Engineering Educators Bringing the World Together
2025 ASEE Annual Conference & Exposition
Palais des congrès de Montréal, Montréal, QC • June 22–25, 2025 ASEE
Paper ID #48357

Secured Communication in the Physical Layer: An Interactive Module for Enhancing Cybersecurity Education in Next-Generation Wireless Communications

Mehzabien Iqbal, The University of Toledo, OH, USA

Mehzabien Iqbal is currently pursuing her Ph.D. in Electrical Engineering at the University of Toledo, under the supervision of Dr. Ahmad Y. Javaid, with a research specialization in Physical Layer Security for wireless communication systems. Her academic interests are centered around advanced communication technologies and security frameworks, leveraging methodologies such as Artificial Intelligence, Reinforcement Learning, Game Theory, and Software-Defined Radio. Mehzabien earned her Bachelor of Science degree in Electrical and Electronics Engineering from BRAC University in Dhaka, Bangladesh. In addition to her academic research, she serves as a Doctoral Teaching Assistant at the University of Toledo. She previously demonstrated leadership as President of the Association for Computing Machinery's Women Chapter (ACM-W) at the University of Toledo for two and a half years. Before relocating to the United States, she held the role of Telecommunications Project Engineer at Robi Axiata Limited, a multinational telecommunications company. As the lead contributor to this paper, Mehzabien conceptualized and developed an interactive educational module, including comprehensive teaching materials and pre- and post-module assessment questionnaires designed to evaluate student learning outcomes. Furthermore, she wrote the detailed research manuscript that articulates the module's design process, practical implementation, and its impact on education.

Dr. Ahmad Y Javaid, The University of Toledo
Quamar Niyaz, Purdue University Northwest
Sidike Paheding, Fairfield University

Assistant Professor in the Department of Computer Science and Engineering.

Md Abdus Samad Bhuiyan, Purdue University Northwest

WIP: Introducing an Interactive Educational Module for Teaching Security in a Communication Course

Mehzabien Iqbal*, Md Abdus Samad Bhuiyan†, Ahmad Y Javaid*, Quamar Niyaz†, Sidike Paheding‡, Xiaoli Yang§

*EECS Department, The University of Toledo, Toledo, OH, USA
†ECE Department, Purdue University NW, Hammond, IN, USA
‡CS Department, Fairfield University, Fairfield, CT, USA
§Talwar College of Engineering and Computer Sciences, Fort Wayne, IN, USA
{mehzabien.iqbal, ahmad.javaid}@utoledo.edu, {bhuiyan4, qniyaz}@pnw.edu, spaheding@fairfiled.edu, xxyang@indianatech.edu

As wireless communication continues to advance, particularly with the emergence of 5G and beyond-5G (B5G) technologies, reliance on these systems steadily increases, including their ultra-low latency, enabling smooth support for real-time applications such as telemedicine and interactive online gaming. Yet, this progress challenges traditional security practices, highlighting the need for authentication, encryption, and threat detection expertise. This research proposes incorporating security concepts pertinent to next-generation communications into the current Electrical and/or Computer Engineering (ECE) syllabus to address the critical need for secure communications in today's digital era. We introduce a practical, visualization-based educational tool focusing on Software Defined Radio (SDR) techniques and secure communication fundamentals, targeted at upper-level communication systems courses. This tool aims to instill a security-first approach in system design among students, preparing them to shift to a technological environment. The motivation of this interactive education module is to implement it in an upcoming course, with expected outcomes to reinforce the importance of security considerations in system design. Additionally, this module will be made available publicly for broader academic use via the project's website. This initiative is supported by the National Science Foundation under Awards No. 2021264 and 2021345.

Keywords—Educational Module, Interactive Learning Activities, Software Defined Radio (SDR), Next-Generation Communication, Secured Wireless Communications, Security Awareness, Security-Oriented Mindset

1 Introduction

The rapidly changing field of wireless communication has become more dependent on revolutionary technologies due to the substantial impact of technological advancements, as evidenced by the existence of 5G and the forthcoming introduction of 6G networks. Newer paradigms are poised to integrate diverse cutting-edge technologies, ranging from post-quantum cryptography, artificial intelligence, and machine learning to advanced edge computing, molecular communication, THz, visible light communication, and blockchain Hakeem et al. (2022); Mandloi et al. (2021). The mobility, dynamic topology, broadcasting characteristics, and volatility of the signal channel of wireless communication can make it susceptible to security issues and threats Jiang et al. (2012). These security vulnerabilities include Denial-of-Service (DoS) attacks, leaks, interference, fabrication, and eavesdropping Yu et al. (2015). The adoption of intelligent gadgets has increased the spread of malware and trojan horses, endangering user privacy and consuming a majority of user traffic Zhang et al. (2014). As a result, the lack of understanding of fundamental communication security has emerged as a major barrier to the advancement of wireless connectivity, highlighting the necessity to address secure communication within wireless infrastructure. The contingency for novel approaches in authentication, encryption, access control, communication, and detecting malicious activities becomes paramount to meet the heightened demands of future networks Ahmad et al. (2019); Hakeem et al. (2022).

This paper proposed integrating security-related concepts tailored for next-generation communication into existing Electrical and Computer Engineering (ECE) curricula. This strategic integration aims to position security considerations as a foundational prerequisite in the design phase of any system. In alignment with this vision, the research introduces an innovative, interactive, and visualized hands-on module designed to seamlessly integrate into the current curriculum. Additionally, this module is a comprehensive educational tool, elucidating the intricacies of secured communication processes through Software Defined Radio (SDR) and its fundamentals. Software-defined radio (SDR) technology allows multiform communication over several bands and a wide range of standards through reprogramming and reconfiguration Ulversoy (2010a). The study of SDR is vital for undergraduate students in understanding core communication security, as it helps to visualize the fundamentals of communications. Moreover, the fundamental advantage of SDR is the flexibility with which different wireless communication systems can be implemented on the same device, and the device can be updated so that it does not become obsolete Ulversoy (2010a). It can adapt to the requirements based on the bandwidth ranges and is used for reduced deployment costs. Furthermore, SDR is a hands-on tool for students to grasp complex concepts in communication systems and cybersecurity with low cost Ulversoy (2010a). By engaging with SDR, students can experiment with real-world signal processing and transmission, understanding how communication systems operate and can be compromised. SDR projects enable students to witness firsthand the vulnerabilities and security measures in wireless communications, preparing them for real-world challenges in cybersecurity de Jesús Rugeles Uribe et al. (2022). This hands-on experience is essential in a rapidly evolving field like communication se-

curity, where new threats and technologies emerge constantly. By studying SDR, undergraduate students learn about current security protocols and develop the skills to adapt to future changes and innovations.

The primary objectives of this study encompass several key aspects:

- **Promoting Proactive Security Integration**: This research emphasizes the necessity of embedding secure communication methodologies within the foundational design stages of next-generation communication systems, prioritizing proactive security measures rather than reactive responses.
- **Cultivating Security Awareness Among Students**: The research aims to instill a robust security-oriented mindset in undergraduate students by embedding secure communication principles within core Electrical Engineering and computing-related communication curricula, highlighting the critical role of security in contemporary communication systems.
- **Encouraging Careers in Secure Communication**: Through a detailed exploration of emerging technological advancements, this research seeks to inspire undergraduate students toward pursuing careers in the field of secure communications, showcasing promising professional opportunities and pathways.
- **Identifying and Analyzing Communication Vulnerabilities**: The initial phase of this research involves an in-depth examination of vulnerabilities inherent in unsecured communication systems, providing a comprehensive understanding of potential security threats, weaknesses, and their implications.
- **Implementing Advanced Security Solutions**: Building upon the identified vulnerabilities, the research integrates advanced security approaches and methodologies aimed at significantly enhancing the robustness and resilience of communication systems through fundamental conceptual clarity.
- **Development of Structured Educational Modules**: Ultimately, the research culminates in the creation of structured instructional modules designed to demonstrate complex transceiver modulation and demodulation processes, rooted in fundamental principles derived from traditional Communication System courses.

The rest of the paper is structured as four sections. Section 2 provides an overview of related literature in the field of education. Section 3 elaborates on our interactive modules and various activities. Section 4 describes expected outcomes and surveys with questionnaires related to the interactive educational module. The paper concludes with Section 5.

