TECHNICAL UNIVERSITY OF LIBEREC
Faculty of Mechatronics, Informatics
and Interdisciplinary Studies

Monitoring Software for Wireless Sensor Network in Patients Medical Condition Observation

Master Thesis

Study programme: N0714A150003 Mechatronics
Author: **Zhasurbek Nishanov**
Thesis Supervisors: Ing. Lukáš Hubka, Ph.D.
Institute of Mechatronics and Computer Engineering

Liberec 2022

TECHNICAL UNIVERSITY OF LIBEREC
Faculty of Mechatronics, Informatics
and Interdisciplinary Studies

Master Thesis Assignment Form

Monitoring Software for Wireless Sensor Network in Patients Medical Condition Observation

Name and surname: **Zhasurbek Nishanov**
Identification number: M21000202
Study program: N0714A150003 Mechatronics
Assigning department: Institute of Mechatronics and Computer Engineering
Academic year: **2021/2022**

Rules for Elaboration:

1. Make a review of medical devices and sensors (heart rate, ECG, oximetry, blood pressure, breath monitoring) with wireless communication on the market.
2. Describe in detail the communication protocol for selected devices, the telegram structure, and security.
3. Create a virtual SW model of the device, resp. his communication part. Model should use the real communication interface.
4. Create an HMI (for example on a PC or mobile phone) realizing the data collection and data presentation from several virtual sensors.

Scope of Graphic Work: -
Scope of Report: 40 – 50 pages
Thesis Form: printed/electronic
Thesis Language: English

List of Specialised Literature:

[1] SOFI, A., J. JANE REGITA, Bhagyesh RANE a Hieng Ho LAU. Structural health monitoring using wireless smart sensor network –An overview. Mechanical Systems and Signal Processing [online]. 2022, 163. ISSN 08883270. Available from: doi:10.1016/j.ymssp.2021.108113.

[2] KUMAR, Pardeep a Hoon-Jae LEE. Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. Sensors [online]. 2012, 12(1), 55-91. ISSN 1424-8220. Available from: doi:10.3390/s120100055.

[3] HAO, Yang a Robert FOSTER. Wireless body sensor networks for health-monitoring applications. Physiological Measurement [online]. 2008, 29(11), R27-R56. ISSN 0967-3334. Available from: doi:10.1088/0967-3334/29/11/R01.

[4] GANAPATHY, Kirupa, Bharathi PRIYA, Bhanu PRIYA, DHIVYA, V. PRASHANTH a V. VAIDEHI. SOA Framework for Geriatric Remote Health Care Using Wireless Sensor Network. Procedia Computer Science [online]. 2013, 19, 1012-1019. ISSN 18770509. Available from: doi:10.1016/j.procs.2013.06.141.

Thesis Supervisors: Ing. Lukáš Hubka, Ph.D.
Institute of Mechatronics and Computer Engineering

Date of Thesis Assignment: October 12, 2021
Date of Thesis Submission: May 16, 2022

L.S.

prof. Ing. Zdeněk Plíva, Ph.D.
Dean

doc. Ing. Josef Černohorský, Ph.D.
head of institute

Liberec October 12, 2021

Declaration

I hereby certify, I, myself, have written my master thesis as an original and primary work using the literature listed below and consulting it with my thesis supervisor and my thesis counsellor.

I acknowledge that my master thesis is fully governed by Act No. 121/2000 Coll., the Copyright Act, in particular Article 60 – School Work.

I acknowledge that the Technical University of Liberec does not infringe my copyrights by using my master thesis for internal purposes of the Technical University of Liberec.

I am aware of my obligation to inform the Technical University of Liberec on having used or granted license to use the results of my master thesis; in such a case the Technical University of Liberec may require reimbursement of the costs incurred for creating the result up to their actual amount.

At the same time, I honestly declare that the text of the printed version of my master thesis is identical with the text of the electronic version up-loaded into the IS/STAG.

I acknowledge that the Technical University of Liberec will make my master thesis public in accordance with paragraph 47b of Act No. 111/1998 Coll., on Higher Education Institutions and on Amendment to Other Acts (the Higher Education Act), as amended.

I am aware of the consequences which may under the Higher Education Act result from a breach of this declaration.

May 3, 2022 Zhasurbek Nishanov

Abstract

Nowadays in medical field the patient's health condition monitoring is one of main and primarily researching areas. Implementing the wireless network in this direction opens a lot of opportunities and presents several challenges to researchers such as, reliable sending the datas form several transmitters to the main monitor, preparing the sending data in efficient form for transmitting, security of the private datas etc.

In this thesis the main problematics of the wireless communication are presented, considered weaknesses of using wireless communication, TCP/IP protocol, and offered the solution how to fight with them. It's created wireless virtual patient's health monitoring system on the base of multi-client and multi-server principle by using NI IDE LabView 2021. The health data is simulated ECG datas, which are sent from several clients to the several servers, and they are immediately presented to the doctoral monitor. Transmitting carries out through the Wi-Fi, the TCP/IP protocol.

As a final result it's obtained the working sample of a virtual monitor with required functionality according to the assignment, moreover there are presented theoretical and programming basis for implementation the Blowfish algorithm to protect the data.

Key words:

Bedside monitor, wireless communication, Wi-Fi, TCP/IP protocol, NI LabView, simulation and modelling, multi-Client and multi-Server, ECG data, Encryption and decryption, Blowfish algorithm.

Реферат

В настоящее время в области медицины мониторинг состояния здоровья пациента является одним из основных и очень важных исследовательских направлений. Применение беспроводных сетей в этом направлении открывает много возможностей и в том числе и сложностей для инженеров-разработчиков, такие как надежная передача данных с нескольких передатчиков на главный монитор, подготовка данных в эффективном формате для передачи, безопасность данных и т. д.

В данной работе представлены основные проблемы использования беспроводных связей, слабые стороны протокола TCP/IP, и предлагается решение, как бороться с ними. Разработана виртуальная модель беспроводного монитора состояния здоровья пациента на базе мультисерверного и мультиклиентского принципа с использованием среды разработки NI LabView 2021. Данные регистрируемые с пациента - это ЭКГ сигналы, которые симулируются, отправляются с нескольких клиентов на несколько серверов и одновременно отображаются в мониторе врача. Передача данных осуществляется через Wi-Fi, TCP/IP протокол. В результате, разработан рабочий образец виртуального монитора с требуемой функциональностью в соответствии с заданием, кроме того, здесь представлены теоретические материалы, и программная часть как применять Blowfish алгоритм для защиты данных.

Ключевые слова:

Прикроватный монитор, беспроводная связь, Wi-Fi, протокол TCP/IP, NI LabVIEW, моделирование и моделирование, мультиклиент и мультисервер, данные ЭКГ, шифрование и дешифрование, алгоритм Blowfish.

CONTENT

INTRODUCTION

Currently, medicine and medical technologies are developing, and this area always requires the implementation of all the latest achievements in science and technology. Every day there are more and more difficulties and problems with the use of medical equipment during operation, since all these diagnostic, preventive, therapeutic and surgical equipment are not fully adapted to the daily medical routine. For example, in diagnostic medical equipment there are problems associated with inaccuracy, with non-invasiveness, with pain for the patient, problems of mobility and ease of use by doctors. Therapeutic and preventive technologies bring a lot of problems related to the effectiveness and complications after treatment and the service life of such devices. One of the vital diagnostic devices is a bedside monitor, which is used literally in all wards of medical centres, whether it is a medical diagnostic department, surgery, or intensive care, and even at home it's used simplified versions of a bedside monitor such as a pulse oximeter, a saturation and pressure meter.

Bedside monitors are devices that perform continuous measurement and give doctors constant information about the state of critical body functions. Currently, monitors are an integral and mandatory element of diagnostic, treatment, and intensive care wards. According to the number of parameters observed, by design, type of communication, location in the medical center and by the quality of control, monitors differ and are classified to some extent. There are monitors that measure ECG, EEG, pulse, and respiratory rate, SpO_2, body temperature, blood pressure, etc., but others give information only about one or two of them with more precise and with intellectual functionalities.

The problems of bedside monitors at the moment are their stationarity and the unavailability of the option to move around the clinic with or without the patients, the impossibility of mobile usage the monitors in ambulances and the impossibility of remote access of doctors to the medical data of the measuring monitor. These shortcomings absolutely negatively reflect in the quality of the treatment process. The mobility of medical personnel and medical equipment around the hospital is an important point that will allow continuously monitoring of the patient's condition by doctors, even if they are distant from patients, and it also ensures high-quality and timely diagnosis and treatment of the patient. One of the possibilities to solve these problematics is creating the centralized patient monitoring systems with wireless communication between sensor modules and the main observing monitor and creation of combined monitoring systems with data transmission over a wireless network.

Nowadays wireless technologies are developing at a rapid pace, which are being implemented in not only on IT or telecommunications, automation, mechatronics, but also this technology has the great ambitious and potential in the field of biomedical technologies. In biomedical technologies, special attention is paid to this topic, since the use of wireless connections between medical equipment opens up new horizons in the development of biotechnologies, will provide high-quality monitoring of patients, will facilitate, and simplify the work of medical personnel.

In this paper, the topic of wireless monitoring of the patient's condition is investigated by creating the centralized version of patient monitor with wireless communication between the sensor module and the doctor’s monitor. Moreover, there are presented some problematics of using the wireless communications such as security of transmitting data and methods how to solve these issues.

This topic is relevant, requires research and a lot of work on it on the above-listed problems of using routine old and inconvenient wired medical monitoring devices. Everyday doctors and patients face problems and difficulties associated with the movement of a patient from one ward to another, and face problems on ambulance with a lot of non-convenient constructed wired monitoring devices. For example, suppose that after a certain car accident, an ambulance takes seriously injured people to the hospital. In this case, doctors need to provide the most practical and comfortable conditions for helping patients and save time as much as possible. Wireless sensors and electrodes are attached to the patient, which register data on the patient's condition and send them to the monitor wirelessly. And upon arrival at the hospital, the hospital's wireless sensors are already connected to the patient, which immediately read the data, transmit it to the main station of the doctor, who, in turn, depending on the available data, will already prepare laboratories for analysis, operating rooms, between which the patient will have to be transported mobile and under observation without any interruption.

1 REVIEW OF MONITORS ON THE MARKET

The patient monitor is used in every ward in hospitals as an integral part in patient therapy. Patients monitor repeatedly observes and measures the patient's physiological functions and functionalities of health - support equipment. The obtained result data from the patient monitor will serve for guiding the medical staff in making the decision and in making therapeutic or surgical interventions.

It's known 3 types of bedside monitor by construction and location relative to the patient:

- The device is located near the patient's bed with directly connected sensors. The advantages of such an arrangement are such that the staff can compare their visual impressions of the patient's condition with the measured monitor data, and there is also the possibility of monitoring in case at least one of the measurement channels gives incorrect medical indications. Here, it is possible to connect only the necessary measuring part of the monitor, the measuring unit of the bedside monitor, which is necessary depending on the nature of the patient's disease. This type of connection monitor is very cheap and is widely used because every hospital is allowed to buy this kind of equipment.

- The next type is a centralized patient monitoring system, which has a unit connected to the patient by wired sensors and electrodes at the patient's bedside and transmits all received medical signals of the patient to a central monitor located at the central monitoring station by wire. In this type of monitoring systems, monitoring of several patients is carried out by parallel data transmission channels or sequentially, by using switchboards to switch the monitoring station between patients. This system requires a thoroughly developed flexible system, since it can be changed at the beginning of operation for convenience and expanded in further operation, and additional sensor modules can also be added, and a qualitatively thought-out system in advance will allow it to be modified without any labor and unnecessary costs. The disadvantages of this system are that it is difficult to adapt it to each patient, besides, if the monitoring station fails, then the medical conditions of all patients will be unavailable.

- The third type of monitoring systems is fixed the version, which excludes disadvantages of previous two. This is combined system, which includes a bedside system and at the same time the measurement data is received by the central monitors of doctors (PCs). This type of system is more expensive and difficult to implement, few hospitals will be able to use such a comprehensive system. [1]

Physiological health datas as ECG, pulse and saturation are derived from the sensors, which convert biological health signals such as flow, pressure, or mechanical movement into electrical signals. In the figure 1 it's presented the block diagram of a patient's health condition monitor.

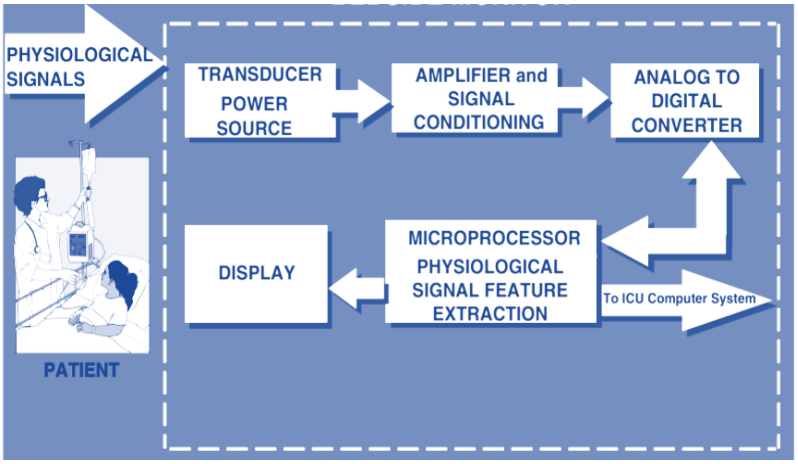

Figure 1 - Patient health condition monitor

Here it's showed that patients health physiological signals are received by sensors (transducers), which convert the health data signal into an electrical one, then it's amplified, filtered, then the signal is presented to the Analog to Digital Converter (ADC). The ADC sends the data to a microcontroller (microprocessor), which extracts parameters such as blood pressure, saturation, heart rate etc. After processing in the microcontroller health data signal is presented in understandable view for the medical staff on the display system. [2]

1.1 Health condition signals of patient

Vital indicators or parameters of the patient's state of health are parameters such as ECG, pulse, arterial blood pressure, oxygen saturation, ECG, temperature of various parts of body, EEG etc. And bedside monitors can allow measure and observe by doctors all of this signals from the patient's body. In this subchapter I presented them in detail.

