A laboratory exercise on 802.15.4 communication between USRP and XBee

Authors:
Boris Kolev
Rob Maunder

Abstract:

The lab studies the IEEE 802.15.4 communication standard for O-QPSK (Offset-Quadrature Phase Shift Keying) modulation and demodulation, implemented on a USRP 2922 (Universal Software Radio Peripheral) and enables the detection of communication between off-the-shelf RF modules working under the 802.15.4 standard, using LabVIEW Communications as the programming environment.

Schedule:

Preparation time	3 hours
Lab time	3 hours
Tools	None
Components	Ethernet cable, MIMO extension cable, 2x RF antennas, 2x FTDI cables
Equipment	2x USRP 2922, 2x XBee S1 (can be any off-the-shelf RF module), 2x Parralax XBee adapters (any RF adapter)
Software	LabVIEW Communications, XCTU

Before you come to the lab, it is essential that you read through this document and complete ***all*** of the preparation work in section 2. Before starting your preparation, read through all sections of these notes so that you are fully aware of what you will have to do in the lab. The marking scheme is shown at the end of the lab notes

1. Aims, Learning Outcomes and Outline

This laboratory exercise aims to:

- Expose you to an actual communication standard and allow you to see how standards are written and implemented in real systems.
- Allow you to get familiar with LabVIEW Communications and see how the program operates.
- Allow you to experience real-life O-QPSK transmission and test the reliability of the transceiver system by observing bit error rate (BER) plots, constellation diagrams and eye diagrams.
- Enable you to analyse how different environments influence the performance of wireless communication systems.
- Allow you to actually implement the wireless system by using real RF modules, which are compliant with the 802.15.4 standard.

Having successfully completed the lab, you will be able to:

- Understand the operation of the USRP module.
- Describe the O-QPSK PHY layer of the 802.15.4 communication standard.
- Analyse transmission data between a transceiver system and actual RF modules.
- Understand how changing different parameters of a wireless system affect the actual signal and analyse BER plots.

2. Preparation

Read through this document so you are aware of what you will be expected to do in the lab.

2.1.Preparation Section 1

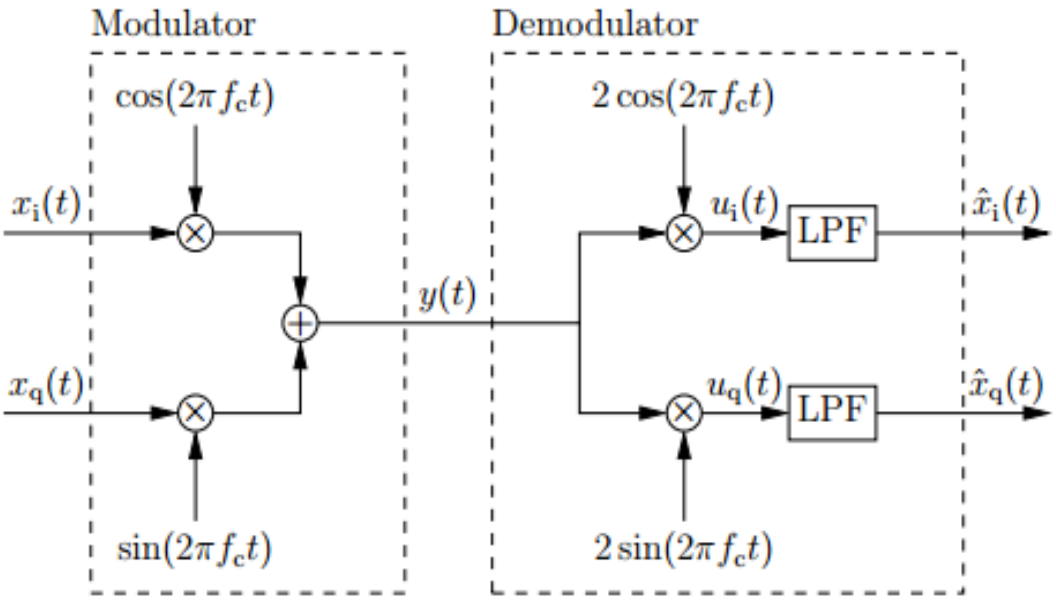

Figure 1. QAM signal processing.

Go to https://www.ni.com/white-paper/12985/en/ and look through the notes for the USRP device and then answer the following questions:

- Task 1: By inspecting Figure 2 from the link provided, briefly comment on the hardware components of the USRP. From this figure, it can be seen that the signal is divided into I and Q phases and is then processed. Relate the signal processing to the QAM modulation/demodulation shown in Figure 1.

Answer:
The USRP implies a common architecture for software-defined radios. It combines direct conversion analog front end with ADCs and DACs. The FPGA is used for the digital down conversion (DDC) and digital upconversion (DUC). When receiving the signal reaches a highly sensitive analog front end, which can receive very small signals, and digitizes it using DDC to In-Phase (I) and Quadrature (Q) baseband signals. From this point, ADC is carried out followed by a DDC, which reduces the sampling rate and packetizes I and Q for transmission over an Ethernet cable. When transmitting from the host PC, where I and Q are generated and transferred over the Ethernet cable. Here a DUC sets up the DAC after which I-Q mixing occurs to directly up-convert the signal and produce the RF signal, which is amplified and transmitted.

The USRP transceiver device follows a simple signal processing structure. The modulated complex values is separated into I - $x_i(t)$ and Q - $x_q(t)$ phases → multiplied by $\cos(2\pi f_c t)$ and $\sin(2\pi f_c t)$ respectively and then summed up to obtain $y(t) = x_i(t)\cos(2\pi f_c t) + x_q(t)\sin(2\pi f_c t)$ → multiplied by $2\cos(2\pi f_c t)$ and $2\sin(2\pi f_c t)$ respectively, to obtain $u_i(t) = 2x_i(t)\cos(2\pi f_c t)\cos(2\pi f_c t) + 2x_q(t)\sin(2\pi f_c t)\cos(2\pi f_c t)$ and $u_q(t) = 2x_q(t)\sin(2\pi f_c t)\sin(2\pi f_c t) + 2x_i(t)\cos(2\pi f_c t)\sin(2\pi f_c t)$ → using the trigonometric identity $2\cos(x)\cos(x) = 1 + \cos(2x)$, $2\sin(x)\sin(x) = 1 - \cos(2x)$ and $2\cos(x)\sin(x) = \sin(2x)$ to obtain $u_i(t) = x_i(t) + x_i(t)\cos(4\pi f_c t) + x_q(t)\sin(4\pi f_c t)$ and $u_q(t) = x_q(t) - x_q(t)\cos(4\pi f_c t) + x_i(t)\sin(4\pi f_c t)$ → Low Pass Filter the signal in order to remove the out of band frequency components ($4\pi f_c t$) which leaves $\widetilde{x_i(t)} = x_i(t)$ and $\widetilde{x_q(t)} = x_q(t)$.

2.2.Preparation Section 2

Go to https://standards.ieee.org/getieee802/download/802.15.4-2011.pdf and download the standard. Read sections 1, 8, 9 and 10 in order to answer the following questions:

- Task 2: Which communication layers does the 802.15.4 standard define? What are the applications for the 802.15.4 standard?

Answer:

This standard is used to define the physical layer (PHY), which represents the radio transceiver, and medium access control (MAC) sublayer characteristics for low-data-rate wireless communications system. The IEEE 802.15.4 network operates devices in the Personal Operating Space (POS), which have the same radio channel and form as the so-called LR-WPAN. These networks provide low-data rate, low-cost and short distance (around 15m radius) communication.

- Task 3: Name the blocks of the O-QPSK PHY modulation from the 802.15.4 standard. What is the data rate when operating in the 2,450 MHz band? How many chips/second are needed in order to obtain such a data rate?

Answer:

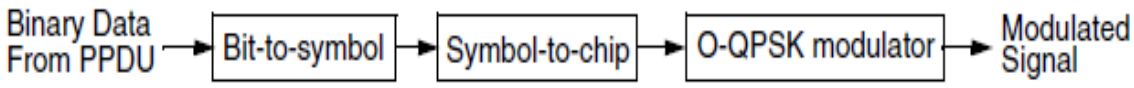

Figure 2. Modulated signal generation.

The data rate shall be 250 kb/s when operating in the 2450 MHz band. The chips per second values are obtained from the IEEE 802.15.4 standard – 250 kbps with every 4 bits of PPDU being converted to 32-length symbols leads to a chip rate of 2,000,000. This value must be constant meaning that $\frac{samples/second}{samples/chip} = 2\,000\,000\ chips/seconds$.

- Task 4: Show how the O-QPSK PPDU packet structure is formatted. How many bits form each octet field? How are the bits transmitted – LSB or MSB first?

Answer:

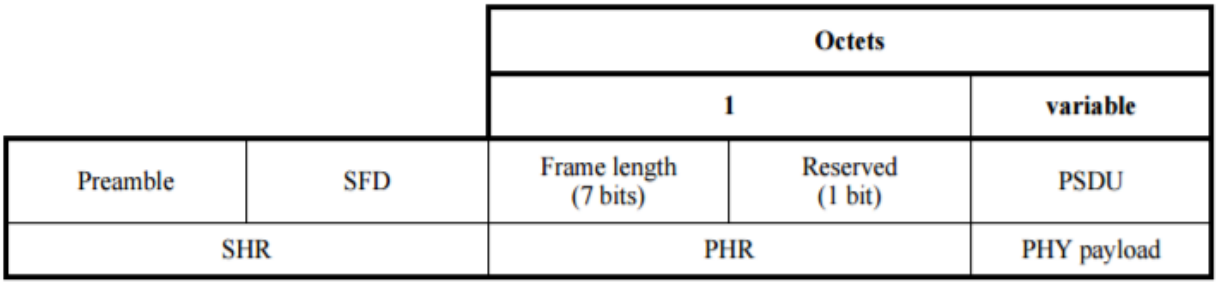

Figure 3. Format of the PPDU packet structure.