2 Related Literature

Recent advancements that have effectively reduced the expenses associated with software-defined radio (SDR) devices have significantly increased their appeal for instructing interactive wireless communications Bykhovsky (2022). One of the outstanding studies by Bykhovsky (2022) outlines an undergraduate course integrating low-cost SDR and Matlab/Simulink software to elucidate fundamental principles of practical digital communication systems. However, the proprietary software employed

in this educational module raises concerns about potential obstacles for students in grasping foundational SDR concepts in digital communication. Secondly, authors from Kragh et al. (2008) introduce an educational module to equip students with the skills to design and implement intricate components or applications, thereby preparing them for the challenges inherent in SDR design within industrial or governmental contexts. While this module provides comprehensive insights into SDR design concepts, it does not address security considerations related to communication. The author of Ulversoy (2010b) explores the fundamental difficulties that SDR raises for users, developers, and security organizations. The author notes that SDR presents substantial challenges for analog RF hardware design and the conversion between the analog and digital domains, particularly in wideband implementations. The primary advantage of SDR is the dynamic reconfigurability. However, security issues arise as a byproduct of the reconfigurability of SDR systems. One such security challenge is preventing the system from loading malicious or unauthorized code. An attacker can download a malicious software module or profile to SDR terminals within the network's coverage region. Accordingly, SDR may be susceptible to malware, worms, and other threats similar to those experienced by personal computers linked to the Internet Baldini et al. (2012). The author states that the SDR platform should feature a digital signature-based authentication system that verifies the downloaded modules. In a different educational approach, authors from González-Rodríguez et al. (2018) present a methodology and tools for infusing competition into the electrical engineering curriculum, fostering accelerated education and innovation in wireless communications through SDR utilization. Their suggested competition, inspired by the European UEFA Champions League format, engages student teams in a manner that enhances creativity and leverages SDR development methodologies and open-source tools for collaborative endeavors. Although their educational strategy is interactive, it does not explicitly incorporate contemporary security.

3 Interactive Modules and Various Activities

3.1 Framework of the Interactive Module

Our goal is to give student users a framework for visualizing various types of vulnerabilities of communication and the necessity of secure communication with the basic concepts of wireless communications, including transmission and reception and relevant hands-on activities. The proposed visualization framework has been developed using the GNU Radio Companion, SDRSharp, which works on Windows, Mac, and Linux environments. It is noted that we have introduced both the simulated and hardware implementations to have flexibility among students. Instead of making the students feel like they are in a class, the tool strives to improve their knowledge using a simple and open-ended framework they can access outside class. The primary research question we attempted to answer was: *"How effective are interactive modules in supporting learning of the physical, simulated, and mathematical aspects of secure communication?"* In addition, we wanted to see if there are differences in learning based on gender and/or race. We have provided the list of questions and results in Section 4 to provide a better insight.

3.2 Development of an Interactive Tool Design

The structural design of our educational tool is composed of four intricately designed phases: (i) Information Acquisition, (ii) Interactive Engagement, (iii) Analytical Explanation, and (iv) Comprehensive Assessment. These phases function as integrated subsystems within the tool. This design enhances and solidifies long-term knowledge retention, particularly in secured communication.

Each phase is tailored to specific communication topics, allowing students to advance through various levels of complexity sequentially. The **Information Acquisition** phase serves as the foundation, where learners can explore and familiarize themselves with the fundamental concepts relevant to each topic presented within the tool, which can initially allow the groundwork for deeper engagement.

In the **Interactive Engagement** phase, students actively participate in activities related to the topic, facilitating hands-on learning experience. This engagement would enable us to build the concepts introduced in the previous stage.

Following the interaction, the **Analytical Explanation** phase allows students to delve deeper, analyzing and understanding the rationale behind the interactions they have just experienced. This stage is pivotal in connecting practical application with theoretical understanding.

The **Comprehensive Assessment** phase involves evaluating the student's grasp of the topic through a series of assessments. These assessments typically encompass a mix of true/false and multiple-choice questions designed to test both the breadth and depth of the student's understanding.

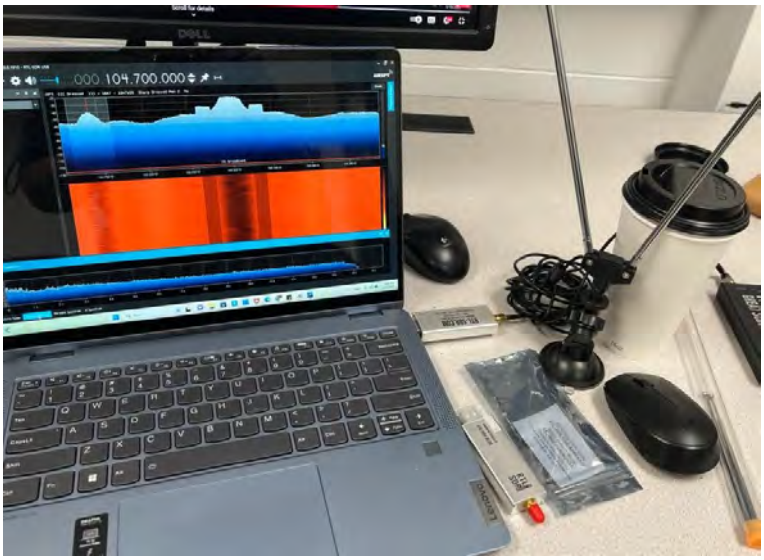
3.3 Modules of the Visualization tool

In this comprehensive educational module, we employed the GNU Radio Companion platform and Software-Defined Radios (SDRs) to explore the complexities of secure communication. The module comprises three interactive components and associated activities: (i) Design and implementation of RF communication systems using SDRs,(ii) Exploration of fundamental communication principles through tools such as GNU Radio and SDRSharp, (iii) Experimenting with secure communication techniques within the context of physical layer security. It is noteworthy to mention that, to ensure interactive and student-friendly learning experiences, our software configuration and implementation have been developed by leveraging resources from entirely open-source platforms.

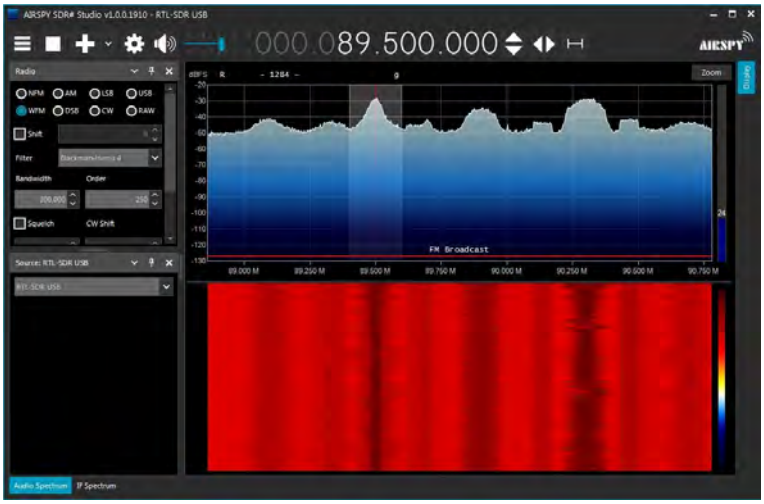
3.3.1 Designing RF Communication Systems Using SDRs

Designing fundamental Radio Frequency (RF) communication systems using Realtek Software Defined Radio (RTL-SDR) involves a systematic approach that aligns with critical principles of RF communication and signal processing. As a versatile and cost-effective tool, RTL-SDR is an excellent platform for this purpose, especially in educational and research settings.

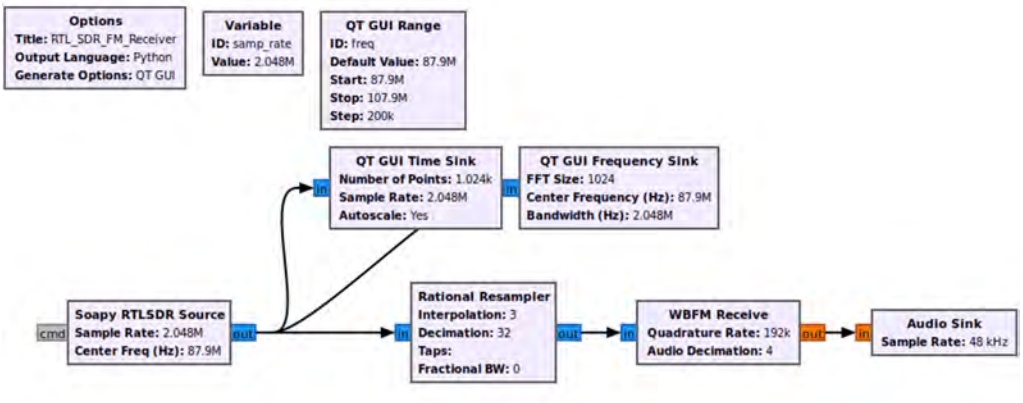
Firstly, a thorough understanding of RF communication principles is introduced with visualization activities. This includes knowledge of frequency modulation (FM), amplitude modulation (AM), phase modulation (PM), and other modulation techniques. RTL-SDR enables the practical application of these concepts, as it can receive and process signals from a wide range of frequencies. The next step is to configure the RTL-SDR setup. This involves installing the necessary drivers and software, such as



(a) Basic setup for listening to FM Broadcasting at SDRSharp using RTL SDR



(b) User Interface of FM Broadcasting at SDRSharp



(c) Simulated blck diagram of FM at GNU radio using RTL SDR

Figure 1: RF wavefrom visualization and SDR setup using SDRSharp and GNU Radio

GNU Radio or SDRSharp (depending on students preference). These software tools provide a user-friendly open source interface for signal processing and visualization, allowing for real-time analysis of RF signals.

Once the setup is complete, students can experiment with RF signals, including capturing FM radio broadcasts, analyzing weather satellite images, or decoding Digital Radio Mondiale (DRM) signals. Each task provides hands-on experience with different aspects of RF communication, from understanding signal propagation to signal decoding and analysis. Integrating RTL-SDR with external hardware like antennas and filters can enhance the learning experience. Selecting the appropriate antenna for specific frequency bands and employing filters to mitigate interference are critical skills in RF communication that students will get insight of.