1) ECG signal is the electrical form signal in millivolts, that is obtained from the electrodes from the body of patient. ECG includes P, Q, R, S, T segments. Every segment can change in some range, i.e., in intervals. On the table 1 it's presented allowed limitations and deviations on ECG measuring.

Table 1 – ECG limitations

Measuring range of input voltage, mV	Limits of permissible relative deviation of the monitor in measuring voltages, %	Limits of the permissible absolute deviation of the monitor in measuring heart rate, min^{-1}
0,5 - 5	5	30 - 250 ± 2

Depending on the change in amplitude and the distance between the segments, doctors monitor the normal functioning of the heart or diagnose various diseases in patients. On the following figure 2 it's presented ECG example diagram.

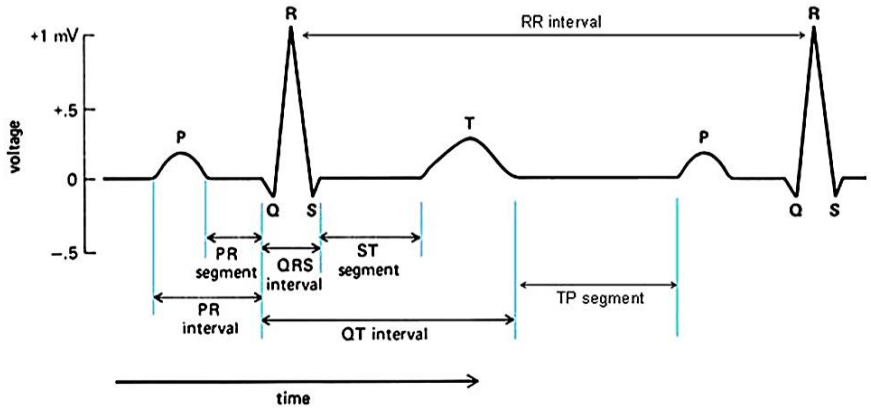

Figure 2 – ECG signal diagram

2) Pulse is the heart rate of patient i.e., it's the number of heart beats per minute. This parameter can change from person to person. Pulse can be low when people are at the rest, and it'll increase when people are doing some exercises. Normal heart rates at rest can be:

- Children in the ages 6–15 may have 70–100 beats per minute,
- Adults in the age 18 and over may have 60–100 beats per minute.

3) Oxygen saturation of blood SpO_2 (peripheral oxygen saturation) is the relation between oxygen-saturated hemoglobin and the whole hemoglobin, which is the sum of unsaturated and saturated hemoglobin in the blood. On the expression below (formula 1) it's presented the formula for calculating the SpO_2

$$SpO_2 = \frac{HbO_2}{HbO_2 + Hb} \quad (1)$$

where HbO_2 is oxygenated hemoglobin and Hb is deoxygenated hemoglobin.

Table 2 – Saturation limitations

Limits of permissible absolute error of the monitor in measuring SpO2, %	Pulse rate measurement range, min^{-1}	Limits of allowed absolute error of pulse rate measurements min^{-1}
(40 – 100) ±2	30 – 250	± 5

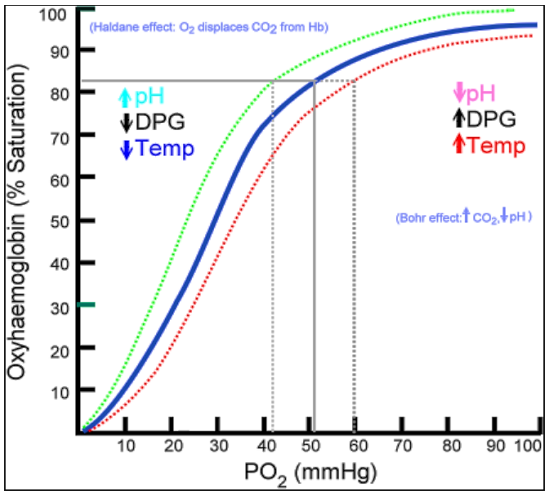

Figure 3 - Curve of hemoglobin saturation

At around 90 % oxygen saturation increases according to an oxygen-hemoglobin dissociation curve and approaches 100 % at partial oxygen pressures of >11 kPa. Humans normal arterial blood oxygen saturation level is about 95-100 percent. [4]

4) Arterial blood pressure is the pressure, which is measured in large arteries. There are systolic blood pressure and diastolic blood pressure. Systolic pressure describes the maximum pressure in the large arteries when the heart muscle shrinks to move blood through the body. Diastolic pressure refers to the lowest pressure in the large arteries during heart muscle relaxation between beatings. Arterial blood pressure changes from person to person and with age. There are AD limits of deviations presented on Table 3. Normal blood pressure for different age periods:

- 16 – 20 years – between 100/70 mmHg to 120/80 mmHg.
- 20 – 40 years – 120/70 mmHg to 130/80 mmHg.
- 40 – 60 up to 140/90 mmHg.
- older than 60 years – up to 150/90 mmHg.

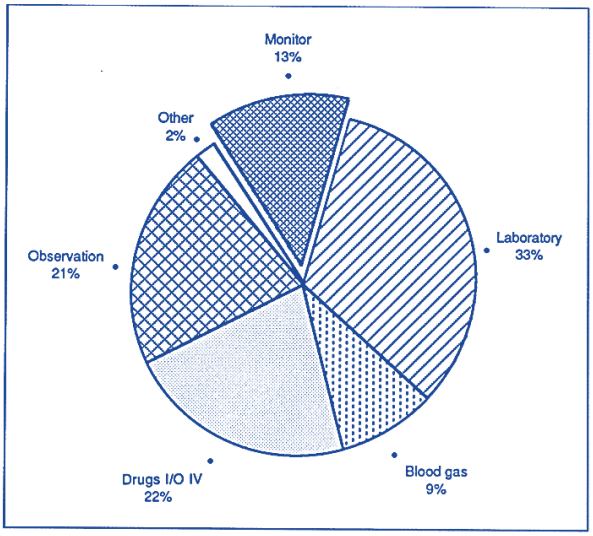

Figure 4 - Pie chart presenting variety of data doctors use in making treatment decisions

As it can be seen, doctors rely on the indications of 13% of the bedside monitor data when making decisions in diagnosis and in the course of treatment.

Table 3 – AD limitations

Measuring range of excessive pressure in the compression cuff, kPa	Limits of permissible absolute error of the monitor when measuring excess pressure in the compression cuff, kPa
0 - 40	0 – 26 ± 0.39 26 – 40 ± 0.52

As we can see from the pie chart that monitor results are one of the most necessary parts of making treatment decision. Moreover, today computer charting systems are able to collect a wide range of data from automated and remote sites, as well as from medical workers at the patient's bedside.

1.2 Wireless bedside monitors

Nowadays medical technologies are developed with high speed, and they are becoming multifunctional with higher efficiency and more comfortable to use in hospitals and in ambulances in mobility conditions. However, the issue of widespread use of wired and stationary devices remains open and thoroughly unexplored, which caused a lot of inconvenience to patients and doctors, as mentioned above. There are several companies, that used the idea of wireless patient health monitoring. Here, it’s illustrated some of them, that were tested by doctoral staff of university hospital in Taxes, USA.

1. **Philips IntelliVue MX40** is a compact patient monitor with the function of wirelessly transmitting information about the state (ECG, heart rate, SpO2, pulse, ST and QT complexes, respiration) of the patient's health to the iX-informational central monitor via Wi-fi 802.11 a/b/g/n. It displays wide variety of parameters including ECG, HR, SpO2, pulse, ST, QT, breathing parameters.

Figure 5 – Patient monitor IntelliVue MX40 [5]

That is, this monitor does not use wireless sensors as such, due to its compact body, the monitor easily fits into the patient's pocket, reads all the patient's health data, and transmits it to the central monitor – to the doctor's monitor.

2. **Dragger Infinity Delta** is patient monitor with universal module, it can work online and can be moved freely from the patient's bed around the hospital without interruption of monitoring due to the wireless connection option. Infinity Delta displays a set of ECG parameters, respiration, analysis of ST segment, EEG, temperature of the body, invasive and non-invasive blood pressure, and complete arrhythmia. Patient information is collected at his bedside and during transportation can be transmitted via the Infinity network to the Infinity Central Station and to the Patient Data Management System (Innovian) for automatic processing and obtaining diagrams.

For sending and receiving Infinity Delta implements the newest wireless communication card, that supports the Enhanced Security Protocol - WPA2 and Wi-Fi technology of type 820.11g for higher bandwidth. The Infinity Delta monitor supports the Infinity OneNet technology. OneNet is an innovative shared network infrastructure, which integrates patient monitoring systems into existing hospital wired and wireless networks and does not require the organization of a separate network. Since Infinity Delta supports operation in any intensive care environment, it is possible to use one monitor throughout the hospital. The Delta monitor shows 5 channels as standard (up to a maximum of 8).

Figure 6 – Patient monitor Drager Infinity Delta [6]

The Infinity Delta monitor receives data on the patient's health data using a special Infinity MultiMed 12 module, which measures: the ECG in 12 leads and the oxygen saturation (SpO2) of the patient (see Figure 7).

Infinity MultiMed 12 features:

- Accuracy ± 2 bpm or ± 1 %.
- The accuracy of registration of the QRS complex is from 0.5 to 5.0 mV;
- The amplitude is from 70 to 120 msec, respectively.
- From the design side, the module housing is protected according to the IP54 standard.

Figure 7 – Modul Infinity MultiMed 12

From examples below, we can say that, both types of wireless monitors are used the almost same idea: patient health datas are registered with classical sensors and collected by transmitting module, which sends all datas to the main monitor via the Wi-Fi. Both monitors are use the typical sensors passing the datas through wire to the transmitting module.

3. Smart watch Polar M430. During the performing of the project, it was decided to include in the project one of the compact and really very common types of monitoring devices -

smart watches that measure Heart rate, SpO2 and some even measure blood pressure. Of course, it should be noted that these devices are not considered medical, because they have big measurement errors.

Figure 8 – Smart watch Polar M430

The built-in pulse oximeter works noninvasively with the use of infrared LEDs of a certain wavelength, without puncture or other damage to the skin, measuring the amount of absorbed light or its attenuation during skin illumination. A watch with an oxygen sensor is not considered a medical device, its measurements cannot be called ultra-precise. But during illness or a significant change in the level of vital signs, the oxygen sensor will monitor significant changes in the level of oxygen in the blood and respond to its critical decrease or increase.

Last times the area of smart watches is developing very fast and there are implemented more and more new high-level technologies, therefore, I think that in the future smartwatch measuring quality and precision will be increased to the comparable level with medical monitoring devices.

1.3 The wireless communication problematics

The development of a wireless healthcare implementing requires a lot of challenges such as safe and accurate data transmission, fast event detection, power management, data receiving in the necessary time without any delay. The main problems of wireless communication usage inside modern reinforced concrete hospital buildings are unequal distribution and attenuation of the radio signal. It requires to increase the power of signal, to implement more accuracy hardware parts and sensors in developing the medical equipment, consequently nowadays the cost of the wireless communicated biotechnologies are more expensive and from the financial point of view efficiency is lower for medical companies to use such types of technologies. And here it is necessary to take into the account that the zone of confident reception at the Wi-Fi hotspot is about 30 meters. Well, for good reception of mobile phones that work in the GSM/UMTS or CDMA2000 standard, it can

be installed special femtocells or a miniature cellular base station. And also, one of the main obstacles in the spread of wireless technologies are problems in sensors related to speed, i.e., the delay between triggering and response, and the limitation of the power supply of sensors.