The PPDU packet structure is comprised of several fields. Each octet field is represented by 8 bits or 1 byte. The structure is made in such a way that the leftmost field is received or transmitted first. All multiple octet (byte) fields are transmitted or received least significant octet first and each octet will be transmitted or received least significant (LSB) first.

- Task 5: Explain the structure of the Preamble field.

Answer:
This field is used for obtaining the chip and symbol synchronization within a message and has 4 octets each of which contains 8 bits which equal 32 bits of all zero bits.

- Task 6: The SFD is 0xA7 (MSB first) in hexadecimal. Transform it into binary and state the order that the bits are transmitted according to your answer in Task 4?

Answer:
0xA7 (MSB first) → 10100111 but LSB is first so it will be transmitted → 11100101.

- Task 7: How many bits are used to represent the frame length of the PHR field? What does it quantify?

Answer:
The frame length field is 7 bits and is used to specify the total number of octets contained in the payload.

- Task 8: What is the maximum PHY payload size (Hint: Look up Table 70 in the standard)? What are the acceptable values for the size of the PHY payload (Hint: Look up Table 72 in the standard)? What conditions should the PHY payload meet according to your answer in Task 4?

Answer:
Maximum PHY packet is 127 and is represented in octets. The range is 9 to 127 octets or 72 to 1016 bits. The PHY input has to be divisible by 8 in bits form to meet the octet range requirement.

- Task 9: Draw a Constellation diagram of O-QPSK and QPSK signals and illustrate the valid transitions between successive constellation points.

Answer:

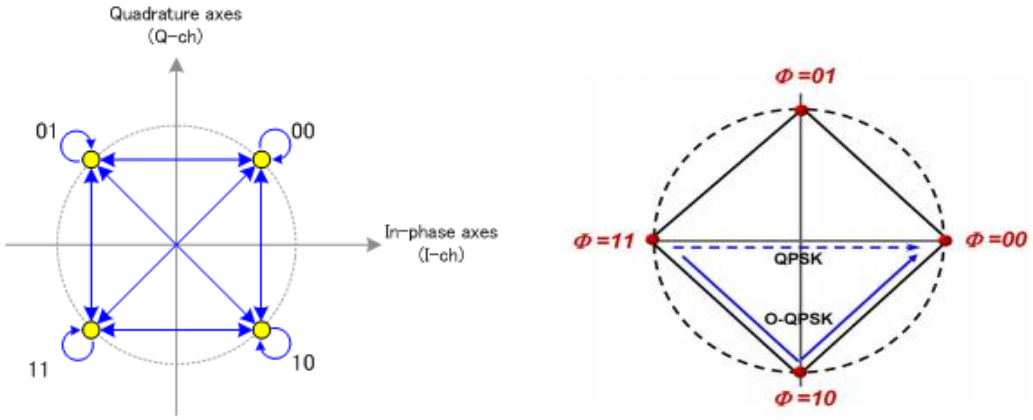

Figure 4. QPSK and O-QPSK constellation - 1) QPSK 2) O-QPSK.

- Task 10: Explain the bits-to-chips mapping procedure in the 802.15.4 standard. Give an example of an actual bits-to-chips mapping if the inputted bits are 1100 (Hint: Look up Table 73 from the standard).

Answer:
Firstly, the bits will be mapped to data symbols in the way that the 4 LSBs (b0, b1, b2, b3) of each octet are mapped to one data symbol, where b0 is the least significant bit, and then the 4 MSBs (b4, b5, b6, b7) are mapped to the next data symbol. This is done by converting the binary numbers into decimals in the range 0-15. The LSBs are processed first and the MSBs are processed second. Afterwards, for the 2450 MHz band, every one of the data symbols will be mapped to a 32-chip PN sequence in such a way that the PN sequences are all related. 1100 → 00000111011110111000110010010110.

- Task 11: Which chips are modulated to the I-phase and which to the Q-phase? How is the offset (Tc) in O-QPSK formed according to the 802.15.4 standard (Hint: Look at Figure 70 in the standard)? What does Tc represent?

Answer:
The even chips are modulated onto the in-phase and the odd chips go to the quadrature phase. Now, in order to form the offset, the Q-phase is delayed by T_c with respect to the I-phase. T_c is the inverse of the chip rate which is 32 times the symbol rate.

- Task 12: Redraw Figure 71 from the standard into your logbooks. What is the sequence

of four bits that is represented by this 32-chip sequence (Hint: Look at Figure 70 in the standard)?

Answer:

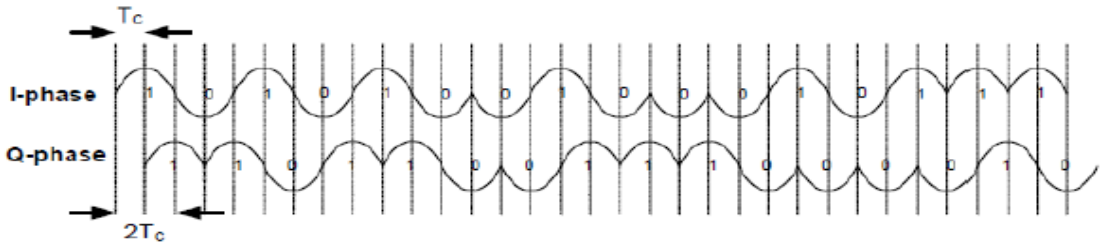

Figure 5. The waveform figure from the standard.

The 32-chip sequence is 11011001110000110101001000101110, which represents the zero data symbol → 0000.

- Task 13: Write the bit sequence of the whole PPDU packet structure if the PHY payload is 9 octets (72 bits) long.

Answer:
An example of a PPDU can be the following 00000000000000000000000000000000 (Preamble) 11100101 (SFD) 00000010 (8-bit PHR with a reserved 0-bit) 10...01 (PHY data packet which has a length of 9 octets).

2.3.Preparation section 3

Go to:

- https://www.researchgate.net/publication/224281039_Performance_Evaluation_of_IEEE_802154_Physical_Layer_Using_MatLabSimulink
- https://en.wikipedia.org/wiki/Carrier_frequency_offset

From these documents read on how changing different parameters of the transceiver system affects the quality and BER of the signal.

- Task 14: What happens to the BER performance when the SNR is increased?

Answer:
The higher the Eb/N0 ratio, the less the transmitted signal is affected by noise. This leads to a small error probability thus increasing the BER performance.

- Task 15: What does the carrier frequency offset represent and which two important factors attribute to this phenomenon? How does it affect the signal?

Answer:
The carrier frequency offset represents the difference between transmitting and receiving frequency. This phenomenon can be attributed to two important factors: frequency mismatch in the transmitter and the receiver oscillators; and the Doppler effect as

the transmitter or the receiver is moving. It has the same effect on the signal as multiplying it by a sinusoid with a phase offset equalling the carrier frequency offset, which will lead to a shift in frequency in the received signal.

- Task 16: Does changing the bits/symbol or samples/chip value affect the BER results?

Answer:
The more samples or bits generated, the less the signal is affected by the channel conditions. This is so because when more samples are generated from the modulator, more complex values are received by the demodulator for a more precise restoring of the PHY payload.

3. Lab work

In this laboratory exercise, you will observe an O-QPSK transceiver system, which operates under the IEEE 802.15.4 standard and will be able to compare your practical work by doing simulations on a simulator, which tests the reliability of the system. Finally, as part of the additional work you will test the system by using actual off-the-shelf RF modules and observe how they communicate between each other.

In order to begin, set up the USRP modules as shown in Figure 6, which is an example of how the system can be set-up.

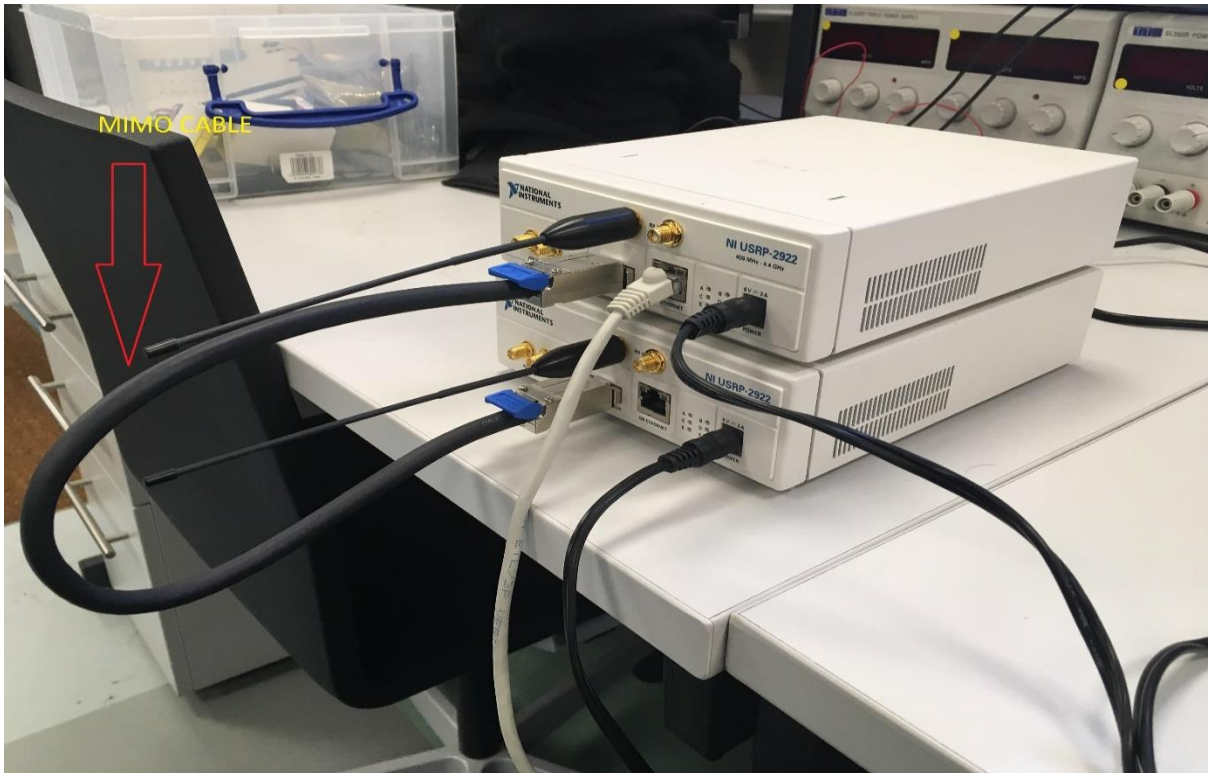

Figure 6. Transceiver USRP set-up.