To advance the educational experience, one can design experiments that challenge students to solve real-world problems using RTL-SDR. For example, tasks could include optimizing signal reception, analyzing spectrum occupancy, or developing basic intrusion detection systems for wireless networks. Fig. 1 shows the simplified SDR setup, while Fig. 1a refers to the RTL-SDR basic setup to listen to FM broadcasts using the SDRSharp open source software. Again, Fig. 1b demonstrated the User Interface of FM broadcasting using SDRSharp. FM broadcasting can also be operated through GNU Radio Companion (GRC), and the block diagram of GRC has been shown in Fig. 1c.

In accordance with that, exploring fundamental Radio Frequency (RF) communication systems using Realtek Software Defined Radio (RTL-SDR) aligns perfectly with the structured phases of (i) Information Acquisition,(ii) Interactive Engagement, (iii) Analytical Explanation, and (iv) Comprehensive Assessment. This RF communications design, ideal for educational and research settings, leverages the cost-effectiveness and versatility of RTL-SDR to provide a comprehensive learning experience.

Information Acquisition: In this initial phase, students are introduced to the core principles of RF communication, including frequency modulation (FM), amplitude modulation (AM), phase modulation (PM), and other modulation techniques. This stage is rich with visualization activities to aid in understanding these concepts, laying the groundwork for more advanced learning.

Interactive Engagement: With the theoretical foundation set, the students proceed to the hands-on phase, configuring the RTL-SDR setup. This involves installing drivers and software like GNU Radio or SDRSharp, offering a user-friendly interface for signal processing. Students actively receive and process signals from a wide frequency range. **Analytical Explanation:** Following the interaction phase, students engage in the analysis stage, where they explore the underlying mechanisms of RF signal propagation, decoding, and interpretation. This phase is designed to deepen their comprehension of real-world applications of RF communication principles while promoting the development of critical thinking and problem-solving abilities.

Comprehensive Assessment: The final phase involves evaluating students' grasp of RF communication concepts through a series of assessments. These could range from theoretical quizzes to practical tasks, such as optimizing signal reception or developing intrusion detection systems for wireless networks. This stage is crucial in measuring the effectiveness of the learning experience and ensuring a thorough comprehension of the subject matter.

By integrating RTL-SDR with external hardware like antennas and filters, the tool offers an enhanced learning experience, teaching students to select appropriate hard-

ware for specific tasks and mitigating interference—critical skills in RF communication. This interactive tool design imparts theoretical knowledge and provides a platform for practical application, ensuring a well-rounded educational experience in RF communication.

3.3.2 Various Filters and QPSK

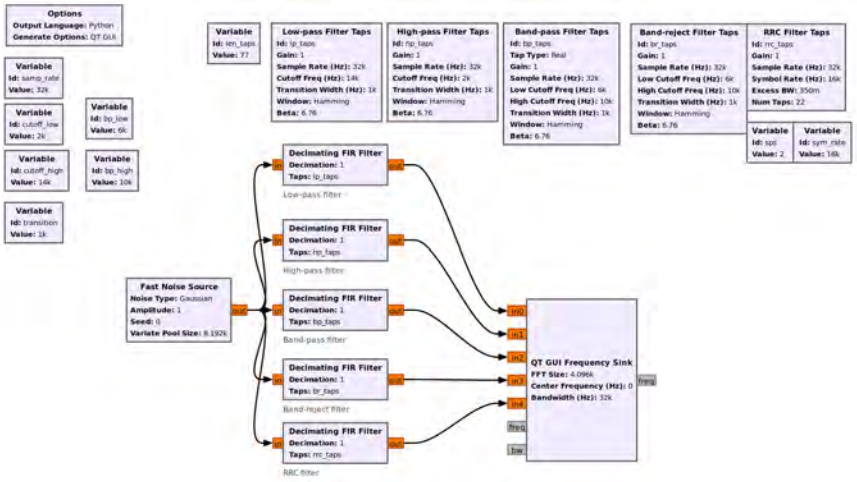
Understanding various filters and Quadrature Phase Shift Keying (QPSK) in the context of GNU Radio is crucial for grasping the fundamentals of communication systems. GNU Radio, a prominent software-defined radio (SDR) framework, enables the practical application of these concepts through its modular signal processing capabilities. Filters, ranging from low-pass to band-pass, play a pivotal role in signal conditioning, essential for noise reduction and signal integrity in RF communications. QPSK, a critical digital modulation scheme, is fundamental for efficient data transmission, offering robustness against noise and channel interference. GNU Radio facilitates the exploration of these concepts through its graphical interface, GNU Radio Companion (GRC), where users can construct and experiment with signal processing flowgraphs Vajdic and Jiang (2016). This hands-on experience with real-time signal processing and modulation techniques in GNU Radio provides invaluable insights into the dynamics of modern communication systems, bridging theoretical knowledge with practical application. For students and professionals in communications and signal processing, mastering filters and QPSK within GNU Radio's versatile environment is indispensable for understanding and innovating in the rapidly evolving field of wireless technology. Fig. 2 demonstrated different types of filters, including low pass, high pass, band pass, band rejects, and RRC's simulated platform in GNU radio without SDR and their corresponding waveforms, Fig. 2a, Fig. 2b. Fig. 2c depicted the Quadrature Phase Shift Keying (QPSK) in the context of GNU Radio with the quadrature result in the Gaussian noise source.

Information Acquisition: This initial phase introduces students to the fundamental concepts of digital communication within the GNU Radio environment. Key topics include an overview of digital filters (such as low-pass, high-pass, band-pass, and band-stop filters) and the basics of QPSK modulation. Educational material, such as hands-on tutorials and lectures integrated within GNU Radio Companion, helps students grasp these concepts visually and theoretically.

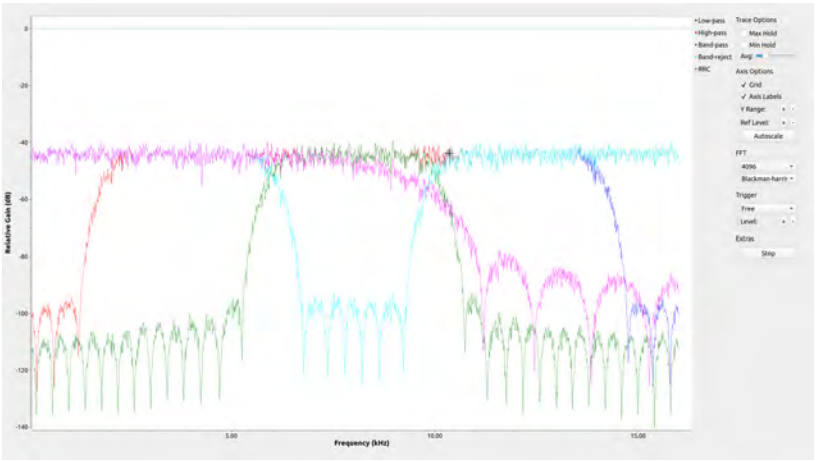
Interactive Engagement: In this phase, students actively engage with GNU Radio to implement and experiment with various filters and QPSK modulation. This hands-on experience involves designing and applying different signal filters and simulating a QPSK communication system within GNU Radio. This interactive approach enables students to see the real-time impact of their modifications and understand signal processing in a practical context.

Analytical Explanation: After engaging with the practical aspects, students move to the analytical phase, where they delve deeper into the workings of filters and QPSK modulation. This stage might involve guided exploration within GNU Radio, where students can manipulate parameters and observe the effects on signal quality, bandwidth efficiency, and error rates. This phase is essential for understanding the "why" behind the "how" of signal processing and modulation techniques.

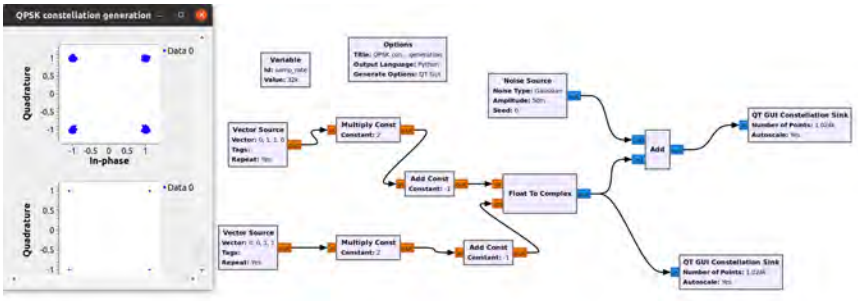
Comprehensive Assessment: The final stage assesses students' understanding and skills through various assessments tailored to the GNU Radio Companion environment. These assessments could include designing a filter to meet specific signal requirements or optimizing a QPSK modulator for a minimal error rate. Students may also be asked



(a) Fundamentals of Communication: Block Diagram Illustrating Simulation of Various Filter Types using GNU Radio



(b) Various filters including low pass, high pass, band pass filters visual waveform



(c) Quadrature Phase-Shift Keying (QPSK) simulation blockdiagram and corresponding constellation generation

Figure 2: Understanding Communication Fundamentals Using GNU radio: various types of filter, and QPSK

to analyze and interpret the results of different signal processing scenarios they created in GNU Radio, providing a comprehensive evaluation of theoretical knowledge and practical skills. Following Fig. 2c, students can brainstorm what procedures can be applied to make the QPSK communication more secure.