Wireless medical networks contain confidential information about patients such as the patient's medical history, current health status, treatment process, physiological data, current activity, and location of the patient. Therefore, the implementing of new technologies in healthcare area without considering and providing the data security makes the privacy of patients unprotected and vulnerable. For example, if a patient has some serious diseases and the leakage of information about it may negatively affect further medical treatment, the patient may lose his job and may have problems in obtaining medical insurance, etc. Such a situation will directly spoil the reputation of this hospital. More importantly, a healthcare provider is subjected to strict civil and criminal penalties. In the following figure 9 it's presented the data attacking process and its distribution on the internet. [7]

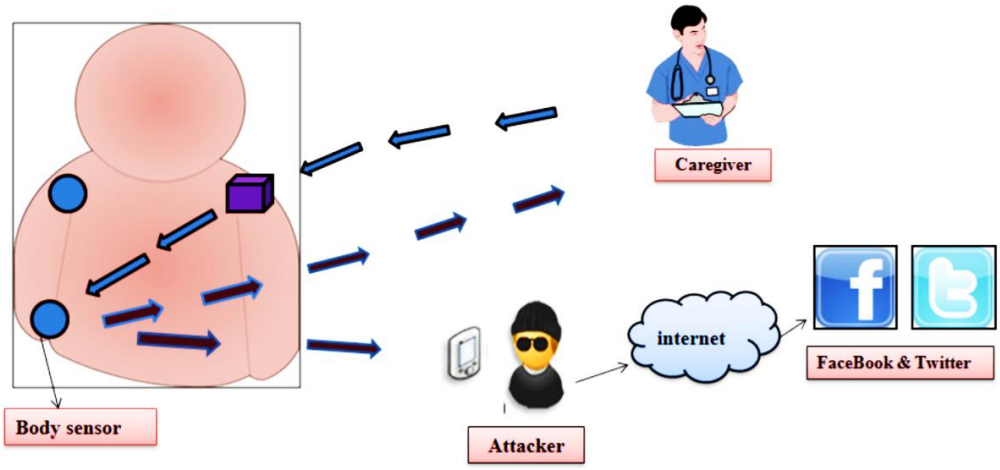

Figure 9 – Data attacking illustration [7]

Nowadays the topic of security in wireless medical sensor network hasn't been properly researched yet. This opens wide opportunity for researching the security of the data in wireless medical communications and applications.

1.4 Simulation and computer modelling

Modelling and simulation of various processes is a professional and reliable approach to conducting computer research. For the time of being the simulation and modelling IDEs are developed and become famous in the researching areas such as robotics, mechanical engineering, biomedical engineering, civil engineering etc. They are implemented from the first stage of designing most complex projects, control systems and production facilities.

Simulation programs are also widely used in teaching process of students in universities, it's used when medical institutions teach their medical staff to surgery and treatment process. Because not all universities and research institutes can afford the whole expensive equipment. But with these modelling applications, the learning process becomes more qualitative and interesting for students, since this approach is to some extent immersion in the environment of the simulated process. The use of simulation programs is a predictive approach to design, it illustrates the development process more accurately, while avoiding expensive and time-consuming prototype development, therefore, it is a less expensive approach to make research and development in any field.

Due to the advantages of the modelling approach, this project uses the IDE modelling environment owned by National Instruments – LabVIEW 2021 to model a multi-client and multi-server monitoring device.

2 THE COMMUNICATION PROTOCOL

By inspiring on reviewed examples of wireless monitors, we decided to use the idea of implementing the Wi-Fi communication to sending and receiving the data between sensor module and the main doctor's monitor (PC). And the chosen communication protocol is the TCP/IP protocol. **Wi-Fi** (Wireless Fidelity) is the popular communication protocol for wireless local area network (WLAN), using the IEEE 802.11 standard through the 2.4 GHz and 5GHz frequencies.

TCP/IP is the Transmission Control Protocol / Internet Protocol is used for such aims like communication protocol in a private PC network and its suite of communication protocols that is used for interconnection of network devices on the internet. The TCP/IP assumes the passage of information through four levels, each of which is described by a rule – transmission protocol. TCP/IP contains several protocols: IP, TCP, UDP and ICMP. These 4 levels are followings:

1. Application layer – provides standard data exchange (HTTP, FTP).
2. Transport layer – provides end-to-end communications across the network. In this layer TCP processes communications of hosts and provides flow control.
3. Internet layer – provides connection of independent networks to transport the packets across network boundaries. The protocols are Internet Control Message Protocol and IP.
4. Link layer – includes Ethernet for LAN, WLAN, Token Ring etc.

The TCP/IP provides with such advantages as

- Reliability — TCP controls the confirmation, repeated transmission, and messages timeout.
- Orderliness — when messages are sent from 2 transmitters sequentially, the first one will be received the recipient application first. If there are sent in a wrong order, then TCP sends them to the buffer until they will be ordered.
- Heaviness — before sending data for TCP, 3 packets are transmitted to implement a socket connection. this protocol strictly monitors congestion and reliability.
- Threading — in TCP, data is received as a stream of bytes and there is no information in the messages to determine their boundaries. [8]

UDP is the simple messaging protocol without making any connection, it does not build allocated connection between two hosts. Communication is achieved by sending the package without any checking the status of receiver. UDP has an advantage over TCP in cases for voice communication over the Internet protocol Voice over UDP (IP, TCP/IP), since here, any "handshake" would interfere with good voice communication. UDP has such properties, as:

- Unreliable — after sending a message, the sender has no information whether the message will reach its destination — it may get lost along the way, i.e., there are no confirmations, retransmission, timeout.
- Disordered — the order of reaching the sent messages is unknown.
- Lightness — There is no connection tracking and message ordering in UDP.
- Datagrams — data is sent separately, if they have arrived, then they are carried out through an integrity check.

To describe the idea of the project, it's made the block diagram – so called schematic view, which presented on the following figure 10:

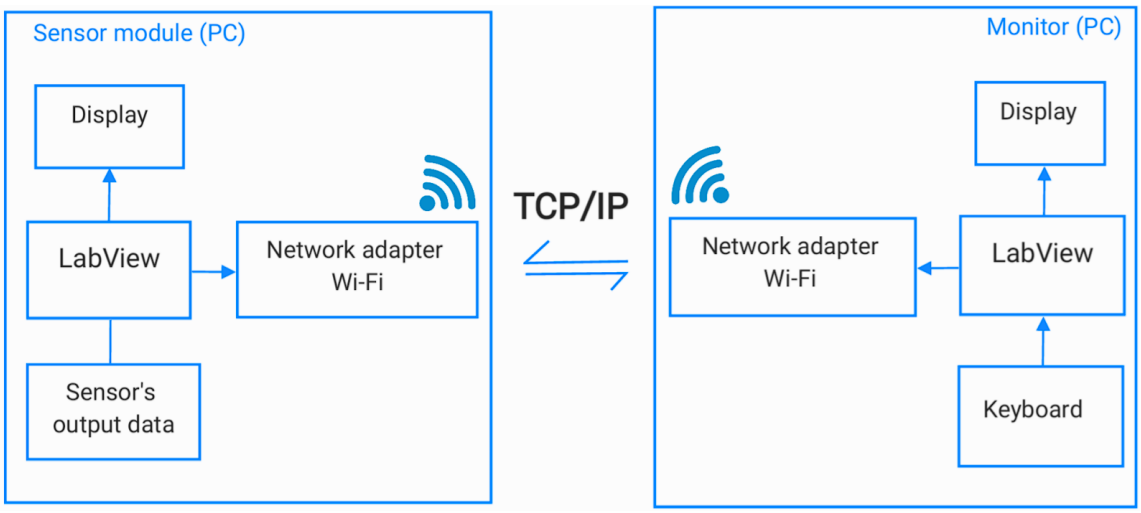

Figure 10 - Block diagram of the communication part of the wireless monitor

It has two parts, sensor module (PC) and the main monitor (PC). They both are built virtual like software, which is simulated by using the Integrated development environment (IDE) LabView.

The choice of Labview is that because Labview is very convenient to create communication software, human - machine interface and simulation of various signals. It has powerful instruments for developing monitoring and communication systems. [9]

The sensor module part of the system includes:

1. The sensors output data – ECG signal, which will be sent to the monitor through the Wi-Fi.
2. The monitor for presenting the simulated ECG signal.

The monitor part is simulated software - the Human Machine Interface (HMI), which receives the health data and presents it to the medical staff, and it include:

1. The main monitor presenting the received health condition data.

2. Keyboards for users tuning some parameters of the software.

TCP/IP protocol weaknesses. TCP/IP contains several protocols: IP, TCP, UDP and ICMP.

The most important is IP, which specifies where to send the data and it was not developed to provide the security of connection and this fact leads us to mention main weaknesses of TCP/IP protocol:

- It hasn't traffic priority.
- Traffic can be injected, and packets can be stolen.
- TCP offers weak authentication, easy IP spoofing.
- It hasn't confidentiality, no encryption of the data etc.

In accordance with the above weaknesses, there may be the attacks on this communication protocol, such as packet sniffing or in the other words eavesdropping, confidentiality attack, spoofing of IP or the data etc.

There are exist methods of protection - the network security:

- Using the encryption algorithms.
- Protecting the network from the outside using the router access list, firewall etc.
- Network monitoring.
- Implementing attack detection systems.

2.1 Data encryption algorithms

In a world, where cybercrime is rising it's necessary to protect the network and the private information by using encrypting algorithms. Data encryption is commonly used and efficient method for protecting the sending information. This process converts the data from readable format into the enciphered piece of information. The data that will be enciphered is termed as clear text. Encryption algorithm is basically mathematical calculation and there are a lot of types of algorithms, each of them has own unique application and security index. In addition to algorithms, it's needed an encryption key, with which the cleartext is converted into the ciphertext and wise versa, so called decryption - converting from the ciphertext into the cleartext. The decryption key may not be the same as the encryption key. Encryption and Decryption of data are the most important issues for every organization with well reputation, the reasons for it are:

- Authentication
- Privacy of client data
- Compliance with regulatory requirements
- Security.

The encryption and decryption processes are illustrated on the Figure 11:

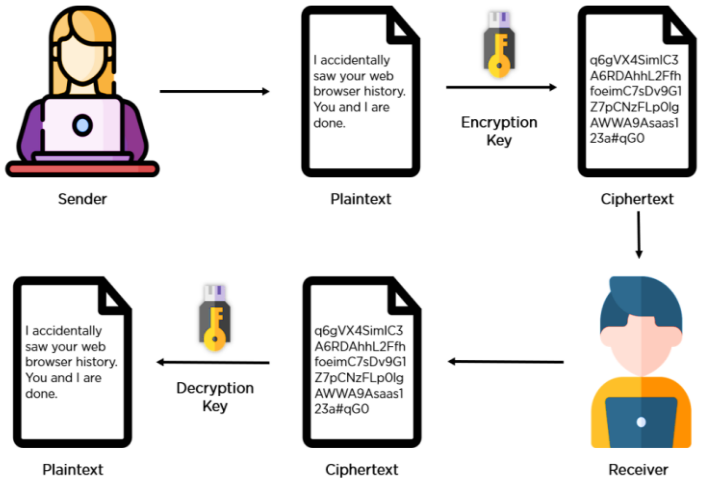

Figure 11 - The encryption and decryption processes

The encryption is divided by the internal security professionals into 3 types: symmetric, asymmetric encryption and hashing.

1. **Symmetric encryption** (secret key algorithm) – the sender and the receiver have the same key, i.e., receiver must have the key, before the message would be decrypted. This method is convenient for the cases when we have the less risk of a third - part intervention. Symmetric algorithm is faster than the asymmetric one, but there it's necessary to both sides to be sure that the key stored safely.

2. **Asymmetric encryption** (public key algorithm) – there are used two keys for the encryption. Sender has a public key for encryption, the receiver has a private one to decrypt the message and private key available only for receiver. It doesn't matter which is chosen for encryption and which one for decryption. They are linked mathematically and both keys are just long numbers that aren't identical, but they are paired with each other.

3. **Hashing** an algorithm, which generates a unique fixed-length signature for a data set or message. Each specific message has its own unique hash, which makes it easy to track minor changes in information. Hashing is a method of verifying data that gives information about whether

the message or data set was distorted or not. Because data encrypted with hashing cannot be decrypted back to its original form.

There are several efficient and widely used encryption algorithms. Depending on whether algorithm includes private or secret key, cryptography methods are classified as on the scheme is presented on a Figure below:

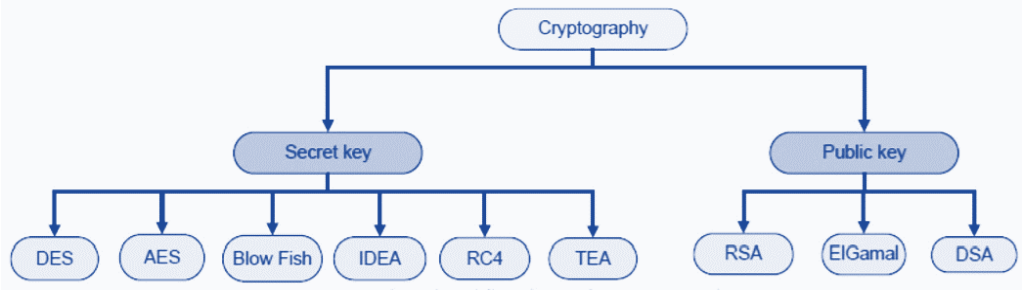

Figure 12 – Classification of cryptography algorithms

- **Advanced Encrypted Standard** (AES, other name Rijndael) is the symmetric key algorithm for encryption the data and it's established in 2001 by the US national institute. This algorithm is more secured than the DES and TRIPL DES and more difficult to implement. AES performs block ciphering with key length 128, 192, 256 bits and ciphers the data in 128-bit blocks. In other words, input data is 128 bits is taken and output is 128 bits of ciphertext. Principle of AES is based on the substitution and permutation network. In AES the key size determines the number of rounds for transformation plaintext into ciphertext:

Table 4 - AES

AES key size, bits	Rounds for transformation
128	10
192	12
256	14

Nowadays AES is integrated in the CPU that improves the transformation speed and security. However, most internet security experts predict that AES will eventually be seen as a universal data encryption standard in the private sector.