In this picture, the Ethernet cable is directly connected to the PC. In order to test if the USRP devices are correctly use the NI-USRP Configuration Utility. After finishing the USRP module set-up, open the O-QPSK.lvproject file provided in the folder for this lab, in order to load the transceiver application. Do not forget to press the LabVIEW run button in order to execute the VIs.

3.1.Transceiver testing

After loading the O-QPSK LabVIEW project, open the O-QPSK Tx component, which represents the UI of the transmitter module. You are encouraged to go through the block diagram of the component to get familiar with the way it transmits data. Figure 7 shows the module.

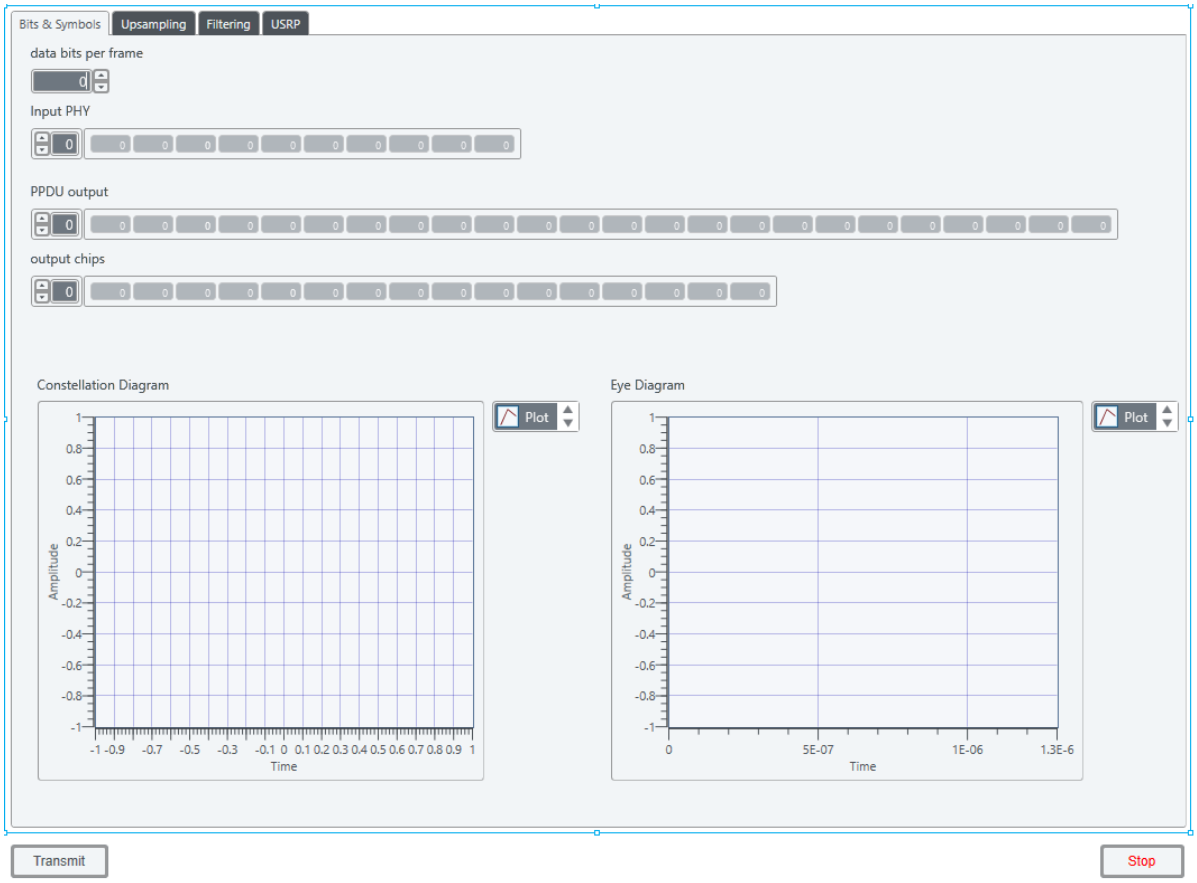

Figure 7. Transmitter UI.

Go through all the tabs in order to see what parameters you can specify before starting the transmission.

- Task 1: What is the allowed range for the data bits per frame field? Try inputting 70, 150 and 1500 and pressing Transmit. What do you observe? Why does 150 give an error?

Answer:

The allowed range is 72 to 1016. When 70 is inputted the following error message should

be obtained:

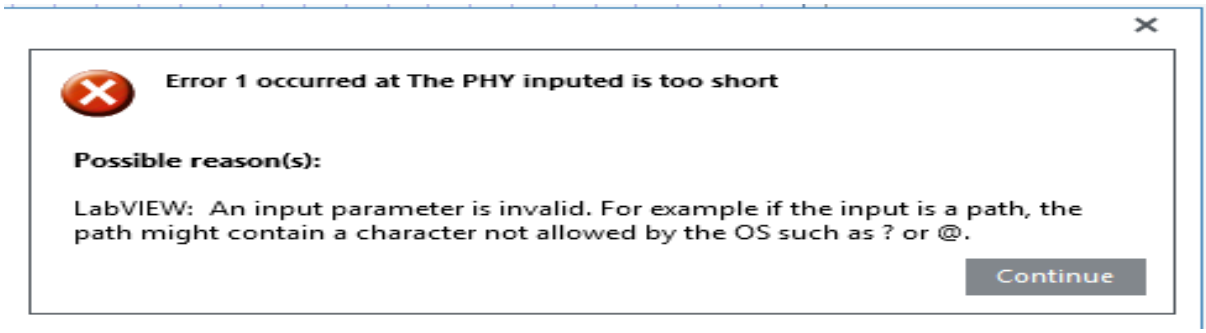

Figure 8. PHY payload is too short error message.

For 150: The PHY packet is in octets, which means that the value should be divisible by 8.

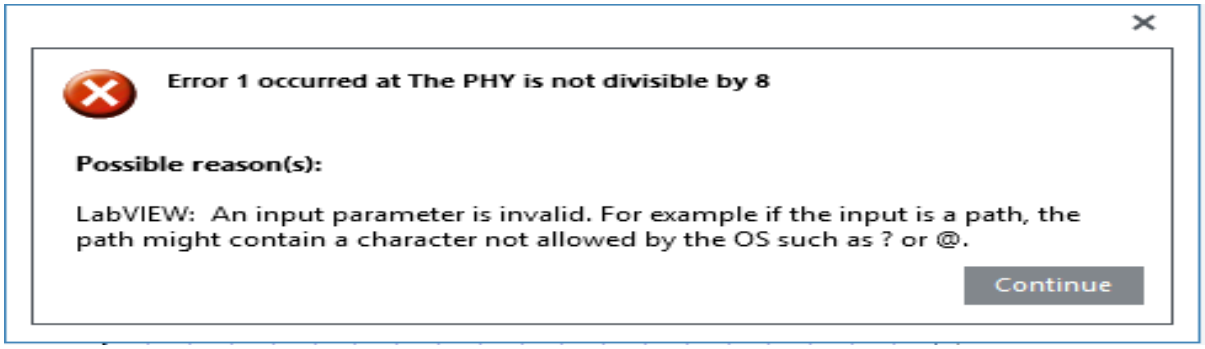

Figure 9. PHY payload is not divisible by 8.

For 1500:

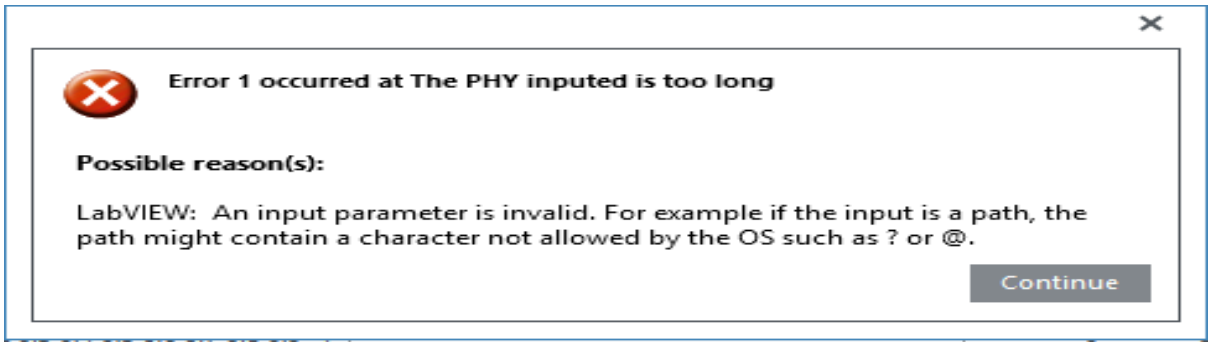

Figure 10. PHY payload is too long error message.

- Task 2: What should the chip rate be in order to obtain a data rate of 250 kbps depending on your preparation answers?

Answer:

The chips per second values are obtained from the IEEE 802.15.4 standard – 250 kbps with every 4 bits of PPDU being converted to 32-length symbols leads to a chip rate of 2,000,000.