3.3.3 WBFM Audio Signal

In GNU Radio, transmitting different data types such as text, voice, and image involves leveraging its comprehensive digital signal processing capabilities. The process begins with converting these data types into a suitable format for transmission Valerio (2008). For text data, this typically involves ASCII encoding, which is then modulated using digital modulation schemes like QPSK or QAM Valerio (2008), tailored to the required transmission characteristics. Voice data, on the other hand, requires an initial analog-to-digital conversion, often followed by compression using codecs like G.711 or G.729 to reduce bandwidth Valerio (2008). This compressed digital audio is then modulated for transmission. For image data, formats like JPEG or PNG are converted into a stream of bytes, potentially compressed, and then modulated similarly to text data.

GNU Radio's modular block structure allows for the assembly of custom signal processing chains for each data type. These chains include necessary blocks for encoding, modulation, and RF front-end controls to manage the transmission process. The modulation stage is critical, as it determines the robustness and efficiency of the data transmission. Advanced features in GNU Radio, such as error correction coding and adaptive modulation, can be employed to enhance the reliability and quality of the transmitted signal Vajdic and Jiang (2016).

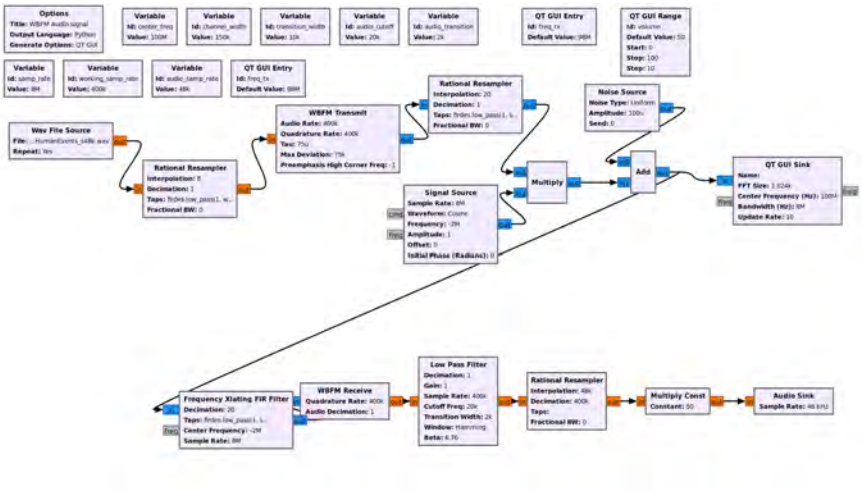
Once modulated, the data is transmitted over the air using SDR hardware compatible with GNU Radio, like RTL-SDR or USRP. The transmitted signals can then be received by a similar SDR setup, where they undergo demodulation and decoding processes to retrieve the original data, be it text, voice, or image. This comprehensive approach in GNU Radio allows for a hands-on exploration of the transmission mechanisms for various data types, providing an invaluable learning experience for those studying and working in digital communications.

Fig. 3 demonstrated the communication fundamentals of transmitting different data, such as audio data, with proper tuning to understand the voice without noise. Students will find the practical implementation very interesting since they can retrieve the actual voice and implement it in the GRC. Students will also learn various audio signal results, including waterfall and frequency results (Fig. 3b, Fig. 3c).

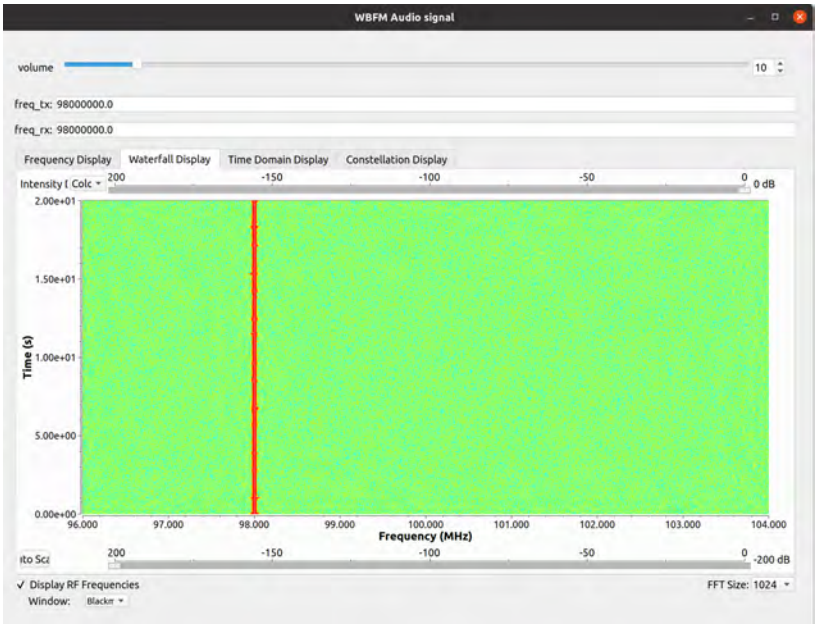
In the context of transmitting different data types like text, voice, and image, can be effectively structured into the educational phases of Information Acquisition, Interactive Engagement, Analytical Explanation, and Comprehensive Assessment.

Information Acquisition: This phase involves introducing students to the basics of digital signal processing in GNU Radio, relevant to data transmission. This includes the theory behind data encoding (like ASCII for text, analog-to-digital conversion for voice, and byte stream conversion for images). Resources such as academic papers, like those by Gandhiraj and Soman (2014); Valerio (2008) can be used to provide a theoretical foundation. Visual aids like Figure 3 can demonstrate the fundamentals of transmitting different data types, focusing on how filters and modulation impact signal quality.

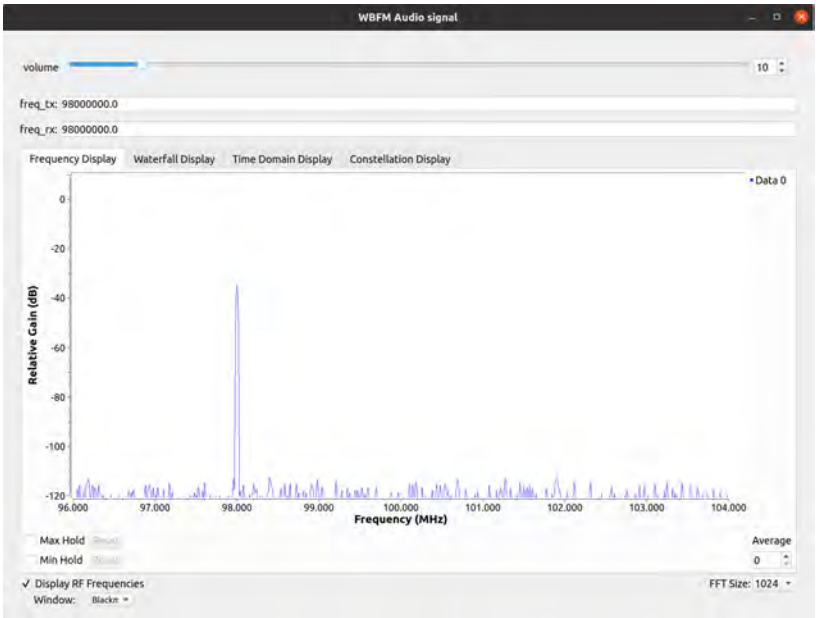
Interactive Engagement: In this phase, students engage with GNU Radio Companion (GRC) to practically implement these concepts. They will experiment with encoding and modulating text, voice, and image data, and RF front-end controls. In-