- **RSA** is an asymmetric algorithm with public and private keys. This algorithm is widely used to protect the information, which is sent through the internet. The idea of RSA is based on the fact, that it is difficult to factor a large integer. The public and private keys consist of two numbers, where one number is the multiplication of two large simple numbers. Therefore, if someone can decompose a large number, the private key will be compromised. In RSA the strength of

encryption depends on the size of the key. The strength of encryption increases exponentially if it's increased the key several times. RSA keys are usually 1024 or 2048 bits long. [10]

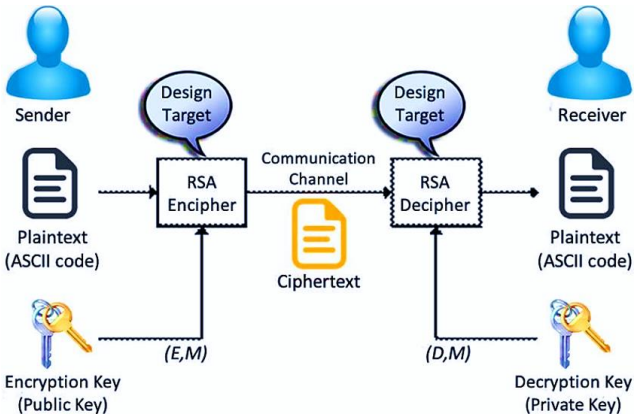

Figure 13 – Illustration of RSA algorithm principle

- **Triple DES** is the modified stronger version of the original DES algorithm. Triple DES is symmetric encryption algorithm with the size of keys 112 or 168 bits and 64 - bit block size. The basic principle is the application of DES three times to each data block. This type of algorithm is widely used in UNIX password encryption and PIN passwords of ATMs. Triple DES with three independent keys has a key length of 168 bits, since there are three 56-bit DES keys, but due to the so-called "meeting in the middle" attack, the effective protection it provides is only 112 bits. The key entry option 2 reduces the effective key size to 112 bits, since the third key is the same as the first. Moreover, this parameter is sensitive to a certain selected or known plaintext, and thus NIST defined it as having only 80 bits of security, which can be considered unsafe, and this algorithm has been deprecated.

- **Blowfish** is symmetric key encryption algorithm with varying key-size about 32 - 448 bits, it divides the message into 64-bit blocks and encrypts them separately. Blowfish has Feistel network structure, and it’s established for speed, flexibility, and for it's unbreakability. The inventor Bruce Schneier created it for general purposes and as the alternative algorithm to DES and IDEA. Blowfish is unpatented algorithm what makes it free for all users in all countries, adding even more to its appeal. Blowfish is commonly used on electronic commerce platforms, securing payments, and in password management tools.

- **Twofish** is the modified version of Blowfish and is also symmetric key and block cipher algorithm with key size 128, 192 or 256 bits, 128-bit block size. Twofish always encrypts data for 16 rounds, regardless of the key size. Twofish was designed to provide several levels of performance tradeoffs, depending on the required encryption speed, memory consumption, key

settings, and other parameters. It is an ideal option for software and hardware environments and is considered one of the fastest algorithms. This algorithm is used in many modern software solutions for encrypting folders and files.

In a diagram below it's presented the time evaluation of main encryption algorithms and their comparison experiment from scientific paper. Here, it was used 6 text files of different size to achieve 6 different comparison experiment. According to the speed, file size and throughput capacity it's defined the performance of each algorithm.

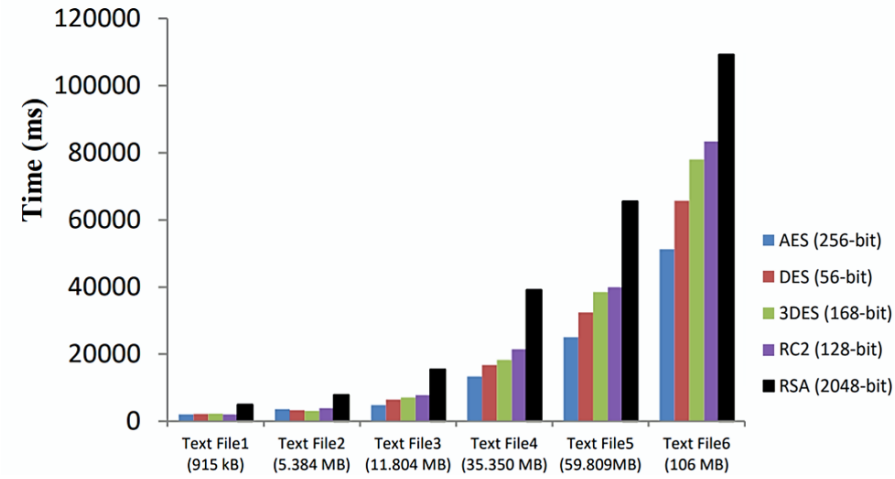

Figure 14 - Time evaluation experiment of cryptography algorithms [10]

Here, we can see that AES has the less processing time and has larger throughput capacity, the second priority algorithm is the DES, but the RSA is the slowest one and has the less throughput capacity than others.

2.2 The wireless communication in medicine and other areas

In modern clinics and medical centers, the availability of a fast and reliable Wi-Fi network is an urgent need, which improves the quality of patient care and provides a number of advantages to doctors, visitors, and the management itself. Therefore, the Wi-Fi network should be able to penetrate through all the thick walls of the ward and laboratories, work with different medical equipment and own applications of medical centers. Also, the wi-fi network must fully comply with HIPAA laws and must be convenient for implementation, expansion, and maintenance by IT personnel. There are some requirements regarding Wi-Fi networks in the medical field.

Here, we will mention requirements to the wireless communication in medicine:

• **Mobility of Wi-Fi**. Mobility of Wi-Fi network is the one of the most important parts. Network must be available everywhere of hospitals territory to monitor clinical datas, to get information about the availability of medicament. Moreover, mobility allows employees to work more convenient and efficient, quickly respond to incoming information, to communicate with each other in real time, regardless of the location of a colleague.

In a modern area of medical technologies, we can't imagine the full progress of the medical centres, which contains doctoral PC's, medical devices with Wi-Fi, communication devices and even result printing equipment's without Wi-Fi mobility.

Figure 15 - Access to the Wi-Fi network in medicine

• **Reliable access to the Wi-Fi network.** The reliability of connection and data storage when transmitting information over secure channels is ensured by the using of network equipment from manufacturers such as Ubiquiti, Mikrotik, Cisco, Linksys, D-Link, ASUS, and others.

A reliable network also includes qualities such as stability, scalability, and sufficient capacity, which allow monitoring equipment, wireless trolleys, and personal devices to receive the wireless communication quality they need to perform their functions efficiently and fully. [14]

Figure 16 – Safe access to the Wi-Fi network by employees and patients

• **Fewer access points should cover more territory.** Reinforced concrete products, metal panels and even leaded walls are used in the construction of hospitals and any medical centers. All

these factors prevent the propagation of the radio signal. And disconnections and constant re-authentication on workstations will lead to a decrease in performance. And this will reduce the speed of response and negative consequences are possible. It is necessary to establish equipment for Wi-Fi networks capable of constantly monitoring situations and the ability to control the Wi-Fi signal in such a way as to direct the signal itself to bypass obstacles.

Figure 17 – Diagnostic rooms with leaded walls [14]

Figure 17 shows a diagnostic magnetic resonance tomography (MRT) room with lead walls, where uninterrupted wireless communication is required.

- **Secured organization of access to corporate network services from the Internet.** One of options is presented here. This network is implemented in such a way that a public network is created for customers, which is accessed through registration and an internal network - a secure network only for employees who have access through special accounts. The main idea is that the nodes accessed from the Internet are included into the special place - Demilitarized Zone (DMZ).

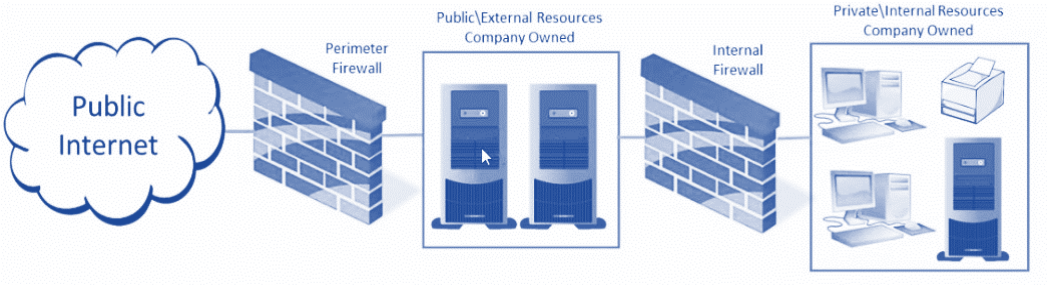

Figure 18 – Illustration of DMZ security approach

DMZ is performed by using separating firewalls from the Internet (Perimeter firewall) and from the internal (internal firewall) network. DMZ method has access tasks:

- control the access from the external network to the DMZ,

- control the access from the internal network to the DMZ;
- control of access from the internal network to the external;
- to block the access from the external network to the internal one.

Figure 19 – The main lows of DMZ method

On the other hand, **offices, hotels, universities, and restaurants** have less strict requires to the Wi-Fi network. For example, if we discuss office, here, the main needs are:

- Providing the personnel with wireless communication.
- Providing the guests internet.
- A wireless network is needed for telephony, video with QoS and seamless roaming.
- Compliance with security policies is required.

Companies need Wi-Fi only for guests with a separate subnet so that guests do not have access to the local network and could not see internal resources of hospital - only guest Internet access. [14]

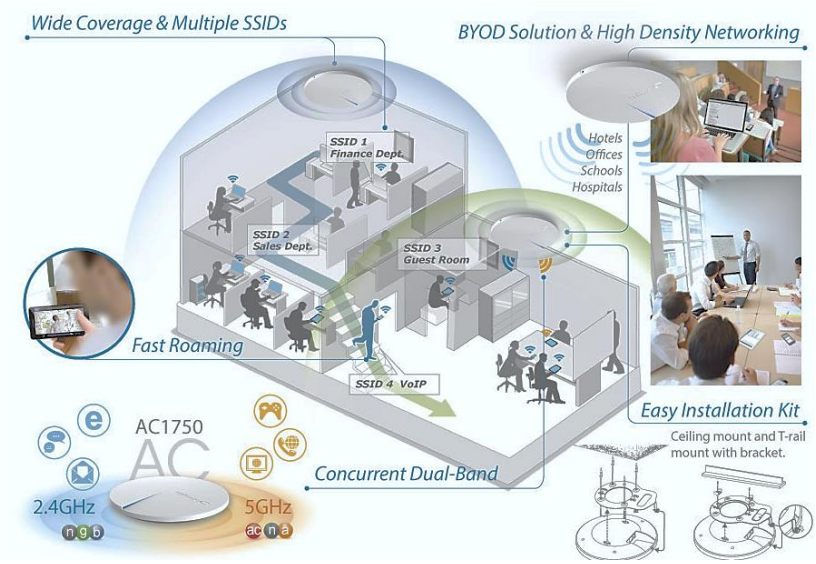

Figure 20 – Wi-Fi network in offices

Most employees require the company to compliance with a comprehensive security policy, including logins/passwords. You need to connect a centralized authentication database (RADIUS) and use a domain controller. After that, any employee will be able to connect to the network using a single login/password, just as when turning on the computer.

3 MODEL OF THE TRANSMITTER DEVICE

The practical part of the project is performed in IDE LabView 2021 and includes the creating model of the wireless centralized patient monitoring system, which consists of multi-Client and Server parts. Client must continuously transmit the patient health condition data (in our case the ECG) through Wi-Fi without any delay, distortions or changing the form. Distortion, delay, and waveform changes will have serious consequences, like incorrect diagnosis, patient treatment, etc. The same requirements are to the Server (receiver) – representing the signal without delay and distortion. Of course, errors and delays will present, and they depend on the hardware part of the transmitter and receiver parts of the application, but they must be in the allowed range of deviations showed in tables 1-3. The transmitter model generates the ECG signal, has own waveform chart to show the signal diagram and using the laptops Wi-Fi network adapter connects with another receiver model. Communication protocol is TCP/IP. The sending data is array of some limited length. The simple block scheme of the transmitter is illustrated in Figure 21.

