Self-Reliant HF/VHF Radio Encryption Using Multi-Radio Frequency Manipulation for Philippine Navy Secure Communication

Rachelle Tigcal, Charmaine C. Paglinawan

School of Electrical, Electronics, and Computer Engineering, Mapua University, Manila, Philippines
Correspondence Email: ratigcal@mymail.mapua.edu.ph

The constant relay of information between units and base stations is fundamental to military operations. Military communications networks must be reliable and secure in any conditions, especially in critical areas where vital information should be securely transmitted. The development of self-reliant, cost-effective High Frequency/Very High-Frequency radio encryption could provide secure, reliable, and practical information exchange within the Philippine Navy (PN). This study aims to develop self-reliant High Frequency (HF)/Very High Frequency (VHF) radio encryption using multi-radio frequency manipulation for PN secure communication lines. This will benefit the entire PN by providing a secure, reliable, and cost-effective radio communications system for voice and data. The algorithm for encryption is multi-radio frequency manipulation. The prototype will be limited to operating under Short-Range Devices (SRD) frequency bands and cannot be integrated with existing commercial radios.

Keywords: radio frequency, self-reliant, secure communication, modulation, encryption, AES.

1. Introduction

The Philippine Navy modernizes its radio communications to ensure reliability and security in critical areas. The Navy procures military-grade radios for its forces, vessels, and Littoral Monitoring Stations. This equipment is crucial for strategic and tactical decisions. The development of self-reliant, cost-effective High Frequency/Very High Frequency radio encryption could provide secure, reliable, and practical information exchange within the PN.

The study "Cryptographic Protection for Military Radio Communications" developed a cryptographic module for information protection in radio communications. The module allows encryption at speeds adapted to the radio's operation, suitable for narrowband and broadband radios. [1] Similarly, the paper "Securing Radio Frequency (RF) Communication

Using AES-256 Symmetric Encryption: A Performance Evaluation" analyzed the sending of unencrypted and encrypted data regarding transmission time and transmission throughput. The AES-256 algorithm was used in this study to provide the best security stronghold for encrypted data.[2]

The main objective of this study is to develop a self-reliant HF/VHF radio encryption using multi-radio frequency manipulation for PN secure communication lines. This objective will be supported by; (a) the building of a transmitter and receiver for data transfer; (b) the use of multiple radio frequency manipulation where multiple frequencies are used to modulate and encrypt data; (c) the building of a modulator and demodulator for data encryption and decryption; (d) derive a formula for multi-frequency modulation; (e)measure modulated frequency output, gain, and frequency sideband noise; (f)tuning of multiple frequency transmission modulation and multiple frequency demodulation.

The device will benefit the entire PN because it will provide security, reliability, and a cost-effective radio communications system for voice and data. Moreover, the organization will be self-reliant in building a secure radio communication infrastructure by developing this equipment. Additionally, the academes, students, teachers, researchers, and engineers will also benefit from this study as it will serve as their reference in the future for a similar research topic.

The study explores using locally produced radio communication lines for PN, using radio frequency devices for voice and data transmission and encryption. The algorithm for encryption is multi-radio frequency manipulation. The prototype is limited to Short-Range Devices and cannot be integrated with existing commercial radios.

2. REVIEW OF RELATED LITERATURE

This chapter will discuss the importance of self-reliant and secure communication as well as the topics that the researcher used as references in conducting the study.

A. Self-Reliance Defense Posture (SRDP) Program

Having a defense industry is a national asset. Military self-reliance will be the foundation of the Self-Reliance Defense Posture (SRDP) Program, which shall protect the country from foreign dependence and promote limited outside support for our defense requirements. The SRDP Program was initiated in 1974 through Presidential Decree No. 415 under the leadership of President Ferdinand Marcos Sr. It aimed to develop a local defense industry that could address and provide the material requirements of the Armed Forces of the Philippines (AFP). It functioned through partnerships between the AFP and civilian establishments while importing items that could not be locally produced to make such things indigenously eventually.[3]