(a) WBFM Audio signal Block diagram

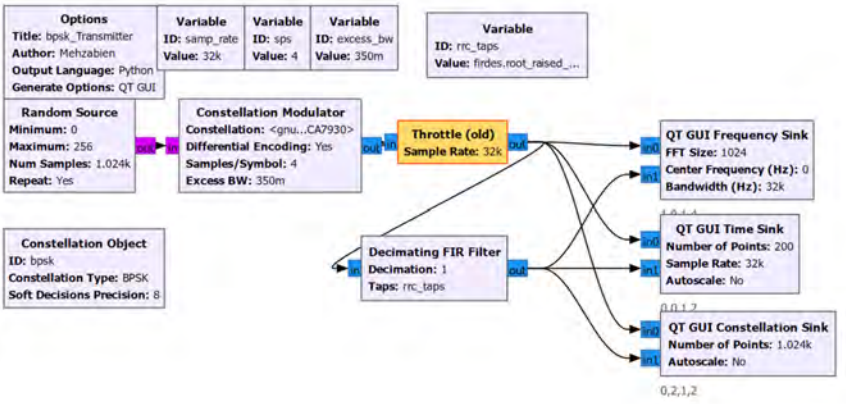


(b) WBFM Audio signal waterfall waveform

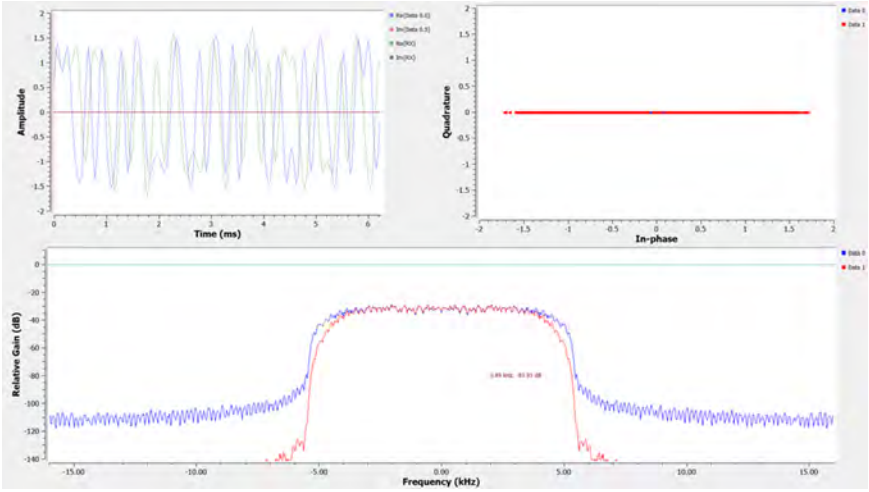


(c) WBFM Audio signal frequency waveform

Figure 3: Fundamentals of Communication: Transmission of waveform Including Audio Signals, Using GNU Radio

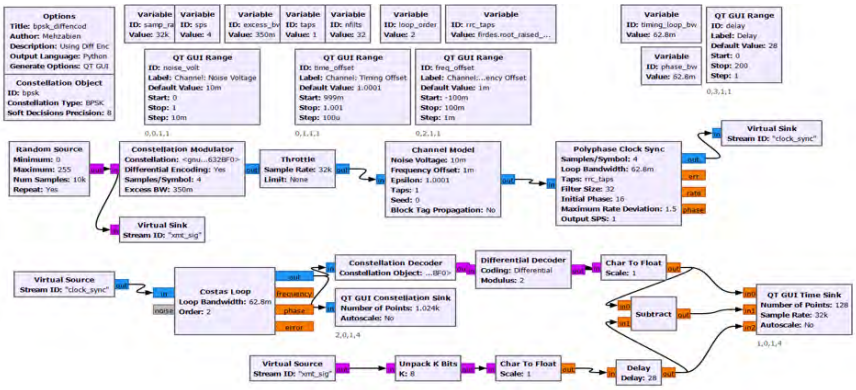


(a) BPSK modulation framework using GNU Radio

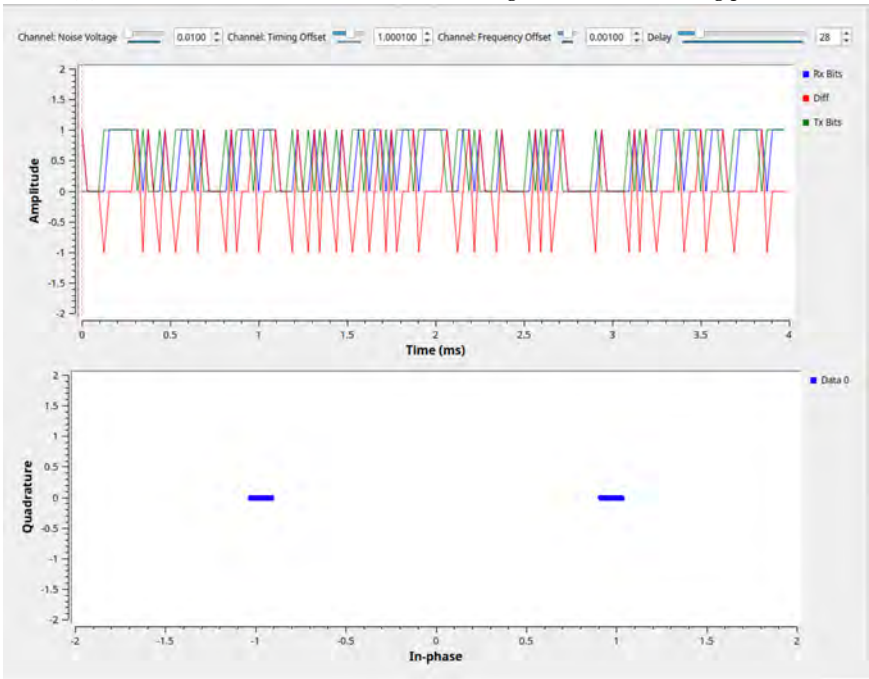


(b) BPSK modulation waveform: Amplitude, quadrature, and relative gain

Figure 4: Theoretical and practical visualization of Binary Shift Keying (BPSK) modulation



(a) Secured BPSK modulation framework using Differential Encoding process



(b) BPSK modulation waveform using Differential Encoding: Amplitude, and quadrature

Figure 5: Visual understanding of the differences between secured and unsecured BPSK modulation

teractive exercises can include tasks like tuning the parameters for voice transmission to achieve clarity and reduce noise, as shown in Fig. 3b and Fig. 3c. This hands-on experience solidifies their understanding of how different data types are processed and transmitted.

Analytical Explanation: Here, students analyze the outcomes of their experiments. They explore how different filters affect signal integrity and the efficiency of QPSK modulation in various scenarios. Discussions and assignments can focus on interpreting signal visualizations, understanding the role of error correction coding, and adaptive modulation in enhancing signal quality, as mentioned in GNU Radio's advanced features.

Comprehensive Assessment: The final phase evaluates students' understanding and skills. Assessments can range from quizzes on theory to practical tasks where students must optimize data transmission for specific types of data using GNU Radio. They might be asked to modify filter parameters or modulation techniques to improve the transmission of a particular data type, demonstrating a comprehensive grasp of the subject.

3.3.4 Fundamental of Secure Communication: BPSK

Binary Phase Shift Keying (BPSK) modulation using GNU Radio involves a process where binary data is represented using two distinct phase states of a carrier wave - typically 0 degrees for a binary '0' and 180 degrees for a binary '1' Joshi et al. (2017). This form of modulation is simple and robust, making it widely used in digital communications.

BPSK Modulation in GNU Radio:

Signal Generation: In GNU Radio, the process starts with generating a binary signal representing the data to be transmitted.

Modulation: The binary signal modulates a carrier wave using BPSK modulation. This is achieved using the BPSK modulator block in GNU Radio, which alters the phase of the carrier wave according to the binary input.

Transmission and Reception: The modulated signal is transmitted, potentially over a simulated radio channel. A BPSK demodulator block is used on the receiving end, which recovers the original binary data from the phase changes in the received signal.

Result Analysis: The output can be observed using tools like time-domain scopes or spectrum analyzers in GNU Radio. The result typically shows two distinct clusters in the phase domain, corresponding to the two-phase states of BPSK (Fig. 4b).

Securing BPSK Modulation with Differential Encoder:

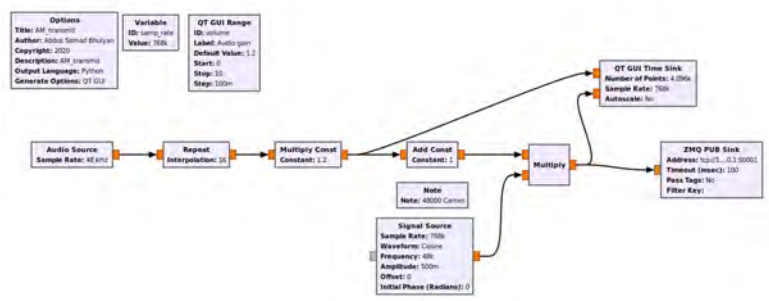
BPSK can be made more secure and robust to phase ambiguities by using a differential encoder. This method does not encode the absolute phase of the carrier but rather the phase change between consecutive bits.

Differential Encoding: The binary data is passed through a differential encoder before modulating the carrier wave. In this process, if the current bit is the same as the previous bit, the phase remains unchanged; if it is different, it is inverted Gini and Giannakis (1998).

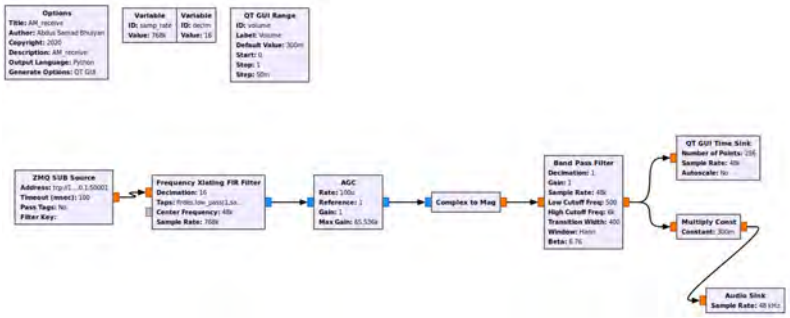
Modulation: The differentially encoded signal is then modulated onto the carrier wave using BPSK.