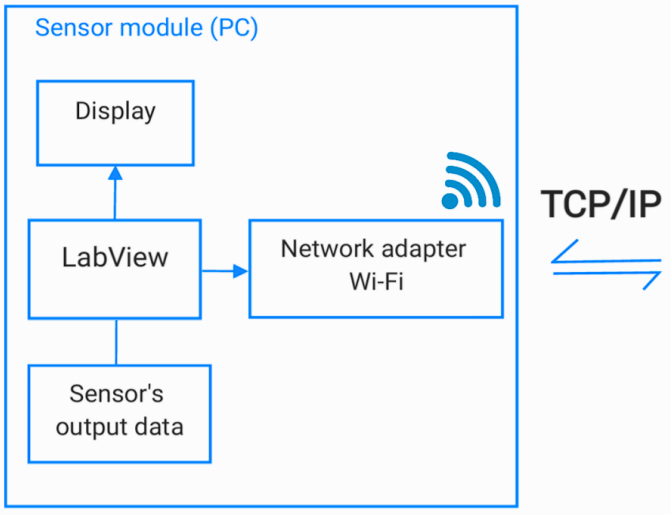

Figure 21 – Transmitter model's block scheme

The IDE LabView supports wireless communications such as Wi-Fi, Bluetooth, IrDA connections with the TCP/IP, UDP, HTTP protocols. There is the whole menu of instruments for using the TCP/IP protocol, which can be found by the following steps:

The list of functions → Data communication → Protocols → TCP/IP protocol

On the following figure the TCP/IP window is presented:

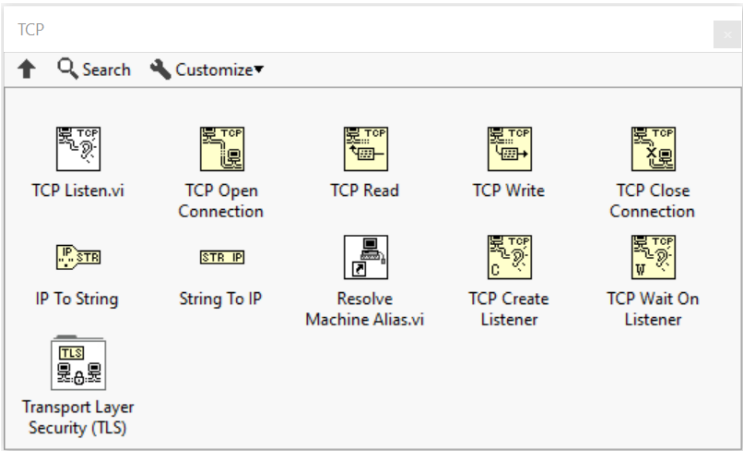

Figure 22 – Menu of TCP/IP protocol [15]

One of the important parts and idea of the project is that the application must provide the multi client server structure, i.e., in the same time user can observe several monitors with sensors output ECG signal. For this reason, the model of the transmitting device contains 2 separate VI's, first of them the Client Launcher and the second one is the Client software.

Client launcher's code included into the *Event* and *For Loop* structures. In Event case "Launch: Value Change" Client Launcher waits the button clicking to create the new Client. Client launcher VI by using the *Static VI Reference* and *Start Asynchronous Call* functions creates the clone of the Client VI every time, when user clicks button "Launch". Thus, user is able open several Clients, which simulated ECG signal and transmitters to the server. The other Event case is just stops running of the application.

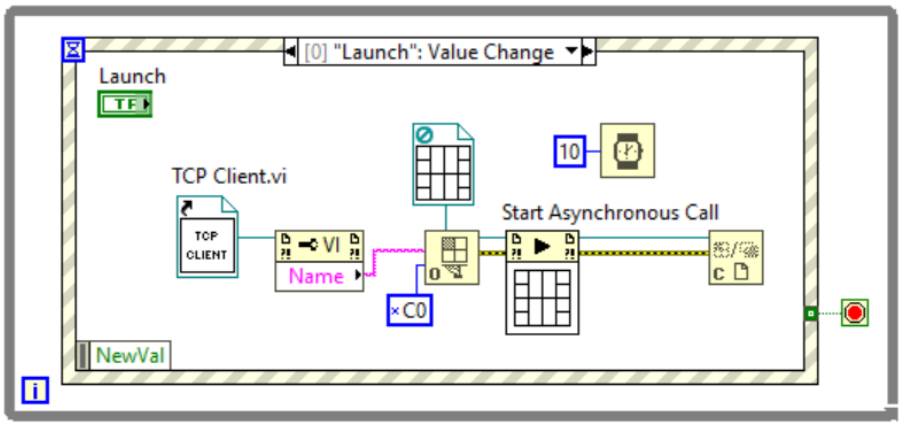

Figure 23 - Client Launcher

Here, palette *Open VI Reference* gets and passes the link of *TCP Client VI* location on the disk to the function *Start Asynchronous Call*.

3.1 The ECG signal simulation software

ECG signal is the recording process of the patient's heart electrical activity, which is used by doctors to diagnose and monitoring the functionality of the heart. In the project it's chosen to create this type of signal from others, because ECG signal is main health data and includes a lot of important information for diagnosing the heart disease, it's a waveform data, from where doctors define artifacts, changes in the heart functionality of the patient.

Detected diseases using an electrocardiogram are Arrhythmia, Myocardiodystrophy, Myocardial infarction, Angina pectoris, Tachycardia, Wolf-Parkinson-White syndrome, Ventricular hypertrophy, Bradycardia, Cardiac aneurysm, Pulmonary embolism, Pericarditis, Myocarditis etc.

I think it's more complicative to send by wireless and represent the data. The simulation of other health data type would include just changing numbers like saturation, heartbeat, and AD without any visualization. Moreover, doctors can measure heart rate, saturation, and AD health datas manually by using some portative devices, but ECG signal can't be measured in so simple way. There're 3 main components of ECG:

- The P segment – representation of a atria depolarization.
- The QRS complex – representation of ventricles depolarization.
- The T segment – representation of the ventricle's repolarization.

In process of ECG simulation, it's important to generate the signal as close to natural behaviour as possible. Ideal signals may be useless for sending and analysing, since a project built for an ideal signal may not function properly, or even give false results at all.

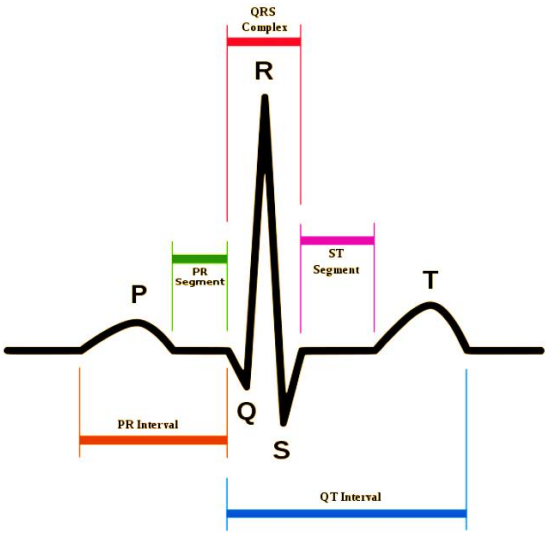

Figure 24 – ECG signal of patient's heart

Creating the virtual transmitter includes such steps as ECG signal simulation and the creating the data transmitting software part. Both parts are realized in one VI. In the project ECG signal is the sensors output signal, which is simulated in IDE LabView. In LabView to simulate the ECG signal we must use signal generation functions and obtain the signal - data in type of array for further to send it to Server software. In the following Figure 25 it's presented part of Block Diagram (Graphical code) of the creating ECG signal segments:

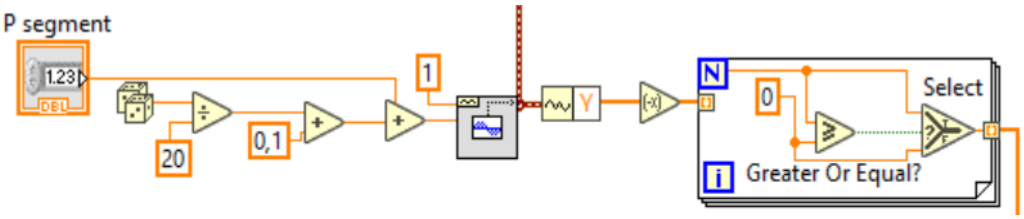

Figure 25 – Generating the P segment of ECG

This part of the code includes sum of amplitude control element and random function to obtain the segment with random behaviour, which will be closer to the real one. And it's modified in a form and passed to the For Loop structure. And the ECG generation graphical code includes the fragments similar to the P segment to generate other Q, R, S, T segments separately. After every waveform function, here's used the *for-loop* structure to set the sign of each segment.

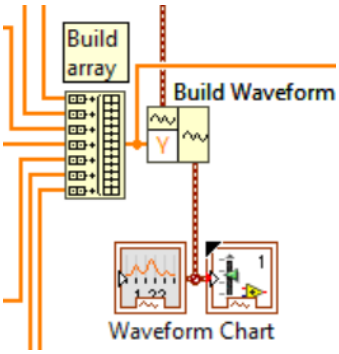

Figure 26 – ECG presenting fragment

Then the output signals (each segment of ECG) of all *for-loop* structures are passed to the function Build array. Function *build array* concatenates multiple arrays or appends elements to an array of N - dimension. After building the array we need to present the ECG signal on understandable view for user, by using the tools *Build Waveform* and *Waveform Chart* (Figure 26).

3.2 Creating the data transmitting software part

The data transmitting part (Client part) of software is created by modifying the ECG simulation code with addition TCP/IP protocol tools. For virtual device communication it's used the Wi-Fi communication and TCP/IP protocol. Therefore, we open and use in LabView:

The list of functions → Programming → Data communication → Protocols → TCP/IP protocol

In the menu of TCP/IP we need such main functions as TCP open connection, TCP write, TCP Read, Error clear and Error out. In the figure below it's presented the fragment of the code, where the IP and port of transmitting part are set.

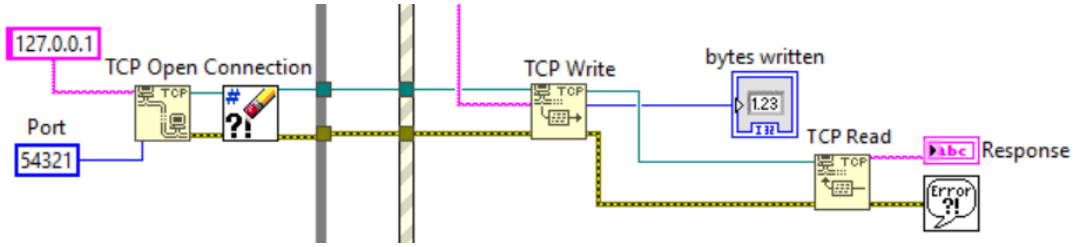

Figure 27 – ECG presenting fragment

TCP Write – allows us to write the data to the TCP network connection. The TCP Write function has the input "data in". Input signal is created and obtained from the ECG simulation software output by converting the data of type array into the string using function *Array to Spread sheet String*. And so, this data is written to the TCP network connection and sent to the Receiver by Wi-Fi connection.

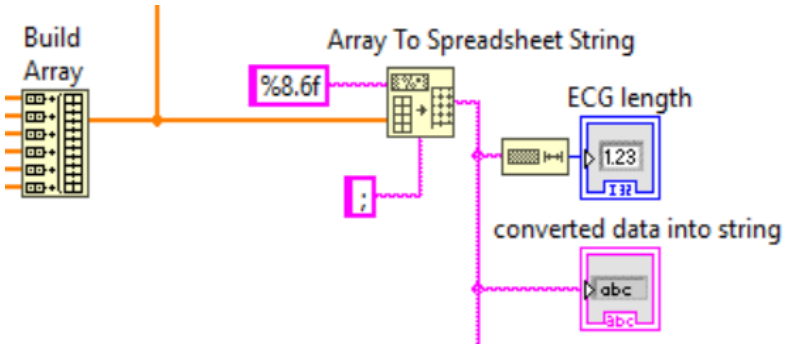

Figure 28 – Usage of Array to Spreadsheet String function to conversion

The transmitter device is included in Event structure. In Timeout Event case application creates ECG and sends continuously, but in the Stop clicking Event case application closes connection and stops ECG simulation.

The whole code of transmitter device is presented in **Attachments.**

4 MODEL OF THE RECEIVING DEVICE

In the practical part of the project, which is created in IDE LabView 2021 by simulation the multi-Client and Server parts. Receiving device (Server) of the wireless centralized patient monitoring system continuously listens to new connection and collects the patient health condition data (in our case the ECG) through Wi-Fi without any delay, distortions or changing the form. The main requirement to the Server is reconstruction the signal in the range of allowed deviation. The simple block scheme of the receiver is showed on the following Figure 29.