Select 2 samples/second and 4 000 000 samples/chip and set the carrier frequency to 2.405 GHz. Set the data bits to 512.

- Task 3: Screenshot what you obtain after running the VI?

Answer:

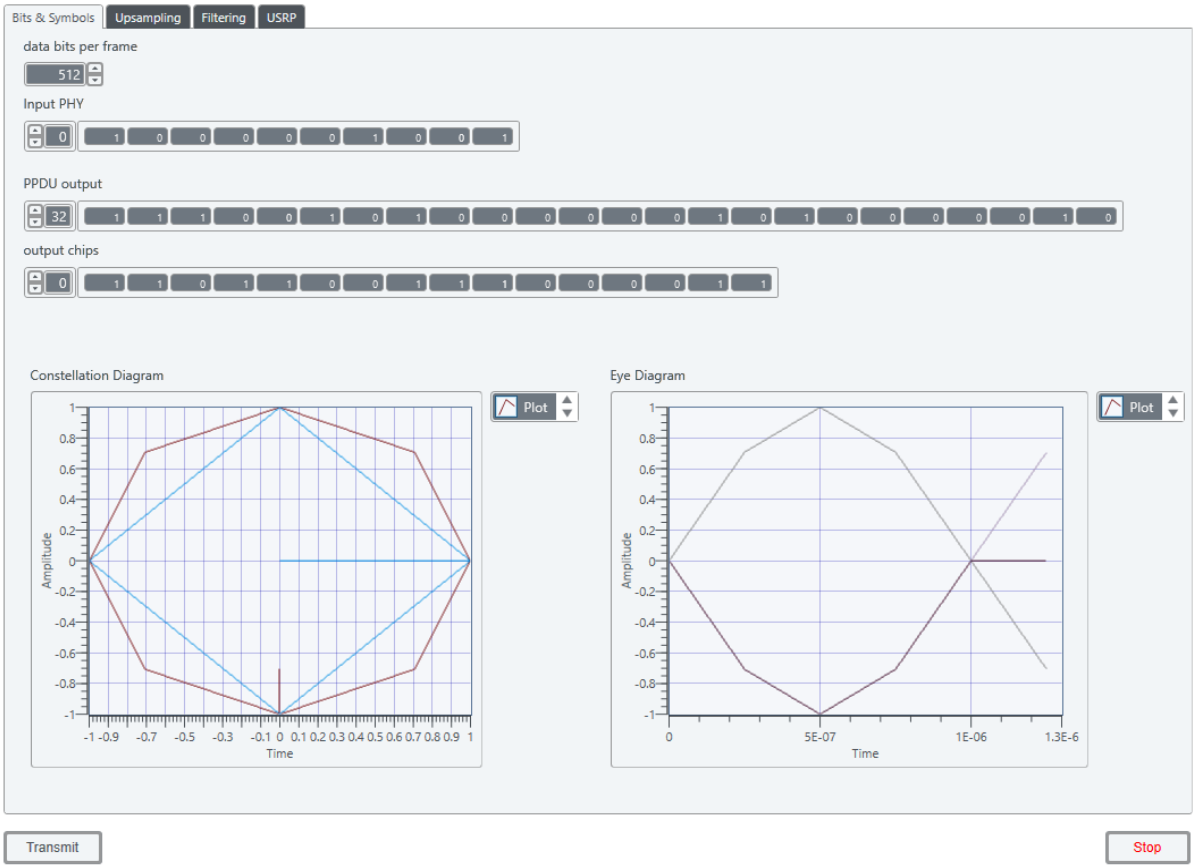

Figure 11. Front panel transmitter visualization.

- Task 4: Look at the PPDU output and explain its structure. Which parts of the LabVIEW code corresponds to which parts of the 802.15.4 standard.

Answer:

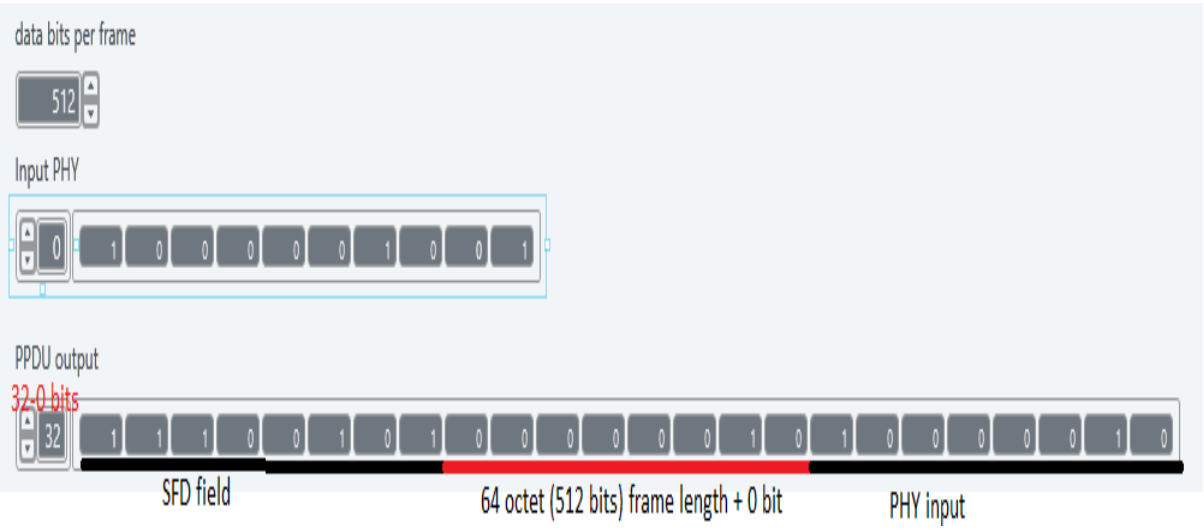

Figure 12. PPDU output generation front panel visualization.

Go to the block diagram of the transmitter module (Figure 13) and double click on Modulation VI. You should see the following screen:

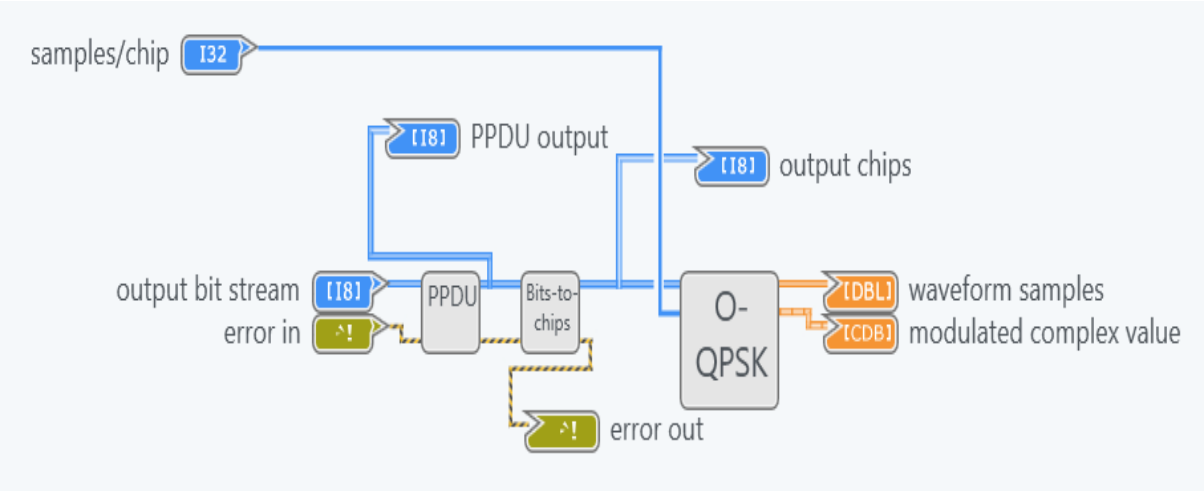

Figure 13. O-QPSK Modulation components.

Double click on the bits-to-chips mapping VI and open its front panel. From the 802.15.4 standard document, you read about how bits are mapped to chips and observed a table, which contained the chip values for the 2.4 GHz O-QPSK modulation scheme.

- Task 5: With regards to that table input the symbol 12 (1100) in binary and observe the chip sequence (Hint: Do you need to input the bits LSB first or MSB first?).

Answer:
The inputs have to be entered LSB first.

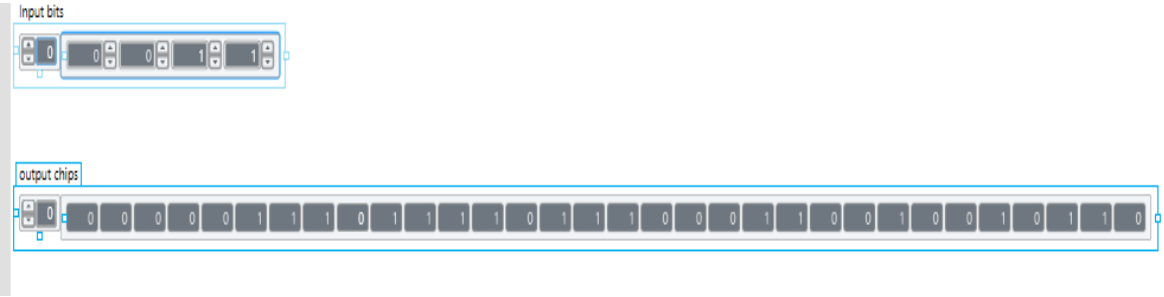

Figure 14. Correctly outputted chip sequence.

Now go back to the modulation block diagram (Figure 13) an open the O-QPSK VI's front panel. Input a sample/chip value and enter the waveform chip sequence from section 2.2 as input chips.

- Task 6: Screenshot your observations? Show the delay Tc between the I and Q phases.