Reception with Differential Decoding: At the receiver, after demodulating the signal, a differential decoder is used to recover the original data. This decoder interprets the phase changes between consecutive bits to determine the original binary data.

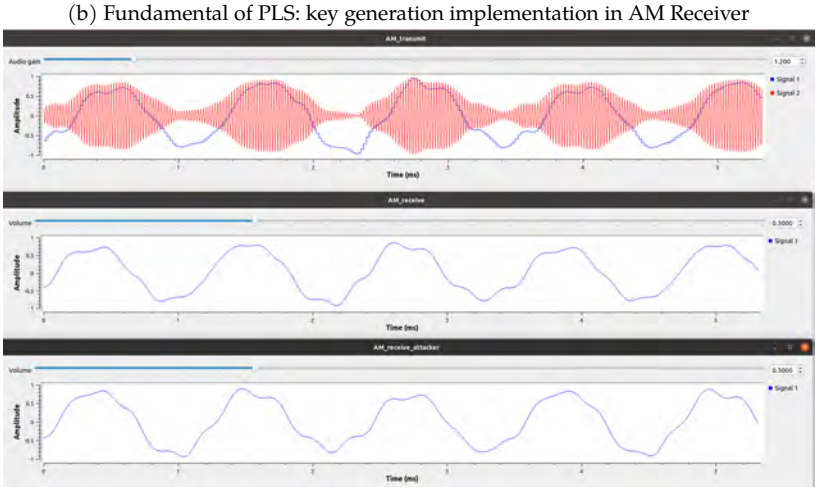
Advantages: This approach makes the system less sensitive to sudden phase shifts



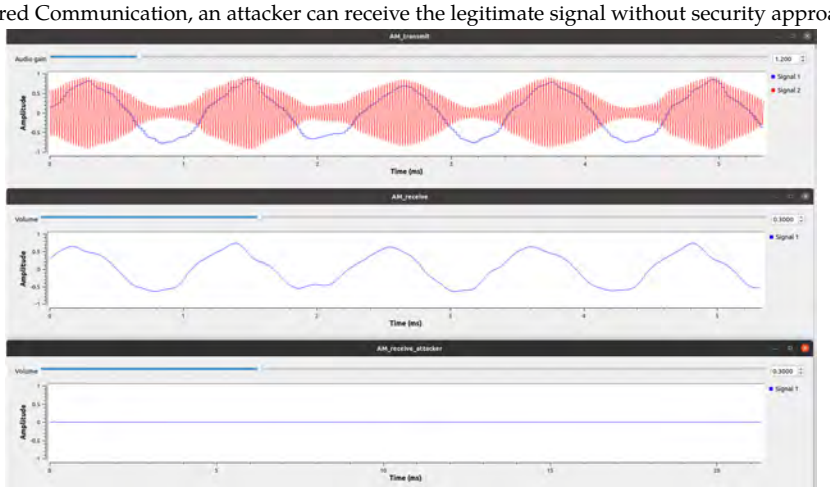
(a) Fundamental of PLS: key generation implementation in AM Transmitter



(b) Fundamental of PLS: key generation implementation in AM Receiver

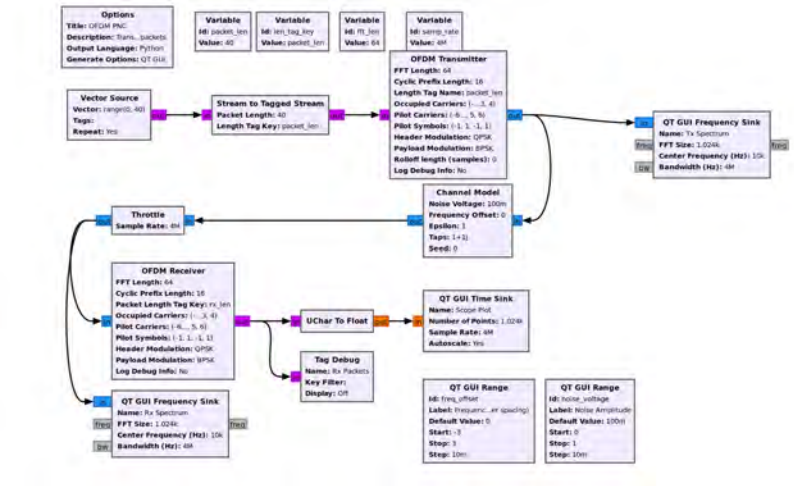


(c) Unsecured Communication, an attacker can receive the legitimate signal without security approach in PLS

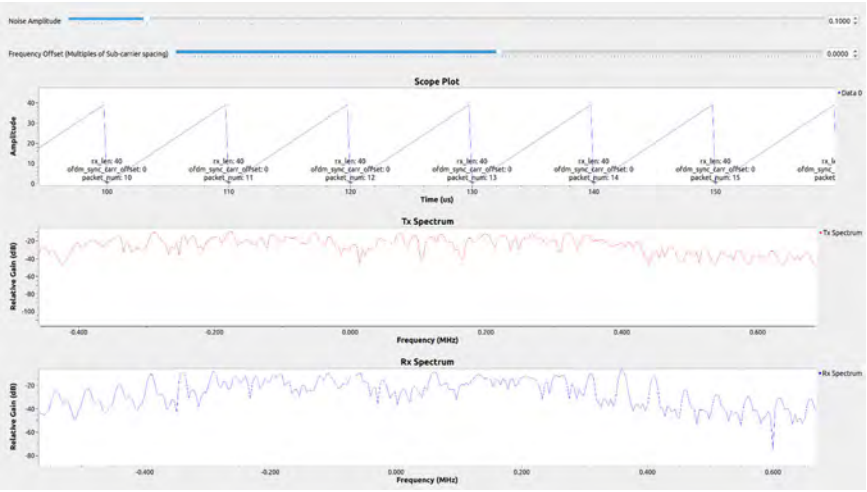


(d) Secured Communication, an attacker cannot receive the legitimate signal by using key generation technique

Figure 6: Physical Layer Security Techniques in AM Transceivers utilizing GNU Radio



(a) Secured OFDM transceiver



(b) Secured OFDM transceiver, result

Figure 7: Comprehensive Analysis of Physical Layer Security Techniques in OFDM Transceivers Utilizing GNU Radio

in the communication channel, which can occur due to multipath propagation. This robustness enhances the security and reliability of BPSK modulation in practical communication systems. Using GNU Radio to simulate and implement BPSK with differential encoding/decoding allows students and practitioners to visualize and understand these concepts effectively, providing a practical understanding of secure communication techniques in digital signal processing (Figure 5. To conduct the interactive learning tool, students will perform the differential encoder technique in QPSK modulation system.

3.3.5 Understanding Secured Communication in Physical Layer Security

AM in GNU Radio and Physical Layer Key generation

The principal objective of this section is to illustrate audio data transmission in AM and physical layer security implementation. The most common physical layer security approaches include authentication, physical layer key generation, and obfuscation using secure multi-antenna. Obfuscation techniques focus on directly obscuring the transmission from an eavesdropper while guaranteeing that the message is securely delivered to the intended receiver. In this study, we utilized physical layer key generation as the security measure. This work aims to visualize the distinction between secured and insecure wireless communication and how simple it is for an adversary to invade someone's privacy when the communication channel is unguarded. This entire project has been carried out using GNU Radio Companion, a software toolkit for researching and implementing Software Defined Radio systems that offer signal operation and processing modules for academic and industrial research and developing wireless communication systems. Fig. 6a, Fig. 6b shows that an AM transmitter and an AM receiver were first constructed independently without using any PSL scheme in GNU Radio. Additionally, an eavesdropper, essentially an additional AM receiver (unauthorized), was developed to demonstrate the security vulnerability. The transport layer (TCP) will function as the communication channel, with the microphone of the Ubuntu computer acting as the input and the speaker as the output.

Since there are no security precautions in place initially, the system will, henceforth, be vulnerable to an attacker (eavesdropper) when they attempt to monitor the communication between the genuine transmitter and receiver. Fig. 6c displays that the eavesdropper also acquires the data broadcasted by the transmitter in addition to the legitimate receiver. Physical layer encryption, as previously defined, essentially creates a shared characteristic between the genuine transmitter and receiver. The ZMQ PUB Sink and Source blocks have a Filter Key parameter readily available which offers a key or label generation feature when building the transmitter and the receiver. Physical layer encryption has been implemented using this functionality as I introduced a shared key between the transmitter and receiver to demonstrate their utilization. As illustrated in Figure 04, because of the common characteristic between the transmitter and the receiver, data is accessible only to the intended receiver. Since the newly generated key is unknown to the eavesdropper, they are no longer able to monitor the data traffic broadcasted by the transmitter.