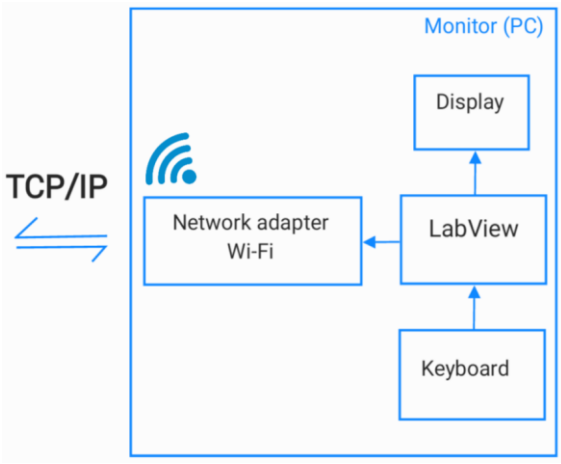

Figure 29 – Receiver model's block scheme

The receiving device is the server of the software and consists of 2 VI's. The first one is the TCP Server.VI and other is TCP Handler VI. Server listens and waits the TCP network connecting. The Static VI Reference Function has the reference to the TCP Handler VI, which is opened when connection is achieved. At the moment of connection Server saves the connection by using the array, then it asynchronously creates a TCP handler and gives the connection ID. The function Start Asynchronously Call can be found on Menu of pallets:

The list of functions → Programming → Application Control → The Start Asynchronously Call

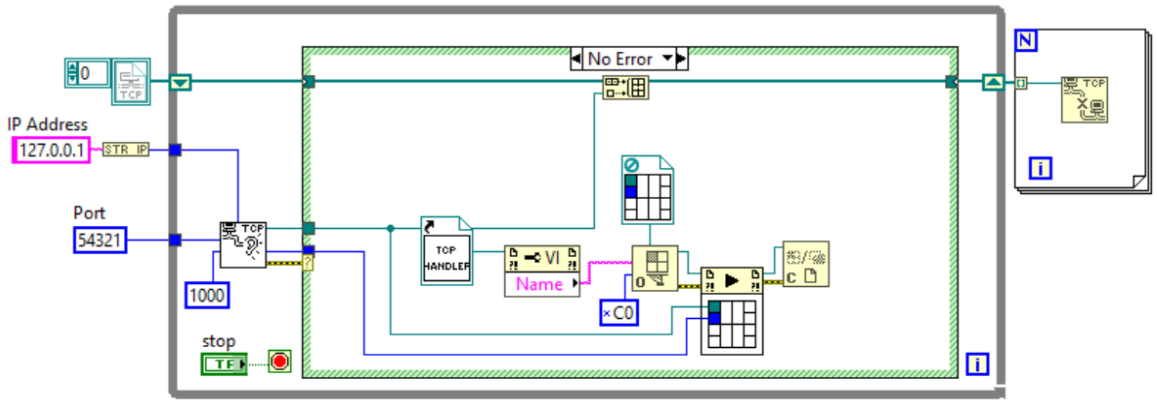

Figure 30 – Server VI's block diagram

The whole code is in *For Loop* structure and server listens the connection 1000 ms, after timeout it also continues waiting for. Other pallets are the same pallets, which are used in Client Launcher VI. The Static VI Reference Function can be found on menu of pallets:

The list of functions → Programming → Application Control → The Static VI Reference Function

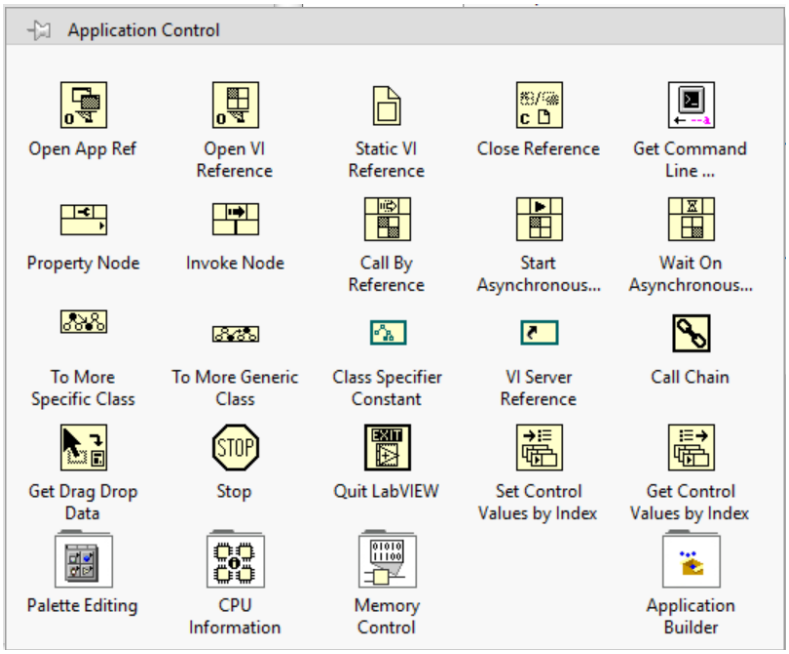

Figure 31 – Menu of Application Control [15]

The Menu Application Control is widely used in opening and using in one project the other VIs as reference.

4.1 Creating the receiving device

Receiver (TCP handler) is the doctoral ECG observer monitor, which gets data from according to data transmitting TCP Client. This part uses such functions as TCP Listen, TCP Write, TCP Read, TCP Close Connection, Spread sheet String to Array etc.

- TCP Listen – within this function we create a listener and wait for connection at the specified port, then we need to tune inputs of the function:
  - In input "net address" by using the converter *String to IP* it's given net address of localhost 127.0.0.1.
  - In input "port" it's used the controller from the Front Panel, where we can set the number of the port.

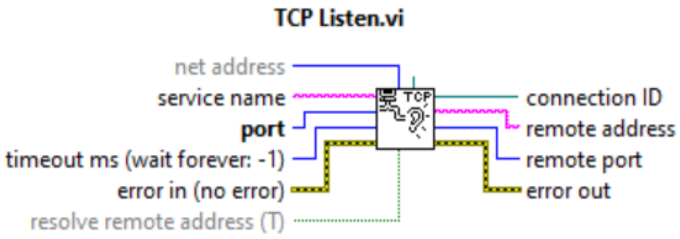

Figure 32 – TCP Listen inputs and outputs

- TCP Read – gets the ECG data from the connection.

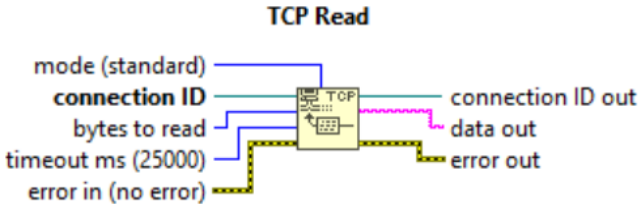

Figure 33 – TCP Read pallet

Output "Data out" is string type data (the ECG) obtained from TCP Client software.

And so, to observe the ECG data on server monitor we need to reconstruct the string data into array and build diagram. It's realised by using function *Spread Sheet string to Array*. This fragment is illustrated on Figure

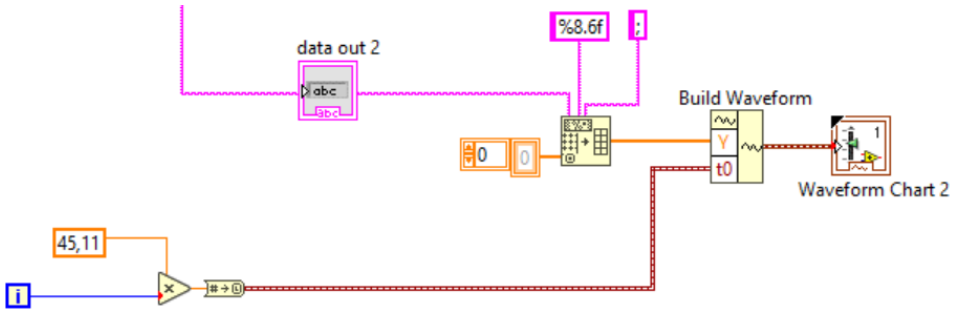

Figure 34 – Data converting fragment string to array

- TCP Close Connection is used after ending the transmmition to close correct the TCP connection.

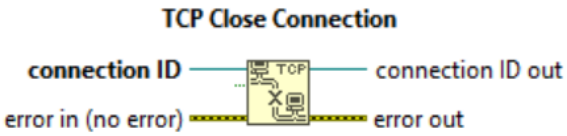

Figure 35 – TCP Close Connection input/outputs

All VIs and library DLL files are combined into one project TCP.lvproj.

4.2 Data security

As we mentioned on subchapter 2.2 in wireless communication it's paid most attention to security of transmitting data. In this project to fix the security weakness of TCP/IP protocol it's used Blowfish data encryption/decryption algorithm. Depending on the required encryption/decryption reliability, performance, simplicity, by using simple operations that reduce the probability of an error in the implementation of the algorithm, and for enciphering efficiency it's selected Blowfish algorithm, moreover from the economical point of view it's efficient option, because this algorithm is absolutely free license algorithm. The general scheme of algorithm can be represented as in figure 36:

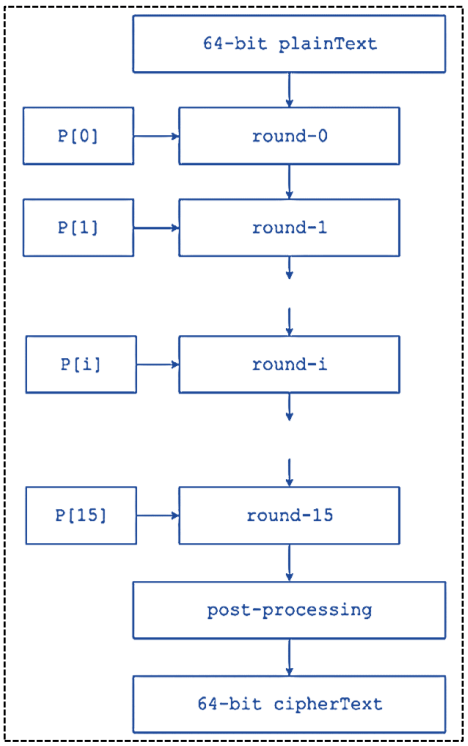

Figure 36 – Blowfish encryption Scheme

Blowfish encryption algorithm has 3 main steps:

1. **Generation of subkeys.**

In processes of encryption and decryption 18 subkeys: P[0], P[1], ..., P[17] are needed. These subkeys are collected in some P array. Each element of the P array is 32 – bit number, that initialized with the digits of π. It looks like:

P[0] = "713b5a77"

P[1] = "253g01d3"

.....

P[17] = "3920bf1".

Then, all subkeys are modified by using following operations. An XOR operation is performed on subkey P1 with the first 32 bits of the key:

P[0] = P[0] XOR first 32 bits of input key

P[1] = P[1] XOR second 32 bits of key

.....

P[17] = P[17] XOR 18^{th} 32 bits of key

If the key K is shorter, then it is superimposed cyclically. The final version of P-array stores the 18 subkeys, which are used during the whole process of encryption.

2. **Initializing the Substitution boxes.**

In both encryption and decryption processes it's necessary to get 4 Substitution S-boxes *S[0]…S[4*]. Each S-box have 256 records: *S[i][0]…S[i][255]*, where each entry is 32-bit. It is initialized with the digits of π.

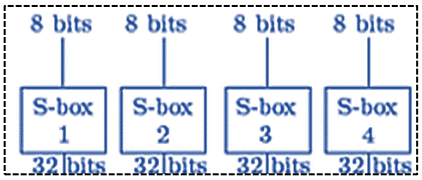

Figure 37 – Blowfish S-boxes

3. **Encryption**, which includes Rounds and Post processing parts.

a) Rounds. The encryption process contains 16 rounds. Every encryption round takes as input the Plaintext from previous iteration (R_i round) and respective subkey P_i.

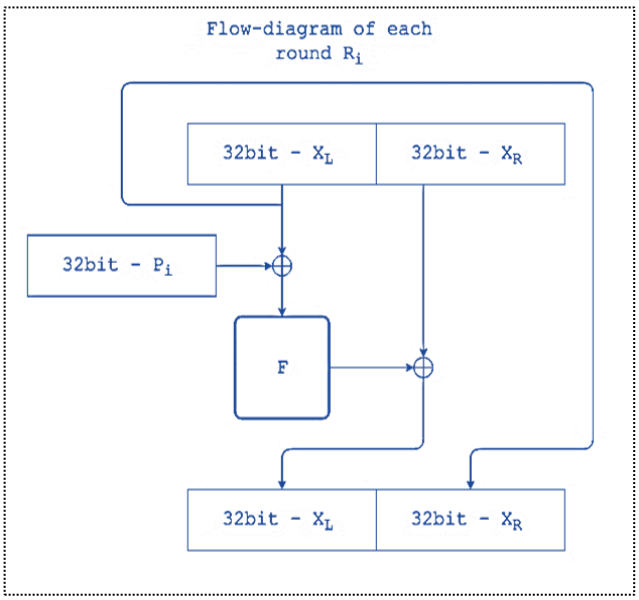

Figure 38 – Description diagram of each encryption round

F - function performs following operations with input block of 32 bit:

- the 32-bit input is splitted into four 8-bit blocks (X_1, X_2, X_3, X_4) and is used as input to the S-boxes. Every x_i is the index of arrays S_1 .... S_4.
- the S-boxes accept 8-bit input and produce 32-bit output.
- the outputs $S_1[X_1]$ and $S_2[X_2]$ are added modulo 2^{32} then are added modulo 2 (XORed) with $S_3[X_3]$ and finally are added modulo 2^{32} with $S_4[X_4]$ to produce the final 32-bit output.

$$F(X_1,X_2,X_3,X_4) = ((((S_1[X_1] + S_2[X_2] \mod 2^{32}) \text{ XOR } S_3[X_3] + S_4[X_4] \mod 2^{32}) \quad (1)$$

On Figure 39 it's described the obtaining process of function F.