Importance of Securing PN Communication Line

Having reliable and secure communication in the military is always vital because it carries information between units and base stations that are fundamental to military operations. The Naval Information and Communications Technology Center (NICTC) is one of the Philippine Navy’s support units responsible for providing fast, reliable, and secure

Command and Control, Communications, Information Systems, Surveillance, Target Acquisition, and Reconnaissance (C4ISTAR) systems to support the accomplishment of the Philippine Navy’s mission.[4]

The fundamental objective of C4ISTAR systems is to get critical and relevant information to the right place and time. The following functions support this objective:

a. Collect. We are acquiring or gathering, and initial filtering information based on a planned need, determining time sensitivity, and putting the data into a form suitable for transporting.

b. Transport. We are moving or communicating the information to appropriate receptacles for processing.

c. Process. We are storing, recalling, manipulating, filtering, and fusing data to produce the minimum essential information in a usable form on which the warfighter can take appropriate actions.

d. Disseminate. We distribute processed information to the appropriate users of the data.

e. Protect. We ensure the secure flow and processing of information and access only by authorized personnel.

Radio Encryption

Cryptography is a set of techniques for encrypting data so that only the authorized person can access and restore it to its original form. It provides a robust and cost-effective foundation for maintaining data security and integrity on computer systems. Cryptography can be used to safeguard the secrecy of data in storage or in transit in the national and international information and communication networks and technologies, as well as the growth of electronic commerce. [5]

This project was also related to the paper entitled “Securing Radio Frequency (RF) Communication Using AES-256 Symmetric Encryption: a Performance Evaluation,” which was about the encryption method integrated into RF client-server communication and provided a security solution using a symmetric encryption method for reliable RF transmission in the Internet of Things (IoT) technology then analyzed the sending of unencrypted (plaintext) and encrypted (ciphertext) data in terms of transmission time and data transmission throughput. [2]

Moreover, in the research entitled, “IoT-based Fire Mitigation and Detection System with AES-256 Encryption and Android Application”, it was mentioned that a study by Ilyas et al. (2018) proved that the use of AES-256 encryption leads to lower power consumption than other algorithm methods and protects the data acquired from the user to prevent unwanted attacks when transmitting data from the system to the authorities and users.[6]

3. Methodology

The Philippine Navy (PN) uses military-grade secure radios in some areas for secure communication lines, especially during missions. Still, it also utilizes commercial-grade radios, which lack encryption and have no built-in military-grade security features that make the system vulnerable to interception, jamming, and eavesdropping. This chapter will describe research for designing and developing a self-reliant high frequency (HF)/ very high frequency (VHF) radio encryption using multi-frequency manipulation for PN secure communication within the frequency range of 3 MHz to 30 MHz as a replacement to the commercial-grade radios. The following specific objectives guided the determination of the requirements of the project:

a. Building of a transmitter and receiver for data transfer. To design and construct devices to send and receive data wirelessly;

b. The use of multiple radio frequency manipulation where multiple frequencies are used to modulate and encrypt data. To use techniques that will help enhance security and reduce interference in data transmission;

c. Building of a modulator and demodulator for data encryption and decryption. To design the decryption circuit required to modulate the base frequency and demodulate the received frequency;

d. Derive a formula for multi-frequency modulation. To derive a formula for combining multiple frequencies to achieve multi-frequency modulation; and for data transmission;

e. Measure modulated frequency output, gain, and frequency sideband noise. To assess the performance of the system and ensure that it is operating correctly; and

f. Tuning of multiple frequency transmission modulation and multiple frequency demodulation. To maintain signal integrity and ensure effective communications.

4. Conceptual Framework

Figure 1 shows the conceptual framework of this study. This framework helped the researcher put the idea in order and use it to conceptualize the project. After dedicated reviews, this concept has strong support and structure to pursue the project's development. The discoveries and learnings from the study of related literature about secure communications have contributed significantly to the final conceptual framework of this project.