To summarize, PLS approaches place a lot of emphasis on making use of the unique characteristics of the channel between the intended communicants to provide the intended receiver an edge over eavesdroppers. However, since this work was implemented in simulations, there were a few constraints. Instead of using SDR transmitter and receiver hardware, necessary for physical layer security implementation, we adopted TCP as the transmission channel which prevented us from employing more

physical layer security techniques. On the contrary, the simulation through the GNU radio is far more accessible for the students than the SDR hardware which can be very expensive depending on the range. Secured communication using Orthogonal Frequency-Division Multiplexing (OFDM) and understanding it through GNU Radio involves a comprehensive approach to digital communication, particularly beneficial in environments prone to multipath interference, like wireless networks. GNU Radio, with its flexible software-defined radio (SDR) framework, provides a practical platform for exploring and implementing OFDM-based communication systems (Figure 7.

3.3.6 Understanding OFDM

Multiplexing Technique: OFDM is a type of frequency-division multiplexing where multiple data streams are transmitted simultaneously over a large number of closely spaced orthogonal sub-carriers.
Robustness to Multipath: One of the key advantages of OFDM is its robustness to multipath fading and delay spread, making it ideal for wireless communication.
Implementation: In OFDM, the data stream is divided into several parallel streams, each modulated on a separate sub-carrier. A Fast Fourier Transform (FFT) algorithm is typically used to efficiently process these sub-carriers.

3.3.7 Secured Communication with OFDM:

Encryption: To secure OFDM communication, data encryption is applied before the modulation process. Techniques like AES (Advanced Encryption Standard) can be used to encrypt the data, ensuring that only authorized receivers can decode the transmitted message.
Error Correction: OFDM systems often use error correction codes like Convolutional codes or LDPC (Low-Density Parity-Check) codes to protect the integrity of the transmitted data against noise and interference.

3.3.8 Implementing OFDM in GNU Radio:

GNU Radio Companion (GRC): GNU Radio offers a graphical tool, GRC, which allows the design of OFDM transceivers through a drag-and-drop interface.
OFDM Blocks: GNU Radio provides specific blocks for OFDM such as OFDM Transmitter and Receiver, FFT, IFFT, and Channel Estimation blocks that can be interconnected to simulate a complete OFDM communication system.

3.3.9 Simulation and Analysis:

Users can simulate an OFDM system, visualize the signal at various stages using FFT plots or constellation diagrams, and analyze the system's performance under different channel conditions.

3.3.10 Customization for Security:

GNU Radio allows for the integration of custom encryption and error correction modules within the OFDM framework. By incorporating encryption blocks before the OFDM modulation blocks, users can simulate a secure communication system.

3.3.11 Experimentation:

With compatible SDR hardware like USRP or RTL-SDR, users can transmit and receive OFDM-modulated signals in real-time, providing an end-to-end understanding of secure OFDM communication. In summary, understanding secured communication using OFDM in the context of GNU Radio offers a rich learning experience. It combines theoretical knowledge of digital signal processing with practical skills in SDR, essential for modern wireless communication systems. This approach not only deepens the understanding of OFDM and its applications in secure communication but also provides valuable hands-on experience in implementing and testing these concepts in a real-world-like environment.

Interactive learning of secured communication using Orthogonal Frequency-Division Multiplexing (OFDM) through GNU Radio offers a dynamic educational experience, blending theoretical concepts with hands-on practice. This approach enables students to visually construct, simulate, and analyze OFDM-based systems, providing deep insights into how data is encrypted, modulated across multiple subcarriers, transmitted, and then decrypted and demodulated at the receiver. By using GNU Radio's graphical interface and compatible software-defined radio (SDR) hardware, learners actively engage in the process of designing and implementing secure communication systems. This immersive method not only solidifies their understanding of key communication principles like OFDM, encryption, and error correction but also enhances their practical skills, preparing them for real-world challenges in digital communications.

Table 1: ELAAS: Evaluation of Learning Attitudes for Security and Safety Questionnaires

No.	Questions
1	I think that cyberattacks can happen to me in day-to-day life.
2	It is useful for me to be aware of various cyberattacks that may target me while I am using the Internet.
3	All messages I send and receive using my electronic devices (phone, laptop, tablet, etc.) are secure. Other than me and the receiver, no one can read them.
4	Using a single password for all my accounts is a good practice. It's easy to remember and I don't need to write it down, hence, it is more secure.
5	Phishing attacks can only happen on the Internet.
6	It is safe to use online banking through a public and free Wi-Fi network (e.g. in coffee shops, airports, etc.).
7	If my smartphone has a biometric password (fingerprint, facial recognition, etc.), no one can hack it.
8	If I have a problem with my phone, I usually assume that the device settings have been changed.
9	All cyberattacks are aimed at stealing money.
10	This is a strong password: "strongpassword".
11	Spending less than 30 minutes a day on the Internet will save me from becoming a victim of cyberattacks.
12	It is unsafe to click on the hyperlinks in a spam email.
13	If I receive a notification to upgrade my mobile app, I will update it by clicking on the notification and following the instructions without having to waste my time checking with the App Store or the Play Store.
14	If available, I always connect to public and free Wi-Fi and browse the internet.
15	It is good to share information about my day-to-day activity on social media with my friends and family.
16	It is safe to save my university login credentials on my school lab computer.
17	If I do not share my password, my account will be safe.
18	It is okay to respond to spam messages or emails.
19	Saving your social security number in your phone contacts or notes is safe and easier to fetch when required.
20	Cyberbullying occurs when you talk to strangers.
21	It is safe to use an administrator account on desktops and laptops.

4 Results and Discussions

The findings will be based on pre-and post-surveys completed before and after module sessions. We plan to use this module in the communication system course for the upcoming semester at the University of Toledo, OH, USA. Various surveys will be conducted in pre/post format for the topics covered in the framework, as well as lectures and other hands-on activities. The framework includes three topics: general communication security concepts, students' attitudes and perceptions about secured communication, and Internet security based on gender. The results of these surveys will be analyzed to understand perception, attitude,as explained to the students during the lecture sessions. In order to develop firm understanding we plan to provide reading materials to students after the pre-survey and before engaging in the module/interactive tool.This work explicitly analyzes these aspects in more detail in the following subsections, including developing questions for surveys and inplemenation towards student's learning and feedback. In additions, the questions are being prepared with the suggestions of cybersecurity and communications systems teaching expertise from the University of Toledo.

4.1 Reading Material

The primary purpose of the reading material is to deliver an extensive overview of cybersecurity fundamentals specifically tailored for core and wireless communication systems. It emphasizes the critical necessity of identifying, assessing, and mitigating cyber threats to maintain the confidentiality, integrity, and availability of communication infrastructures. Initially, the document defines security in wireless communications, explaining its role in safeguarding data transmission and preventing unauthorized access or disruptions. The importance of security is underscored by highlighting vulnerabilities shared between wired (core) and wireless communication technologies, especially considering the proliferation of IoT and 5G networks that intensify security risks.

The material extensively discusses various types of cybersecurity threats specific to wireless systems, including passive eavesdropping, Man-in-the-Middle (MITM) attacks, Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks, replay attacks, rogue access points, and specialized Bluetooth-based threats so that students grasp conceptual idea of various types of attacks. Additionally, it outlines practical preventive measures such as strong encryption, secure wireless protocols, mutual authentication, and regular security audits to combat these threats. Furthermore, the document identifies unique challenges inherent in securing wireless systems—such as the open nature of wireless media, resource constraints on IoT devices, dynamic network topologies due to device mobility, and vulnerabilities arising from limited physical security. In response, recommended mitigation strategies include lightweight cryptographic techniques, dynamic key management, decentralized authentication, and tamper-resistant hardware.

Consequently, the reading material explores emerging cybersecurity measures essential to securing wireless communications in multiple layers, including robust encryption methodologies like AES, ECC, and TLS protocols. It emphasizes the importance of proper key management—generation, distribution, secure storage, and timely revocation—and addresses potential challenges of encryption, such as computational overhead, interoperability, and regulatory compliance. Forward-looking trends such as quantum-resistant cryptography and leveraging AI-enhanced security protocols

are also discussed, reflecting an awareness of evolving security in communications requirements.

Physical layer security is another significant component covered, emphasizing its critical role as a foundational defense layer against interception, eavesdropping, and jamming. Techniques such as spread spectrum technologies (FHSS, DSSS), physical layer encryption, ultra-wideband transmission, beamforming, and antenna array strategies, channel coding, physical unclonable functions (PUFs), wireless fingerprinting, and watermarking are discussed as viable security measures. Challenges such as implementation complexity, cost, scalability, and environmental influences on the effectiveness of physical-layer security are also explored.

For cybersecurity and secured communications awreness assessment, the material outlines rigorous methodologies specific to the physical layer, including evaluating vulnerabilities related to signal integrity, interception susceptibility, and potential manipulation. Spectrum analysis, vulnerability scanning (using tools like Wireshark and Aircrack-NG), and penetration testing are recommended assessment tools and practices. It also emphasizes regular security assessments as critical in maintaining compliance with security standards, optimizing security protocols, and proactively addressing vulnerabilities.

Lastly, real-world case studies such as the TJX Wi-Fi breach, Maroochy sewage spill incident, Silicon Valley substation sniper attack, the Stuxnet malware incident, and the Equifax data breach illustrate the severity and diverse impacts of physical-layer vulnerabilities. These examples underscore the importance of a layered security approach, continuous monitoring, and rapid response capabilities to strengthen the overall cybersecurity posture in wireless communications.