Answer:

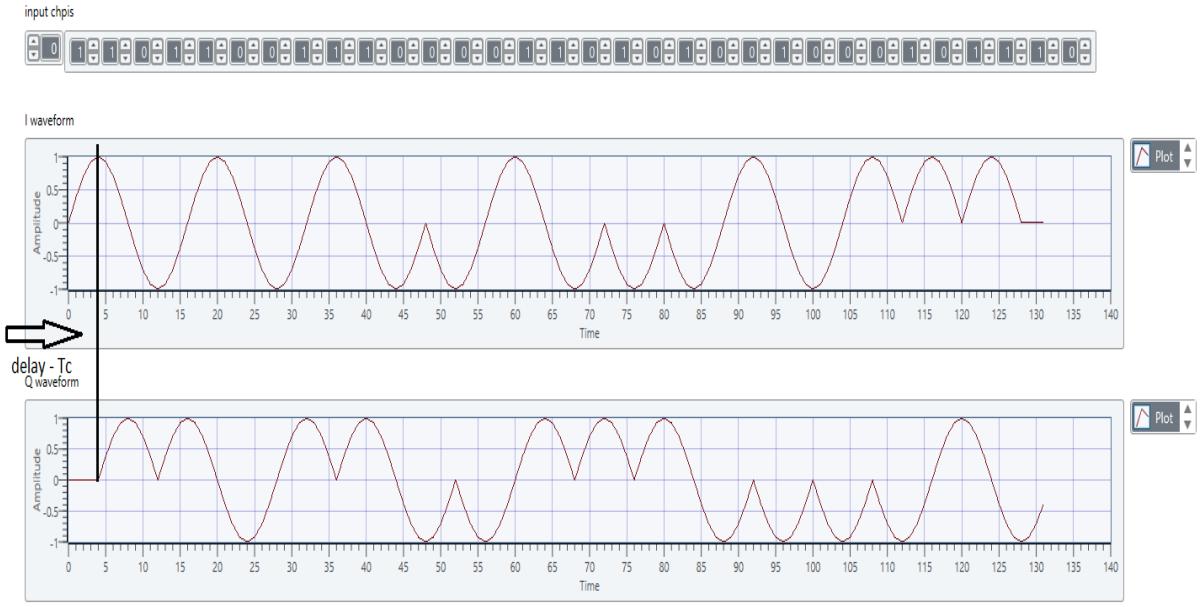

Figure 15. I and Q waveforms and the delay Tc.

Now go back to the front panel of the Transmitter (Figure 7) and press the transmit button.

- Task 7: By observing the eye and constellation diagram what, can you conclude about the transmitter? Screenshot your results.

Answer:

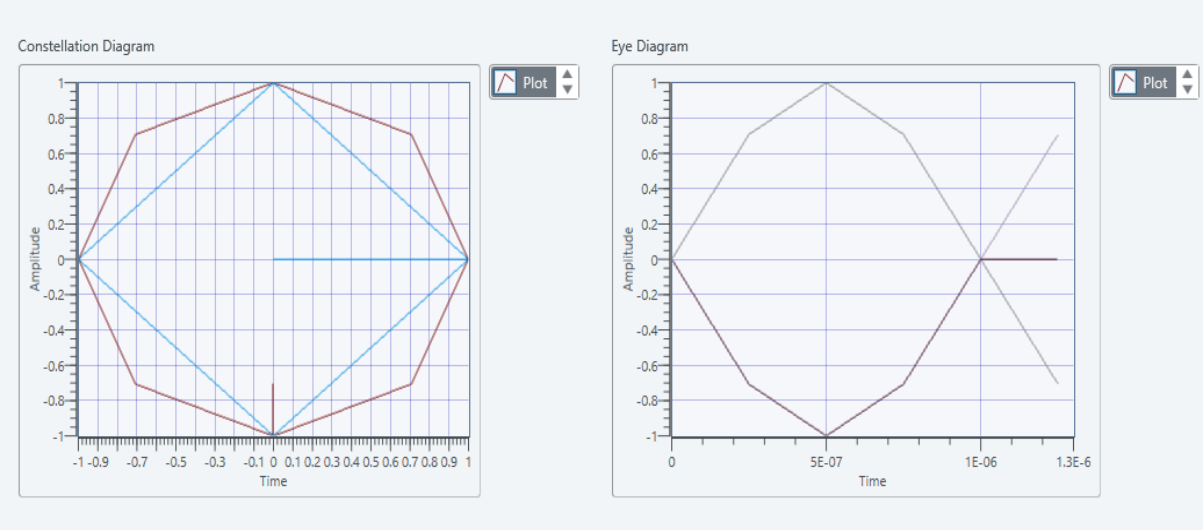

Figure 16. Eye and Constellation diagrams.

From these results, it can be seen that the constellation diagram correctly represents the O-QPSK modulated signal and that the transition between two diagonally opposite phases passes through an intermediate phase removing the ±180º phase shift as described

in the preparation. The eye diagram is a "perfect" open eye showing that the transmitted data follows the constellation circle.

Now open the O-QPSK Rx module from the project files. Set the USRP settings to be the same as the transmitter ones. Play around with the value of the threshold sample magnitude until you reach a value that allows the receiver to only detect a signal when the Transmit button on the transmitter is pressed (Hint: 0.001 should be a suitable value).

- Task 8: Observe the receiver's front panel. Screenshot your observations and comment on them.

Answer:
By inspecting Figure 17 it can be seen that the receiver correctly demodulates the transmitted data. The signal detected? (1) Boolean lights up when the data is transmitted. It can be seen that the waveforms of both the I and Q phases of the received SHR are similar to the original samples They are not exactly identical due to the fact that the transceiver is being subject to changing channel environments. When the input and output PHY (3) and are compared it can be seen that the values are identical and match the input PHY. Finally, by observing the BER result (4), which is 0, it can be concluded that the receiver can successfully receive signals from the USRP transceiver device.

Figure 17. Front panel of receiver.

3.2.Simulator testing

Now open the Simulator file from the O-QPSK project. Observe all the different parameters and set the data bets to 512, the Eb/N0 offset to 5, samples/symbol to 2, samples per second to 4 000 000, carrier frequency offset to 0, no fading profile. Initially set the minimal error value to 300 in order to obtain a smoother BER plot but in order to save time use a value of 10 for the next questions. Take note of the av. BER value!

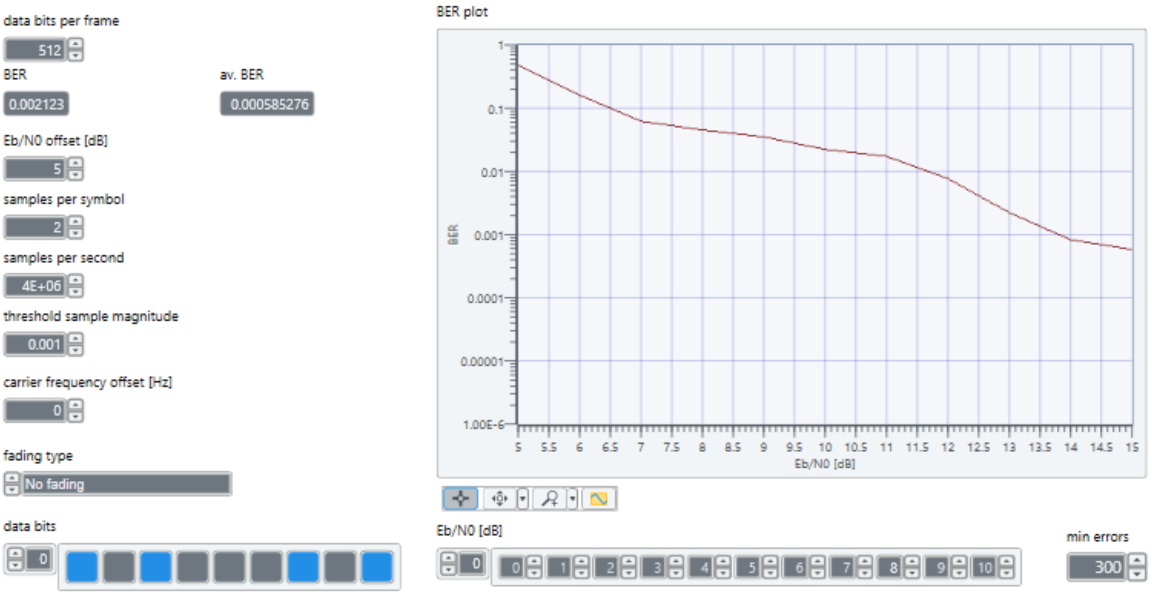

Figure 18. Simulator testing.

- Task 9: Change the values of the samples per symbol to 3 and the samples per second to 6,000,000. Screenshot your results. Now change the values to 4 and 8,000,000 respectively. Record your results. Why does the BER improve as the sample values are increased (Hint: compare the av. BER values)?