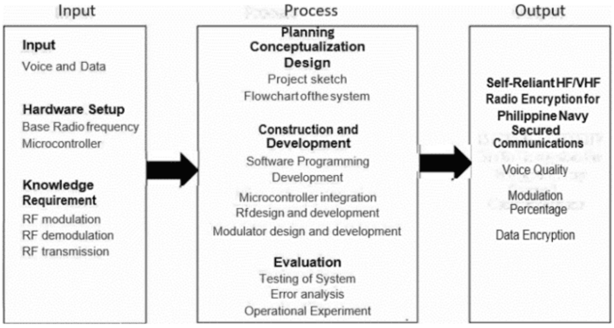


Figure 1: Conceptual Framework

Block Diagram

The block diagram of the prototype is shown in Figure 2. The transmitter module has an op-amp that will cut the input frequency and send it to the carrier frequency. The controllers (the Raspberry Pi and Arduino Uno) will control the sequence of data distribution. The signal, divided into three parts, will now be sent using three different frequencies generated from a function generator. Continuous noise input or sending of random data is to maintain transmission security. On the other hand, the receiver module has band pass filters to pass frequencies within the range of HF/VHF and rejects frequencies outside that range. Op-amp will assemble the decrypted signal, and then the demodulator will separate the signal from the modulated carrier. The synthesizer will then combine the signal to assemble the output.

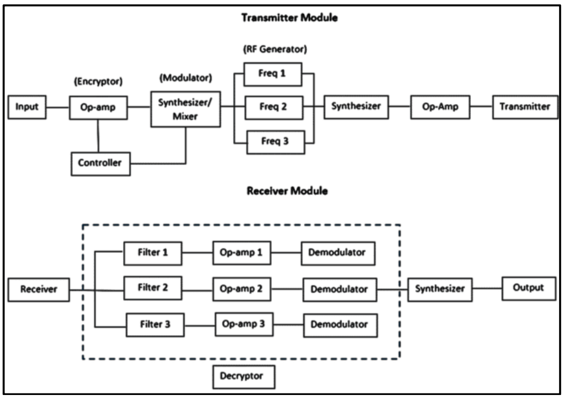
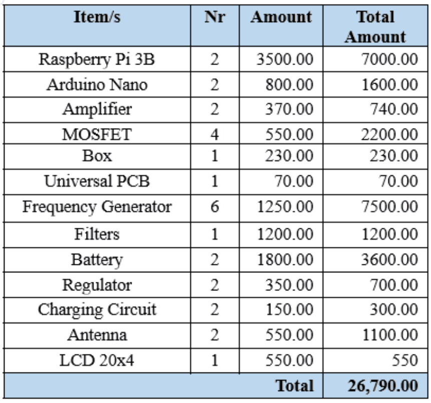


Figure 2: Block Diagram of the Hardware

Materials and Costing

Shown in Table I is the list of materials needed with a total amount of Php 26,790.00.

Table I: Materials and Costing



Item/s	Nr	Amount	Total Amount
Raspberry Pi 3B	2	3500.00	7000.00
Arduino Nano	2	800.00	1600.00
Amplifier	2	370.00	740.00
MOSFET	4	550.00	2200.00
Box	1	230.00	230.00
Universal PCB	1	70.00	70.00
Frequency Generator	6	1250.00	7500.00
Filters	1	1200.00	1200.00
Battery	2	1800.00	3600.00
Regulator	2	350.00	700.00
Charging Circuit	2	150.00	300.00
Antenna	2	550.00	1100.00
LCD 20x4	1	550.00	550
		Total	**26,790.00**

Prototype

The multi-radio frequency manipulation algorithm will utilize the jumping frequency technique to encrypt and decrypt signals. This technique has almost the same concept as

Frequency Hopping Spread Spectrum (FHSS) transmission, only that the algorithm will be used in a low-frequency carrier signal. This carrier signal will be integrated with the Amplitude Shift Keying (ASK) method for the modulation.

a. Jumping Frequency Technique

This technique is used to counter eavesdropping and frequency jamming during transmission. It will also minimize the effects of various interference or unwanted noise. To interrupt this signal, the enemy needs to know the pattern of the jumping frequencies known to both sender and receiver. During transmission, three frequencies will be used to transmit the data. Thus, the data transmission will be divided into three groups. The first group of data will be sent using the current frequency, and the next group on the other frequency, up until the last data group. Further, jamming is complex if the frequency channel or hopping algorithm is undisclosed. [7]

b. Amplitude Shift Keying (ASK)