Therefore, the motivation to share the reading material is to advocate for a comprehensive and multi-layered cybersecurity strategy that encompasses robust encryption, dynamic physical-layer protections, continuous monitoring, and rigorous assessment practices to ensure resilience against increasingly sophisticated threats to communication systems.

Table 2: Secured Communications Awareness Questionnaires

No.	Questions
1	On a scale of 1-5, how would you rate your understanding of secured core communication principles?
2	Please rate the importance of Key Management in secure communication on a scale of 1-5.
3	Please rate the importance of Secure Protocol in secure communication on a scale of 1-5.
4	Please rate the importance of Data Integrity in secure communication on a scale of 1-5.
5	How important do you think secure communication is in today's digital world?
6	Online banking and financial transactions: Please rate its importance in secure communication on a scale of 1-5.
7	Government and military communications: Please rate its importance in secure communication on a scale of 1-5.
8	Healthcare data exchange (e.g., patient records): Please rate its importance in secure communication on a scale of 1-5.
9	Secure messaging apps (e.g., end-to-end encrypted chats): Please rate its importance in secure communication on a scale of 1-5.
10	Please rate your awareness of the potential risks and threats associated with unsecured communications on a scale of 1-5.
11	Phishing and social engineering attacks: Please rate their importance as common vulnerabilities in communication systems on a scale of 1-5.
12	Man-in-the-middle attacks: Please rate their importance as common vulnerabilities in communication systems on a scale of 1-5.
13	Please rate your experience with prior coursework or training related to communication security on a scale of 1-5.
14	How effective do you believe physical layer security measures are in protecting wireless communication systems from unauthorized access?

4.2 ELASS: (Evaluation of Learning Attitudes for Security and Safety)

We are planning to use this visualization tool to help the students develop a secure communication mindset. This set of questions focused on general attitudes towards security and attempted to evaluate improvement in that domain, using 21 questions (Table 1. The reason behind conducting this survey is to understand the concept of security and safety among the students before and after the module.

4.3 Secured Communication Perception

The students' perceptions of secured communication have become important. We aim to survey perceptions of the general concept of secured communication. To assess the students' knowledge, we are planning to provide a 5-point Likert scale. Table 2 shows the questions mentioned in the communication perception survey, which had 14 questions. The results will indicate a potential understanding of the conduct and effectiveness of this course module.

4.4 Knowledge Based After Completing the Module

The students' perceptions of secured communication learning are also essential and indicate how they learn about this topic and try to stay up to date. We are planning to survey perceptions of secured communication learning through a 9-questions survey (including pre and post). To assess the students' knowledge, we used a 5-point scale similar to previous surveys. Table 3 shows the questions mentioned in the secured core communication learning perception survey. Additionally, the pre- and post-surveys will be an effective way to assess the understanding and perception of secured core communication among undergraduate students.

Table 3: Communication Security Learning Questionnaires

No.	Questions
1	I have a clear understanding of how security implementation in the physical layer can be used in wireless communication systems.
2	I am aware of the security vulnerabilities present in physical layer communication systems.
3	I believe that encryption is a key element in securing core wireless communication systems.
4	I am familiar with the role of PLS in enhancing security within 5G and future wireless networks.
5	I can identify potential cyber threats in wireless communication systems.
6	I am interested in learning more about how PLS can be used to detect and mitigate security threats.
7	I believe that machine learning can enhance the security of communication systems.
8	I am confident in my ability to design secure communication systems.
9	I believe that understanding core wireless communication protocols (e.g., LTE, 5G) is essential for improving PLS-based security.
10	Has your perception of the importance of secure communication changed after completing this course (post-survey only)?
11	Which of the following concepts in secure communication did you find most enlightening (post -survey only)?
12	What aspect of the course/module did you find most beneficial? (post-survey only)
8	I am confident in my ability to design secure communication systems (post-survey only).
9	I believe that understanding core wireless communication protocols (e.g., LTE, 5G) is essential for improving PLS-based security (post-survey only).

5 Conclusion

In conclusion, this educational module strategically addresses the burgeoning demands of learning the concept of secure communication in the evolving wireless

technology landscape. By instilling a proactive security mindset among Electrical and Computer Engineering undergraduate students, the module bridges theoretical knowledge with practical application and inspires careers in secure communication. Leveraging GNU Radio Companion and Software Defined Radio, the module's hands-on activities, simulated attack scenarios, and real-world applications, particularly from fundamental communication systems to OFDM-based 5G communication, enhance students' understanding and engagement regarding the necessity of secured communication.

We plan to implement this module in the upcoming academic year at the University of Toledo. Post-implementation surveys will be conducted to assess the module's effectiveness in significantly improving students' grasp of secured communication concepts. These surveys are expected to affirm the module's success, positioning it as a valuable addition to the curriculum, and equipping students to navigate the complexities of next-generation communication systems with confidence and proficiency. This ongoing work aims to continuously refine and enhance the module to better meet the needs of students and the evolving demands of the wireless technology landscape.

References

Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei Gurtov, and Mika Ylianttila. Security for 5g and beyond. *IEEE Communications Surveys Tutorials*, 21(4):3682–3722, 2019. doi: 10.1109/COMST.2019.2916180.

Gianmarco Baldini, Taj Sturman, Abdur Rahim Biswas, Ruediger Leschhorn, Gyozo Godor, and Michael Street. Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead. *IEEE Communications Surveys Tutorials*, 14(2):355–379, 2012. doi: 10.1109/SURV.2011.032511.00097.

Dima Bykhovsky. Hands-on undergraduate course based on software-defined radio and matlab/simulink. *International Journal of Electrical Engineering & Education*, 59 (1):71–80, 2022. doi: 10.1177/0020720919837853. URL `https://doi.org/10.1177/0020720919837853`.

José de Jesús Rugeles Uribe, Edward Paul Guillen, and Leonardo S. Cardoso. A technical review of wireless security for the internet of things: Software defined radio perspective. *Journal of King Saud University - Computer and Information Sciences*, 34(7):4122–4134, 2022. ISSN 1319-1578. doi: https://doi.org/10.1016/j.jksuci.2021.04.003. URL `https://www.sciencedirect.com/science/article/pii/S1319157821000896`.

R Gandhiraj and KP Soman. Modern analog and digital communication systems development using gnu radio with usrp. *Telecommunication Systems*, 56:367–381, 2014.

F. Gini and G.B. Giannakis. Generalized differential encoding: a nonlinear signal processing perspective. *IEEE Transactions on Signal Processing*, 46(11):2967–2974, 1998. doi: 10.1109/78.726810.

Marta González-Rodríguez, Antoni Gelonch-Bosch, and Vuk Marojevic. A software radio challenge accelerating education and innovation in wireless communications. In *2018 IEEE Frontiers in Education Conference (FIE)*, pages 1–9, 2018. doi: 10.1109/FIE.2018.8658736.

Shimaa A. Abdel Hakeem, Hanan H. Hussein, and Hyung-Chan Kim. Security requirements and challenges of 6g technologies and applications. *Sensors (Basel, Switzerland)*, 22, 2022. URL `https://api.semanticscholar.org/CorpusID:247266574`.

Tingting Jiang, Tongtong Li, and Jian Ren. Toward secure cognitive communications in wireless networks. *IEEE Wireless Communications*, 19(4):82–88, 2012. doi: 10.1109/MWC.2012.6272427.

PMP Joshi, SA Patil, and DC Shimpi. Design and implementation of bpsk audio transmitter & receiver using sdr. *International Journals of Advanced Research in Computer Science and Software Engineering*, 7(6):268–271, 2017.

Frank Kragh, Jeffrey Reed, Carl Dietrich, and Donna Miller. Education in software defined radio design engineering. In *2008 Annual Conference & Exposition*, pages 13–460, 2008.

Manish Mandloi, Devendra Gurjar, Prabina Pattanayak, and Ha Nguyen. *5G and Beyond Wireless Systems*. Springer, 2021.

Tore Ulversoy. Software defined radio: Challenges and opportunities. *IEEE Communications Surveys Tutorials*, 12(4):531–550, 2010a. doi: 10.1109/SURV.2010.032910.00019.

Tore Ulversoy. Software defined radio: Challenges and opportunities. *IEEE Communications Surveys & Tutorials*, 12(4):531–550, 2010b.

Stephan Vajdic and Fan Jiang. A hands-on approach to the teaching of electronic communications using gnu radio companion and the universal software radio peripheral. In *2016 IEEE Integrated STEM Education Conference (ISEC)*, pages 19–21, 2016. doi: 10.1109/ISECon.2016.7457529.

Danilo Valerio. Open source software-defined radio: A survey on gnuradio and its applications. *Forschungszentrum Telekommunikation Wien, Vienna, Technical Report FTW-TR-2008-002*, 2008.

Fei Yu, Chin-Chen Chang, Jian Shu, Iftikhar Ahmad, Jun Zhang, Jose Maria de Fuentes, et al. Recent advances in security and privacy for wireless sensor networks. *Journal of Sensors*, 2015, 2015.

Weizhe Zhang, You Zhang, and Tai-Hoon Kim. Detecting bad information in mobile wireless networks based on the wireless application protocol. *Computing*, 96:855–874, 2014.