAN). WBAN can undoubtedly provide very comprehensive, accurate and ubiquitous real-time human health monitoring. The continued growth of portable and WBAN-related keywords in Google Scholar can be seen as its increasing importance as a research topic. In 2015, the number of visits to keywords related to mobile phones and related to WBAN increased by nearly 7 times and 3 times compared to 2009, respectively. From a business perspective, the wearable technology market is expected to reach a market value of US$57.653 billion by 2022, almost three times its market value Compared to 2016 ($19.633 billion) [1]. In the expected market share of major IoT applications by 2025, the healthcare sector will occupy a huge market share of 41%, which undoubtedly shows the economic impact of WBAN [2]. Therefore, the challenge of establishing reliable communications in WBAN must be taken seriously.

Background and Motivation

Regarding communication technology, the IEEE 802.15.4 standard is most suitable for WBAN because it is generally used to transmit information over a relatively short distance. Unlike wireless local area networks (WLAN), it hardly involves infrastructure. It also allows the use of small solutions that are not very powerful and cheap in heterogeneous sensor networks such as WBAN. Figure 1 illustrates the general structure of WBAN, including five different body sensors, such as respiration sensor (R), blood pressure sensor (B), ECG sensor (E), pulse oximeter (P) and accelerometer (A). They detect the corresponding physiological parameters and communicate the detected raw data to Processing Unit (LPU). The LPU processes these locally collected data and then transmits the aggregated data to the medical server for 24/7 health monitoring. In this article, we are focusing on WBAN internal communication, that is, wireless communication based on IEEE 802.15.4 between the sensor device and the LPU. Therefore, before describing the exact problem scenario, we need to briefly discuss the functional overview of the IEEE 802.15.4 standard, especially its MAC protocol. This standard allows the use of star and peer types. In our case, we consider a star topology, where the LPU acts as a central hub and collects data from the associated sensor devices, as shown in Figure 1, and also acts as a WBAN coordinator. According to the IEEE 802.15.4 standard, in beacon activation mode, the coordinator periodically broadcasts beacon frames in order to communicate synchronously with connected devices. The time interval between two consecutive beacon transmissions is called a super frame. The structure of the super frame is shown in Figure 2. A super frame is composed of two parts, namely active part and inactive part. In the inactive part, the device can enter standby mode. The active part can be divided into two parts-conflict access period (CAP) and conflict free period (CFP). The CFP contains a guaranteed time slot (GTS), which is allocated by the coordinator to the sensor device according to the GTS request from the sensor device. However, in CAP, sensor devices follow the CSMA-CA (Carrier Sense Multiple Access-Collision Avoidance) algorithm to compete for access channels. In this article, our attention is limited to this particular algorithm. The main essence of the CSMA-CA algorithm is to detect the channel before transmission. According to the IEEE 802.15.4 standard, the channel is tested twice during each data packet transmission cycle. This process is called open channel assessment (CCA). If the channel is found to be inactive in these two consecutive CCAs, only the node is authorized to transmit its data packets.

However, if the channel is found to be busy in one of the CCAs (inactive in CCA-1 but busy in CCA-2, or busy in both CCA-1 and CCA-2), the counter It will track the number interrupt (NB, counting from 0) plus 1, the node continues to retransmit the data packet. Continue this process until the value of NB exceeds the value of mac Max CSMA Bakeoffs, which is the MAC parameter. The value of this parameter can be between 0 and 5. The MACs of all sensor devices have a predefined value for this parameter, which determines the degree of retransmission capacity of this particular node. If a node's NB value exceeds its mac Max CSMA Bakeoffs value in a transmission or retransmission attempt, the node will reject its current data packet, which indicates that the transmission of that particular data packet failed. Then, the node selects the next data packet from its buffer for transmission, and again follows the above steps of the CSMA-CA slot algorithm. The main goal of this article is to establish a relationship between reliable communication and the MAC parameter mac Max CSMA Bakeoffs. Through reliable communication, we mean that there is a high probability of successfully transmitting data packets. Compared with the randomly selected mac Max CSMA Bakeoffs value, we also show how to choose the mac Max CSMA Bakeoffs value wisely for the body sensor, especially for the critical value, which will produce a successful packet transmission probability (or reliability).

RELATED WORKS

In this section, we discuss some existing work that is close to the proposed work. Samanta et al. [4] proposed a mechanism to minimize computational complexity and traffic load through the formation of WBAN groups. Initially, WBAN established a relevant patient group (RPG) based on the similarity of disease types. Finally, a key WBAN is selected from each RPG through a decision process to form a virtual patient group (VPG) with a balanced flow load. The process takes into account some parameters, such as the factors of disease transmission and the proximity to the access point , Remaining energy factor and critical index. In another job, Samanta et al. [5] First proposed a fault-tolerant mechanism to ensure the dynamic connection with WBAN, and has a lower mean square error. Subsequently, an energy management process was proposed to provide WBAN with sufficient resources in the absence of decent link quality. However, this work is mainly applicable to the communication between WBAN. Some interesting work [6], [7] try to ensure QoS in WBAN internal communication level. Misra et al. [6] proposed a theoretical method of cooperative game, namely Nash Negotiation Solution (NBS), to adjust the data rate of sensor nodes related to WBAN. Sensor nodes set their minimum data rate requirements and participate in cooperative negotiations to adjust their respective data rates so that the solution at least meets their respective minimum requirements. The usefulness of sensor nodes is determined by considering various attributes, including the severity of the detected data. Using these utilities, the proposed NBS wisely adjusted the sensor data rate. Moulik, etc. [7] proposed a mechanism to adjust the priority load for WBAN. The author first used a fuzzy inference system (FIS) and quantified the severity of health parameters. During quantification and the severity of physiological parameters, the author also considered the influence of external attributes such as age. Then, they used the Markov Decision Process (MDP) to determine the payload range of each sensor. The quantitative gravity value (called the critical index) corresponding to each sensor plays an important role in this decision.

CONCLUSION

In this paper, we first propose a simple two-dimensional analysis of the Markov model based on the WBAN's CSMA-CA time slot algorithm, in which the human sensor nodes follow the standard average access mechanism IEEE 802.15.4 communication. The proposed method adjusts the mac Max CSMA Bakeoffs MAC parameter for all body sensors based on the corresponding severity level of the detected data. The results show that this method increases the probability of successfully transmitting data packets by 25%. In the future, this work can be expanded in solutions that use peer-to-peer topology. In star topology and peer-to-peer networks, the influence of other MAC parameters can also be utilized.