Amplitude Shift Keying (ASK) aims to change or improve the voltage characteristics by increasing the amplitude of the input binary signal concerning the carrier signal during transmission. [8]

c. Set-up

1. Figure 3 shows the system consists of a 20x4cm LCD that displays the name and the mode of the prototype. The mode consists of three combinations of HF and VHF. The volume knob controls the signal input which is the audio jack and output of the system. The power switch is to power the system and the mode button is to change the mode from one to three. Lastly, the PTT is the push-to-talk button.

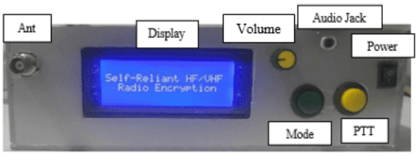


Figure 3: Front View of the Prototype

2. The prototype is 14cm x 22.5cm x 8cm and has a built-in battery and a plastic cover.

Figure 4: Outside the Prototype

3. Shown in Figure 5 are the major components of the prototype.

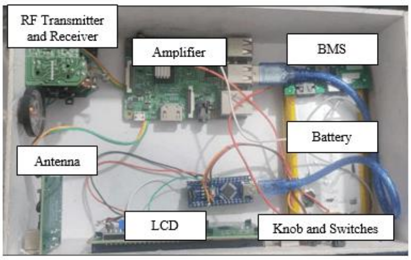


Figure 5: Inside the Prototype

4. The antenna consists of a copper tube of 3m in length.

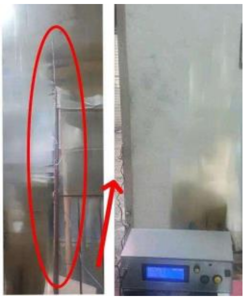


Figure 6: The Antenna Set-up

5. Figure 7 shows the three modes of the prototype.

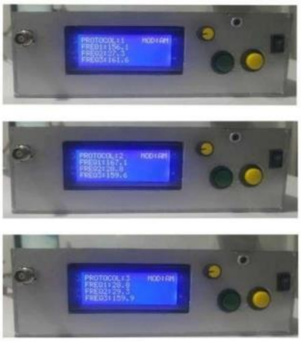


Figure 7: Three Modes of the Prototype

6. Figure 8 is the test on a private pool with a dimension of 40x20m, which was filled with seawater for project simulation. The proper standard of the device was tested, and the parameters were set as needed for military use. The parameters and standards needed were compiled during the testing. The prototype was designed to have a maximum distance of 50 meters of simultaneous data transmission as a requirement of International Innovative Development Solution (IIDS), the third-party entity that evaluated the integrity of the data gathered during the testing.

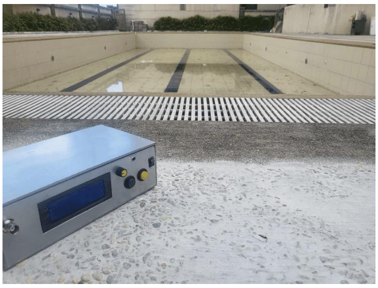


Figure 8: Testing of Prototype

d. Programming Language

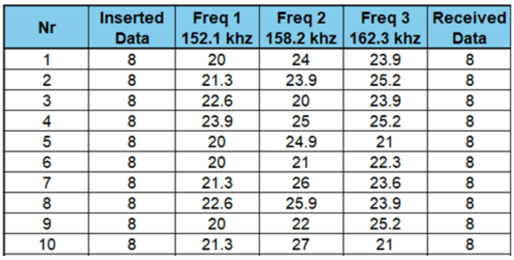
The Python programming language was used for programming the Raspberry PI while C language was used in Arduino IDE to program the hardware since Python controls the logic of the system the Arduino IDE ensures that the hardware can display the correct data while letting Python focus on its logic to maximize the computing power of the Python for the task.