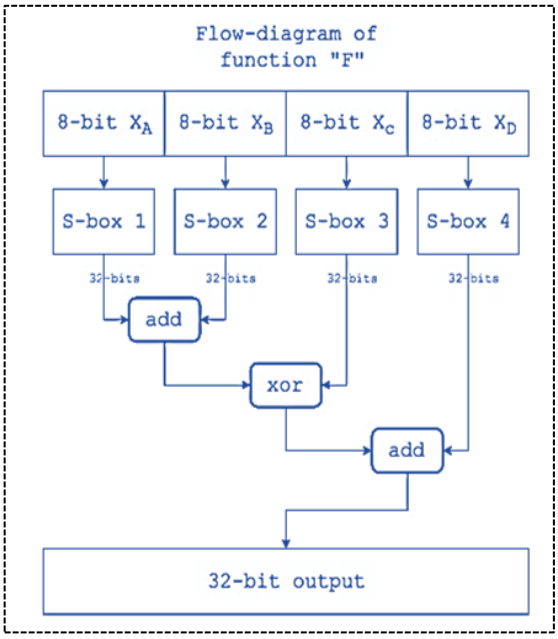

Figure 39 – Description of F-function

b) Post processing parts:

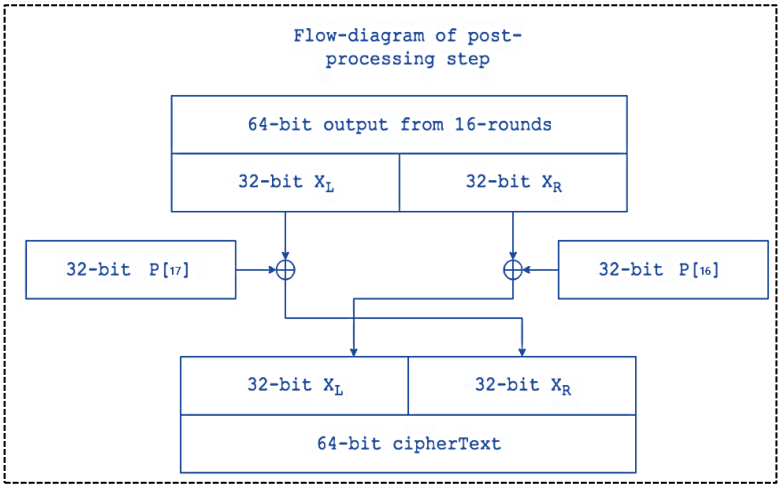

Figure 40 – Description of Post processing

After performing the encryption 16 rounds, X_L and X_R are obtained, and both are 32-bit. The last step is just performing the operations X_L *XOR* P[16] and X_R *XOR* P[17]. Then exchange the X_L and X_R into right and left sides. And finally, it's obtained the 64-bit encrypted text. [18]

Decryption algorithm is the same as encryption one, but subkeys are used in opposite order (P[17] ..... P[0]). This algorithm also has 3 steps. The description block scheme is showed in following figure:

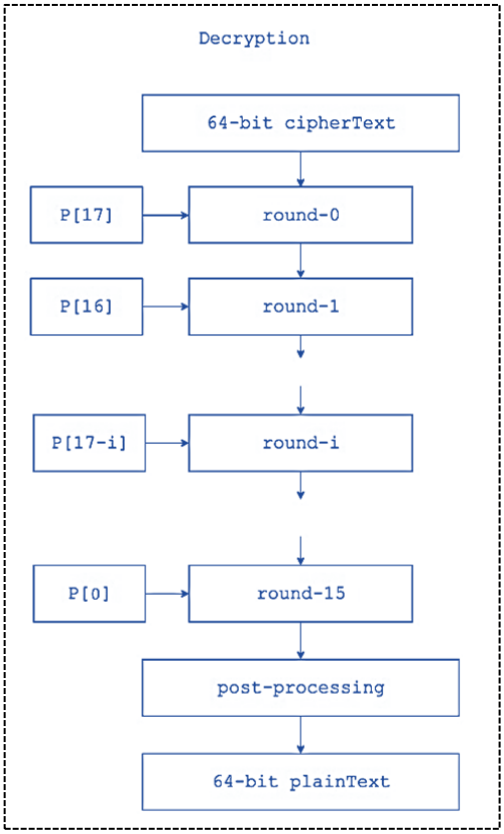

Figure 41 – Decryption algorithm

1) Generation of subkeys P[0] .... P[17]. Here also, for decryption it's used 18 subkeys, which are in P-array. Every element of array is 32-bit digits of π and they are represented in hexadecimal form. Then these subkeys are changed with respect to the input keys like in encryption algorithm.

2) Initializing the Substitution boxes. It has four S – boxes, each of box includes 256 records and each record is 32-bit.

3) Decryption. This process also includes Rounds and Post-processing.

a) The algorithm has 16 rounds. In every round it takes cipher Text of previous round and according subkey P[17], reverse subkey for decryption.

b) Post-process has the same number of rounds and after 16th it's performed the same operation like on encryption, which is described on the following figure.

After performing the decryption 16 rounds, X_L and X_R are obtained, and both are 32-bits. The last step is just performing the operations X_L *XOR* P[0] and X_R *XOR* P[1]. Then exchange the X_L and X_R into right and left sides. And finally, it's obtained the 64-bit decrypted text. [18]

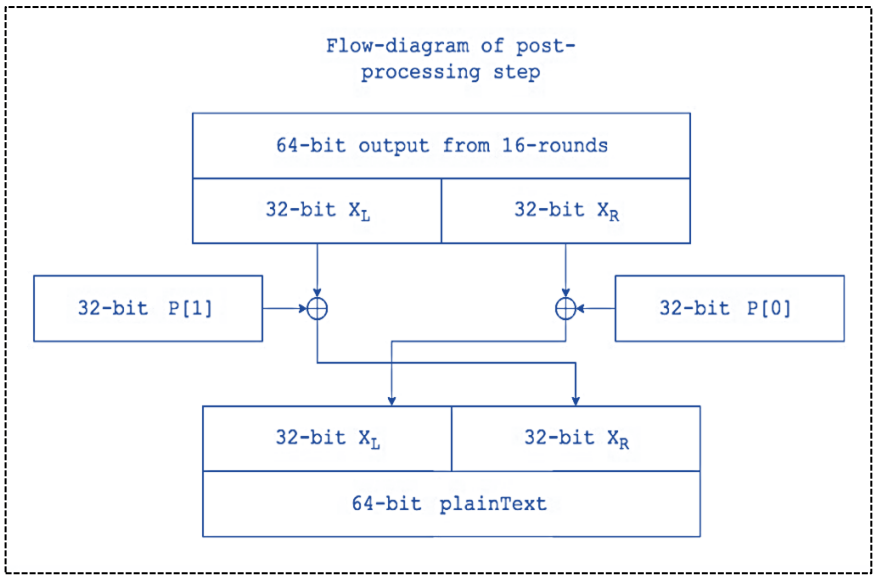

Figure – 42 Post processing of Decryption algorithm

Blowfish algorithm is already done in the form of library (in DLL format) for usage in LabView VI. And there is finished version of the algorithm on a National Instruments forum website. [19] On the basis of this library in the current work I made some modification and used on my project. Implementation the Blowfish algorithm in the application is carried out by using the ready algorithm. After adding the library, the whole project contains the following list of VIs:

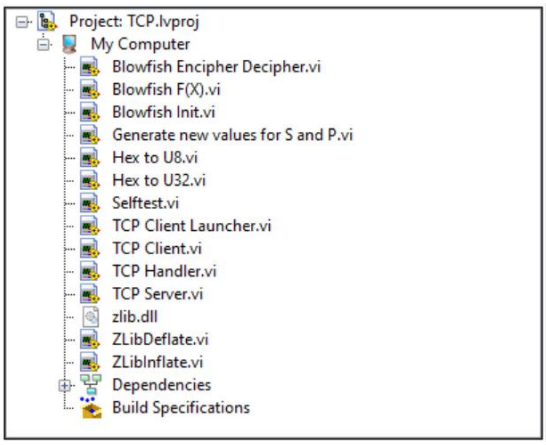

Figure – 43 The list of VIs in the project

The Blowfish algorithm's main block diagram is shown on the following figure:

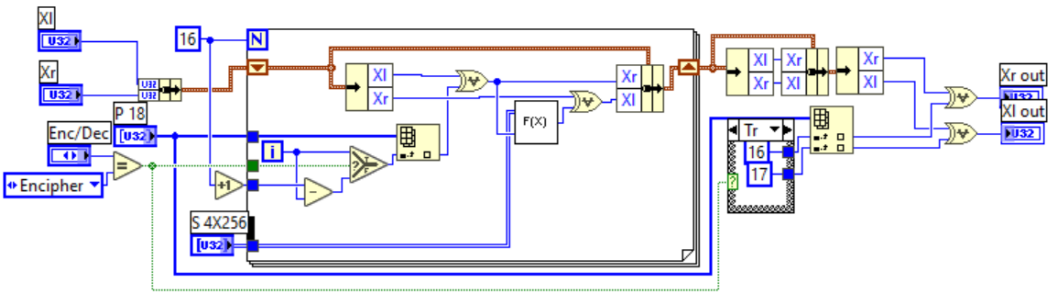

Figure – 44 The Block diagram of Blowfish algorithm

Here is used the F(x) function, which is realised in another VI, it's illustrated below:

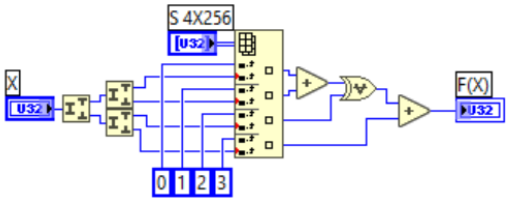

Figure – 45 The Block diagram of F(x) function

The idea of using the algorithm is such as, in the Client VI (transmitting model) of the project it's implemented the algorithm and included between ECG signal generation and Write TCP network function, i.e., generated data is encrypted by algorithm and is sent to the receiver part of the project.

In the receiver part the algorithm is used in the same way, i.e., received data is crypted, we need to decrypt by turning the input of pallet Blowfish into "Decipher" mode.

4.3 Human machine interface

HMI is also one of the important parts of application. It's should include necessary elements of control, convenient elements for information and diagram presenting.

In this software the user works with Client and Handler VIs. The front panel – interface of them illustrated on the Attachments B and C.

The TCP client interface (data sending device) includes the following elements: an ECG signal display window, an ECG signal segment adjustment panel, and windows for displaying encrypted and unencrypted data – a window for the developer. Almost same elements are included on TCP Handler VI interface.

4.4 Illustration of the software performance

This subchapter describes the working results of the software part of the project. As I mentioned on previous chapter the software is created on the idea of multi-client and multi-server. So, it can be created and run multi sensor modules with according to simulated ECG signals and the same number of signals receiving modules. In the following figures I presented them:

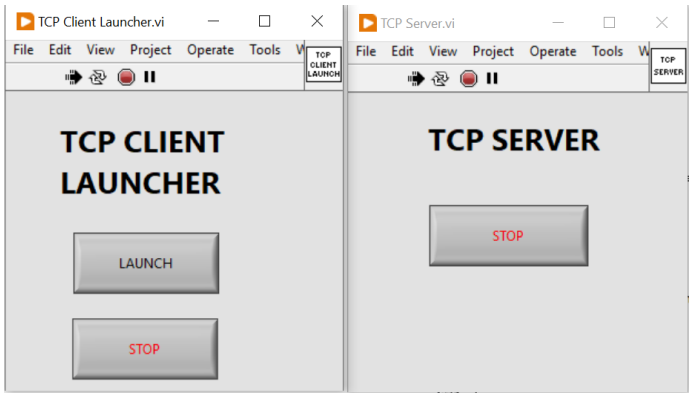

Figure – 46 TCP Client launcher and TCP Server running

After running the TCP Client launcher and TCP Server, it should be clicked the bottom “Launch” to start the simulation ECG data and sending the data to the receiver.

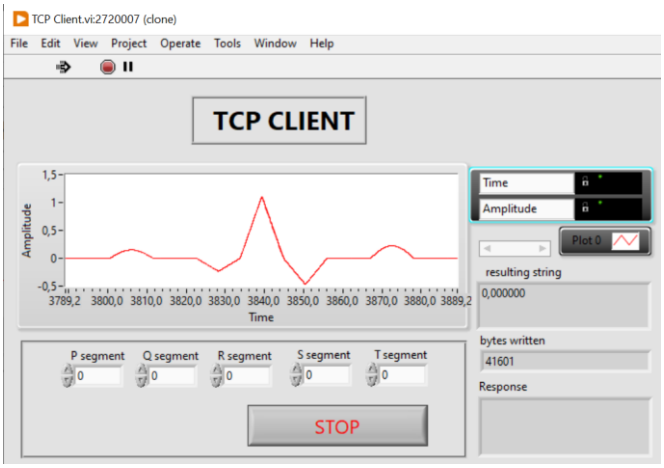

Figure – 47 Simulated and sent data on TCP Client

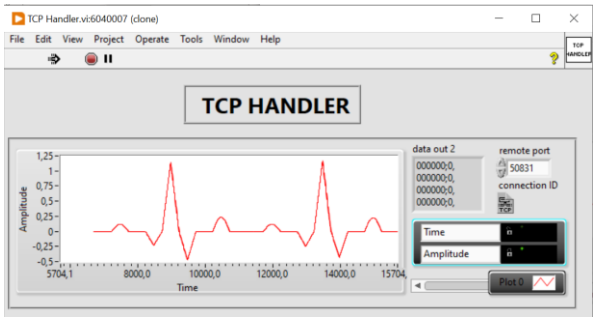

Figure – 48 Received data on TCP Handler

CONCLUSION

In the modern world, medical technologies are developing with high intensity, but this is not enough in front of the problems of modern medicine, because in this area there are several problems and issues that need to be addressed to improve the quality of medicine. One of the needs in medicine is the usage of wireless technologies in patient monitoring, diagnostic equipments for convenience and improvements in the quality of treatment. Since when using wired medical equipment, patients and medical workers are provided with a lot of inconveniences in treatment and restrictions in movement around the medical center. Implementation of wireless technologies in patient health monitoring systems improves the treatment quality and allows patients move freely in whole medical center with sensors, connected to their body.