Answer:

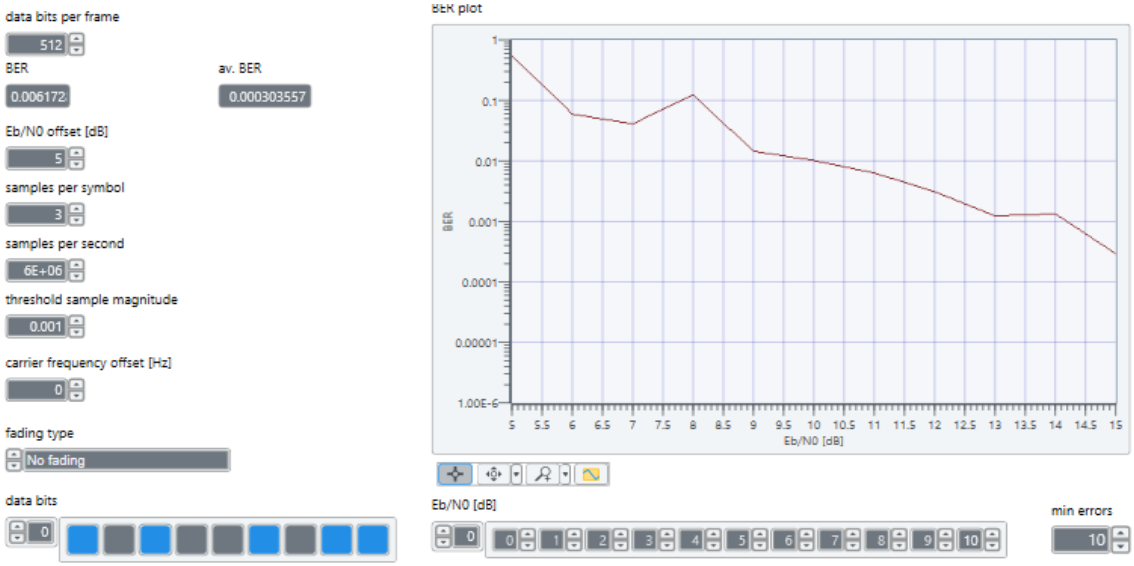

Figure 19. BER results with 3 samples/symbol.

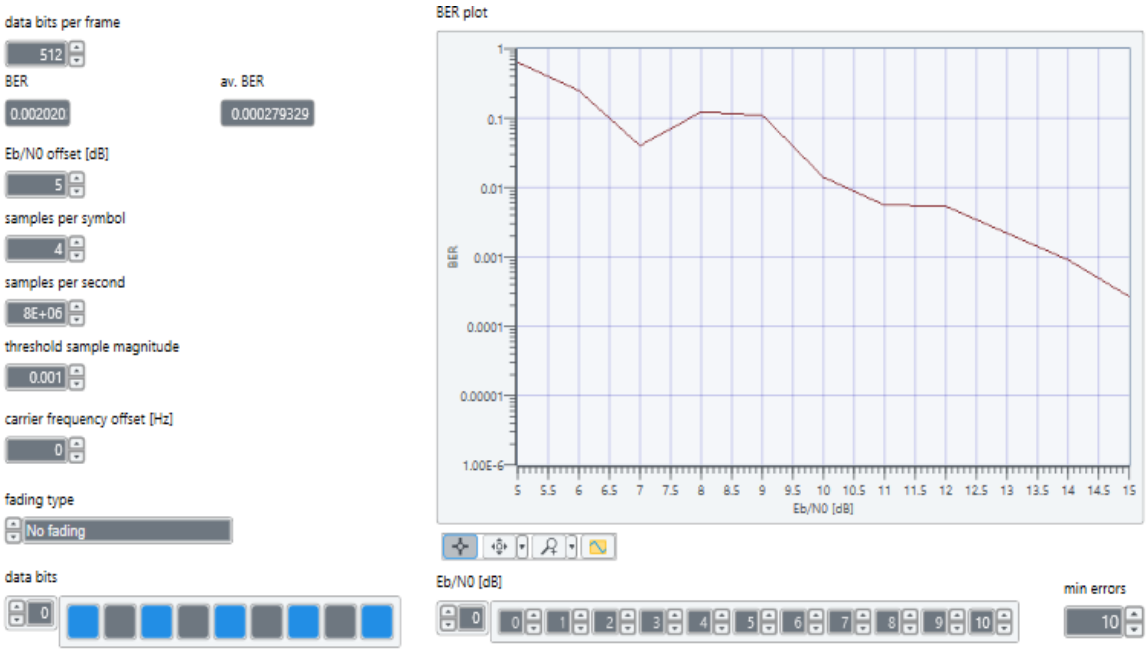

Figure 20. BER results with 4 samples/symbol.

It can be seen that the more samples generated, the less the signal is affected by the channel conditions. This is so because when more samples are generated from the modulator, more complex values are received by the demodulator for a more precise restoring of the PHY payload and thus resulting in an improved BER performance.

- Task 10: Change the value of the Carrier Frequency Offset to 3000 Hz and 3,500 Hz. Run the simulation and record your observations. Why does the 3,500 Hz CFO distort the signal?

Answer:

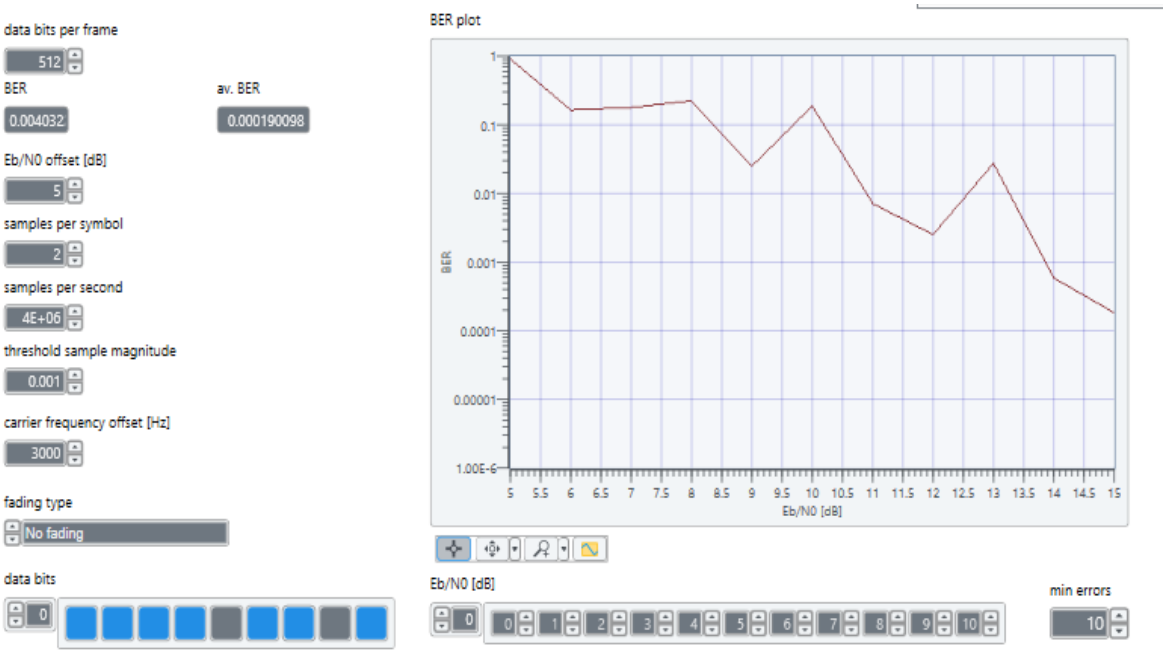

Figure 21. BER results with a CFO of 3,000 Hz.

Figure 22. BER results with a CFO of 3,500 Hz

As the CFO increases the phase shift of the sinusoid with which the signal is multiplied increases thus resulting in a difference between the transmitted and the received data.

- Task 11: Change the fading types to uncorrelated narrowband and to block narrowband Rayleigh fading. Record your observations.

Answer:

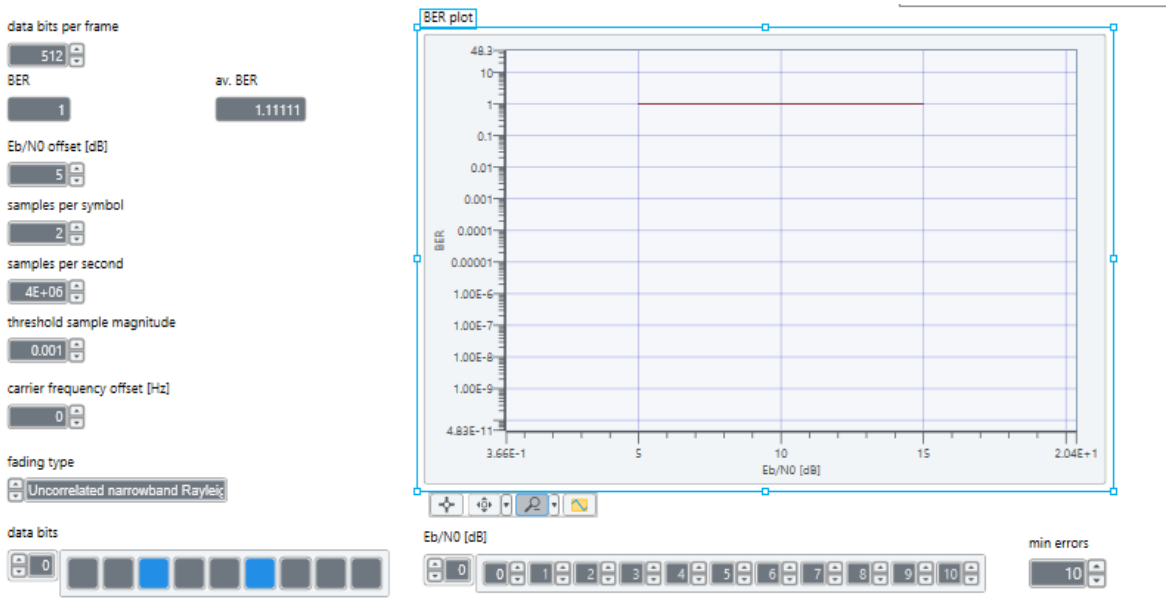

Figure 23. BER results with uncorrelated narrowband Rayleigh fading.