5. Result and Discussion

a. The building of a transmitter and receiver for data transfer;

Table II shows the testing of transmission of serial data in bits at 9600 baud, per letter is transmitted to the receiver end in the 40 m range, each 8-bit represents 1 ASCII character and a parity bit. In modulation, it is transmitted in the three frequency carriers.

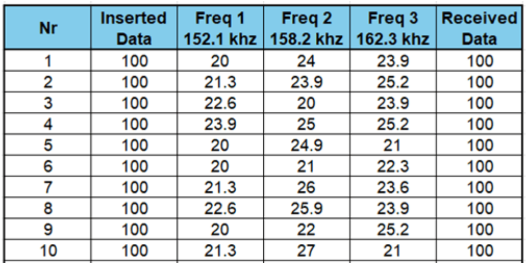
Table II: Serial Data Transmission



Nr	Inserted Data	Freq 1 152.1 khz	Freq 2 158.2 khz	Freq 3 162.3 khz	Received Data
1	8	20	24	23.9	8
2	8	21.3	23.9	25.2	8
3	8	22.6	20	23.9	8
4	8	23.9	25	25.2	8
5	8	20	24.9	21	8
6	8	20	21	22.3	8
7	8	21.3	26	23.6	8
8	8	22.6	25.9	23.9	8
9	8	20	22	25.2	8
10	8	21.3	27	21	8

Table III shows the testing of transmission of Universal Serial Bus (USB) data in bits with 100 kb data. The USB signal is modulated and transmitted to other devices and then demodulated on the other end.

Table III: Universal Serial Bus Data Transmission

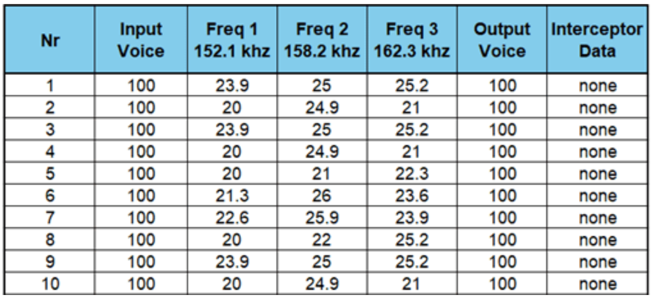


Nr	Inserted Data	Freq 1 152.1 khz	Freq 2 158.2 khz	Freq 3 162.3 khz	Received Data
1	100	20	24	23.9	100
2	100	21.3	23.9	25.2	100
3	100	22.6	20	23.9	100
4	100	23.9	25	25.2	100
5	100	20	24.9	21	100
6	100	20	21	22.3	100
7	100	21.3	26	23.6	100
8	100	22.6	25.9	23.9	100
9	100	20	22	25.2	100
10	100	21.3	27	21	100

b. The use of multiple radio frequency manipulation where multiple frequencies are used to modulate and encrypt data;

Table IV shows the testing of transmission of the analog signal through the prototype It shows that the sent analog signal is received on the receiving side and can be clearly understood

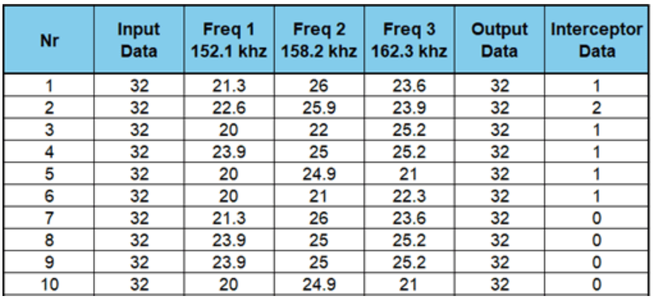
Table IV: Voice Encryption Testing



Nr	Input Voice	Freq 1 152.1 khz	Freq 2 158.2 khz	Freq 3 162.3 khz	Output Voice	Interceptor Data
1	100	23.9	25	25.2	100	none
2	100	20	24.9	21	100	none
3	100	23.9	25	25.2	100	none
4	100	20	24.9	21	100	none
5	100	20	21	22.3	100	none
6	100	21.3	26	23.6	100	none
7	100	22.6	25.9	23.9	100	none
8	100	20	22	25.2	100	none
9	100	23.9	25	25.2	100	none
10	100	20	24.9	21	100	none

Table V shows the testing of the encryption quality in terms of encryption and decryption. It shows that the system may have noise but in a minimal situation and may be affected by other transmission line data. Still, it can receive the data in a complete set. The use of multiple radio frequency manipulation where multiple frequencies are used to modulate and encrypt data.