The current work includes descriptions of the issues of wireless network usage in the monitoring system of patient's condition in wards, intensive care, the operating room, etc. There the problematics of wireless communication in the medical area were presented. And also, it's offered the solutions how to fix these problematics and weaknesses. For communication between sensors data transmitting module and doctor monitor it's used Wi-Fi communication, TCP/IP protocol. On the chapter 2 the scheme of the device is presented and described the main software parts of the project.

In this work in IDE LabView 2021 by a simulation the multi-Client and Server applications are created as SubVIs of the project. The main idea of the project was to focus on the communication between the sensor output data transmitter and the main data collecting monitor of the doctor. The created software combines several SubVIs. The first of them includes sensors output signal generation (patient ECG data) of random behaviour with transmitting device and the second one provides the data receiving, pre-processing, and presenting it in understandable form to the doctor. During the running the software user can launch several data transmitters and receivers to monitor the several ECG health datas at the same time. There are presented several data enciphering algorithms such as Blowfish, AES, Twofish, DEC etc. But because of advantageous of the Blowfish, in this work I presented the further theoretical and programming basis in LabView and shown how to implement the famous and efficient Blowfish encryption/decryption algorithm to secure the health data.

REFERENCES

[1] Patients' health care monitors [online]., [seen 02. 03. 2022]. Novosibirsk: Studopedia, 2019. Available from: https://studopedia.ru/5_145079_monitori-dlya-intensivnogo-nablyudeniya.html.

[2] Reed M. Gardner., M. Michael Shabot., Patient-Monitoring Systems, Philadelphia: W.B. Saunders., 2007.

[3] Health condition data of patient. [online]. [seen 10. 03. 2022]., Available from: https://www.ncbi.nlm.nih.gov/books/NBK216088, 2018

[4] Wikipedia – Oxygen saturation SpO_2 measurement. [seen 10.03.2022]., Available from: https://en.wikipedia.org/wiki/Oxygen_saturation_(medicine), 2020.

[5] Phillips – Wireless Patients Monitor IntelliVue MX40. [online]. Phillips. [seen 11. 03. 2022]., Available from: https://www.usa.philips.com/healthcare/product/HC865350/intellivue-mx40-patient-wearable-monitor

[6] Dragger - Wireless Patients Monitor Infinity Delta. [online]. Dragger. [seen 17. 03. 2022]., Available from: https://www.draeger.com/ru_ru/Products/Infinity-Delta-Series

[7] SOFI, A., J. JANE REGITA, Bhagyesh RANE a Hieng Ho LAU., Structural health monitoring using wireless smart sensor network – An overview. Mechanical Systems and Signal Processing [online]. 2022, 163 [seen 17. 03. 22]. ISSN 08883270. Available from: doi:10.1016/j.ymssp.2021.108113.

[8] Target network – TCP/IP protocol. [seen 20.03.2022]. Available from: https://www.techtarget.com/searchnetworking/definition/TCP-IP., 2019.

[9] Ghilezan A., Hnatiuc M., The ROV communication and control", IEEE 23rd International Symposium for Design and Technology in Electronic Packaging, 2017.

[10] Israa Hashim Latif., Time Evaluation Of Different Cryptography Algorithms Using Labview, IOP Conference Series: Materials Science and Engineering, 2020.

[11] Weidong Liu, Guang Li ,Li'e Gao ,Le Li, Zeyu Li., Monitoring and Communication System Design for A Deep-sea Unmanned Submersible, School of Marine Science and Technology, Northwestern Polytechnical University, 2018.

[12] Tianbing Ma, Fei Du,Chuanzhi Fang., Sensors State Monitoring based on LabVIEW and Wireless Nodes, College of Mechanical Engineering, Anhui University of Science and Technology., 2011.

[13] KUMAR, Pardeep a Hoon-Jae LEE. Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. Sensors [online]. 2012, 12(1), 55-91 [seen 30. 03. 22]. ISSN 1424-8220. Available from: doi:10.3390/s120100055.

[14] Wireless communications in the medical area [online]., Kyiv: Network tool, 2020. [seen 18. 04. 2022]. Available from: https://ntools.com.ua/information/faq/wi-fi-v-klinikakh-bolnitsakh-i-meditsinskikh-tsentrakh.

[15] LabView – Protocol and application control Pallets. [online]., USA: NI LabView, 2021, [seen 20. 04. 2022]. Available from: https://forums.ni.com/t5/Developer-Center-Resources/LabVIEW-Palette-Guidelines/ta-p/3511823.

[16] HAO, Yang a Robert FOSTER. Wireless body sensor networks for health-monitoring applications. Physiological Measurement [online]. 2008, 29(11), R27-R56 [seen 20. 04. 22]. ISSN 0967-3334. Available from: doi:10.1088/0967-3334/29/11/R01.

[17] GANAPATHY, Kirupa, Bharathi PRIYA, Bhanu PRIYA, DHIVYA, V. PRASHANTH a V. VAIDEHI. SOA Framework for Geriatric Remote Health Care Using Wireless Sensor Network. Procedia Computer Science [online]. 2013, 19, 1012-1019 [seen 22. 04. 22]. ISSN 18770509. Available from: doi:10.1016/j.procs.2013.06.141.

[18] Geeksforgeeks – Blowfish encryption algorithm. [online]., 2020, [seen 23. 04. 2022]. Available from: https://www.geeksforgeeks.org/blowfish-algorithm-with-examples.

[19] NI forum – Blowfish encryption algorithm. [online]., 2019, [26. 04. 2022]. Available from: https://forums.ni.com/t5/Example-Code/The-Blowfish-Encryption-Algorithm/ta-3996463

ATTACHMENTS

A – Client-side data sending fragment

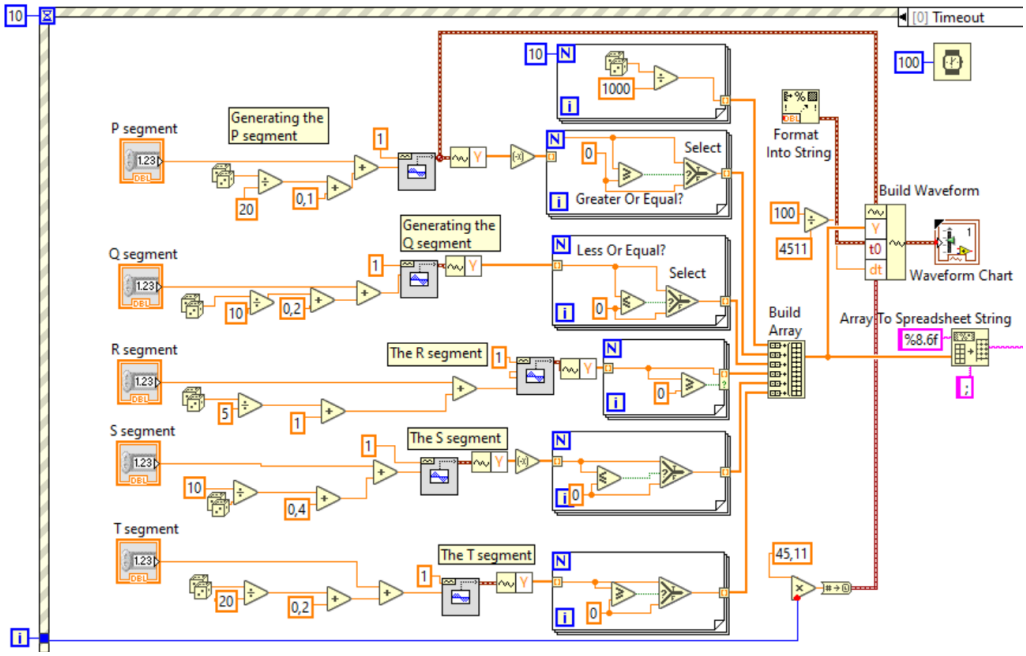

Figure 49 – Data simulation fragment of the device

B – Data receiving fragment of Handler

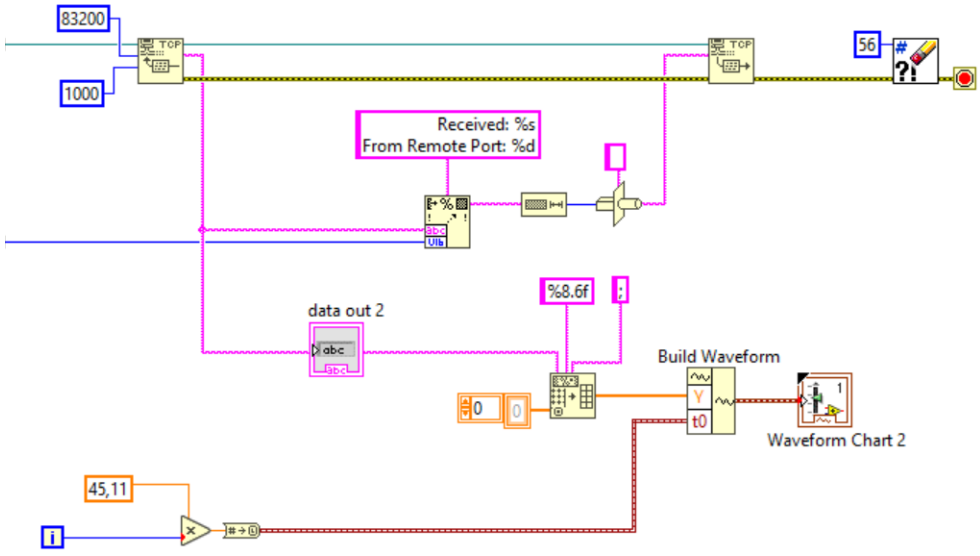

Figure 50 – Data receiving fragment of the device

C - Client-side Interface

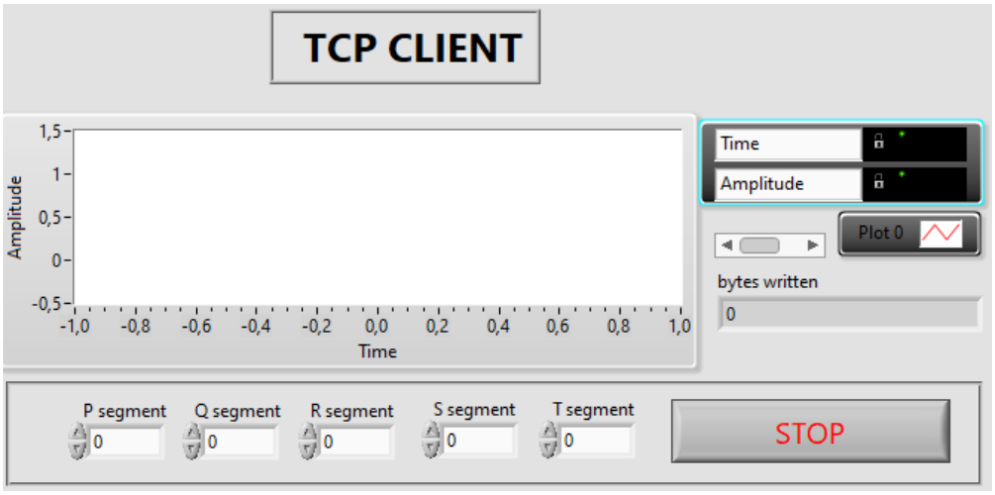

Figure 51 – Interface of data sending device

D – TCP handler interface

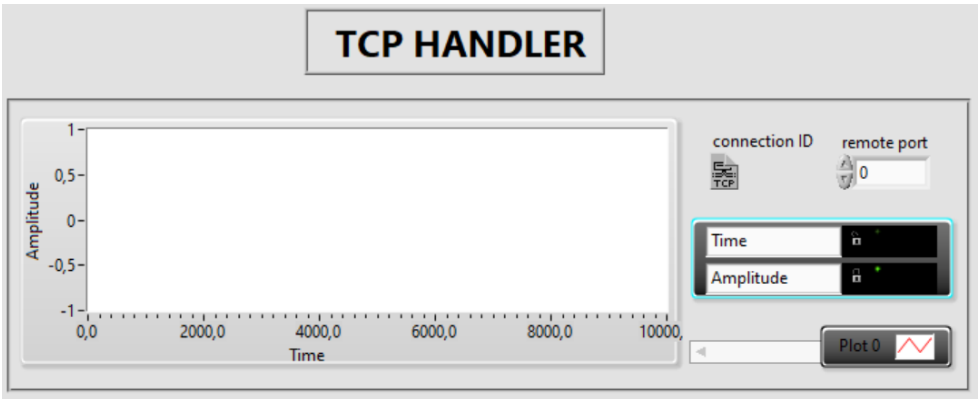

Figure 52 – Interface of data receiving device