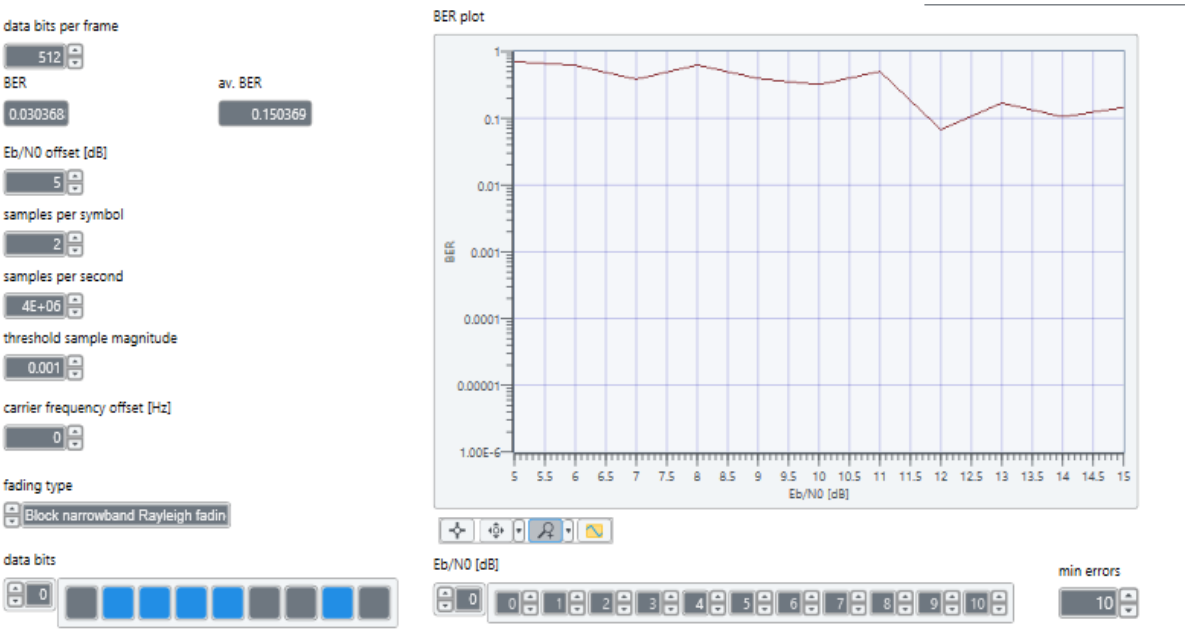

Figure 24. BER results with Block narrowband Rayleigh fading.

3.3.Actual RF module testing

After testing the transceiver system you will now work with actual RF modules and try to detect communication between them. For this case XBee modules will be investigated together with serial to USB adapters and FTDI cables. XCTU is used in order to interface the XBees and the PC.

3.3.1. XBee set-up

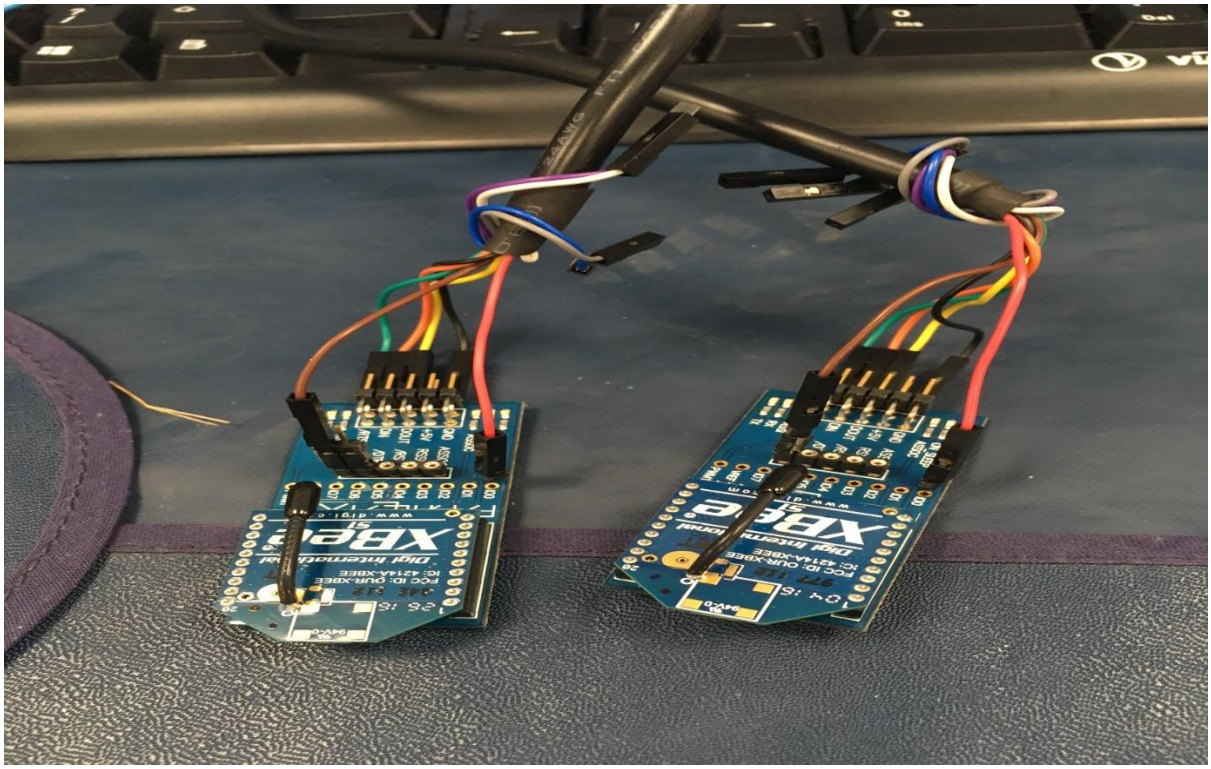

Figure 25. XBee set-up.

Figure 25 shows the set-up of the connection between the XBee devices and the PC. The modules are connected to the PC via FTDI cables (1). The FTDI cables have 10 wires for serial connection each serving a different purpose. For this project, only 6 of them are needed:

- GND (black) – Device ground supply pin.
- POWER (red) – Power output which can be customized to output +3.3V or +5V.
- RTS (green) – Request to send control output (Handshake signal).
- CTS (brown) – Clear to send control output (Handshake signal).
- TXD (orange) – Transmit synchronous data.
- RXD (yellow) – Receive synchronous data.

The XBees are connected to FTDI cables via adapters (2), which have the same pin set-up and serve as a convenient interface for the modules.

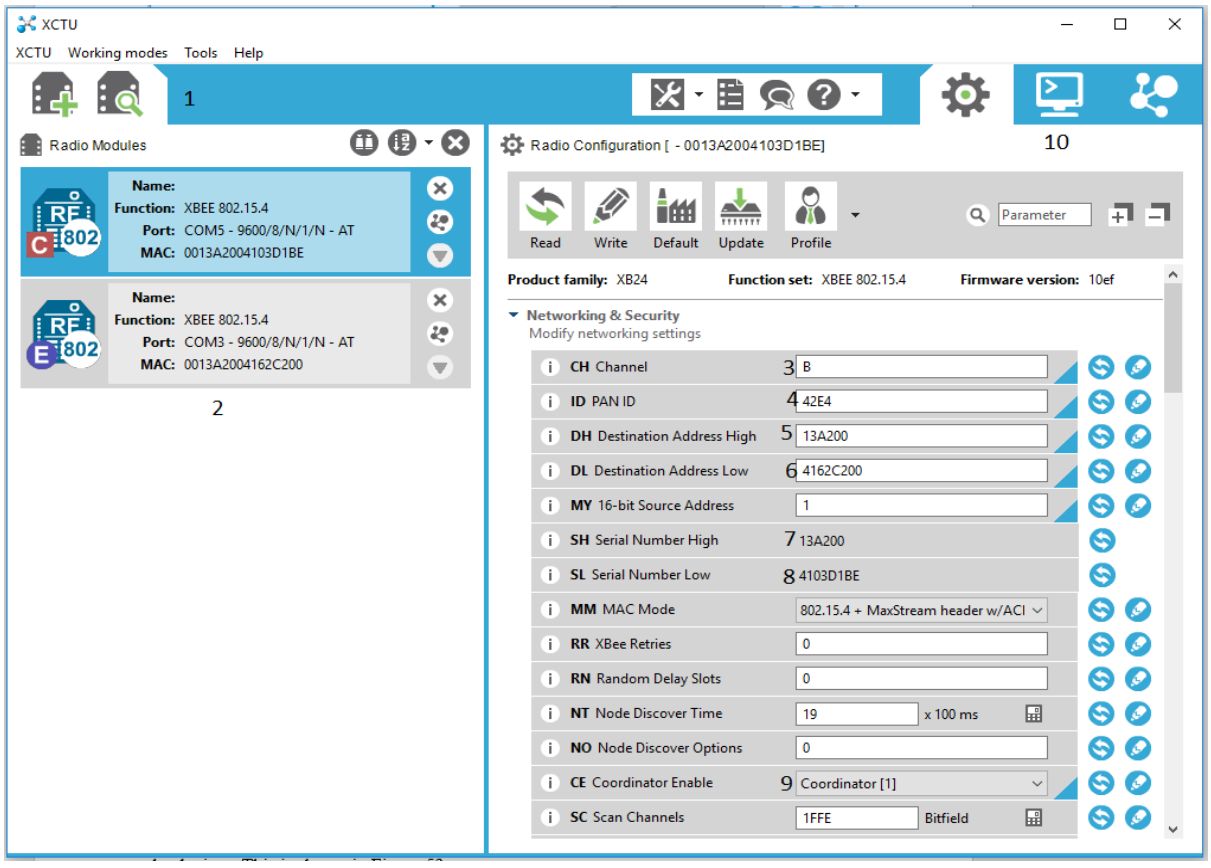

Figure 26. XCTU user interface.