Table V: Data Encryption Testing

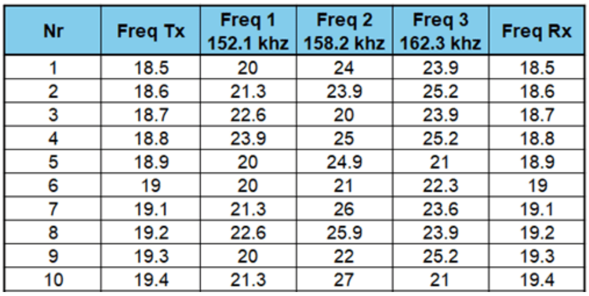


Nr	Input Data	Freq 1 152.1 khz	Freq 2 158.2 khz	Freq 3 162.3 khz	Output Data	Interceptor Data
1	32	21.3	26	23.6	32	1
2	32	22.6	25.9	23.9	32	2
3	32	20	22	25.2	32	1
4	32	23.9	25	25.2	32	1
5	32	20	24.9	21	32	1
6	32	20	21	22.3	32	1
7	32	21.3	26	23.6	32	0
8	32	23.9	25	25.2	32	0
9	32	23.9	25	25.2	32	0
10	32	20	24.9	21	32	0

c. The building of a modulator and demodulator for data encryption and decryption;

Tables VI and VII show the result of the noise injection test at the shore and ship during radio frequency transmission for a duration of one second. The noise injected is in kilohertz. The interpretation of the given information is that during radio frequency, the noise injection test was conducted at both shore and sea locations.

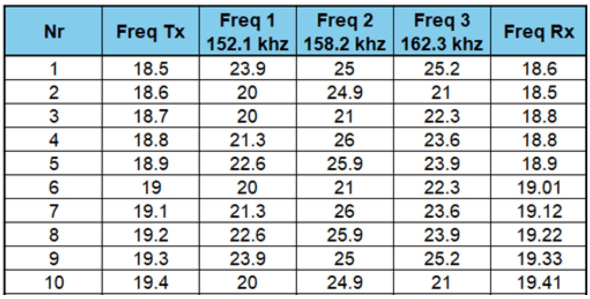
Table VI: Noise Injection Test at Shore Transmission



Nr	Freq Tx	Freq 1 152.1 khz	Freq 2 158.2 khz	Freq 3 162.3 khz	Freq Rx
1	18.5	20	24	23.9	18.5
2	18.6	21.3	23.9	25.2	18.6
3	18.7	22.6	20	23.9	18.7
4	18.8	23.9	25	25.2	18.8
5	18.9	20	24.9	21	18.9
6	19	20	21	22.3	19
7	19.1	21.3	26	23.6	19.1
8	19.2	22.6	25.9	23.9	19.2
9	19.3	20	22	25.2	19.3
10	19.4	21.3	27	21	19.4

Table VII shows the result of the signal modulated by the system. The signals were received with the same data as it were transmitted. Thus, it proves that the encryption can be properly decrypted on the other end of the system. In this table, we can also interpret that the three carrier frequencies can be used to modulate a signal from the transmitting entity to the receiving end.

Table VII: Noise Injection Test at Ship Transmission



Nr	Freq Tx	Freq 1 152.1 khz	Freq 2 158.2 khz	Freq 3 162.3 khz	Freq Rx
1	18.5	23.9	25	25.2	18.6
2	18.6	20	24.9	21	18.5
3	18.7	20	21	22.3	18.8
4	18.8	21.3	26	23.6	18.8
5	18.9	22.6	25.9	23.9	18.9
6	19	20	21	22.3	19.01
7	19.1	21.3	26	23.6	19.12
8	19.2	22.6	25.9	23.9	19.22
9	19.3	23.9	25	25.2	19.33
10	19.4	20	24.9	21	19.41

At shore, after one second of noise injection, the transmitted frequency matched the received frequency perfectly. However, at sea, there was an average difference of 0.0175 kHz between the transmitted and received frequencies after noise injection. This difference could be due to several factors such as environmental conditions or interference at sea. Despite this, the encryption performance tests revealed promising results. The selected encryption algorithms demonstrated efficient encryption/decryption speeds with manageable complexity.

d. Derive a formula for multi-frequency modulation;

1. Multi-Frequency Modulation

Multi-frequency carrier one modulation in VHF (Very High Frequency) and HF (High Frequency) amplitude modulation (AM) involves modulating a carrier signal with multiple audio frequencies simultaneously. Let's derive a formula for this process.

Let:

- $\boxed{Ac}$ be the amplitude of the carrier signal.
- $\boxed{fc}$ be the frequency of the carrier signal.
- $\boxed{Am1, Am2..., Amn}$ be the amplitudes of the modulating signals.
- $\boxed{fm1, fm2..., fmn}$ be the frequencies of the modulating signals.

The formula for multi-frequency carrier one modulation can be expressed as:

$$\boxed{s(t)=Ac\cdot\cos(2\pi fct+\phi)\ \cdot\prod i=1n\cos(2\pi fmit+\phi i)}$$

Where:

- $\boxed{\phi}$ is the phase of the carrier signal.
- $\boxed{\phi i}$ are the phases of the modulating signals.

This formula represents the carrier signal modulated by the product of cosine waves corresponding to each modulating signal. Each modulating signal is represented by its amplitude, frequency, and phase.

This multi-frequency modulation scheme results in a complex waveform where the carrier signal is modulated by the combined effect of multiple modulating signals.

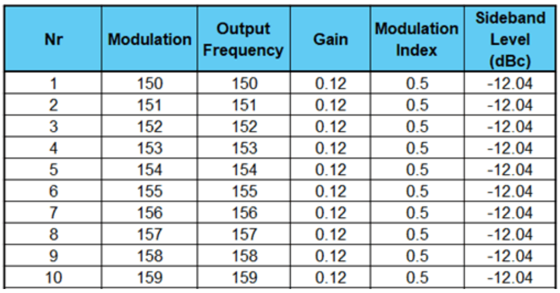
2. Frequency Division Multiplexing

Consider three frequency bands, each with a known finite bandwidth of 200 kHz (for data and voice transfer) and separated by three guard bands of 20 kHz each to accommodate all the bands, the communication channel should have a capacity of (200 x 4) + (20 x 3) = 860 kHz

e. Measure modulated frequency output, gain, and frequency sideband noise;

Table VIII shows the testing of frequency before and after modulation. The consistency of the carrier frequency is evident since the frequency and the gain is constant.

Table VIII: Modulated Frequency, Gain, and Sideband Noise

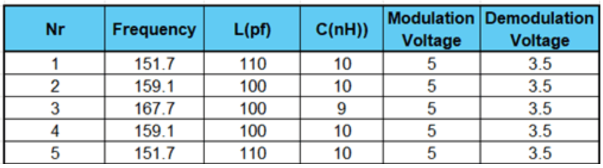


Nr	Modulation	Output Frequency	Gain	Modulation Index	Sideband Level (dBc)
1	150	150	0.12	0.5	-12.04
2	151	151	0.12	0.5	-12.04
3	152	152	0.12	0.5	-12.04
4	153	153	0.12	0.5	-12.04
5	154	154	0.12	0.5	-12.04
6	155	155	0.12	0.5	-12.04
7	156	156	0.12	0.5	-12.04
8	157	157	0.12	0.5	-12.04
9	158	158	0.12	0.5	-12.04
10	159	159	0.12	0.5	-12.04

f. Tuning of multiple frequency transmission modulation and multiple frequency demodulation.