In order to interface the XBee modules with the PC a free multi-platform application, called XCTU, is used. The program is specially designed for XBee modules and offers a simple-to-

use graphical interface as shown in Figure 26. The first step for interfacing with the XBee modules is to detect the devices (1). When detected they appear as separate icons in the Radio Modules field (2). In order to establish a connection between the XBee's, their channels (3) and PAN (Personal Area Network) have to have the same value. Here the channel value goes from 0x0B to 0x1A (11-26) which represent the channel numbering of the 2.4 GHz frequency band – $F_c = 2405 + 5(k - 11)$ in megahertz, for k=11,12,..26. Furthermore, the destination address DH and DL (5 and 6) on one of the XBees have to be identical to the serial numbers SH and SL (7 and 8) on the other XBee and vice-versa. In order to meet the 802.15.4 network topology requirements, one of the XBee modules is set to be a PAN coordinator (9) in order to establish a star topology. Finally, the console working mode (10) is entered so that data can be inputted and transmitted between the devices. This is shown in Figures 27 and 28.

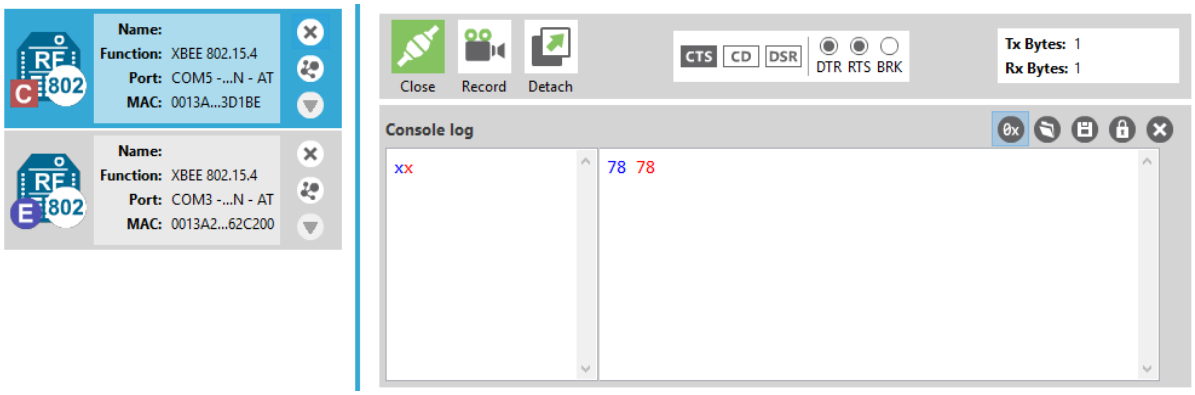

Figure 27. Coordinator sending data (blue) and receiving data (red).

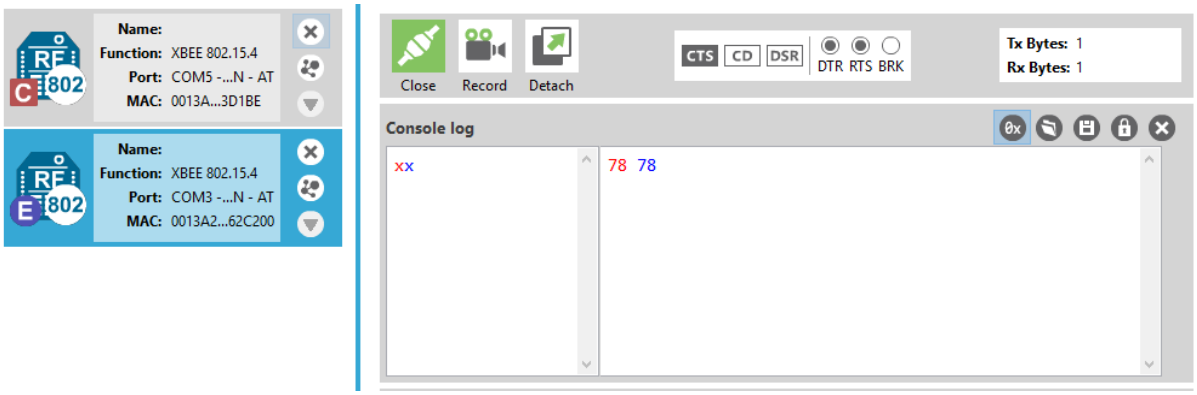

Figure 28. End device receiving data (red) and sending data (blue).

In order to establish a connection between the USRP and the XBees the carrier frequency must be set in order to match the channel of the XBees. From Figure 26 the channel is B which from hexadecimal is 11 → carrier frequency of 2.405 GHz must be chosen (Note: The USRP suffers from high carrier frequency offset, which is more than the 802.15.4 standard can cope with.).

Now run the Rx module and start transmitting data between the XBees. Carefully look at the waveforms and the BER value.

- Task 12: Are the original and the received waveforms identical? If no, why? Manually adjust the receive carrier frequency by 0.01 GHz at a time, both up and down, until you can successfully receive the signal. Screenshot your observations.

Answer:

By inspecting Figure 29, it can be seen that the receiver module successfully detects the communication between the two XBees from Figure 25. The signal detection button lights up and waveform samples are obtained. However, the data obtained is not the correct representation of the transmission due to the fact that the carrier offset frequency between the USRP device and the XBees is too high which leads to high BER results.

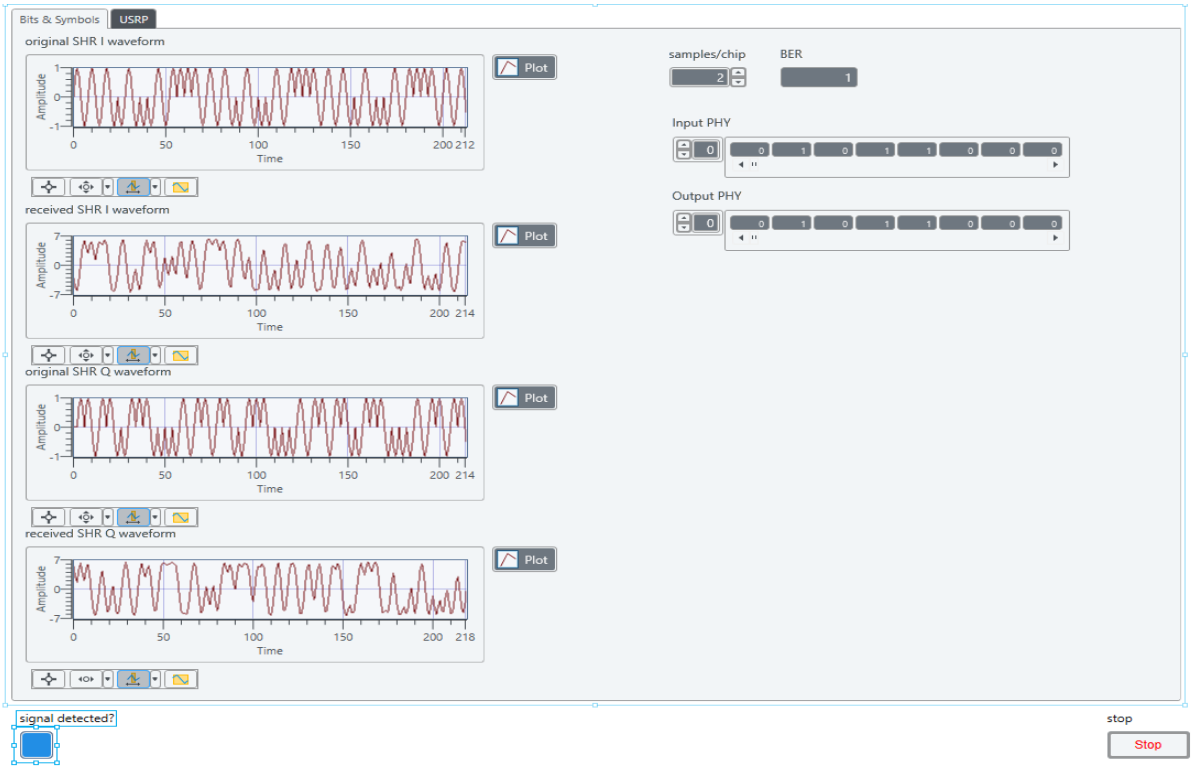

Figure 29. Receiver detection of the communication between the XBee device.

Marking Scheme

This scheme serves only for guidance. Supervisors can change it depending on their needs.

	0	1	2	3	4	5
Preparation	No preparation undertaken before the exercise	Very few Preparation section tasks are completed with many mistakes (only 1 section tasks answered)	Some of the Preparation section tasks are completed with many mistakes (1or 2 section tasks answered)	Some of the Preparation section tasks are completed with few mistakes (1 or 2 section tasks answered)	Almost all of the Preparation section tasks are completed with few mistakes (answered at least 2 sections)	All of the Preparation section tasks are completed with no mistakes (all tasks of the 3 sections)
Understanding	No understanding shown during the lab exercise	Very few of the Lab work section tasks are completed with many mistakes (only section 3.1 tasks)	Some of the Lab work section tasks are completed with many mistakes (up to section 3.2 tasks)	Some of the Lab work section tasks are completed with few mistakes (up to section 3.2 tasks)	All of the Lab work section tasks are completed with few mistakes (all 3 sections tasks)	All of the Lab work section tasks are completed with no mistakes (all 3 sections tasks)
Progress	No Lab work section tasks have been completed	Only some of the tasks were attempted (only section 3.1 attempted)	Almost all of the Lab work section tasks are completed (all tasks up to section 3.1)	Almost all of the Lab work section tasks are completed (all tasks up to section 3.2)	Almost all of the Lab work section tasks are completed (all tasks up to section 3.3)	All of the Lab work section tasks are completed (all tasks of the 3 sections)
Logbook use	No documentation of any observations	Many screenshots and notes missing but all sections up to 3.1 have been covered	Many screenshots and notes missing but all sections up to 3.2 have been covered	Some screenshots and notes missing but all sections up to 3.2 have been covered	Very few screenshots are missing in the logbook together with very few notes missing (almost all of the section 3.1 and 3.2 screenshots and their notes)	All of the required screenshots are shown in the logbook together with all the required notes (all of the screenshots and notes required for the 3 sections)