Table IX shows the calibration of the LC circuit to obtain the right frequency. It also shows the initial modulation and the demodulation value.

Table IX: Tuning of Multiple Frequency Transmission



Nr	Frequency	L(pf)	C(nH))	Modulation Voltage	Demodulation Voltage
1	151.7	110	10	5	3.5
2	159.1	100	10	5	3.5
3	167.7	100	9	5	3.5
4	159.1	100	10	5	3.5
5	151.7	110	10	5	3.5

The effectiveness of frequency manipulation techniques was evident in enhancing the security and reliability of our communication system. Empirical data and simulations illustrated how frequency manipulation mitigated signal interception and jamming attempts, thus bolstering the system's resilience in hostile environments.

6. Conclusion

The test result shows a capable, self-reliant, and secure HF/VHF radio encryption using multi-radio frequency. The current configuration of the radio has a capability of low-speed transmission that can be classified as good for search and rescue operations. The radio served its purpose as intended based on the testing results. While there were many testing issues, the fundamentals of the design held perfectly, and the prototype was capable of a 50-meter effective range of simultaneous transmission using a 5V power bank supply. In conclusion, the research presents a comprehensive framework for HF/VHF radio encryption using multi-radio frequency manipulation, offering robust security and reliable communication for the Philippine Navy.

7. Recommendation

Based on the test results, the first and most important improvement is an upgrade to the amplification and frequency generator. The current design does not allow long-range transmission due to the frequency transmission limitation of the device. It should also be able to reach the noise-like encryption of data for maximum encryption. Future researchers must go through extensive testing of the current system to analyze the areas of improvement, such as efficiency, viability, and safety. Further, the PN must develop long-term sustainability plans for the self-reliant encrypted communication system, including provisions for technology refresh cycles, lifecycle management, and budget allocations which are recommended to ensure the implementation of the project.

References

1. R. Białas, M. Grzonkowski, and R. Wicik, “Cryptographic protection for military radio

communications," International Journal of Electronics and Telecommunications, vol. 66, no. 4, pp. 687–693, Nov. 2020, doi: 10.24425/ijet.2020.134028.

2. A. Jamaluddin, N. N. Mohamed, and H. Hashim, "Securing RF communication using AES-256 symmetric encryption: A performance evaluation," International Journal of Engineering and Technology(UAE), vol. 7, no. 4, pp. 217–222, 2018, doi: 10.14419/ijet.v7i4.11.20810.
3. D. Lazo and J. Mercader, "THE AFP SELF-RELIANT DEFENSE POSTURE (SRDP) PROGRAM: LEADING THE NATION TOWARDS A NEW DIRECTION".
4. P. Navy, "PHILIPPINE NAVY MANUAL."
5. E. B. Blancaflor, L. A. M. Competente, J. D. Fallar, N. F. J. Magadan, K. J. R. Piopongco, and L. N. L. Salinas, "A Case Study of using Cryptography for the Improvement of Data Security in E-commerce Industry in the Philippines," in 2023 8th International Conference on Computer and Communication Systems, ICCCS 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 695–700.doi:10.1109/ICCCS57501.2023.10150939.
6. A. N. Yumang, E. D. Dimaunahan, C. K. M. Centino, and A. R. J. Doroteo, "IoT-based Fire Mitigation and Detection System with AES-256 Encryption and Android Application," in 2023 2nd International Symposium on Sensor Technology and Control, ISSTC 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 201–206. doi: 10.1109/ISSTC59603.2023.10281116.
7. S. A. Mohammed, "Securing Physical Layer for FHSS Communication System Using Code andPhase Hopping Techniques in CDMA, System Design and Implementation," Journal of Engineering, vol. 26, no. 7, pp. 190–205, Jul. 2020, doi: 10.31026/J.ENG.2020.07.13.
8. [8] "Amplitude Shift Keying." Accessed: Oct. 06, 2022. [Online].Available:https://www.tutorialspoint.com/digital_communication/digital_communication_amplitude_shift_keying.htm